Private Private Information*

Kevin He[†] Fedor Sandomirskiy[‡] Omer Tamuz[§]

January 14, 2022

Abstract

In a *private* private information structure, agents' signals contain no information about the signals of their peers. We study how informative such structures can be, and characterize those that are on the Pareto frontier, in the sense that it is impossible to give more information to any agent without violating privacy. In our main application, we show how to optimally disclose information about an unknown state under the constraint of not revealing anything about a correlated variable that contains sensitive information.

*The paper benefited from numerous suggestions and comments of our colleagues. We are grateful (in alphabetic order) to Marina Agranov, Nageeb Ali, Itai Arieli, Eric Auerbach, Yakov Babichenko, Dirk Bergemann, Alexander Bloedel, Aislinn Bohren, David Dillenberger, Piotr Dworczak, Federico Echenique, Jeffrey Ely, Drew Fudenberg, Hanming Fang, David Kempe, Toygar Kerman, Victoria Kostina, Elliot Lipnowski, George Mailath, Moritz Meyer-ter-Vehn, Xiaosheng Mu, Luciano Pomatto, Andy Postlewaite, Ran Spiegler, Bruno Strulovici, Ina Taneva, Tristan Tomala, Nicolas Vieille, Leeat Yariv, and seminar participants at Caltech, University College London, UC Riverside, Hong Kong Joint Theory Seminar, HSE Moscow and St. Petersburg, University of Maryland, Northwestern University, University of Pennsylvania, 2021 LA Theory Conference, Retreat on Information, Networks, and Social Economics, and Stony Brook Workshop on Strategic Communication and Learning.

[†]University of Pennsylvania. Email: hesichao@gmail.com.

[‡]Caltech and Higher School of Economics, St.Petersburg. Email: fsandomi@caltech.edu. Fedor Sandomirskiy was partially supported by grant 19-01-00762 of the Russian Foundation for Basic Research and the Basic Research Program of the National Research University Higher School of Economics.

[§]Caltech. Email: tamuz@caltech.edu. Omer Tamuz was supported by a grant from the Simons Foundation (#419427), a Sloan fellowship, a BSF award (#2018397) and a National Science Foundation CAREER award (DMS-1944153).

1 Introduction

Economists have long used private information as a basic modeling tool to capture settings where different people have different information about an uncertain state of nature. Typically, each agent observes a signal that induces a belief over this state. The same signal could also alter the agent's belief over other people's beliefs. In this paper, we study a special case of private information where the information available to each agent reveals nothing at all about the information available to her peers. That is, we consider private signals that are literally private, which we call *private* private signals.

As a simple example of private private information, suppose three agents each receive an independent binary signal, and the unknown state of nature is the majority of these three signals.[1] Because of independence, each agent holds the same belief about others' signal realizations when her own signal is high and when it is low. And yet, every signal is informative about the state. On the other hand, conditionally independent private signals are not private private. For instance, consider a binary state and conditionally independent binary signals that match the state with a certain probability. Here, each agent's signal contains information about the others' signals: when an agent observes a high signal, she becomes more confident that her peers also got high signals.

The main question that we address in this paper is: how informative can private private signals be? There is an inherent tension between the privacy of an information structure and its informativeness. For example, it is clearly impossible for two agents to both have signals that perfectly reveal the state while maintaining privacy. What is the maximum amount of information that can be conveyed through private private signals? We formalize this question using the notion of Pareto optimality with respect to the Blackwell order: a private private information structure is *Pareto optimal* if it is impossible to give more information to any agent—in the Blackwell sense—without violating privacy.

In the case of two agents and a binary state, we give a simple description of the Pareto frontier that allows for a straightforward test of optimality and a constructive procedure for finding optimal structures. We also study Pareto optimality in

[1] Similar information structures are used in the social learning literature (Gale, 1996; Çelen and Kariv, 2004a,b).

the general case with any number of agents, where our characterization provides a surprising connection to the field of mathematical tomography and the study of sets of uniqueness. A subset of $[0,1]^n$ is called a *set of uniqueness* if it is uniquely determined by the densities of its projections to the coordinate axes. Understanding such sets has been an active area of research since the 1940s (Lorentz, 1949). This problem gained more prominence with the advent of tomography, a technology to reconstruct three-dimensional objects from their projections (Gardner, 1995). We show that private private information structures for n agents can be identified with subsets of $[0,1]^n$, and that the Pareto optimal ones correspond exactly to sets of uniqueness. In the two-dimensional case—which corresponds to the case of two agents and a binary state—the complete characterization of the sets of uniqueness is known (Lorentz, 1949) and leads to our characterization of the Pareto frontier. With more agents, we rely on more recent results on sets of uniqueness for $n \geqslant 3$ (Fishburn et al., 1990) to provide some sufficient conditions and some necessary conditions for Pareto optimality. With three or more states, an analogous equivalence holds between between Pareto optimality and a generalization of sets of uniqueness that we term *partitions of uniqueness*.

Finally, using a information-theoretic approach, we provide simple constraints on the informativeness of private private signals. We show that the sum of mutual information of private private signals cannot exceed the entropy of the state, which is not true for general information structures. We also prove an improved bound on the sum of mutual information of private private signals, which might be of independent interest in information theory.

Our focus on the maximal informativeness of private private signals is relevant to a number of economic settings:

(1) In causal inference, a *collider* is a causal structure where a number of independent random variables together determine a state (see, e.g., Pearl, 2009), as in the majority signal example above. Characterizing Pareto optimality of private private signals lets us bound the causal strengths of the various causes in a collider structure (Janzing et al., 2013).

(2) Suppose agents compete in a zero-sum game, and a designer who knows the state wishes to influence how agents' actions correlate with the state. We show that equilibrium signals must be private private. So, our bounds on the informativeness of private private signals limit how much the designer can adapt the agents' actions

to the state and thus constrain the designer's payoffs.

(3) In our main application of *optimal private disclosure*, we consider the problem of designing a maximally informative signal about the state under the constraint of not revealing any information about a correlated random variable. Consider an employer deciding whether to hire an applicant. The employer wants to know an unknown state, which is the applicant's productivity type. The employer solicits a letter from a recommender who knows the applicant's type. Barring any constraints, the recommender could perfectly reveal this state to the employer. But the obstacle is that there is an additional piece of information—a health condition of the applicant—that is also known to the recommender, that is correlated with the productivity type, and that the recommender is not allowed to reveal. Indeed, we assume the recommender's message must be completely independent of the applicant's health, so that the employer learns nothing about the applicant's health from the letter. Thus, the applicant's health condition and the recommender's letter comprise two private private signals about the applicant's productivity type.

When the state is binary (i.e., the applicant's productivity type takes one of two values), our results on Pareto optimal private private information imply a complete solution to the optimal private disclosure problem. As we show, in this case there is a unique optimal private disclosure: a way to write the recommendation letter so that it Blackwell dominates the information contained in any other letter that preserves the applicant's privacy. Our proof is constructive and gives a simple recipe for generating this optimal signal.

Related literature. The question of which belief distributions can arise in private private information structures was addressed in Gutmann et al. (1991) and Arieli et al. (2021). They provide a characterization for two agents under additional symmetry assumptions; we discuss the relation to our work below. More generally, a related question is which joint belief distributions are feasible without the privacy constraint (see, e.g., Dawid et al., 1995; Burdzy and Pal, 2019; Burdzy and Pitman, 2020; Arieli et al., 2021; Cichomski and Osękowski, 2021). Hong and Page (2009) look at a special case of private private signals where there are as many signals as there are states of nature. But they do not characterize private private information in general or study how informative these structures can be.

Private private signals arise as the worst-case information structure for the auctioneer in some problems of robust mechanism design: see Bergemann et al. (2017) and Brooks and Du (2021). Private private signals also appear as counterexamples of information aggregation in financial markets: see the discussion in Ostrovsky (2012) and similar observations in the computer science literature (Feigenbaum et al., 2003).

Our application to influencing competitors in zero-sum games relates to the literature of information design in games (Bergemann and Morris, 2016; Taneva, 2019; Mathevet et al., 2020). Our application to optimal private disclosure has a conceptual connection to Eliaz et al. (2020), who also consider an optimization problem on random variables under an independence constraint.

