Private Private Information

Kevin He, Fedor Sandomirskiy, Omer Tamuz

University of Pennsylvania
Caltech and Higher School of Economics
Department of Economics and Mathematics at Caltech

May 27, 2022

Introduction

- In reality, different agents observe different signals that induce beliefs about the states.
- The same signal could also alter the agent's belief over other people's beliefs.
- In this work, we focus on a **private private signals**: the information available to each agent reveals nothing at all about the information available to her peers.
- Applications:
  - causal inference
  - zero-sum game
  - optimal private disclosure

Model

- A group of agents $N = \{1, 2, 3, ..., n\}$.
- Each agent i observes a signal s_i contains information about nature state $\omega \in \Omega = \{1, 2, ..., m-1\}$.
- All agents start with a common, full-support prior belief about the state.
- We call the tuple $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ an information structure.
- Let $p(s_i)$ denotes the posterior associated with s_i.
- In the case of a binary state, we let $p(s_i)$ take value in [0,1] by setting

$$p(s_i) = \mathbb{P}[\omega = 1 \mid s_i].$$

Definition (1.)

We say that $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ is a private private information structure if $(s_1, \ldots, s_n)$ are **independent** random variables.

A partial order on private private information structures

Definition (2.)

Let $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ and $\hat{\mathcal{I}} = (\omega, \hat{s}_1, \ldots, \hat{s}_n)$ be private private information structures. We say that $\mathcal{I}$ dominates $\hat{\mathcal{I}}$, and write $\mathcal{I} \geq \hat{\mathcal{I}}$, if for every i it holds that (ω, s_i) Blackwell dominates $(\omega, \hat{s}_i)$. We say that $\mathcal{I}$ and $\hat{\mathcal{I}}$ are equivalent if $\mathcal{I} \geq \hat{\mathcal{I}}$ and $\hat{\mathcal{I}} \geq \mathcal{I}$.

- For the single-agent case (n=1) , recall that an information structure (ω, s) Blackwell dominates $(\omega, \hat{s})$ if for every continuous convex $\varphi : \Delta(\Omega) \to \mathbb{R}$ it holds that
$$\mathbb{E}[\varphi(p(s))] \geqslant \mathbb{E}[\varphi(p(\hat{s}))].$$
- A first question that arises is that of feasibility: which n-tuples $(\mu_1, \mu_2, \ldots, \mu_n)$ represent some private private information structure?

Pareto optimality

Definition (3.)

We say that a private private information structure $\mathcal{I}$ is Pareto optimal if, for every private private information structure $\hat{\mathcal{I}}$ such that $\hat{\mathcal{I}} \geq \mathcal{I}$, the structure $\hat{\mathcal{I}}$ is equivalent to $\mathcal{I}$.

- Pareto optimality: which private private information structures provide a maximal amount of information to the agents, so that more information cannot be supplied without violating privacy?
- There is some tension between the privacy of an information structure and its informativeness.
- For example, the most informative structure from the point of view of agent 1 is the one where s_1 completely reveals the state, i.e., $p(s_1) = \delta_\omega$. Likewise, agent 2 would benefit most from a structure where s_2 perfectly reveals the state. But then $p(s_1) = p(s_2)$, and so s_1 and s_2 are not independent.

Optimal Private Disclosure

- An informed party who wishes to disclose as much information as possible about the state of nature ω using a message s_2, but must not reveal any information about a correlated random variable s_1 in the process.
- An uninformed company wants to learn about a decision-relevant type ω of an applicant (fit for a job?).
- An informed party (credit-rating company) knows both this type and a legally protected trait s_1 of the applicant that correlates with the type.
- The informed party faces the problem of optimal private disclosure: convey as much information as possible about the applicant without revealing any information about her protected trait.

Definition (4.)

Given a one-agent information structure (ω, s_1) , a signal s_2 is an optimal private disclosure for (ω, s_1) if $\mathcal{I} = (\omega, s_1, s_2)$ is a Pareto optimal private private information structure.

