Private Private Information

arXiv:2112.14356

Kevin He **Fedor Sandomirskiy** Omer Tamuz

USC Theory Seminar, January 24 2022

Question: How to disclose information optimally respecting privacy?

Question: How to disclose information optimally respecting privacy?

Model

Question: How to disclose information optimally respecting privacy?

Model

- A finite set of agents $\{1, ..., n\}$

Question: How to disclose information optimally respecting privacy?

Model

- A finite set of agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$

Question: How to disclose information optimally respecting privacy?

Model

- A finite set of agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$
- A common prior probability $p \in (0, 1)$ for event $\{\omega = h\}$

Question: How to disclose information optimally respecting privacy?

Model

- A finite set of agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$
- A common prior probability $p \in (0, 1)$ for event $\{\omega = h\}$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**

Question: How to disclose information optimally respecting privacy?

Model

- A finite set of agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$
- A common prior probability $p \in (0, 1)$ for event $\{\omega = h\}$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**
- A joint distribution $\mathbb{P}$ over $(\omega, s_1, ..., s_n)$ defines the **private information structure**

Private Information May Not Be Private

- Some examples:

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = ... = s_n] = 1$

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = ... = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, ..., s_n)$ are drawn independently across agents

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = ... = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, ..., s_n)$ are drawn independently across agents
- Are agents' information in these examples really private?

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = \ldots = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, \ldots, s_n)$ are drawn independently across agents
- Are agents' information in these examples really private?
- Public signals are not private at all

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = ... = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, ..., s_n)$ are drawn independently across agents
- Are agents' information in these examples really private?
- Public signals are not private at all
- Even conditionally independent signals are not very private

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = \ldots = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, \ldots, s_n)$ are drawn independently across agents
- Are agents' information in these examples really private?
- Public signals are not private at all
- Even conditionally independent signals are not very private
  - Suppose prior $\mathbb{P}[\omega = h] = 1/2$

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = \ldots = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, \ldots, s_n)$ are drawn independently across agents
- Are agents' information in these examples really private?
- Public signals are not private at all
- Even conditionally independent signals are not very private
  - Suppose prior $\mathbb{P}[\omega = h] = 1/2$
  - Binary signals with $\mathbb{P}[s_i = \omega \mid \omega] = 3/4$

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = \dots = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, \dots, s_n)$ are drawn independently across agents
- Are agents' information in these examples really private?
- Public signals are not private at all
- Even conditionally independent signals are not very private
  - Suppose prior $\mathbb{P}[\omega = h] = 1/2$
  - Binary signals with $\mathbb{P}[s_i = \omega \mid \omega] = 3/4$
  - Before observing s_1, P1 assigns belief $1/2$ to $\{s_2 = h\}$

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = \ldots = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, \ldots, s_n)$ are drawn independently across agents
- Are agents' information in these examples really private?
- Public signals are not private at all
- Even conditionally independent signals are not very private
  - Suppose prior $\mathbb{P}[\omega = h] = 1/2$
  - Binary signals with $\mathbb{P}[s_i = \omega \mid \omega] = 3/4$
  - Before observing s_1, P1 assigns belief $1/2$ to $\{s_2 = h\}$
  - After learning $s_1 = h$, P1 assigns belief $5/8$ to $\{s_2 = h\}$

Private Information May Not Be Private

- Some examples:
  - **Public** signals — $\mathbb{P}[s_1 = s_2 = \ldots = s_n] = 1$
  - **Conditionally independent** signals — given ω, $(s_1, \ldots, s_n)$ are drawn independently across agents
- Are agents' information in these examples really private?
- Public signals are not private at all
- Even conditionally independent signals are not very private
  - Suppose prior $\mathbb{P}[\omega = h] = 1/2$
  - Binary signals with $\mathbb{P}[s_i = \omega \mid \omega] = 3/4$
  - Before observing s_1, P1 assigns belief $1/2$ to $\{s_2 = h\}$
  - After learning $s_1 = h$, P1 assigns belief $5/8$ to $\{s_2 = h\}$
  - s_1 contains info about s_2, so P2's info not fully private

Private Private Information

Definition

A ***private*** **private information structure** is one where the signals $(s_1, ..., s_n)$ are independent.

Private Private Information

Definition

A ***private*** **private information structure** is one where the signals $(s_1, ..., s_n)$ are independent.

- Signals must be independent, not conditionally independent

Private Private Information

Definition

A ***private*** **private information structure** is one where the signals $(s_1, \ldots, s_n)$ are independent.

- Signals must be independent, not conditionally independent
- Private private signals contain info about the state, but not about each other

Private Private Information

Definition

A ***private* private information structure** is one where the signals $(s_1, \ldots, s_n)$ are independent.

- Signals must be independent, not conditionally independent
- Private private signals contain info about the state, but not about each other
- Is it possible for everyone to have **informative** private private signals?

Private Private Information

Definition

A ***private*** **private information structure** is one where the signals $(s_1, ..., s_n)$ are independent.

- Signals must be independent, not conditionally independent
- Private private signals contain info about the state, but not about each other
- Is it possible for everyone to have **informative** private private signals?
  - Paradoxical at first: s_1 informative about ω, ω correlated with s_2, yet P1 learns nothing about s_2?

Private Private Information

Definition

A ***private* private information structure** is one where the signals $(s_1, \ldots, s_n)$ are independent.

- Signals must be independent, not conditionally independent
- Private private signals contain info about the state, but not about each other
- Is it possible for everyone to have **informative** private private signals?
  - Paradoxical at first: s_1 informative about ω, ω correlated with s_2, yet P1 learns nothing about s_2?
  - It is possible!

Private Private Information

Definition

A ***private*** **private information structure** is one where the signals $(s_1, \ldots, s_n)$ are independent.

- Signals must be independent, not conditionally independent
- Private private signals contain info about the state, but not about each other
- Is it possible for everyone to have **informative** private private signals?
    - Paradoxical at first: s_1 informative about ω, ω correlated with s_2, yet P1 learns nothing about s_2?
    - It is possible!
    - Tension between informativeness and privacy: impossible for everyone to have **perfectly** informative private private signals

Private Private Information

Definition

A ***private*** **private information structure** is one where the signals $(s_1, ..., s_n)$ are independent.

