Private Private Information

Kevin He (UPenn) **Fedor Sandomirskiy** (Caltech) Omer Tamuz (Caltech)
EC'22

Our question: how to disclose information optimally if constrained by privacy?

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, ..., n\}$

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$, common prior $\mathbb{P}[\omega = h] = p$

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$, common prior $\mathbb{P}[\omega = h] = p$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$, common prior $\mathbb{P}[\omega = h] = p$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**
    - s_i may carry info about s_j: public signals is a particular case
    - private information may not be private

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, \ldots, n\}$
- A **binary state** $\omega \in \{\ell, h\}$, common prior $\mathbb{P}[\omega = h] = p$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**
  - s_i may carry info about s_j: public signals is a particular case
  - private information may not be private

Definition

A joint distribution $\mathbb{P}$ over $(\omega, s_1, \ldots, s_n)$ is a **private private information structure** if $(s_1, \ldots, s_n)$ are independent

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$, common prior $\mathbb{P}[\omega = h] = p$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**
    - s_i may carry info about s_j: public signals is a particular case
    - private information may not be private

Definition

A joint distribution $\mathbb{P}$ over $(\omega, s_1, ..., s_n)$ is a **private private information structure** if $(s_1, ..., s_n)$ are independent

- Private private signals contain info about ω, not about each other

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$, common prior $\mathbb{P}[\omega = h] = p$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**
    - s_i may carry info about s_j: public signals is a particular case
    - private information may not be private

Definition

A joint distribution $\mathbb{P}$ over $(\omega, s_1, ..., s_n)$ is a **private private information structure** if $(s_1, ..., s_n)$ are independent

- Private private signals contain info about ω, not about each other
- Can everyone get **informative** private private signals?

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, ..., n\}$
- A **binary state** $\omega \in \{\ell, h\}$, common prior $\mathbb{P}[\omega = h] = p$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**
    - s_i may carry info about s_j: public signals is a particular case
    - private information may not be private

Definition

A joint distribution $\mathbb{P}$ over $(\omega, s_1, ..., s_n)$ is a **private private information structure** if $(s_1, ..., s_n)$ are independent

- Private private signals contain info about ω, not about each other
- Can everyone get **informative** private private signals?
    - Paradoxical: s_1 informative about ω, ω correlated with s_2, yet P1 learns nothing about s_2?

Our question: how to disclose information optimally if constrained by privacy?

- Agents $\{1, \ldots, n\}$
- A **binary state** $\omega \in \{\ell, h\}$, common prior $\mathbb{P}[\omega = h] = p$
- Agent i gets signal $s_i \in S_i$ about ω, her **private information**
  - s_i may carry info about s_j: public signals is a particular case
  - private information may not be private

Definition

A joint distribution $\mathbb{P}$ over $(\omega, s_1, \ldots, s_n)$ is a **private private information structure** if $(s_1, \ldots, s_n)$ are independent

- Private private signals contain info about ω, not about each other
- Can everyone get **informative** private private signals?
  - Paradoxical: s_1 informative about ω, ω correlated with s_2, yet P1 learns nothing about s_2?
- It is possible! We study tension between informativeness and privacy

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:**
  - 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 $(\omega, s_1, \ldots, s_n)$ **Blackwell dominates** $(\omega, s'_1, \ldots, s'_n)$ 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.

Characterization of Pareto Optimality for $n = 2$

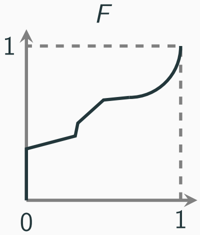
- Let F be a cdf of a distribution on $[0, 1]$ with mean p

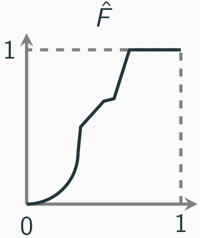
Characterization of Pareto Optimality for $n = 2$