As mentioned above, our work is related to the mathematics of sets of uniqueness and mathematical tomography (Lorentz, 1949; Fishburn et al., 1990; Kellerer, 1993). These techniques have been applied in economics, for example by Gershkov et al. (2013) to show the equivalence of Bayesian and dominant strategy implementation in an environment with linear utilities and one-dimensional types.

2 Model

We consider a group of agents $N = \{1, \dots, n\}$ where each agent i has a signal s_i containing information about a state of nature ω taking value in $\Omega = \{0, 1, \dots, m-1\}$, and all agents start with a common, full-support prior belief about the state. We call the tuple $\mathcal{I} = (\omega, s_1, \dots, s_n)$ an *information structure*. Formally, fix a standard nonatomic Borel probability space $(X, \Sigma, \mathbb{P})$, and let $\omega, s_1, \dots, s_n$ be random variables defined on this space that take values in $\Omega \times S_1 \times \cdots \times S_n$, where each S_i is a measurable space.[2] The marginal distribution of ω is the prior over the state.

Denote by $p(s_i)$ the posterior associated with s_i. Formally, $p(s_i)$ is the random variable taking value in $\Delta(\Omega)$ given by $p(s_i)(k) = \mathbb{P}[\omega = k \mid s_i]$. In the case of a binary state (i.e., when $\Omega = \{0, 1\}$), 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* $\mathcal{I} = (\omega, s_1, \dots, s_n)$ *is a* private private information structure *if* $(s_1, \dots, s_n)$ *are independent random variables.*

Private private signals should not be confused with *conditionally* independent signals, where $(s_1, \dots, s_n)$ are independent given ω. This is a different notion, and

[2] An alternative approach would be to define an information structure as a joint distribution over $\Omega \times S_1 \times \cdots \times S_n$.

indeed conditionally independent signals cannot be private private, unless they are fully uninformative about the state.

As a simple example of a private private information structure for two agents and a binary state, let s_1, s_2 be independently and uniformly distributed on $[0,1]$, and let ω be the indicator of the event that $s_1 + s_2 > 1$, as illustrated in Figure 1. The distribution of (s_1, s_2) conditioned on $\omega = 1$ is the uniform distribution on the upper right triangle of the unit square. Conditioned on $\omega = 0$, (s_1, s_2) have the uniform distribution on the bottom left triangle. Note that the posterior beliefs are $p(s_i) = s_i$ in this information structure, so both agents have strictly informative signals. While the two signals are independent, they are not conditionally independent given the state ω.

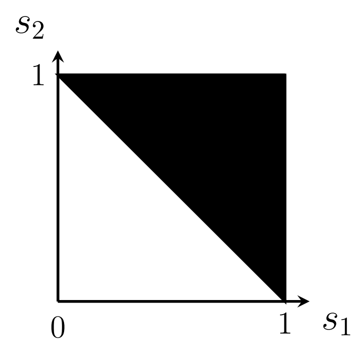

Figure 1: The pair of signals (s_1, s_2) is uniformly distributed on the unit square, with $\omega = 1$ in the black area and $\omega = 0$ in the white area. The induced posteriors $p(s_1), p(s_2)$ coincide with the signals.

This paper focuses on characterizing the private private signals that are maximally informative for the group of agents, formalized through the concept of *Pareto optimality* of private private information structures. For the single-agent case ($n = 1$), recall that an information structure (ω, s) *Blackwell dominates* $(\omega, \hat{s})$ if for every continuous convex $\varphi\colon \Delta(\Omega) \to \mathbb{R}$ it holds that $\mathbb{E}[\varphi(p(s))] \geqslant \mathbb{E}[\varphi(p(\hat{s}))]$.

This notion captures a strong sense in which s contains more information about ω than $\hat{s}$ does: in any decision problem, an agent maximizing expected utility performs better when observing s than when observing $\hat{s}$.

For more than one agent, our next definition introduces a partial order on private private information structures that captures Blackwell dominance for each agent.

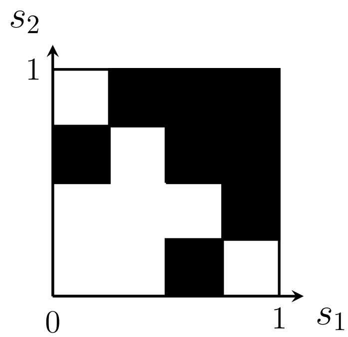

Figure 2: The pair of signals (s_1, s_2) is uniformly distributed on the unit square, with $\omega = 1$ in the black area and $\omega = 0$ in the white area. The induced posteriors $p(s_1), p(s_2)$ are binary, and equally likely to be either $1/4$ or $3/4$.

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 $\mathcal{I} \succeq \hat{\mathcal{I}}$, 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 $\mathcal{I} \succeq \hat{\mathcal{I}}$ and $\hat{\mathcal{I}} \succeq \mathcal{I}$.*

It follows from this definition that $\mathcal{I}$ is equivalent to $\hat{\mathcal{I}}$ if and only if, for each i, the distributions of $p(s_i)$ and $p(\hat{s}_i)$ coincide. Thus we can partition the set of private private information structures into equivalence classes, with each class represented by n distributions $(\mu_1, \ldots, \mu_n)$ on $\Delta(\Omega)$. A first question that arises is that of feasibility: which n-tuples $(\mu_1, \ldots, \mu_n)$ represent some private private information structure? We address this question in §6.

Figure 2 illustrates another example of a private private information structure, where the signals are again uniform on $[0, 1]$, but each agent's posterior belief is equally likely to be either $1/4$ or $3/4$. Thus this structure is equivalent to a structure where agents receive binary signals. More generally, a structure $(\omega, s_1, \ldots, s_n)$ is always equivalent to the "direct revelation" structure $(\omega, p(s_1), \ldots, p(s_n))$ in which agent i observes the posterior belief induced by s_i.

We use the concept of dominance to define 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?

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 $\hat{\mathcal{I}} \succeq \mathcal{I}$, the structure $\hat{\mathcal{I}}$*

is equivalent to $\mathcal{I}$.

In other words, $\mathcal{I}$ is Pareto optimal if there is no private private information structure $\hat{\mathcal{I}}$ that gives as much information to each agent (in the Blackwell sense), and gives a strictly Blackwell dominating signal to at least one agent. In the Appendix (Lemma 4), we show that Pareto optimal structures exist, and that, moreover, every private private information structure is weakly dominated by a Pareto optimal one.

As we explain in the introduction, 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. The question is thus: what are the ways to maximally inform the agents, while still maintaining privacy?

3 Applications of Pareto Optimal Private Private Signals

Before turning to our main results, we provide some motivation for studying Pareto optimal private private signals by discussing two applications.

3.1 Optimal Private Disclosure

Optimal private disclosure is the problem of 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. In this application, we should interpret s_1 not as the "signal" given to some agent, but as a pre-existing trait that must be kept secret for legal or security reasons.

As a concrete example, suppose an uninformed company wants to learn about a decision-relevant type ω of an applicant (e.g., whether she is a good fit for a job or whether she will pay her rent on time), and an informed party (e.g., a recommender or a credit-rating company) knows both this type and a legally protected trait s_1 of the applicant that correlates with the type: this could be the applicant's private medical information, or a protected attribute like gender or race. 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, so that the company's downstream decision based solely on the disclosure will be independent of the protected trait and therefore not cause disparate impact. Note that even disclosure that does not explicitly contain the protected trait may cause disparate impact, if such disclosure contains correlates of the trait.

A less economic (but more colorful) story is that of a government who would like to reveal a piece of intelligence ω, but without revealing any information about the identity of its source s_1. These could be naturally correlated: for example, if ω is the location of a weapons facility and the source s_1 is likely to live close to it. So the government's disclosure s_2 should contain as much information as possible about ω, while not revealing any information about s_1.

The problem of optimal private disclosure can be phrased in terms of finding a Pareto optimal private private information structure for two "agents" with a given marginal distribution on (ω, s_1).

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.*

When ω and s_1 are correlated, s_2 cannot be a completely revealing signal, as it would provide information about s_1. A priori, it is not obvious whether there exists a unique solution to the optimal private disclosure problem, or whether there are multiple Blackwell unordered signals s_2 that are optimal for different decision problems. Our characterization of the Pareto optimal private private signals will show that the solution is unique and provide a simple recipe to calculate it, when the state is binary.