- Signals must be independent, not conditionally independent
- Private private signals contain info about the state, but not about each other
- Is it possible for everyone to have **informative** private private signals?
  - Paradoxical at first: s_1 informative about ω, ω correlated with s_2, yet P1 learns nothing about s_2?
  - It is possible!
  - Tension between informativeness and privacy: impossible for everyone to have **perfectly** informative private private signals
  - We focus on this tension and study how informative private private signals can be

Application: optimal recommendation

- You are writing a recommendation letter. You know:

Application: optimal recommendation

- You are writing a recommendation letter. You know:
  - applicant's fit $\omega \in \{\ell, h\}$

Application: optimal recommendation

- You are writing a recommendation letter. You know:
    - applicant's fit $\omega \in \{\ell, h\}$
    - if a medical condition correlated with the fit is present s_1

Application: optimal recommendation

- You are writing a recommendation letter. You know:
    - applicant's fit $\omega \in \{\ell, h\}$
    - if a medical condition correlated with the fit is present s_1
- You want the letter s_2 to be informative of ω

Application: optimal recommendation

- You are writing a recommendation letter. You know:
    - applicant's fit $\omega \in \{\ell, h\}$
    - if a medical condition correlated with the fit is present s_1
- You want the letter s_2 to be informative of ω
- **Privacy concerns / laws:** s_2 must be uninformative of the medical condition s_1

Application: optimal recommendation

- You are writing a recommendation letter. You know:
  - applicant's fit $\omega \in \{\ell, h\}$
  - if a medical condition correlated with the fit is present s_1
- You want the letter s_2 to be informative of ω
- **Privacy concerns / laws:** s_2 must be uninformative of the medical condition s_1
- (ω, s_1, s_2) must be **private private**

Application: optimal recommendation

- You are writing a recommendation letter. You know:
    - applicant's fit $\omega \in \{\ell, h\}$
    - if a medical condition correlated with the fit is present s_1
- You want the letter s_2 to be informative of ω
- **Privacy concerns / laws:** s_2 must be uninformative of the medical condition s_1
- (ω, s_1, s_2) must be **private private**
- **The question:** Given (ω, s_1), find maximally informative s_2 under privacy constraint.

Application: optimal recommendation

- You are writing a recommendation letter. You know:
  - applicant's fit $\omega \in \{\ell, h\}$
  - if a medical condition correlated with the fit is present s_1
- You want the letter s_2 to be informative of ω
- **Privacy concerns / laws:** s_2 must be uninformative of the medical condition s_1
- (ω, s_1, s_2) must be **private private**
- **The question:** Given (ω, s_1), find maximally informative s_2 under privacy constraint.
- Privacy $\simeq$ demographic parity w.r.t. a protected trait s_1 in fair machine learning
  - Barocas, Hardt, Narayanan. Fairness in machine learning. NeurIPS tutorial 2017

Other occurrences of private private signals

- Consulting company's problem:

Other occurrences of private private signals

- Consulting company's problem:
  - A consulting company sells information about ω to competitors

Other occurrences of private private signals

- Consulting company's problem:
  - A consulting company sells information about ω to competitors
  - Competitors may demand a privacy guarantee: no competitor can use their signal realization to infer anything about mine

Other occurrences of private private signals

- Consulting company's problem:
    - A consulting company sells information about ω to competitors
    - Competitors may demand a privacy guarantee: no competitor can use their signal realization to infer anything about mine
    - The company should rely on private private signals

Other occurrences of private private signals

- Consulting company's problem:
    - A consulting company sells information about ω to competitors
    - Competitors may demand a privacy guarantee: no competitor can use their signal realization to infer anything about mine
    - The company should rely on private private signals
    - How informative can signals be while preserving privacy?

Other occurrences of private private signals

- Consulting company's problem:
  - A consulting company sells information about ω to competitors
  - Competitors may demand a privacy guarantee: no competitor can use their signal realization to infer anything about mine
  - The company should rely on private private signals
  - How informative can signals be while preserving privacy?
- Causal inference:

Other occurrences of private private signals

- Consulting company's problem:
  - A consulting company sells information about ω to competitors
  - Competitors may demand a privacy guarantee: no competitor can use their signal realization to infer anything about mine
  - The company should rely on private private signals
  - How informative can signals be while preserving privacy?
- Causal inference:
  - Collider is a common model in causal Bayesian networks: $s_1 \rightarrow \omega \leftarrow s_2$

Other occurrences of private private signals

- Consulting company's problem:
  - A consulting company sells information about ω to competitors
  - Competitors may demand a privacy guarantee: no competitor can use their signal realization to infer anything about mine
  - The company should rely on private private signals
  - How informative can signals be while preserving privacy?
- Causal inference:
  - Collider is a common model in causal Bayesian networks: $s_1 \rightarrow \omega \leftarrow s_2$
  - Causal strength quantifies how much s_i influences ω

Other occurrences of private private signals

- Consulting company's problem:
  - A consulting company sells information about ω to competitors
  - Competitors may demand a privacy guarantee: no competitor can use their signal realization to infer anything about mine
  - The company should rely on private private signals
  - How informative can signals be while preserving privacy?
- Causal inference:
  - Collider is a common model in causal Bayesian networks: $s_1 \to \omega \leftarrow s_2$
  - Causal strength quantifies how much s_i influences ω
  - Relates to informativeness of s_i as a signal of ω

Other occurrences of private private signals

- Consulting company's problem:
  - A consulting company sells information about ω to competitors
  - Competitors may demand a privacy guarantee: no competitor can use their signal realization to infer anything about mine
  - The company should rely on private private signals
  - How informative can signals be while preserving privacy?
- Causal inference:
  - Collider is a common model in causal Bayesian networks: $s_1 \rightarrow \omega \leftarrow s_2$
  - Causal strength quantifies how much s_i influences ω
  - Relates to informativeness of s_i as a signal of ω
  - How strong can independent causes be?

Other occurrences of private private signals 2

Other occurrences of private private signals 2

- Worst-case information structures in robust mechanism design:
  - Bergemann, Brooks, Morris *First-price auctions with general information structures:Implications for bidding and revenue* Econometrica 2017
  - Brooks and Du *Optimal auction design with common values: An informationally robust approach* Econometrica 2021

Other occurrences of private private signals 2

- Worst-case information structures in robust mechanism design:
  - Bergemann, Brooks, Morris *First-price auctions with general information structures:Implications for bidding and revenue* Econometrica 2017
  - Brooks and Du *Optimal auction design with common values: An informationally robust approach* Econometrica 2021
- Counterexamples to information aggregation in exchange economies
  - Ostrovsky *Information aggregation in dynamic markets with strategic traders* Econometrica 2012

Other occurrences of private private signals 2

- Worst-case information structures in robust mechanism design:
  - Bergemann, Brooks, Morris *First-price auctions with general information structures:Implications for bidding and revenue* Econometrica 2017
  - Brooks and Du *Optimal auction design with common values: An informationally robust approach* Econometrica 2021
- Counterexamples to information aggregation in exchange economies
  - Ostrovsky *Information aggregation in dynamic markets with strategic traders* Econometrica 2012
- Feasible joint distributions of posterior beliefs
  - Arieli, Babichenko, Sandomirskiy, Tamuz *Feasible joint posterior beliefs* Journal of Political Economy 2021

How to compare informativeness?