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

Characterization of Pareto Optimality for $n = 2$

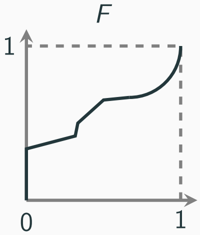
- Let F be a cdf of a distribution on $[0, 1]$ with mean p
- Denote $\hat{F}(x) = 1 - F^{-1}(1 - x)$
- Then $\hat{F}$ is also a cdf of a distribution on $[0, 1]$ with mean p, obtained by reflecting F around the anti-diagonal

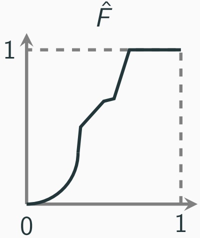




Characterization of Pareto Optimality for $n = 2$

- 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

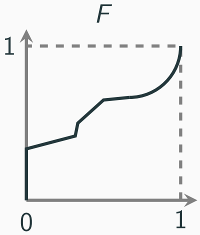


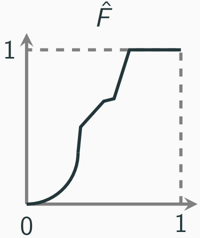


- Call F and $\hat{F}$ **conjugates**

Characterization of Pareto Optimality for $n = 2$

- 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: fairness, equity, and privacy in rating design

Application: fairness, equity, and privacy in rating design

- $\omega \in \{\ell, h\}$ is borrower's creditworthiness

Application: fairness, equity, and privacy in rating design

- $\omega \in \{\ell, h\}$ is borrower's creditworthiness
- s_1 is a private or legally protected trait, correlated with ω

Application: fairness, equity, and privacy in rating design

- $\omega \in \{\ell, h\}$ is borrower's creditworthiness
- s_1 is a private or legally protected trait, correlated with ω
- rating agency knows ω and s_1

Application: fairness, equity, and privacy in rating design

- $\omega \in \{\ell, h\}$ is borrower's creditworthiness
- s_1 is a private or legally protected trait, correlated with ω
- rating agency knows ω and s_1
- sends a signal s_2 about the borrower's creditworthiness

Application: fairness, equity, and privacy in rating design

- $\omega \in \{\ell, h\}$ is borrower's creditworthiness
- s_1 is a private or legally protected trait, correlated with ω
- rating agency knows ω and s_1
- sends a signal s_2 about the borrower's creditworthiness
- regulations / privacy laws may require s_2 to be independent of s_1 (demographic parity)

Application: fairness, equity, and privacy in rating design

- $\omega \in \{\ell, h\}$ is borrower's creditworthiness
- s_1 is a private or legally protected trait, correlated with ω
- rating agency knows ω and s_1
- sends a signal s_2 about the borrower's creditworthiness
- regulations / privacy laws may require s_2 to be independent of s_1 (demographic parity)
- **Observation:** finding the most informative s_2 independent of s_1 $\Leftrightarrow$ finding a Pareto optimal (ω, s_1, s_2) with the given (ω, s_1) marginal

Application: fairness, equity, and privacy in rating design

- $\omega \in \{\ell, h\}$ is borrower's creditworthiness
- s_1 is a private or legally protected trait, correlated with ω
- rating agency knows ω and s_1
- sends a signal s_2 about the borrower's creditworthiness
- regulations / privacy laws may require s_2 to be independent of s_1 (demographic parity)
- **Observation:** finding the most informative s_2 independent of s_1 $\Leftrightarrow$ finding a Pareto optimal (ω, s_1, s_2) with the given (ω, s_1) marginal

Corollary

For given (ω, s_1), 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: fairness, equity, and privacy in rating design

- $\omega \in \{\ell, h\}$ is borrower's creditworthiness
- s_1 is a private or legally protected trait, correlated with ω
- rating agency knows ω and s_1
- sends a signal s_2 about the borrower's creditworthiness
- regulations / privacy laws may require s_2 to be independent of s_1 (demographic parity)
- **Observation:** finding the most informative s_2 independent of s_1 $\Leftrightarrow$ finding a Pareto optimal (ω, s_1, s_2) with the given (ω, s_1) marginal

Corollary

For given (ω, s_1), 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.