3.2 Influencing Competitors in Zero-Sum Games

As another motivation for private private signals, we 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, and the utilities are given by $u_1 = -u_2 = u$ for some $u\colon A_1 \times A_2 \to \mathbb{R}$. We assume that this game has a unique mixed Nash equilibrium, which holds for generic zero-sum games (Viossat, 2008).

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 $u_d\colon \Omega \times A_1 \times A_2$ 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.

As a simple example, suppose the game is rock-paper-scissors, so that $A_1 = A_2 = \{R, P, S\}$ and $u(a_1, a_2)$ equals 1 on $\{(P, R), (R, S), (S, P)\}$, zero on the diagonal, and -1 on the remaining action pairs. The state ω takes values in $\{0, 1\}$ and is equal to 1 with probability $1/2$. The designer gets a payoff of 1 for each player who chooses scissors in the high state or chooses rock in the low state.

A pure strategy of player i is a map $f_i\colon S_i \to A_i$, and a mixed strategy σ_i is a random pure strategy. An equilibrium consists of an information structure together with a strategy profile (σ_1, σ_2) such that each agent maximizes her expected utility given her signal. That is, for every $s_i \in S_i$ and $a_i \in A_i$

$$\mathbb{E}[u_i(\sigma_i(s_i), \sigma_{-i}(s_{-i}))|s_i] \geqslant \mathbb{E}[u_i(a_i, \sigma_{-i}(s_{-i}))|s_i].$$

This is just the incentive compatibility condition of a correlated equilibrium, and so, by a direct revelation argument, we can assume that $S_i = A_i$ and that σ_i is always the identity: in equilibrium, the designer recommends an action to each agent, and the agents follow the recommendations. We refer to such equilibria as direct-revelation equilibria.

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.*

Proof. A zero-sum game with a unique Nash equilibrium has a unique correlated equilibrium which is equal to that Nash equilibrium (Forges, 1990). Thus (s_1, s_2) form a Nash equilibrium, and in particular s_1 must be independent of s_2. □

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}. Note that Claim 1 applies beyond generic zero-sum games to any game with any number of players, provided that it has a unique correlated equilibrium.[3]

In the rock-paper-scissors example above, the joint distribution of (s_1, s_2) must be uniform over $\{R, P, S\} \times \{R, P, S\}$, by Claim 1. However, the designer is free to choose the joint distribution between (s_1, s_2) and ω. Thus his problem is to maximize $\mathbb{E}[u_d(\omega, s_1, s_2)]$ over all structures in which (s_1, s_2) is uniform over $\{R, P, S\} \times \{R, P, S\}$. Choosing (s_1, s_2) independently of ω yields a payoff of 6/9. A straightforward calculation shows that an optimal structure yields him a payoff of $^8/_9$. By comparison, in a relaxed problem where the designer is allowed to dictate the players' actions without worrying about the privacy constraint, he can achieve utility 2 by revealing the state to both players, telling them to both choose scissors when the state is high and rock when the state is low.

Beyond the specifics of the rock-paper-scissors example, the fact that equilibrium signals are private private means that any bound on the informativeness of private private signals yields a bound on the designer's equilibrium utility: if the designer's recommendations only contain a limited amount of information about the state, then he cannot hope that the players' actions efficiently adapt to the state and yield him high utility. Thus our results below, including Theorem 1 and Propositions 3, 4 and 5, constrain what can be achieved by the designer in any such setting.

4 Pareto Optimality and Conjugate Distributions

The question of Pareto optimality of private private information structures is already non-trivial in the case of two agents and a binary state. For example, is the structure given in Figure 1 Pareto optimal? What about the structure in Figure 2? In this section, we give a simple description of the Pareto frontier, making it easy to check if a structure is Pareto optimal. In particular, our results imply that the structure in Figure 1 is Pareto optimal while the one in Figure 2 is not.

[3]The set of games with a unique correlated equilibrium is open (Viossat, 2008), so a small enough perturbation of (for example) the rock-paper-scissors game will still have a unique correlated equilibrium, although it will not be zero-sum. As a side note, we are unaware of interesting examples of three player games with a unique correlated equilibrium. In particular, the following question is open, to the best of our knowledge: does there exist a three player game with a unique correlated equilibrium in which no player plays a pure strategy?

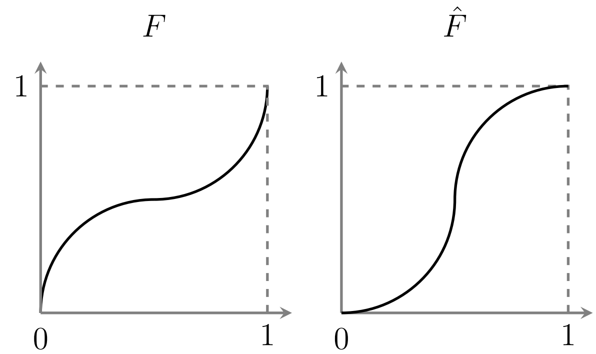

Figure 3: An example of a cumulative distribution function F and its conjugate $\hat{F}$. The shapes under the curves are congruent: the transformation that maps one to the other is reflection around the anti-diagonal. Qualitatively, F corresponds to the belief distribution of a more informative signal,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

To state this result, we introduce *conjugate distributions* on $[0,1]$. Let $F\colon [0,1] \to [0,1]$ be the cumulative distribution function of a probability measure in $\Delta([0,1])$. The associated *quantile function*, which we denote by F^{-1}, is given by

$$F^{-1}(x) = \min\{y \,:\, F(y) \geqslant x\}. \tag{1}$$

Since cumulative distribution functions are right-continuous, this minimum indeed exists, and so F^{-1} is well defined. When F is the cumulative distribution function of a full support and nonatomic measure, then F is a bijection and F^{-1} is its inverse. More generally, $F^{-1}(x)$ is the smallest number y such that an x-fraction of the population has value less than or equal to y.

Definition 5. *The* conjugate *of a cumulative distribution function* $F\colon [0,1] \to [0,1]$ *is the function* $\hat{F}\colon [0,1] \to [0,1]$*, which is given by*

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

Graphically, (x, y) is on the graph of F if and only if $(1-y, 1-x)$ is on the graph of $\hat{F}$: in other words, $\hat{F}$ is the reflection of F around the anti-diagonal of the unit square. An example is depicted in Figure 3.

As we show in the Appendix (Claim 2), $\hat{F}$ is also a cumulative distribution function. Thus, given a measure $\mu \in \Delta([0,1])$, we can define its conjugate measure $\hat{\mu} \in \Delta([0,1])$ as the unique measure whose cumulative distribution function is the conjugate of the cumulative distribution function of μ. It is easy to verify that the conjugate of $\hat{\mu}$ is again μ.

The main result of this section is that Pareto optimality can be characterized in terms of conjugates.

Theorem 1. *For a binary state ω and two agents, a private private information structure $\mathcal{I} = (\omega, s_1, s_2)$ is Pareto optimal if and only if the distributions of beliefs $p(s_1)$ and $p(s_2)$ are conjugates.*

Our proof of Theorem 1 combines our more general characterization of Pareto optimality in the n agents case (Theorem 3) together with a classical result of Lorentz (1949) about so-called "sets of uniqueness," which we discuss in detail in §5; these are subsets of $[0,1]^n$ that are uniquely determined by their projections to each of the n axes.

Figure 3 suggests that on the Pareto frontier, when s_1 is very informative, s_2 must be very uninformative. We formalize this in the Appendix (Proposition 6), where we show that if both (ω, s_1, s_2) and (ω, t_1, t_2) are Pareto optimal, and if t_1 dominates s_1, then t_2 is dominated by s_2. That is, giving agent 1 more information must come at the cost of giving agent 2 less.

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 $\hat{\mu}$. Figure 4 illustrates this construction.

We can use Theorem 1 to understand whether the structures of Figures 1 and 2 are optimal. The uniform distribution on $[0,1]$ is its own conjugate. Hence, using Theorem 1's belief conjugacy test, we can conclude that Figure 1's information structure is Pareto optimal.