Influencing Competitors in Zero-Sum Games

- Consider a zero-sum game played by two players.
- The action set of player $i \in \{1, 2\}$ is A_i , which we take to be finite.
- The utilities are given by $u_1 = -u_2 = u$ for some $u : A_1 \times A_2 \to \mathbb{R}$.
- There is a random state ω taking value in Ω.
- The two players do not know the state and their payoffs do not depend on it.
- But, there is another agent (the designer) who knows the state and has a utility function $u_d : \Omega \times A_1 \times A_2$ that depends on the state and the actions of the players.
- This can model a setting where a designer wants to influence the actions of two competitors, with the designer's preference over actions given by his private type ω .
- The designer commits to a (not necessarily private private) information structure (ω, s_1, s_2) .
- When the state ω is realized, the designer observes it and sends the signal s_1 to player 1 and s_2 to player 2 . The players choose their actions after observing the signals.

Influencing Competitors in Zero-Sum Games

- The next claim shows that private private information structures arise endogenously in this setting.

Claim (1.)

In every direct-revelation equilibrium, the information structure (ω, s_1, s_2) is a private private information structure.

- The intuition behind this result is simple: revealing to player i any information about the recommendation given to player $-i$ gives i an advantage that she can exploit to increase her expected utility beyond the value of the game. But player $-i$ can guarantee that i does not get more than the value, and hence s_i cannot contain any information about s_{-i}.

Influencing Competitors in Zero-Sum Games

- The next claim shows that private private information structures arise endogenously in this setting.

Claim (1.)

In every direct-revelation equilibrium, the information structure (ω, s_1, s_2) is a private private information structure.

- The intuition behind this result is simple: revealing to player i any information about the recommendation given to player $-i$ gives i an advantage that she can exploit to increase her expected utility beyond the value of the game. But player $-i$ can guarantee that i does not get more than the value, and hence s_i cannot contain any information about s_{-i}.

Conjugate Distributions

Definition (5.)

The conjugate of a cumulative distribution function $F : [0,1] \to [0,1]$ is the function $\hat{F} : [0,1] \to [0,1]$, which is given by

$$\hat{F}(x) = 1 - F^{-1}(1-x).$$

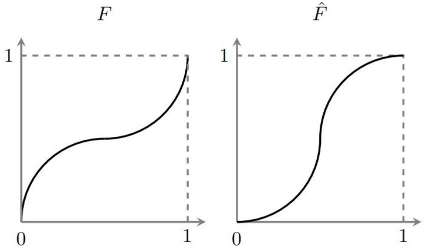

Figure 3: An example of a cumulative distribution function F and its conjugate $\hat{F}$. The shapes under the curves are congruent: the transformation that maps one to the other is reflection around the anti-diagonal. Qualitatively, F corresponds to the belief distribution of a more informative signal, and $\hat{F}$ corresponds to that of a less informative signal.

Construction of Conjugate Distributions

- Note that for every pair of conjugate distributions μ and $\hat{\mu}$, there exists a private private information structure $\mathcal{I} = (\omega, s_1, s_2)$ where $p(s_1)$ has the distribution μ and $p(s_2)$ has the distribution $\hat{\mu}$. By Theorem 1, this structure will be Pareto optimal.
- To explicitly construct such a structure, calculate the cumulative distribution function F of μ and its conjugate $\hat{F}$, choose (s_1, s_2) uniformly from the unit square (so that they are independent and each distributed uniformly on $[0, 1]$), and let $\omega = h$ be the event that $s_2 \geqslant \hat{F}(1 - s_1)$.
- A simple calculation shows that $\hat{F}(1 - s_1)$ is equal to the posterior $p(s_1)$ and has the distribution μ , and $p(s_2)$ has the distribution $\hat{\mu}$.

Optimal Private Disclosures

Theorem (2.)

For a binary state ω, there exists an optimal private disclosure $s_2^\star$ for every (ω, s_1). This disclosure is unique up to equivalence: the distribution of $p\left(s_2^\star\right)$ is the conjugate of the distribution of $p\left(s_1\right)$. Furthermore, every signal s_2 independent of s_1 is Blackwell dominated by $s_2^\star$.