- for ≥ 3 states ω, there may be a continuum of optimal s_2

Canonical representation of private private info structures

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

Canonical representation of private private info structures

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

Canonical representation of private private info structures

- 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

Canonical representation of private private info structures

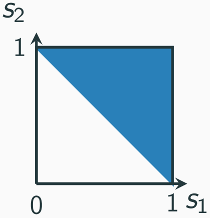
- Fix $A \subset [0,1]^n$ with measure p
- Define a **private private structure associated with** A:
    - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
    - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \backslash A$

Canonical representation of private private info structures

- 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

Canonical representation of private private info structures

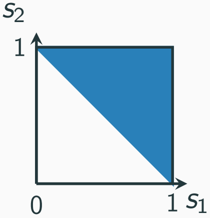
- Fix $A \subset [0,1]^n$ with measure p
- Define a **private private structure associated with** A:
  - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
  - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \backslash A$
  - Signals are uniform on $[0,1]^n$, hence, private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



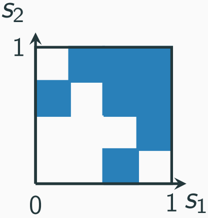
beliefs:
uniform on $[0,1]$

Canonical representation of private private info structures

- 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



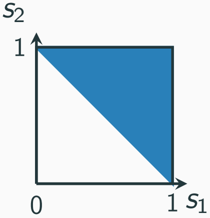
beliefs:
uniform on $[0,1]$



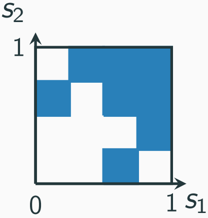
beliefs:
$1/4$ and $3/4$

Canonical representation of private private info structures

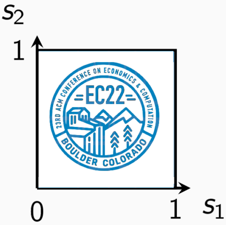
- Fix $A \subset [0,1]^n$ with measure p
- Define a **private private structure associated with** A:
  - When $\omega = h$, choose $(s_1, ..., s_n)$ uniformly from A
  - When $\omega = \ell$, choose $(s_1, ..., s_n)$ uniformly from $[0,1]^n \backslash A$
  - Signals are uniform on $[0,1]^n$, hence, private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



beliefs:
uniform on $[0,1]$

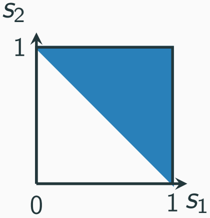


beliefs:
$1/4$ and $3/4$

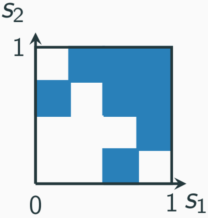


Canonical representation of private private info structures

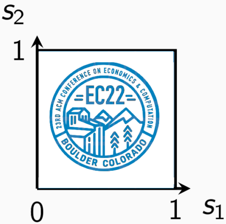
- Fix $A \subset [0,1]^n$ with measure p
- Define a **private private structure associated with** A:
  - When $\omega = h$, choose $(s_1, \ldots, s_n)$ uniformly from A
  - When $\omega = \ell$, choose $(s_1, \ldots, s_n)$ uniformly from $[0,1]^n \backslash A$
  - Signals are uniform on $[0,1]^n$, hence,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



beliefs:
uniform on $[0,1]$



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

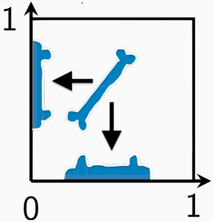


Proposition

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

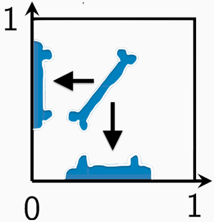
Pareto optimality and tomography

Tomography reconstructs objects from lower-dimensional projections



Pareto optimality and tomography

Tomography reconstructs objects from lower-dimensional projections



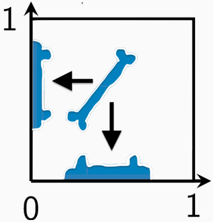
We need a concept from math tomography:

Definition

$A \subseteq [0,1]^n$ is a **set of uniqueness** if its n projections to n coordinate axes suffice to reconstruct A