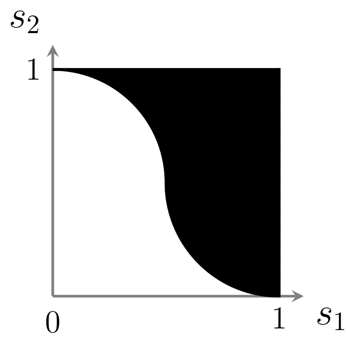

Figure 4: A private private information structure, where the beliefs $p(s_1)$ and $p(s_2)$ are distributed according to the pair of conjugate distributions F and $\hat{F}$ from Figure 3: the signals are uniform on $[0,1]^2$, and $\omega = h$ if and only if $s_2 \geqslant \hat{F}(1-s_1)$ (black region).

To understand the structure of Figure 2, consider, more generally, a discrete distribution μ on $[0,1]$ with k atoms. Its conjugate $\hat{\mu}$ is also atomic: each atom of μ with weight w corresponds to an interval of zero mass with length w for $\hat{\mu}$ and, symmetrically, each interval of length l carrying no atoms in μ becomes an atom of weight l in $\hat{\mu}$ (see Figure 5). In particular, $\hat{\mu}$ has either $k-1$, k or $k+1$ atoms, corresponding to the cases that (1) μ places positive mass on both 0 and 1, (2) μ places positive mass on exactly one of $\{0,1\}$, and (3) μ places zero mass on $\{0,1\}$.

We conclude that the information structure of Figure 2, where both signals induce beliefs $1/4$ or $3/4$ is not Pareto optimal, since two discrete distributions with the same number of atoms can only be conjugates if each of them assigns a non-zero weight to exactly one of $\{0,1\}$.

4.1 Optimal Private Disclosures

Using Theorem 1, we solve the optimal private disclosure problem for binary states.

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 $p(s_2^\star)$ is the conjugate of the distribution of $p(s_1)$. Furthermore, every signal s_2 independent of s_1 is Blackwell dominated by $s_2^\star$.*

The last statement in Theorem 2 implies that every decision maker would find the signal $s_2^\star$ optimal, regardless of the decision problem at hand. For example, no s_2 that

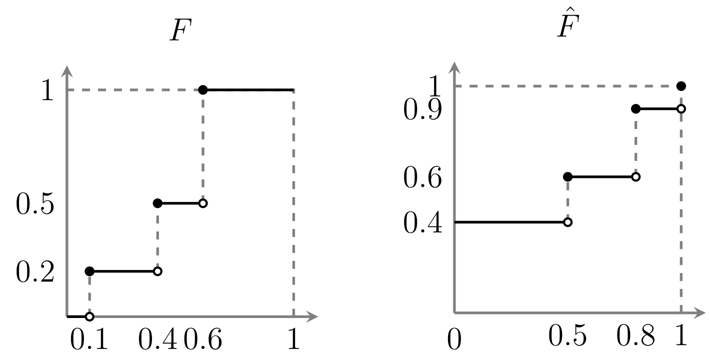

Figure 5: The conjugate of a discrete distribution F with three atoms at 0.1, 0.4, and 0.6. Each atom becomes an interval of zero measure with length equal to the atom's weight, and vice versa. Since F does not have atoms at the endpoints of $[0, 1]$, the number of intervals of zero measure exceeds the number of atoms by one, so its conjugate $\hat{F}$ has four atoms at 0, 0.5, 0.8, and 1.

is independent of s_1 can have higher mutual information with ω or lower quadratic loss. This uniqueness of the optimal private disclosure is a rather surprising property as one could expect that, for given (ω, s_1), there are non-equivalent choices of $s_2^\star$ that are both maximal and incomparable in the Blackwell order. In Appendix B.2, we demonstrate that uniqueness is a feature of the binary-state case by considering an example with three states, binary s_1 and a continuum of optimal private disclosures.

Figure 6 shows the optimal private disclosure when the two states are equally likely and s_1 is a symmetric binary signal that matches the state with probability $3/4$. The optimal disclosure $s_2^\star$ is trinary: it completely reveals the state with probability $1/2$, and gives no information with the remaining probability. More generally, when the states are equally likely and s_1 is a symmetric binary signal that matches the state with probability $r \in [1/2, 1]$, the optimal disclosure will be trinary. It completely reveals the state with probability $2(1-r)$, and gives no information with the complementary probability. Thus, as the correlation between s_1 and ω increases, the optimal private disclosure becomes less informative.

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:

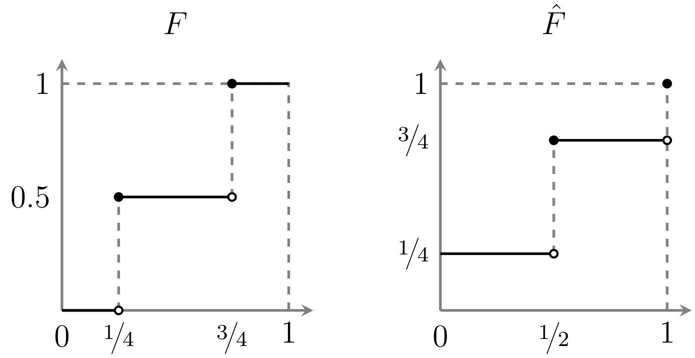

Figure 6: Optimal private disclosure when a 3/4-binary signal s_1 must be kept secret. The left panel depicts the cumulative distribution function F of posteriors induced by the symmetric binary signal s_1 matching the state with probability 3/4. The optimal private disclosure $s_2^\star$ corresponds to the conjugate distribution $\hat{F}$ depicted in the right panel. We see that $s_2^\star$ is trinary: it is completely uninformative with probability 1/2 and fully reveals the state with the complementary chance, inducing the posteriors 0 or 1 with equal probabilities.

- Calculate $p(s_1)$, the conditional probability of $\omega = 1$ given s_1.
- If $\omega = 1$, sample $s_2^\star$ uniformly from the interval $[1 - p(s_1),\, 1]$.
- If $\omega = 0$, sample $s_2^\star$ uniformly from the interval $[0,\, 1 - p(s_1)]$.

This procedure yields an $s_2^\star$ that, conditioned on s_1, is distributed uniformly on $[0, 1]$, and hence is independent of s_1. It is simple to verify that $s_2^\star$ is optimal (see the proof of Theorem 2).

This procedure can be simplified if the posterior $p(s_1)$ only takes finitely many values, in which case there exists an optimal private disclosure that is also finitely valued. Let $[0, 1] = \bigsqcup_{k=0}^{K} I_k$ be a partition of the unit interval into subintervals using the values of $p(s_1)$. The belief $p(s_2^\star)$ is constant when $s_2^\star$ ranges within I_k. Hence, the constructed optimal private disclosure $s_2^\star$ with values in $[0, 1]$ is equivalent to a signal $t_2^\star \in \{0, \ldots, K\}$ such that $t_2^\star = k$ whenever $s_2^\star \in I_k$. The signal $t_2^\star$ is also an optimal private disclosure and takes at most one more value than the number of values of $p(s_1)$.

Consider the symmetric binary s_1 matching ω with probability 3/4 from Figure 6. An optimal private disclosure $s_2^\star$ of the state can be generated as follows. It takes three values, $\{0, 1, 2\}$. If $s_1 = \omega$, then $s_2^\star = 2 \cdot \omega$, and if $s_1 \neq \omega$ then $s_2^\star = 1$ with probability $2/3$ and $s_2^\star = 2 \cdot \omega$ with probability $1/3$. As a result, the realization $s_2^\star = 1$ is completely uninformative and $s_2^\star \in \{0, 2\}$ completely reveals ω.

4.2 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 $u_i(\omega, a_i)$. Our only assumption is that u_i is bounded from above.

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?

Clearly, every maximizing structure must lie on the Pareto frontier. But while the Pareto frontier contains a rich set of information structures, including some that induce a continuum of beliefs, the ones that maximize social welfare have a simpler form.

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.*

By permuting the roles of s_1 and s_2, we deduce that there is also a welfare-maximizing structure in which s_2 takes two values and s_1 takes three. The proposition is proved in Appendix A.7 using a combination of an extreme-point argument and the characterization of Pareto optimal structures via conjugate distributions (Theorem 1).