- What does it mean that a signal s is more informative about ω than s'?

How to compare informativeness?

- What does it mean that a signal s is more informative about ω than s'?
- Denote $p(s) = \mathbb{P}[\omega = h \mid s]$ the posterior belief induced by s

How to compare informativeness?

- What does it mean that a signal s is more informative about ω than s'?
- Denote $p(s) = \mathbb{P}[\omega = h \mid s]$ the posterior belief induced by s

Definition

A signal s **Blackwell dominates** s' if for any convex φ on $[0, 1]$

$$\mathbb{E}[\varphi(p(s))] \geq \mathbb{E}[\varphi(p'(s'))].$$

How to compare informativeness?

- What does it mean that a signal s is more informative about ω than s'?
- Denote $p(s) = \mathbb{P}[\omega = h \mid s]$ the posterior belief induced by s

Definition

A signal s **Blackwell dominates** s' if for any convex φ on $[0, 1]$

$$\mathbb{E}[\varphi(p(s))] \geq \mathbb{E}[\varphi(p'(s'))].$$

- **Equivalent definition:**

How to compare informativeness?

- What does it mean that a signal s is more informative about ω than s'?
- Denote $p(s) = \mathbb{P}[\omega = h \mid s]$ the posterior belief induced by s

Definition

A signal s **Blackwell dominates** s' if for any convex φ on $[0, 1]$

$$\mathbb{E}[\varphi(p(s))] \geq \mathbb{E}[\varphi(p'(s'))].$$

- **Equivalent definition:**
  - in any decision problem s gives higher expected utility than s'

How to compare informativeness?

- What does it mean that a signal s is more informative about ω than s'?
- Denote $p(s) = \mathbb{P}[\omega = h \mid s]$ the posterior belief induced by s

Definition

A signal s **Blackwell dominates** s' if for any convex φ on $[0, 1]$

$$\mathbb{E}[\varphi(p(s))] \geq \mathbb{E}[\varphi(p'(s'))].$$

- **Equivalent definition:**
  - in any decision problem s gives higher expected utility than s'

Definition

An information structure $(\omega, s_1, \dots, s_n)$ **Blackwell dominates** $(\omega, s'_1, \dots, s'_n)$ if each agent's signal s_i dominates s'_i.

How to compare informativeness?

- What does it mean that a signal s is more informative about ω than s'?
- Denote $p(s) = \mathbb{P}[\omega = h \mid s]$ the posterior belief induced by s

Definition

A signal s **Blackwell dominates** s' if for any convex φ on $[0,1]$

$$\mathbb{E}[\varphi(p(s))] \geq \mathbb{E}[\varphi(p'(s'))].$$

- **Equivalent definition:**
  - in any decision problem s gives higher expected utility than s'

Definition

An information structure $(\omega, s_1, \ldots, s_n)$ **Blackwell dominates** $(\omega, s'_1, \ldots, s'_n)$ if each agent's signal s_i dominates s'_i.

A private private structure is **Pareto optimal** if it is not dominated by another private private structure.

$n = 2$: characterization of Pareto optimal structures

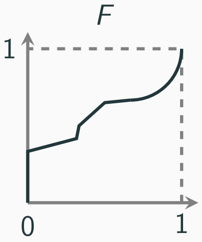
- Let F be a cdf of a distribution on $[0, 1]$ with mean p

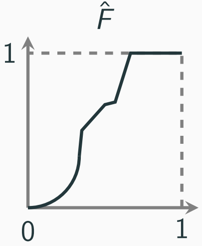
$n = 2$: characterization of Pareto optimal structures

- Let F be a cdf of a distribution on $[0, 1]$ with mean p
- Denote $\hat{F}(x) = 1 - F^{-1}(1 - x)$

$n = 2$: characterization of Pareto optimal structures

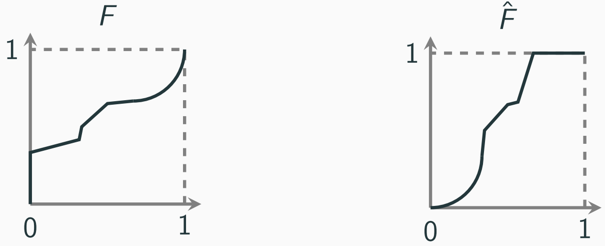
- Let F be a cdf of a distribution on $[0, 1]$ with mean p
- Denote $\hat{F}(x) = 1 - F^{-1}(1 - x)$
- Then $\hat{F}$ is also a cdf of a distribution on $[0, 1]$ with mean p, obtained by reflecting F around the anti-diagonal





$n = 2$: characterization of Pareto optimal structures

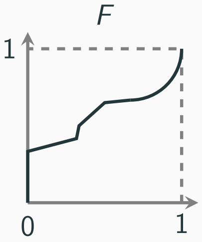
- Let F be a cdf of a distribution on $[0, 1]$ with mean p
- Denote $\hat{F}(x) = 1 - F^{-1}(1 - x)$
- Then $\hat{F}$ is also a cdf of a distribution on $[0, 1]$ with mean p, obtained by reflecting F around the anti-diagonal

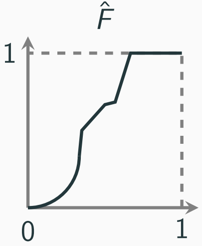


- Call F and $\hat{F}$ **conjugates**

$n = 2$: characterization of Pareto optimal structures

- Let F be a cdf of a distribution on $[0, 1]$ with mean p
- Denote $\hat{F}(x) = 1 - F^{-1}(1 - x)$
- Then $\hat{F}$ is also a cdf of a distribution on $[0, 1]$ with mean p, obtained by reflecting F around the anti-diagonal





- Call F and $\hat{F}$ **conjugates**

Theorem 1

For $n = 2$, a private private info structure is Pareto optimal if and only if the belief distributions induced by s_1 and s_2 are conjugates.