Pareto optimality and tomography

Tomography reconstructs objects from lower-dimensional projections



We need a concept from math tomography:

Definition

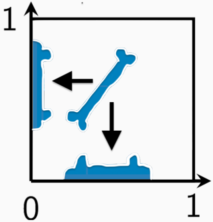
$A \subseteq [0,1]^n$ is a **set of uniqueness** if its n projections to n coordinate axes suffice to reconstruct A

Theorem 2

A private private info structure is Pareto optimal $\iff$ equivalent to a structure associated with a set of uniqueness

Pareto optimality and tomography

Tomography reconstructs objects from lower-dimensional projections



We need a concept from math tomography:

Definition

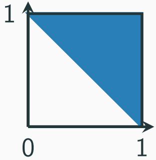
$A \subseteq [0,1]^n$ is a **set of uniqueness** if its n projections to n coordinate axes suffice to reconstruct A

Theorem 2

A private private info structure is Pareto optimal $\iff$ equivalent to a structure associated with a set of uniqueness

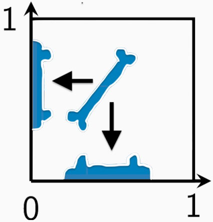
Fishburn, Lagarias, Reeds, Shepp 1990

For $n = 2$, A is a set of uniqueness $\Leftrightarrow$ upward-closed up to a measure-preserving transformations of axes



Pareto optimality and tomography

Tomography reconstructs objects from lower-dimensional projections



We need a concept from math tomography:

Definition

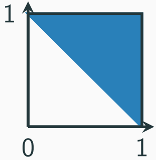
$A \subseteq [0,1]^n$ is a **set of uniqueness** if its n projections to n coordinate axes suffice to reconstruct A

Theorem 2

A private private info structure is Pareto optimal $\iff$ equivalent to a structure associated with a set of uniqueness

Fishburn, Lagarias, Reeds, Shepp 1990

For $n = 2$, A is a set of uniqueness $\Leftrightarrow$ upward-closed up to a measure-preserving transformations of axes



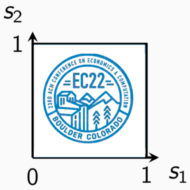
Corollary: characterization of Pareto Optimality via conjugates (Th 1)

Summary

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

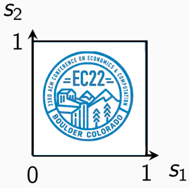
Summary

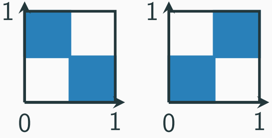
- **Private private information structures**: signals of different agents $(s_1, s_2, ..., s_n)$ are unconditionally independent
- Can **represent** all such info structures as subsets of $[0, 1]^n$



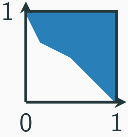
Summary

- **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**





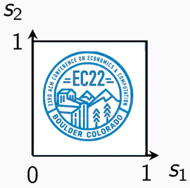
(not Pareto optimal)

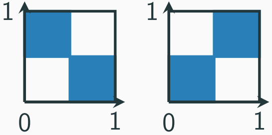


(Pareto optimal)

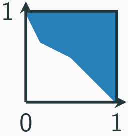
Summary

- **Private private information structures**: signals of different agents $(s_1, s_2, \ldots, s_n)$ 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





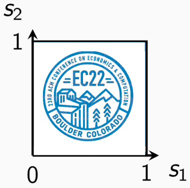
(not Pareto optimal)



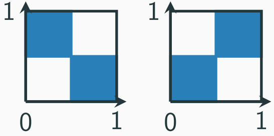
(Pareto optimal)

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 $[0, 1]^n$

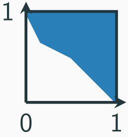


- Pareto optimal private private info structures are associated with **sets of uniqueness**
    - For $n = 2$, a simple criterion of Pareto optimality: distributions of posteriors must be conjugate



(not Pareto optimal)

Thank you!



(Pareto optimal)

Other occurrences of private private signals

Other occurrences of private private signals

- 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

- 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

- 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