For an example of a social welfare maximizing structure, consider the canonical example with two equally likely states, $A_i = \Omega = \{0, 1\}$, where 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. Such a structure exists as this distribution is its own conjugate: see also Figure 7. Then the social

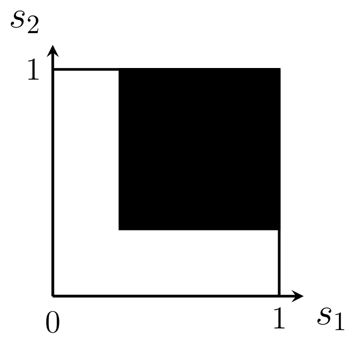

Figure 7: A social welfare maximizing private private information structure for the decision problem in which $u_1(\omega, a) = u_2(\omega, a) = 2|\omega - a| - 1$.

welfare is $4 - 2\sqrt{2} \approx 1.17$. Let us check that this is the highest possible social welfare across all private private information structures.

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.

5 Pareto Optimality and Sets of Uniqueness

In this section, we study Pareto optimality of private private information in the general setting of n agents and a state ω that takes value in $\Omega = \{0, \ldots, m-1\}$. Our main result shows that Pareto optimality can be characterized using "sets of uniqueness": subsets of $[0,1]^n$ that are uniquely determined by their projections to the n axes.

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 (see Figures 1 and 2, as well as 8 in the Appendix).

More formally, let $\mathcal{A} = (A_0, \ldots, A_{m-1})$ 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* $\mathcal{A} = (A_0, \ldots, A_{m-1})$ *is* $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ *where* $(s_1, \ldots, s_n)$ *are distributed uniformly on* $[0,1]^n$ *and* $\{\omega = k\}$ *is the event that* $\{(s_1, \ldots, s_n) \in A_k\}$.

Note that if $\mathcal{A}$ and $\mathcal{A}'$ are partitions such that each symmetric difference $A_k \triangle A'_k$ has zero Lebesgue measure, then both are associated with the same information structure, in the strong sense that the joint distributions of $(\omega, s_1, \ldots, s_n)$ coincide. Accordingly, we henceforth consider two subsets of $[0,1]^n$ to be equal if they only differ on a zero-measure set.

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* $\mathcal{I}$*.*

While the general proof contained in Appendix A.2 is not constructive, for structures with a finite number of signals and a binary state, we show in Appendix B.3 how to construct a partition with an equivalent associated structure.

The ideas behind the proof of this proposition are the following. Using standard results, one can always reparameterize the signals so that they are uniformly distributed in $[0,1]$. Thus the main challenge is to ensure that the state is determined by the signals. To this end, given signals that do not determine the state, we add a signal t that resolves the remaining uncertainty, so that ω is a deterministic function of $(s_1, \ldots, s_n, t)$. Then, we use a "secret sharing" technique (Shamir, 1979) to create a pair of independent random variables t_1, t_2 such that t is determined by the pair (t_1, t_2), but each t_i is uninformative about the state and the other signals. We then reveal to agents 1 and 2 the additional signals t_1 and t_2, respectively. Thus the information structure $\big(\omega, (s_1, t_1), (s_2, t_2), \ldots, s_n\big)$ is equivalent to $(\omega, s_1, \ldots, s_n)$, but now the signals determine the state.

Proposition 2 implies that for the purpose of studying the Pareto optimality of private private signals, one can assume without loss of generality that information structures are always associated with partitions. In particular, the question of Pareto optimality can now be phrased as a question about partitions: when does a partition $\mathcal{A}$ correspond to a Pareto optimal structure? Our next result answers this question. We state this result for the case of a binary state, as it involves significantly simpler notation; the result for a general finite state space is given in Appendix A.3. In the case of a binary state, a partition $\mathcal{A} = (A_0, A_1)$ is determined by A_1, since A_0 is its complement. Hence we will represent $\mathcal{A}$ by a single set $A = A_1$. The information structure associated with A will refer to the structure associated with the partition (A^c, A).

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

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

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 $(\alpha_1^A, \ldots, \alpha_n^A) = (\alpha_1^B, \ldots, \alpha_n^B)$, it holds that $A = B$.*

Less formally, A is a set of uniqueness if it is determined by the projections $(\alpha_1^A, \ldots, \alpha_n^A)$.

The main result of this section characterizes Pareto optimality in terms of 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 $A \subseteq [0,1]^n$.*

To prove that Pareto optimality implies that A is a set of uniqueness, suppose A is not a set of uniqueness, so that $B \neq A$ has the same projections. Hence the structure associated with A is equivalent to the one associated with B. By considering a convex combination of the two structures, we arrive at another equivalent structure, one in which the signals do not always determine the state. We resolve this residual uncertainty via an additional informative signal t, which is independent of $(s_1, \ldots, s_n)$. Now, revealing this new signal to agent 1 results in a private private information structure $\big(\omega, (s_1, t), s_2, \ldots, s_n\big)$ that dominates the structure associated with A.

Conversely, suppose the information structure associated with A is not Pareto optimal. By considering a Pareto dominating information structure and garbling the signals, we can find a density $f : [0,1]^n \to [0,1]$ that is not an indicator function, but has the same marginals as A. We next apply a result of Gutmann et al. (1991): the set of densities valued in $[0,1]$ with given marginals is a convex set whose extreme points are indicator functions. Since f is not an indicator function, the corresponding convex set is not a singleton and must have at least two different extreme points. There exists some other set with the same marginals as A, so A is not a set of uniqueness.

Theorem 3 shows an equivalence between the two *a priori* unrelated notions of Pareto optimality and sets of uniqueness; a similar result in Appendix A.3 establishes an analogous equivalence for arbitrary finite state spaces, generalizing sets of uniqueness to *partitions of uniqueness*. This connection lets us use characterization results about sets of uniqueness to study Pareto optimality. Sets of uniqueness have been studied since Lorentz (1949), who gives a simple characterization in the two dimensional case. A version of his characterization, as we explain below, leads to Theorem 1. Beyond the two dimensional case, sets of uniqueness have also been more recently studied in the *mathematical tomography* literature (e.g., Fishburn et al., 1990). We discuss below how these newer results help us understand Pareto optimal structures.

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 $x = (x_1, \ldots, x_n) \in B$ implies that $y = (y_1, \ldots, y_n) \in B$ 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.*

This formulation is different than the one that appears in the paper by Lorentz

(1949). We therefore show in the Appendix that it is an equivalent characterization. Theorem 1 is a consequence of Theorems 4 and 3.

When $n > 2$, the known characterizations of sets of uniqueness are more involved (Kellerer, 1993). Nevertheless, a simple sufficient condition for uniqueness (Fishburn et al., 1990) is to be an *additive* set: this holds when there are bounded $h_i \colon [0,1] \to \mathbb{R}$ 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 (and equivalently, of the Pareto optimal structures). 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. With $n \geqslant 3$, Kemperman (1991) demonstrated that there are sets of uniqueness that are not additive. However, additivity is "almost necessary": Kellerer (1993) characterizes the class of sets of uniqueness as the closure, in a certain topology, of the class of additive sets.

6 Feasibility

In §2 we discussed the fact that a private private information structure $(\omega, s_1, \ldots, s_n)$ is equivalent to the "direct revelation" structure $(\omega, p(s_1), \ldots, p(s_n))$. Equivalence classes of information structures correspond to n-tuples $(\mu_1, \ldots, \mu_n)$ of measures on $\Delta(\Omega)$, where μ_i is the distribution of $p(s_i)$. In this section, 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 $p(s_i)$.*

For example, Figure 2 shows that for symmetric binary states and two agents, it is feasible for both agents to have binary signals that induce beliefs of either $1/4$ or

$^3/_4$. That is, (μ_1, μ_2) is feasible for

$$\mu_1 = \mu_2 = \frac{1}{2}\delta_{1/4} + \frac{1}{2}\delta_{3/4}.$$

The question of feasibility was studied by Gutmann et al. (1991) and Arieli et al. (2021). The latter investigate feasibility for two agents, symmetric binary states, and focus on the case of $\mu_1 = \mu_2$. They show that if μ is symmetric to reflection around $^1/_2$ (i.e., to permuting the states), then (μ, μ) is feasible if and only if μ is a mean-preserving contraction of the uniform distribution on $[0, 1]$. It follows, for example, that $^3/_4$ is the strongest possible binary signal that two players can have in a symmetric private private information structure with a symmetric binary state. To the best of our knowledge, little is known about feasibility beyond this result.