- It implies that every decision maker would find the signal s_2 optimal, regardless of the decision problem at hand.
- We provide a simple practical procedure for generating an optimal private disclosure $s_2^\star$, given realizations of (ω, s_1). We know that s_1 and $s_2^\star$ induce conjugate belief distributions, so we can use the general procedure outlined in Figure 4 to construct $s_2^\star$ as follows:
  - Calculate $p\left(s_1\right)$, the conditional probability of $\omega = 1$ given s_1.
  - If $\omega = 1$, sample $s_2^\star$ uniformly from the interval $[1 - p\left(s_1\right), 1]$.
  - If $\omega = 0$, sample $s_2^\star$ uniformly from the interval $[0, 1 - p\left(s_1\right)]$.

Welfare Maximizing Private Private Information Structures

- Suppose that each agent $i \in \{1, 2\}$ has to choose an action $a_i \in A_i$ after observing a signal s_i , and receives payoff according to a utility function $u_i(\omega, a_i)$.
- For a given binary ω, the social welfare of a given structure (ω, s_1, s_2) is

$$\sum_{i=1,2} \mathbb{E}\left[\sup_{\sigma_i : S_i \to A_i} u_i(\omega, \sigma_i(s_i))\right].$$

- What are the private private information structures (ω, s_1, s_2) that maximize social welfare?

Welfare Maximizing Private Private Information Structures

Proposition (1.)

Given a binary ω, and given u_1 and u_2, there exists a welfare maximizing private private information structure (ω, s_1, s_2) such that s_1 takes two values, s_2 takes three values, and the distributions of beliefs induced by s_1 and s_2 are conjugates.

- Example: $A_i = \Omega = \{0, 1\}$. Each agent gets utility 1 from matching the state and utility -1 from mismatching it, so that

$$u_1(\omega, a) = u_2(\omega, a) = 2|\omega - a| - 1.$$

- If we reveal the state to agent 1 and give agent 2 no information, then the social welfare is 1 .
- Consider instead a private private information structure where each agent has a posterior belief of $\sqrt{1/2}$ with probability $\sqrt{1/2}$ and a posterior belief of 0 with the complementary probability.
- Then the social welfare is $4 - 2\sqrt{2} \approx 1.17$.

Welfare Maximizing Private Private Information Structures

- To show it is indeed optimal, by Proposition 1, we can assume that the distribution of posteriors μ induced by s_1 is supported on two points. It has mean 1 / 2 since the average posterior equals the prior, and thus can be represented as

$$\frac{\alpha}{\alpha+\beta}\delta_{\frac{1}{2}} - \beta + \frac{\beta}{\alpha+\beta}\delta_{\frac{1}{2}+\alpha}$$

  for some constants $\alpha, \beta \in (0, 1/2]$, where δ_x denotes the point mass at x.
- The contribution of the first agent to the welfare is therefore $\frac{4\alpha\beta}{\alpha+\beta}$.
- The conjugate distribution $\hat{\mu}$ takes the form

$$\left(\frac{1}{2} - \alpha\right)\delta_0 + (\alpha+\beta)\delta_{\frac{\beta}{\alpha+\beta}} + \left(\frac{1}{2} - \beta\right)\delta_1.$$

- As the problem is state-symmetric, we can assume $\beta \geqslant \alpha$ without loss of generality and, hence, the middle atom of $\hat{\mu}$ is above $1/2$. Therefore, the second agent contributes $1 - 2\alpha$ to the welfare, and the total welfare equals $\frac{4\alpha\beta}{\alpha+\beta} + 1 - 2\alpha$.
- A simple calculation shows that this is maximized when $\beta = 1/2$ and $\alpha = \sqrt{1/2} - 1/2$, which yields the structure described above.

Pareto Optimality and Sets of Uniqueness

- As a first step, we show that it is without loss of generality to focus on information structures that are constructed similarly to the examples we have considered above: each s_i is distributed uniformly on $[0,1]$, and each value of ω corresponds to some subset of $[0,1]^n$. That is, ω is a deterministic function of the signals.
- More formally, let $\mathcal{A} = (A_0, \dots, A_{m-1})$ be a partition of $[0,1]^n$ into measurable sets. That is, each A_k is a measurable subset of $[0,1]^n$, the sets in $\mathcal{A}$ are disjoint, and their union is equal to $[0,1]^n$.

Definition (6.)