Application: optimal recommendation

- ω — a state of interest

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait
- The joint distribution of (ω, s_1) is given

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait
- The joint distribution of (ω, s_1) is given
- Want to find s_2:

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait
- The joint distribution of (ω, s_1) is given
- Want to find s_2:
    - **as informative as possible** about ω

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait
- The joint distribution of (ω, s_1) is given
- Want to find s_2:
  - **as informative as possible** about ω
  - but **independent** of s_1

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait
- The joint distribution of (ω, s_1) is given
- Want to find s_2:
    - **as informative as possible** about ω
    - but **independent** of s_1
- Equivalently: find a **Pareto optimal** (ω, s_1, s_2) with the **given** (ω, s_1) **marginal**

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait
- The joint distribution of (ω, s_1) is given
- Want to find s_2:
  - **as informative as possible** about ω
  - but **independent** of s_1
- Equivalently: find a **Pareto optimal** (ω, s_1, s_2) with the **given** (ω, s_1) **marginal**

Corollary

For any given (ω, s_1), the optimal s_2 is unique, i.e., s_2 dominates any other s_2' independent of s_1. Belief distributions induced by s_1 and s_2 are conjugates.

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait
- The joint distribution of (ω, s_1) is given
- Want to find s_2:
  - **as informative as possible** about ω
  - but **independent** of s_1
- Equivalently: find a **Pareto optimal** (ω, s_1, s_2) with the **given** (ω, s_1) **marginal**

Corollary

For any given (ω, s_1), the optimal s_2 is unique, i.e., s_2 dominates any other s_2' independent of s_1. Belief distributions induced by s_1 and s_2 are conjugates.

- Optimal recommendation is the same for all decision problems

Application: optimal recommendation

- ω — a state of interest
- s_1 — a protected trait
- The joint distribution of (ω, s_1) is given
- Want to find s_2:
  - **as informative as possible** about ω
  - but **independent** of s_1
- Equivalently: find a **Pareto optimal** (ω, s_1, s_2) with the **given** (ω, s_1) **marginal**

Corollary

For any given (ω, s_1), the optimal s_2 is unique, i.e., s_2 dominates any other s_2' independent of s_1. Belief distributions induced by s_1 and s_2 are conjugates.

- Optimal recommendation is the same for all decision problems
- For ≥ 3 states ω, there may be a continuum of optimal s_2

Application: optimal recommendation

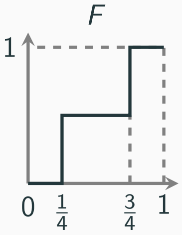
Example

- $\omega \in \{\ell, h\}$ is a job fit
- $s_1 \in \{y, n\}$ presence of a medical condition (yes/no)
- $\mathbb{P}(\omega = h) = \mathbb{P}(s_1 = y) = 1/2$
- $\mathbb{P}(\omega = h \mid s_1 = y) = \frac{3}{4}, \quad \mathbb{P}(\omega = h \mid s_1 = n) = \frac{1}{4}$
- **Goal:** find s_2 that is informative of ω but independent of s_1

Application: optimal recommendation

Example

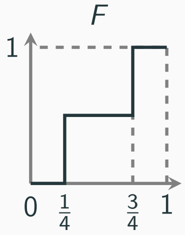
- $\omega \in \{\ell, h\}$ is a job fit
- $s_1 \in \{y, n\}$ presence of a medical condition (yes/no)
- $\mathbb{P}(\omega = h) = \mathbb{P}(s_1 = y) = 1/2$
- $\mathbb{P}(\omega = h \mid s_1 = y) = \frac{3}{4}, \quad \mathbb{P}(\omega = h \mid s_1 = n) = \frac{1}{4}$
- **Goal:** find s_2 that is informative of ω but independent of s_1

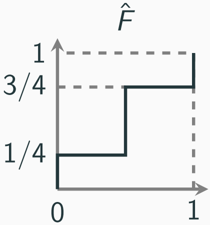
- 

Application: optimal recommendation

Example

- $\omega \in \{\ell, h\}$ is a job fit
- $s_1 \in \{y, n\}$ presence of a medical condition (yes/no)
- $\mathbb{P}(\omega = h) = \mathbb{P}(s_1 = y) = 1/2$
- $\mathbb{P}(\omega = h \mid s_1 = y) = \frac{3}{4}, \quad \mathbb{P}(\omega = h \mid s_1 = n) = \frac{1}{4}$
- **Goal:** find s_2 that is informative of ω but independent of s_1

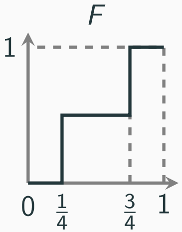
- 

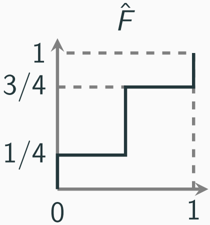


Application: optimal recommendation

Example

- $\omega \in \{\ell, h\}$ is a job fit
- $s_1 \in \{y, n\}$ presence of a medical condition (yes/no)
- $\mathbb{P}(\omega = h) = \mathbb{P}(s_1 = y) = 1/2$
- $\mathbb{P}(\omega = h \mid s_1 = y) = \frac{3}{4}, \quad \mathbb{P}(\omega = h \mid s_1 = n) = \frac{1}{4}$
- **Goal:** find s_2 that is informative of ω but independent of s_1

- 



- Optimal s_2 is trinary and induces posteriors (0, 1/2, 1) with probabilities (1/4, 1/2, 1/4)

Ideas behind Theorem 1

- Theorem 1 is a corollary of a general theorem applicable for $n \geq 2$

Ideas behind Theorem 1

- Theorem 1 is a corollary of a general theorem applicable for $n \geq 2$
- To formulate it, we need two ingredients

Ideas behind Theorem 1

- Theorem 1 is a corollary of a general theorem applicable for $n \geq 2$
- To formulate it, we need two ingredients
  - A structural result: private private structures $\leftrightarrow$ subsets of $[0, 1]^n$

Ideas behind Theorem 1

- Theorem 1 is a corollary of a general theorem applicable for $n \geq 2$
- To formulate it, we need two ingredients
  - A structural result: private private structures $\leftrightarrow$ subsets of $[0,1]^n$
  - Results from mathematical tomography

Private private structures as sets

- Fix $A \subset [0,1]^n$ with measure p

Private private structures as sets

- Fix $A \subset [0,1]^n$ with measure p
- Define a private private structure associated with A:

Private private structures as sets

- Fix $A \subset [0,1]^n$ with measure p
- Define a private private structure associated with A:
  - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A

Private private structures as sets

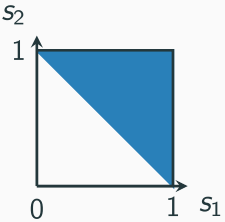
- Fix $A \subset [0,1]^n$ with measure p
- Define a private private structure associated with A:
  - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
  - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \backslash A$