A necessary condition for feasibility is given by the 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.

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 $(\mu_1, \ldots, \mu_n)$.

This observation, together with Theorem 1, gives the following characterization for the case of a binary state and two agents.

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.*

This result generalizes the symmetric case addressed in Proposition 2 of Arieli et al. (2021): in our result, the two states need not be equally likely, the two agents need not have the same belief distribution, and their belief distributions need not be symmetric around $^1/_2$. It offers a simple tool for checking feasibility. Indeed, by applying a standard characterization of mean-preserving spreads, the pair (μ_1, μ_2)

is feasible if and only if they have the same expectation, and the corresponding cumulative distribution functions (F_1, F_2) satisfy

$$\int_y^1 F_2(x)\,\mathrm{d}x \geqslant \int_y^1 \hat{F}_1(x)\,\mathrm{d}x$$

for every $y \in [0,1]$.

In the general case of m states and n agents, we do not have a simple characterization of feasibility. Nevertheless, we now present a necessary condition for feasibility, which relies on information-theoretic ideas. We will require two standard definitions.

The *Shannon entropy* of a measure $q \in \Delta(\Omega)$ is

$$H(q) = -\sum_{k \in \Omega} q(k) \log_2(q(k)). \tag{2}$$

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

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

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:

$$I(\mu_i) = H\left(\int q\,\mathrm{d}\mu_i(q)\right) - \int H(q)\,\mathrm{d}\mu_i(q). \tag{3}$$

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

In information theory, entropy is often used to quantify the amount of randomness in a distribution. Mutual information is then the expected reduction in this randomness, and is used as a measure for the amount of information contained in a signal. These notions are also used in economics, e.g., in the rational inattention literature (Sims, 2010; Matějka and McKay, 2015). In our setting, mutual information is useful as it provides the following necessary condition for feasibility of private private information structures.

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 fact that $I(\mu_i) \leqslant H(p)$ follows immediately from the definition of mutual information. For general information structures (e.g., conditionally independent signals), there are no further restrictions on the tuple $(I(\mu_1), \ldots, I(\mu_n))$: each can take any value between 0 and $H(p)$. Proposition 3 shows that the situation is different when it comes to private private information structures. Here, the sum of mutual information is bounded by the entropy of the prior over ω, so that the entropy of ω behaves like a finite resource that needs to be split between the agents. The proof of this proposition uses standard information-theoretic tools.

Proposition 3 raises a natural question: is this condition tight? That is, does the picture of entropy as a finite resource to be split between the agents tell the whole story, or is there a tighter inequality that relates $\sum_i I(\mu_i)$ and $H(p)$?

Our next proposition shows that Proposition 3 can be strengthened in the case of a binary state.

Proposition 4. *The tuple $(\mu_1, \ldots, \mu_n)$ 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*

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

As far as we know this proposition is a novel information-theoretic inequality, which might have some independent interest. 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). This is a special property of the binary-state setting. For example, if ω is uniformly distributed over $\{0,1\} \times \{0,1\}$, then the structure in which s_1 is equal to the first coordinate of ω and s_2 is equal to the second satisfies Proposition 3 with equality.

The mutual information I is the expected utility associated with a particular decision problem: one in which the indirect utility is given by a constant minus the entropy. Does an analog of Proposition 3 hold for other decision problems? A positive answer would give additional necessary conditions for feasibility. The next proposition shows that for another natural indirect utility function—a quadratic one—an analogous statement indeed holds. Curiously, the proof of this proposition is different than that of Proposition 3, and we do not know of a unifying principle that yields both results. Moreover, we do not know of any other indirect utility that yields the same type of result.

In analogy to (2) and (3), for $q \in \Delta(\Omega)$ denote $\bar{H}(q) = \sum_{k\in\Omega} q(k)(1 - q(k))$, and for a measure μ 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 $(\mu_1, \dots, \mu_n)$ 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 $\sum_i \bar{I}(\mu_i) \leqslant \bar{H}(p)$.*

While this statement is completely analogous to that of Proposition 3, the proof uses a different technique, exploiting the L^2 orthogonality of independent random variables. Indeed, we do not know of a unifying argument that implies both propositions, and we furthermore do not know of additional decision problems that yield analogous statements. We note that Proposition 5 is a generalization—from the binary state case—of the "concentration of dependence" principle of Mossel et al. (2020). A very similar idea appeared earlier in the economics literature (Al-Najjar and Smorodinsky, 2000) and is standard in the analysis of Boolean functions (see, e.g., Kahn et al., 1988; O'Donnell, 2014).

References

N. I. Al-Najjar and R. Smorodinsky. Pivotal players and the characterization of influence. *Journal of Economic Theory*, 92(2):318–342, 2000.

C. Aliprantis and K. Border. *Infinite Dimensional Analysis: A Hitchhiker's Guide (3rd Edition)*. Springer Berlin Heidelberg New York, 2006.

I. Arieli, Y. Babichenko, F. Sandomirskiy, and O. Tamuz. Feasible joint posterior beliefs. *Journal of Political Economy*, 129(9):2546–2594, 2021.

D. Bergemann and S. Morris. Bayes correlated equilibrium and the comparison of information structures in games. *Theoretical Economics*, 11(2):487–522, 2016.

D. Bergemann, B. Brooks, and S. Morris. First-price auctions with general information structures: Implications for bidding and revenue. *Econometrica*, 85(1): 107–143, 2017.

D. Blackwell. Comparison of experiments. In *Proceedings of the Second Berkeley Symposium on Mathematical Statistics and Probability*, pages 93–102. University of California Press, 1951.

B. Brooks and S. Du. Optimal auction design with common values: An informationally robust approach. *Econometrica*, 89(3):1313–1360, 2021.

K. Burdzy and S. Pal. Contradictory predictions. *arXiv preprint arXiv:1912.00126*, 2019.

K. Burdzy and J. Pitman. Bounds on the probability of radically different opinions. *Electronic Communications in Probability*, 25, 2020.

B. Çelen and S. Kariv. Distinguishing informational cascades from herd behavior in the laboratory. *American Economic Review*, 94(3):484–498, 2004a.

B. Çelen and S. Kariv. Observational learning under imperfect information. *Games and Economic Behavior*, 47(1):72–86, 2004b.

S. Cichomski and A. Osękowski. The maximal difference among expert's opinions. *Electronic Journal of Probability*, 26:1–17, 2021.

A. Dawid, M. DeGroot, and Mortera. Coherent combination of experts' opinions. *Test*, 4(2):263–313, 1995.

K. Eliaz, R. Spiegler, and Y. Weiss. Cheating with models. *American Economic Review: Insights*, 2020.

J. Feigenbaum, L. Fortnow, D. M. Pennock, and R. Sami. Computation in a distributed information market. In *Proceedings of the 4th ACM Conference on Electronic Commerce*, pages 156–165, 2003.

P. Fishburn, J. Lagarias, J. Reeds, and L. A. Shepp. Sets uniquely determined by projections on axes i. continuous case. *SIAM Journal on Applied Mathematics*, 50 (1):288–306, 1990.

F. Forges. Correlated equilibrium in two-person zero-sum games. *Econometrica*, 58 (2):515, 1990.

D. Gale. What have we learned from social learning? *European Economic Review*, 40(3-5):617–628, 1996.

R. J. Gardner. *Geometric Tomography*. Cambridge University Press, 1995.

A. Gershkov, J. K. Goeree, A. Kushnir, B. Moldovanu, and X. Shi. On the equivalence of Bayesian and dominant strategy implementation. *Econometrica*, 81(1):197–220, 2013.

S. Gutmann, J. Kemperman, J. Reeds, and L. A. Shepp. Existence of probability measures with given marginals. *The Annals of Probability*, pages 1781–1797, 1991.

L. Hong and S. Page. Interpreted and generated signals. *Journal of Economic Theory*, 144(5):2174–2196, 2009.

D. Janzing, D. Balduzzi, M. Grosse-Wentrup, and B. Schölkopf. Quantifying causal influences. *The Annals of Statistics*, 41(5):2324–2358, 2013.