The private private information structure associated with a partition $\mathcal{A} = (A_0, \dots, A_{m-1})$ is $\mathcal{I} = (\omega, s_1, \dots, s_n)$ where $(s_1, \dots, s_n)$ are distributed uniformly on $[0,1]^n$ and $\{\omega = k\}$ is the event that $\{(s_1, \dots, s_n) \in A_k\}$.

Pareto Optimality and Sets of Uniqueness

Proposition (2.)

For every private private information structure $\mathcal{I}$, there exists a partition $\mathcal{A}$ whose associated information structure $\mathcal{I}'$ is equivalent to $\mathcal{I}$.

Pareto Optimality and Sets of Uniqueness

- Given a measurable set $A \subseteq [0,1]^n$, we define n functions $\left(\alpha_1^A, \ldots, \alpha_n^A\right)$ that capture the projections of A to the n coordinate axes. Denote by λ the Lebesgue measure on $[0,1]^{n-1}$. The projection $\alpha_i^A : [0,1] \to [0,1]$ of A to the i th axis is

$$\alpha_i^A(t) = \lambda\left(\{y_{-i} : (y_i, y_{-i}) \in A, y_i = t\}\right)$$

- If $(\omega, s_1, \ldots, s_n)$ is the information structure associated with A , then $\alpha_i^A(t)$ is the posterior of agent i when she observes $s_i = t$.

Definition (7.)

A measurable $A \subseteq [0,1]^n$ is a set of uniqueness if for every measurable $B \subseteq [0,1]^n$ such that $\left(\alpha_1^A, \ldots, \alpha_n^A\right) = \left(\alpha_1^B, \ldots, \alpha_n^B\right)$, it holds that $A = B$.

Pareto Optimality and Sets of Uniqueness

Theorem (3.)

A private private information structure is Pareto optimal if and only if it is equivalent to a structure associated with a set of uniqueness $A \subseteq [0,1]^n$.

Pareto Optimality and Sets of Uniqueness

- To characterize sets of uniqueness in two dimensions, we will need the following definitions.
- Say that $A \subseteq [0,1]^2$ is a rearrangement of $B \subseteq [0,1]^2$ if for $i = 1, 2$ and every $q \in [0,1]$, the sets $\{t \in [0,1] : \alpha_i^A(t) \leqslant q\}$ and $\{t \in [0,1] : \alpha_i^B(t) \leqslant q\}$ have the same Lebesgue measure. That is, α_i^A and α_i^B, when viewed as random variables defined on $[0,1]$, have the same distribution.
- This has a simple interpretation in terms of information structures: A is a rearrangement of B if and only if the two associated information structures are Blackwell equivalent.
- This is immediate, since in the information structure associated with $A, \alpha_i^A(t)$ is the belief of agent i after observing $s_i = t$.
- Recall that $B \subseteq [0,1]^n$ is upward-closed if $x = (x_1, \dots, x_n) \in B$ implies that $y = (y_1, \dots, y_n) \in B$ for all $y \geqslant x$.

Theorem (4. Lorentz (1949))

A measurable subset $A \subseteq [0,1]^2$ is a set of uniqueness if and only if it is a rearrangement of an upward-closed set.

Pareto Optimality and Sets of Uniqueness

- When $n > 2$, a simple sufficient condition for uniqueness is to be an additive set: this holds when there are bounded $h_i : [0,1] \to \mathbb{R}$ such that

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

- In two dimensions a set is additive if and only if it is a rearrangement of an upward-closed set, and so additivity provides another characterization of the sets of uniqueness.
- In higher dimensions (i.e., with three or more agents), the sufficiency of additivity implies that every additive set is associated with a Pareto optimal structure.

Feasibility

- We consider the question of feasibility: which tuples $(\mu_1, \ldots, \mu_n)$ represent some private private information structure?

Definition (8.)

An n-tuple $(\mu_1, \ldots, \mu_n)$ of probability measures on $\Delta(\Omega)$ is said to be feasible if there exists a private private information structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ such that μ_i is the distribution of $p\,(s_i)$.