Private private structures as sets

- Fix $A \subset [0,1]^n$ with measure p
- Define a private private structure associated with A:
    - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
    - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \setminus A$
    - Signals are uniform on $[0,1]^n$, hence, private private

Private private structures as sets

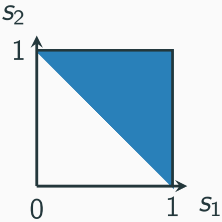
- Fix $A \subset [0,1]^n$ with measure p
- Define a private private structure associated with A:
  - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
  - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \backslash A$
  - Signals are uniform on $[0,1]^n$, hence, private private



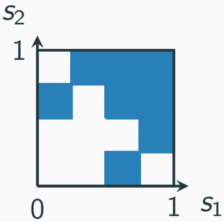
beliefs uniform on $[0,1]$

Private private structures as sets

- Fix $A \subset [0,1]^n$ with measure p
- Define a private private structure associated with A:
  - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
  - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \backslash A$
  - Signals are uniform on $[0,1]^n$, hence, private private



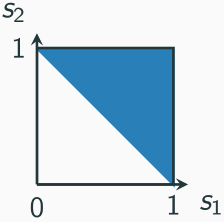
beliefs uniform on $[0,1]$



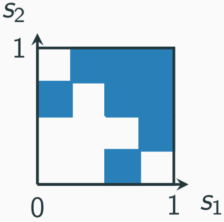
beliefs 1/4 and 3/4

Private private structures as sets

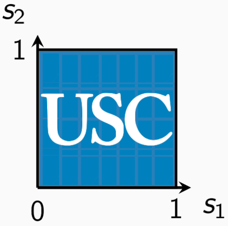
- Fix $A \subset [0,1]^n$ with measure p
- Define a private private structure associated with A:
  - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
  - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \backslash A$
  - Signals are uniform on $[0,1]^n$, hence, private private



beliefs uniform on $[0,1]$

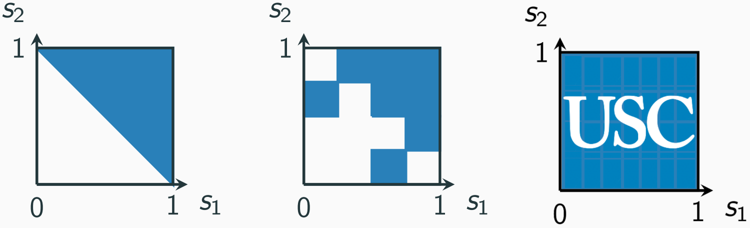


beliefs $1/4$ and $3/4$



Private private structures as sets

- Fix $A \subset [0,1]^n$ with measure p
- Define a private private structure associated with A:
  - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
  - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \backslash A$
  - Signals are uniform on $[0,1]^n$, hence, private private



beliefs uniform on $[0,1]$ beliefs $1/4$ and $3/4$

Proposition

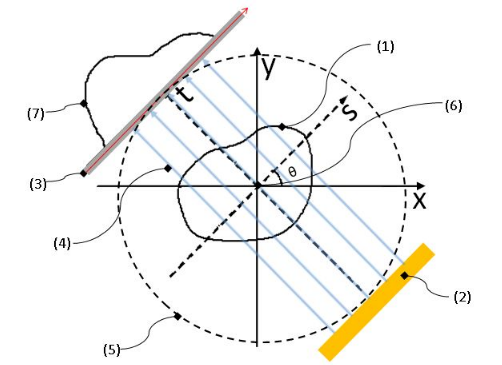
Any private private info structure is equivalent to a structure associated with some $A \subseteq [0,1]^n$

Tomography

- **Tomography** is an imaging technique that investigates the shape of an object by running x-ray through it

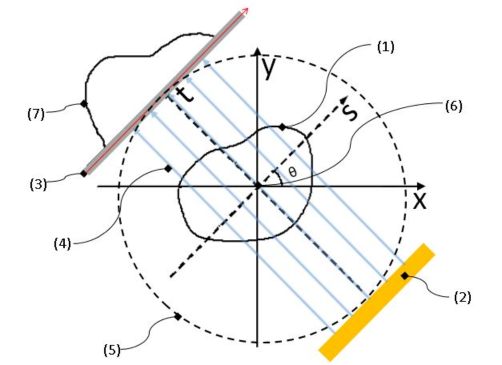
Tomography

- **Tomography** is an imaging technique that investigates the shape of an object by running x-ray through it



Tomography

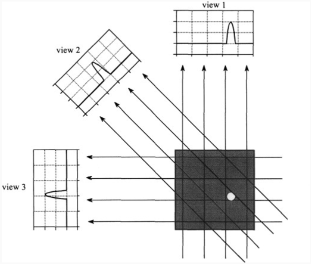
- **Tomography** is an imaging technique that investigates the shape of an object by running x-ray through it



- Produces a lower-dimensional projection of the object by looking at how much x-ray is absorbed at different points

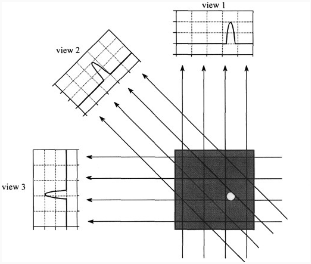
Tomography and Sets of Uniqueness

- Typically, must run x-ray from many different angles to get a good understanding of the object's geometry



Tomography and Sets of Uniqueness

- Typically, must run x-ray from many different angles to get a good understanding of the object's geometry



Definition

$A \subseteq [0,1]^n$ is a **set of uniqueness** if it is determined by its n coordinate projections, i.e., for any A' such that the uniform density on A and A' has the same one-dimensional marginals, $A' = A$ a.e. in $[0,1]^n$.

Pareto Optimality and Sets of Uniqueness

Theorem 2

For any $n \geq 2$, a private private info structure is Pareto optimal $\Leftrightarrow$ it is equivalent to a structure associated with a set of uniqueness $A \subseteq [0,1]^n$.

Pareto Optimality and Sets of Uniqueness

Theorem 2

For any $n \geq 2$, a private private info structure is Pareto optimal $\Leftrightarrow$ it is equivalent to a structure associated with a set of uniqueness $A \subseteq [0, 1]^n$.