J. Kahn, G. Kalai, and N. Linial. The influence of variables on boolean functions. In *Proceedings of the 29th Annual Symposium on Foundations of Computer Science*, pages 68–80, 1988.

H. G. Kellerer. Uniqueness in bounded moment problems. *Transactions of the American Mathematical Society*, 336(2):727–757, 1993.

J. Kemperman. Sets of uniqueness and systems of inequalities having a unique solution. *Pacific Journal of Mathematics*, 148(2):275–301, 1991.

G. Lorentz. A problem of plane measure. *American Journal of Mathematics*, 71(2): 417–426, 1949.

F. Matějka and A. McKay. Rational inattention to discrete choices: A new foundation for the multinomial logit model. *American Economic Review*, 105(1):272–98, 2015.

L. Mathevet, J. Perego, and I. Taneva. On information design in games. *Journal of Political Economy*, 2020.

E. Mossel, M. Mueller-Frank, A. Sly, and O. Tamuz. Social learning equilibria. *Econometrica*, 88(3):1235–1267, 2020.

R. O'Donnell. *Analysis of Boolean functions*. Cambridge University Press, 2014.

M. Ostrovsky. Information aggregation in dynamic markets with strategic traders. *Econometrica*, 80(6):2595–2647, 2012.

J. Pearl. *Causality: Models, Reasoning and Inference*. Cambridge University Press, 2009.

A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

C. Sims. Rational inattention and monetary economics. *Handbook of Monetary Economics*, 3:155–181, 2010.

I. Taneva. Information design. *American Economic Journal: Microeconomics*, 11(4): 151–85, 2019.

Y. Viossat. Is having a unique equilibrium robust? *Journal of Mathematical Economics*, 44(11):1152–1160, 2008.

G. Winkler. Extreme points of moment sets. *Mathematics of Operations Research*, 13(4):581–587, 1988.

Appendix

A Omitted Proofs

Note that we sometimes prove results in a different order than the order that they appear in the main text, since some of the results we state earlier are implied by some of the later results.

A.1 Preliminary Lemmas

Let $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ be a private private information structure. The signals $s_1, \ldots, s_n$ can be combined into a new signal $s = (s_1, \ldots, s_n)$. The following lemma gives a lower bound on the informativeness of the combined signal s in terms of the informativeness of the individual signals. It can be seen as superadditivity of mutual information for independent signals.

Lemma 1. *For a private private information structure* $(\omega, s_1, \ldots, s_n)$ *the following inequality holds*

$$\sum_{i=1}^{n} I\big(\omega\,;\, s_i\big) \leqslant I\big(\omega\,;\, (s_1, \ldots, s_n)\big). \tag{4}$$

Proof. The result for $n \geqslant 3$ follows from the result for $n = 2$ by applying it sequentially to $(s_1, \ldots, s_k)$ for $k \leqslant n$. Consequently, in the rest of the proof we assume $n = 2$.

Our goal is to show that

$$\Delta = I\big(\omega\,;\, (s_1, s_2)\big) - I\big(\omega\,;\, s_1\big) - I\big(\omega\,;\, s_2\big) \geqslant 0.$$

Let $p_1(k) = p(s_1)(k) = \mathbb{P}[\omega = k \,|\, s_1]$, define p_2 likewise, and let $p_{12}(k) = p(s_1, s_2)(k) = \mathbb{P}[\omega = k \,|\, s_1, s_2]$. Let p denote the prior distribution of ω. By the martingale property $\mathbb{E}[p_{12} \,|\, p_i] = p_i$ and $\mathbb{E}[p_i] = p$.

Using this notation and the definition of mutual information, we can write for $i \in \{1, 2\}$

$$I\big(\omega\,;\, s_i\big) = \mathbb{E}\left[\sum_k p_i(k) \log \frac{p(k)}{p_i(k)}\right] \quad \text{and} \quad I\big(\omega\,;\, s_1, s_2\big) = \mathbb{E}\left[\sum_k p_{12}(k) \log \frac{p(k)}{p_{12}(k)}\right].$$

By the martingale property we can replace the first p_i by p_{12}:

$$I\big(\omega\,;\, s_i\big) = \mathbb{E}\left[\sum_k p_{12}(k) \log \frac{p(k)}{p_i(k)}\right].$$

Thus

$$\Delta = \mathbb{E}\left[\sum_k p_{12}(k) \log \frac{p_1(k) p_2(k)}{p_{12}(k) p(k)}\right].$$

Applying Jensen's inequality to the logarithm, we get that

$$\Delta \geqslant \log \mathbb{E}\left[\sum_k p_{12}(k) \frac{p_1(k)p_2(k)}{p_{12}(k)p(k)}\right].$$

Cancelling and rearraging we get

$$\Delta \geqslant \log \sum_k \frac{1}{p(k)} \mathbb{E}[p_1(k)p_2(k)].$$

Since $p_1(k)$ and $p_2(k)$ are independent,

$$\Delta \geqslant \log \sum_k \frac{1}{p(k)} \mathbb{E}[p_1(k)]\mathbb{E}[p_2(k)].$$

By the martingale property $\mathbb{E}[p_i(k)] = p(k)$, and so $\Delta \geqslant \log \sum_k p(k) = 0$. □

Note that this proof only used the independence of (s_1, s_2) to the extent that it implies that $p(s_1)$ is uncorrelated with $p(s_2)$.

To show that a given private private information structure $\mathcal{I} = (\omega, s_1, \dots, s_n)$ is Pareto dominated, we will often use the following technique: construct an additional informative signal t independent of $s_1, \dots, s_n$, and reveal it to one of the agents, say, the first one. The new information structure $\mathcal{I}' = (\omega, (s_1, t), s_2, \dots, s_n)$ strictly dominates $\mathcal{I}$ thanks to the following direct corollary of Lemma 1.

Corollary 2. *Fix ω, and consider a pair of signals s and t such that*

- *s and t are independent, and*
- *t is not independent of ω.*

Then the information structure $(\omega, (s, t))$ strictly dominates (ω, s) with respect to the Blackwell order.

Proof. Clearly (ω, s) is weakly dominated by $(\omega, (s, t))$. We show that this domination is strict.

Since t is informative, $I(\omega; t) > 0$. Hence, by Lemma 1,

$$I(\omega; (s, t)) \geqslant I(\omega; s) + I(\omega; t) > I(\omega; s).$$

Since $I(\omega; s)$ is the value of a particular decision problem (see the discussion in §6), it follows that $(\omega, (s, t))$ strictly dominates (ω, s). □

The next lemma shows that, without loss of generality, induced posteriors are equal to signals, which can be seen a version of the revelation principle for private private information structures.

Lemma 2. *Any private private information structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ is equivalent to $\mathcal{J} = (\omega, t_1, \ldots, t_n)$ where each agent's signal t_i is her posterior $p(s_i)$ in the structure $\mathcal{I}$.*

Proof. By the law of total expectation, $p(t_i) = t_i$. It follows that $p(s_i)$ and $p(t_i)$ have the same distribution, and so are Blackwell equivalent. □

For a private private information structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$, recall that we denote by $\mu_i \in \Delta(\Delta(\Omega))$ the distribution of the belief $p(s_i)$. Let $\mathcal{M} \subset \Delta(\Delta(\Omega))^n$ be the set of feasible distributions $\mu_1, \ldots, \mu_n$, i.e., those that correspond to some private private information structure $\mathcal{I}$.

Lemma 3. *The set of feasible distributions $\mathcal{M}$ is compact in the topology of weak convergence.*

Proof. Since the set of probability measures $\Delta(\Delta(\Omega))$ is compact, to prove the compactness of $\mathcal{M}$, it is enough to check that it is closed. In other words, we need to check that if a sequence of feasible distributions $(\mu_1^l, \ldots, \mu_n^l)$ weakly converges to $(\mu_1^\infty, \ldots, \mu_n^\infty)$ as $l \to \infty$, then the limit is also feasible.