- A necessary condition for feasibility is given by the so-called martingale condition (i.e., by the law of iterated expectations).
- It implies that if the posterior $p\,(s_i)$ has distribution μ_i then the expected posterior $\int q \; \mathrm{d}\mu_i(q)$ must equal to the prior distribution of ω.
- Thus a necessary condition for feasibility is that

$$\int q \; \mathrm{d}\mu_i(q) = \int q \; \mathrm{d}\mu_j(q)$$

for all agents i and j.

Feasibility

- The question of feasibility is closely related to that of Pareto optimality. Indeed, one answer is that $(\mu_1, \ldots, \mu_n)$ is feasible if and only if there exists a Pareto optimal structure represented by some $(\nu_1, \ldots, \nu_n)$, such that each μ_i is a mean-preserving contraction of ν_i.
- This holds since mean-preserving contractions of the posterior belief distributions correspond to Blackwell dominance. By Blackwell's Theorem, one can take a structure with posteriors $(\nu_1, \ldots, \nu_n)$, and apply an independent garbling to each agent's signal to arrive at a structure with posteriors $(\mu_1, \ldots, \mu_n)$.

Corollary (1.)

The pair (μ_1, μ_2) of distributions on $[0, 1]$ is feasible if and only if μ_2 is a mean preserving contraction of the conjugate of μ_1.

Feasibility

- We now present a necessary condition of feasibility for general m states and n agents, which relies on information-theoretic ideas.
- The Shannon entropy of a measure $q \in \Delta(\Omega)$ is

$$H(q) = -\sum_{k \in \Omega} q(k) \log_2(q(k))$$

- Given a signal (ω, s_i), denote the mutual information between ω and s_i by

$$I(\omega; s_i) = H(\mathbb{E}[p(s_i)]) - \mathbb{E}[H(p(s_i))].$$

- Note that $I(\omega; s_i)$ can be written in terms of the distribution of posteriors μ_i, and so it is an equivalence invariant:

$$I(\mu_i) = H\left(\int q \, \mathrm{d}\mu_i(q)\right) - \int H(q) \mathrm{d}\mu_i(q)$$

- In this expression, the first expectation $\int q \, \mathrm{d}\mu_i(q)$ is the prior distribution of ω.

Feasibility

Proposition (3.)

With n agents and m states, the tuple $(\mu_1, \ldots, \mu_n)$ of distributions on $\Delta(\Omega)$ is feasible only if all μ_i have the same expectation $p = \int q \, \mathrm{d}\mu_i(q)$ and

$$\sum_i I(\mu_i) \leqslant H(p).$$

- The sum of mutual information is bounded by the entropy of the prior of ω.
- Allocating finite resource among agents.

Feasibility

- Is the previous bound tight?

Proposition (4.)

The tuple $(\mu_1, \dots, \mu_n)$ of distributions on $\Delta(\{0,1\})$ is feasible only if all μ_i have the same expectation $p = \int q \, \mathrm{d}\mu_i(q)$ and

$$\sum_i I(\mu_i) \leqslant H(p) - \frac{\ln 2}{8} \sum_{i<j} I(\mu_i) I(\mu_j).$$

- It shows that for a binary state, while entropy is a finite resource, it cannot be fully divided among the agents: the sum of mutual information is strictly less than the entropy of ω (as long as at least two signals are informative).

Feasibility

- The connection to some decision problems: quadratic utility function.
- For $q \in \Delta(\Omega)$ denote

$$\bar{H}(q) = \sum_{k \in \Omega} q(k)(1 - q(k)),$$

and for a measure $\mu on \Delta(\Omega)$ define

$$\bar{I}(\mu) = \bar{H}\left(\int q \, \mathrm{d}\mu(q)\right) - \int \bar{H}(q) \mathrm{d}\mu(q).$$

Loosely speaking, for a distribution μ over posterior beliefs, $\bar{I}(\mu)$ is the expected reduction in the variance of the agent's belief.

Proposition (5.)

With n agents and m states, the tuple $(\mu_1, \ldots, \mu_n)$ of distributions on $\Delta(\Omega)$ is feasible only if all μ_i have the same expectation $p = \int q \, \mathrm{d}\mu_i(q)$ and

$$\sum_i \bar{I}(\mu_i) \leqslant \bar{H}(p).$$

Thanks!