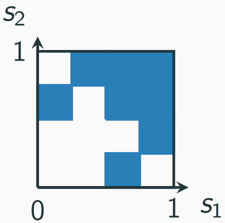
- An unexpected connection between Pareto optimality and tomography

Pareto Optimality and Sets of Uniqueness

Theorem 2

For any $n \geq 2$, a private private info structure is Pareto optimal $\Leftrightarrow$ it is equivalent to a structure associated with a set of uniqueness $A \subseteq [0,1]^n$.

- An unexpected connection between Pareto optimality and tomography
- We know that



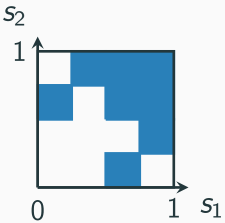
is not Pareto optimal (s_2 can be replaced by a more informative trinary signal)

Pareto Optimality and Sets of Uniqueness

Theorem 2

For any $n \geq 2$, a private private info structure is Pareto optimal $\Leftrightarrow$ it is equivalent to a structure associated with a set of uniqueness $A \subseteq [0,1]^n$.

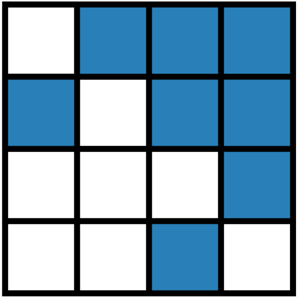
- An unexpected connection between Pareto optimality and tomography
- We know that



  is not Pareto optimal (s_2 can be replaced by a more informative trinary signal)
- Hence, the blue area not a set of uniqueness. Let's check!

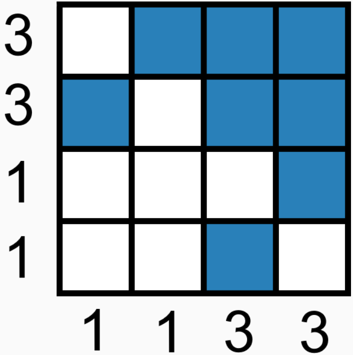
A Puzzle!

Problem for a newspaper puzzle column: is there another coloring of the 4x4 grid that preserves all column-wise and row-wise counts of colored squares?



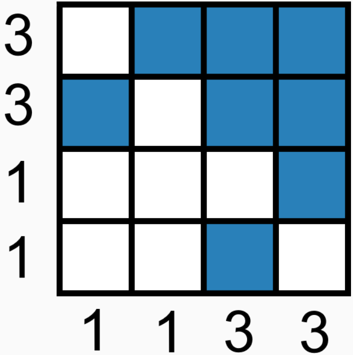
A Puzzle!

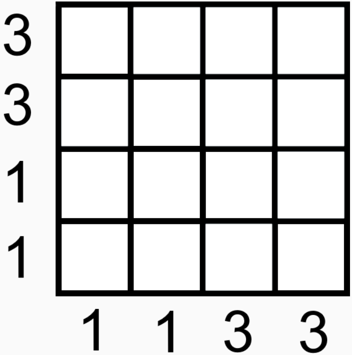
Problem for a newspaper puzzle column: is there another coloring of the 4x4 grid that preserves all column-wise and row-wise counts of colored squares?



A Puzzle!

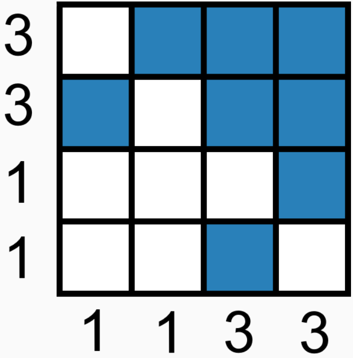
Problem for a newspaper puzzle column: is there another coloring of the 4x4 grid that preserves all column-wise and row-wise counts of colored squares?

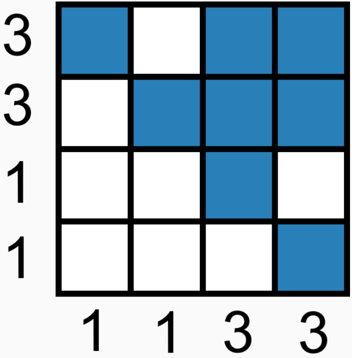




A Puzzle!

Problem for a newspaper puzzle column: find another coloring of the 4x4 grid that preserves all column-wise and row-wise counts of colored squares?





Existing Results about Sets of Uniqueness

- By our theorem, this shows the binary info structure that induces beliefs 1/4 or 3/4 is not itself Pareto optimal

Existing Results about Sets of Uniqueness

- By our theorem, this shows the binary info structure that induces beliefs 1/4 or 3/4 is not itself Pareto optimal
- Can disprove Pareto optimality by finding another set with same marginal projections

Existing Results about Sets of Uniqueness

- By our theorem, this shows the binary info structure that induces beliefs 1/4 or 3/4 is not itself Pareto optimal
- Can disprove Pareto optimality by finding another set with same marginal projections
- How do we prove Pareto optimality?

Existing Results about Sets of Uniqueness

- By our theorem, this shows the binary info structure that induces beliefs 1/4 or 3/4 is not itself Pareto optimal
- Can disprove Pareto optimality by finding another set with same marginal projections
- How do we prove Pareto optimality?
- That is, how do we prove a set is a set of uniqueness?

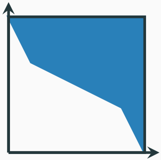
Existing Results about Sets of Uniqueness

- By our theorem, this shows the binary info structure that induces beliefs 1/4 or 3/4 is not itself Pareto optimal
- Can disprove Pareto optimality by finding another set with same marginal projections
- How do we prove Pareto optimality?
- That is, how do we prove a set is a set of uniqueness?
- Use results about sets of uniqueness from tomography

Existing Results about Sets of Uniqueness

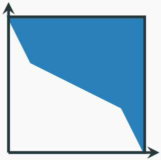
Existing Results about Sets of Uniqueness

- $A \subseteq [0,1]^n$ is **upward closed** if $\vec{x} \in A \Rightarrow \vec{x}' \in A$ for all $\vec{x}' \geq \vec{x}$



Existing Results about Sets of Uniqueness

- $A \subseteq [0,1]^n$ is **upward closed** if $\vec{x} \in A \Rightarrow \vec{x}' \in A$ for all $\vec{x}' \geq \vec{x}$

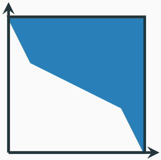


- $A \subseteq [0,1]^n$ is **additive** if there are bounded, non-decreasing $h_i : [0,1] \to \mathbb{R}$ s.t.

$$A = \left\{ \vec{x} \in [0,1]^n : \sum_{i=1}^{n} h_i(x_i) \geq 0 \right\}$$

Existing Results about Sets of Uniqueness

- $A \subseteq [0,1]^n$ is **upward closed** if $\vec{x} \in A \Rightarrow \vec{x}' \in A$ for all $\vec{x}' \geq \vec{x}$



- $A \subseteq [0,1]^n$ is **additive** if there are bounded, non-decreasing $h_i : [0,1] \to \mathbb{R}$ s.t.

$$A = \left\{ \vec{x} \in [0,1]^n : \sum_{i=1}^{n} h_i(x_i) \geq 0 \right\}$$

- Additive implies upward closed, equivalent if $n = 2$

Existing Results about Sets of Uniqueness

Theorem (Fishburn, Lagarias, Reeds, and Shepp 1990)

- *For $n = 2$, upward closed set is a set of uniqueness, and every set of uniqueness is upward closed up to measure-preserving transformations of axes.*

Existing Results about Sets of Uniqueness

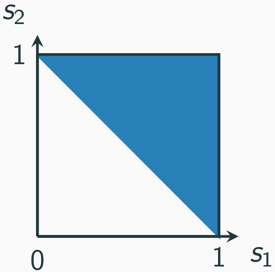
Theorem (Fishburn, Lagarias, Reeds, and Shepp 1990)

- *For $n = 2$, upward closed set is a set of uniqueness, and every set of uniqueness is upward closed up to measure-preserving transformations of axes.*
- *For $n \geq 2$, additive $\Rightarrow$ sets of uniqueness $\Rightarrow$ upward closed.*

Existing Results about Sets of Uniqueness

Theorem (Fishburn, Lagarias, Reeds, and Shepp 1990)

- *For $n = 2$, upward closed set is a set of uniqueness, and every set of uniqueness is upward closed up to measure-preserving transformations of axes.*
- *For $n \geq 2$, additive $\Rightarrow$ sets of uniqueness $\Rightarrow$ upward closed.*

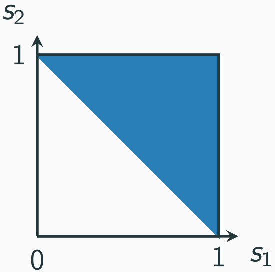


- Blue set is upward closed $\Rightarrow$ Pareto optimal

Existing Results about Sets of Uniqueness

Theorem (Fishburn, Lagarias, Reeds, and Shepp 1990)

- *For $n = 2$, upward closed set is a set of uniqueness, and every set of uniqueness is upward closed up to measure-preserving transformations of axes.*
- *For $n \geq 2$, additive $\Rightarrow$ sets of uniqueness $\Rightarrow$ upward closed.*



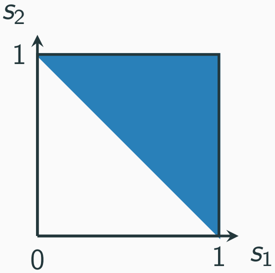
- Blue set is upward closed $\Rightarrow$ Pareto optimal

Fishburn et al.'s theorem & our Theorem 2 $\Rightarrow$

Existing Results about Sets of Uniqueness

Theorem (Fishburn, Lagarias, Reeds, and Shepp 1990)

- *For $n = 2$, upward closed set is a set of uniqueness, and every set of uniqueness is upward closed up to measure-preserving transformations of axes.*
- *For $n \geq 2$, additive $\Rightarrow$ sets of uniqueness $\Rightarrow$ upward closed.*



- Blue set is upward closed $\Rightarrow$ Pareto optimal

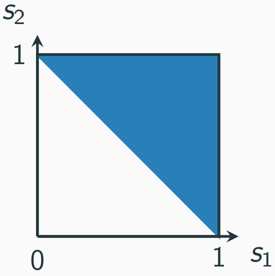
Fishburn et al.'s theorem & our Theorem 2 $\Rightarrow$

- For $n = 2$, characterization of Pareto optimality via conjugate distributions (Theorem 1)

Existing Results about Sets of Uniqueness

Theorem (Fishburn, Lagarias, Reeds, and Shepp 1990)

- *For $n = 2$, upward closed set is a set of uniqueness, and every set of uniqueness is upward closed up to measure-preserving transformations of axes.*
- *For $n \geq 2$, additive $\Rightarrow$ sets of uniqueness $\Rightarrow$ upward closed.*



- Blue set is upward closed $\Rightarrow$ Pareto optimal

Fishburn et al.'s theorem & our Theorem 2 $\Rightarrow$

- For $n = 2$, characterization of Pareto optimality via conjugate distributions (Theorem 1)
- For $n \geq 2$, a necessary and a sufficient condition of Pareto optimality

Connecting Pareto Optimality with Tomography

Theorem 2

For any $n \geq 2$, a private private info structure is Pareto optimal $\Leftrightarrow$ it is equivalent to a structure associated with a set of uniqueness $A \subseteq [0, 1]^n$.

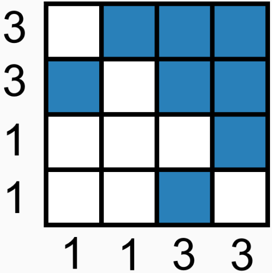
Key idea: A is not a set of uniqueness $\Rightarrow$ the associated structure is dominated and the dominating structure can be constructed explicitly

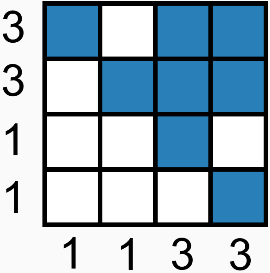
Connecting Pareto Optimality with Tomography

Theorem 2

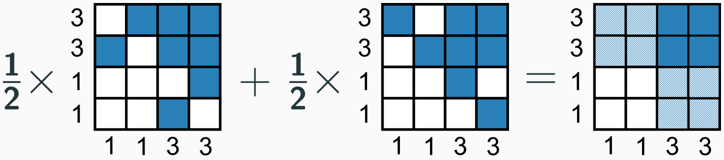
For any $n \geq 2$, a private private info structure is Pareto optimal $\Leftrightarrow$ it is equivalent to a structure associated with a set of uniqueness $A \subseteq [0,1]^n$.

Key idea: A is not a set of uniqueness $\Rightarrow$ the associated structure is dominated and the dominating structure can be constructed explicitly

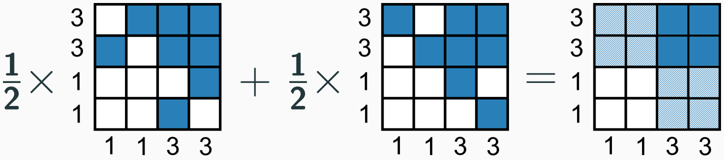




Not a Set of Uniqueness ⇒ Strictly Dominated

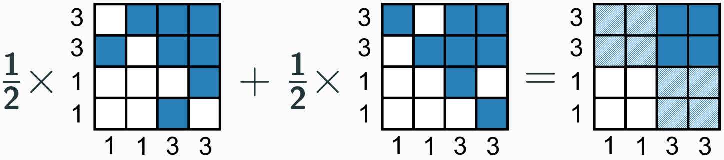


Not a Set of Uniqueness ⇒ Strictly Dominated



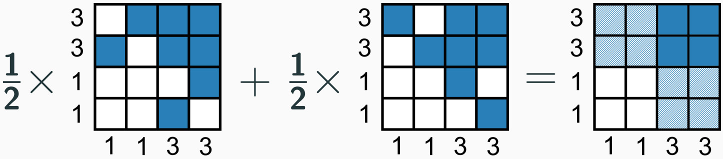
- Each square can now be colored, blank, or **shaded**

Not a Set of Uniqueness ⇒ Strictly Dominated



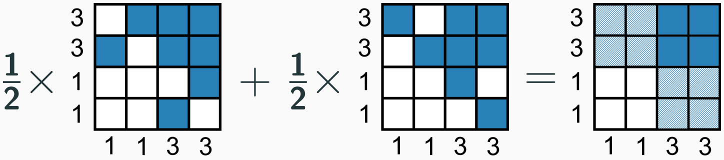
- Each square can now be colored, blank, or **shaded**
- Shaded square = "half of a colored square"

Not a Set of Uniqueness ⇒ Strictly Dominated



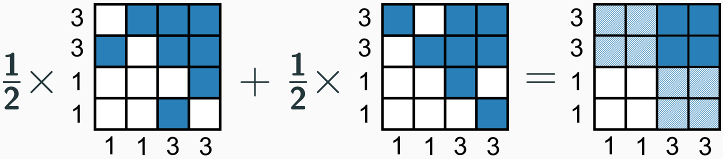
- Each square can now be colored, blank, or **shaded**
- Shaded square = "half of a colored square"
- Draw $s_1, s_2 \overset{\text{i.i.d.}}{\sim} \text{Unif}[0, 1]$. If (s_1, s_2) in shaded region, toss an independent fair coin s_3 to determine state ω

Not a Set of Uniqueness ⇒ Strictly Dominated



- Each square can now be colored, blank, or **shaded**
- Shaded square = "half of a colored square"
- Draw $s_1, s_2 \overset{\text{i.i.d.}}{\sim} \text{Unif}[0,1]$. If (s_1, s_2) in shaded region, toss an independent fair coin s_3 to determine state ω
- This structure generates the same distribution of posteriors

Not a Set of Uniqueness ⇒ Strictly Dominated



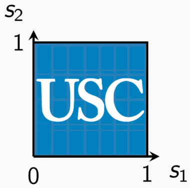
- Each square can now be colored, blank, or **shaded**
- Shaded square = "half of a colored square"
- Draw $s_1, s_2 \overset{\text{i.i.d.}}{\sim} \text{Unif}[0,1]$. If (s_1, s_2) in shaded region, toss an independent fair coin s_3 to determine state ω
- This structure generates the same distribution of posteriors
- Reveal the coin toss to the first player □

Summary

- **Private private information structures**:
  signals of different agents $(s_1, s_2, ..., s_n)$
  are unconditionally independent

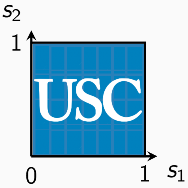
Summary

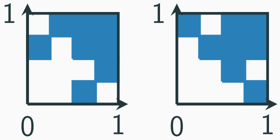
- **Private private information structures**: signals of different agents $(s_1, s_2, ..., s_n)$ are unconditionally independent
- Can **represent** all such info structures as subsets of $[0, 1]^n$



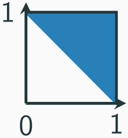
Summary

- **Private private information structures**: signals of different agents $(s_1, s_2, ..., s_n)$ are unconditionally independent
- Can **represent** all such info structures as subsets of $[0, 1]^n$
- Pareto optimal private private info structures are associated with **sets of uniqueness**



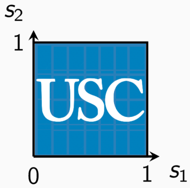


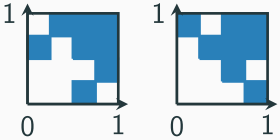
(not Pareto optimal)



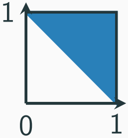
Summary

- **Private private information structures**: signals of different agents $(s_1, s_2, ..., s_n)$ are unconditionally independent
- Can **represent** all such info structures as subsets of $[0, 1]^n$
- Pareto optimal private private info structures are associated with **sets of uniqueness**
  - For $n = 2$, a simple criterion of Pareto optimality: distributions of posteriors must be conjugate



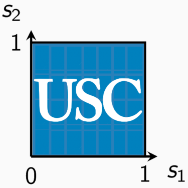


(not Pareto optimal)

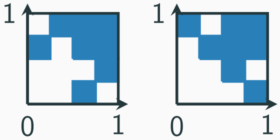


Summary

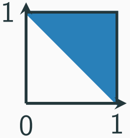
- **Private private information structures**: signals of different agents $(s_1, s_2, ..., s_n)$ are unconditionally independent
- Can **represent** all such info structures as subsets of $[0, 1]^n$



- Pareto optimal private private info structures are associated with **sets of uniqueness**
  - For $n = 2$, a simple criterion of Pareto optimality: distributions of posteriors must be conjugate
  - For $n \geq 2$, a necessary and a sufficient condition

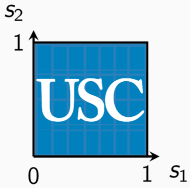


(not Pareto optimal)

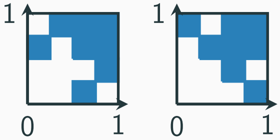


Summary

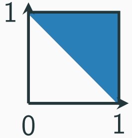
- **Private private information structures**: signals of different agents $(s_1, s_2, ..., s_n)$ are unconditionally independent
- Can **represent** all such info structures as subsets of $[0,1]^n$



- Pareto optimal private private info structures are associated with **sets of uniqueness**
  - For $n = 2$, a simple criterion of Pareto optimality: distributions of posteriors must be conjugate
  - For $n \geq 2$, a necessary and a sufficient condition



(not Pareto optimal)



Thank you!