Let $\mathcal{I}^l = (\omega, s_1^l, \ldots, s_n^l)$ be an information structure inducing $(\mu_1^l, \ldots, \mu_n^l)$. By Lemma 2, we can assume without loss of generality that the signals s_i^l are in $\Delta(\Omega)$ and they coincide with the induced beliefs, i.e., $p\big(s_i^l\big) = s_i$. Let $\psi^l \in \Delta(\Omega \times \Delta(\Omega)^n)$ be the joint distribution of ω and the beliefs $s_1^l, \ldots, s_n^l$. By compactness of the set of probability measures, we can extract a subsequence of ψ^l converging to some ψ^∞. By definition, the marginal of ψ^∞ on the belief coordinates equals $\mu_1^\infty \times \ldots \times \mu_n^\infty$.

Consider a private private information structure $\mathcal{I}^\infty = (\omega, s_1^\infty, \ldots, s_n^\infty)$, where signals s_i^∞ belong to $\Delta(\Omega)$ and the joint distribution of the state and signals is given by ψ^∞. Each signal s_i^∞ has distribution μ_i^∞. Let us check that the induced beliefs coincide with signals, i.e., $p\big(s_i^\infty\big)(k) = s_i^\infty(k)$ almost surely for each $k \in \Omega$. We verify an equivalent integrated version of this identity:

$$\int \left(\sum_k h(k, s_i^\infty) p(s_i^\infty)(k) \right) \mathrm{d}\psi^\infty = \int \left(\sum_k h(k, s_i^\infty) s_i^\infty(k) \right) \mathrm{d}\psi^\infty \tag{5}$$

for any continuous function h on $\Omega \times \Delta(\Omega)$. Since the left-hand side is just the integral of h, this is equivalent to

$$\int h(\omega, s_i^\infty) \mathrm{d}\psi^\infty = \int \left(\sum_k h(k, s_i^\infty) s_i^\infty(k) \right) \mathrm{d}\psi^\infty. \tag{6}$$

For each $l < \infty$, the beliefs in $\mathcal{I}^l$ coincide with the signals, i.e.,

$$\int h(\omega, s_i^l) \mathrm{d}\psi^l = \int \left(\sum_k h(k, s_i^l) s_i^l(k) \right) \mathrm{d}\psi^l.$$

As integration of a continuous function commutes with taking weak limits, letting l go to infinity, we obtain (6).

We conclude that each belief $p\big(s_i^\infty\big)$ in $\mathcal{I}^\infty$ coincides with the signal s_i^∞ and the latter is distributed according to μ_i^∞. Therefore, $(\mu_1^\infty, \dots, \mu_n^\infty)$ is feasible and so the set of feasible distributions is closed and thus compact. □

The next lemma shows that our order on private private information structures is well-behaved, in the sense that each structure is dominated by a Pareto optimal one: each element of the partially ordered set of private private information structures is upper bounded by a maximal element.

Lemma 4. *For any private private information structure $\mathcal{I} = (\omega, s_1, \dots, s_n)$, there exists a Pareto optimal structure $\mathcal{I}' = (\omega, s_1', \dots, s_n')$ that weakly dominates $\mathcal{I}$.*

Proof. Recall that $\mathcal{I} \preceq \mathcal{J}$ if for any continuous convex $\varphi \colon \Delta(\Omega) \to \mathbb{R}$ and any agent $i = 1, \dots, n$,

$$\int \varphi(q) \mathrm{d}\mu_i(q) \leqslant \int \varphi(q) \mathrm{d}\nu_i(q) \tag{7}$$

where μ_i and ν_i are the distributions of agent i's beliefs in $\mathcal{I}$ and $\mathcal{J}$, respectively.

We say that the collection of distributions $(\mu_1, \dots, \mu_n)$ is dominated by $(\nu, \dots, \nu_n)$ if (7) holds. Hence, $\mathcal{J}$ dominates $\mathcal{I}$ if and only if the distributions of beliefs in $\mathcal{J}$ dominate those in $\mathcal{I}$. If $\mu_i^l \to \mu_i^\infty$ and $\nu_i^l \to \nu_i^\infty$ weakly as $l \to \infty$ and $(\nu_1^l, \dots, \nu_n^l)$

dominates $(\mu_1^l, \ldots, \mu_n^l)$, then $(\nu_1^\infty, \ldots, \nu_n^\infty)$ dominates $(\mu_1^\infty, \ldots, \mu_n^\infty)$ as integration of a continuous function φ in (7) is exchangeable with taking weak limits. Thus the dominance order on distributions is continuous in the weak topology.

Let $(\mu_1, \ldots, \mu_n)$ be the distributions of posteriors induced by $\mathcal{I}$ and let $\mathcal{M}$ be the set of feasible distributions endowed with the weak topology. As $\mathcal{M}$ is compact by Lemma 3 and the dominance order is continuous, there is a maximal element $(\nu_1, \ldots, \nu_n) \in \mathcal{M}$ dominating $(\mu_1, \ldots, \mu_n)$. Since $(\nu_1, \ldots, \nu_n)$ is feasible, it is induced by some private private information structure $\mathcal{I}'$. By the construction, $\mathcal{I}'$ dominates $\mathcal{I}$ and is Pareto optimal. □

A.2 Proof of Proposition 2

We need to show that, given a private private information structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ with $\Omega = \{0, \ldots m-1\}$, there is an equivalent structure associated with a partition $\mathcal{A} = (A_0, \ldots, A_{m-1})$ of $[0,1]^n$. The construction relies on two lemmas. Lemma 5 shows that assuming signals s_i are uniform on $[0,1]$ is without loss of generality. Hence it remains to show that there is an equivalent information structure where signal realizations determine the state. This is done using a secret-sharing scheme from Lemma 6.

Lemma 5. *For any private private information structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$, there is an equivalent private private information structure $\mathcal{I}' = (\omega, s_1', \ldots, s_n')$ such that each s_i' is uniformly distributed on $[0,1]$.*

Proof. Consider the information structure $\mathcal{J} = (\omega, t_1, \ldots, t_n)$ where $t_i = (s_i, r_i)$, and each r_i is independent and uniformly distributed on $[0,1]$. Clearly, $\mathcal{I}$ and $\mathcal{J}$ are equivalent. As t_i is nonatomic, and since all standard nonatomic probability spaces are isomorphic, t_i can be reparametrized to be uniform on $[0,1]$. □

We say that a signal t is *split* into r_1 and r_2 if t is a function of r_1 and r_2, i.e., $t = f(r_1, r_2)$.

Lemma 6. *A signal t distributed uniformly on $[0,1]$ can be split into r_1 and r_2 such that each r_i is uniformly distributed on $[0,1]$ and the three random variables t, r_1, and r_2 are pairwise independent. Furthermore, if t' is an additional signal that is independent of t, then we can take r_1, r_2 to be independent of t'.*

This lemma extends the classic secret sharing idea from cryptography which applies to discrete random variables. The proof, by construction, is immediate.[4]

Proof. Denote by $\lfloor x \rfloor$ the fractional part of $x \in \mathbb{R}$. Take r_1 independent of both t and t' and distributed uniformly on $[0,1]$, and let $r_2 = \lfloor r_1 + t \rfloor$. Then $t = \lfloor r_2 - r_1 \rfloor$ and r_1, r_2 and t are easily seen to be pairwise independent and also independent of t' altogether. □

With the help of Lemmas 5 and 6, we are ready to prove Proposition 2.

Proof of Proposition 2. We are given a private private information structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ with sets of signal realizations S_i, $i = 1, \ldots, n$. We aim to construct an equivalent one, $\mathcal{I}'$, where each signal s_i' is uniformly distributed on $[0,1]$ and the realization of signals $(s_1', \ldots, s_n')$ determines the state or, equivalently, $\mathcal{I}'$ is associated with some partition $\mathcal{A} = (A_1, \ldots, A_{m-1})$ of $[0,1]^n$.

By Lemma 5, we can find a private private information structure $(\omega, t_1, \ldots, t_n)$ equivalent to $\mathcal{I}$ where each t_i is uniformly distributed in $[0,1]$. If the signals $(t_1, \ldots, t_n)$ determine the state, then the proof is completed.

Consider the case where $(t_1, \ldots, t_n)$ do not determine the state ω. To capture the uncertainty in ω remaining after the signals have been realized, we construct a new signal t as follows.

Let $q : [0,1]^n \to \Delta(\Omega)$ be a conditional distribution of ω given all the signals, i.e., $q(x_1, \ldots, x_n)(k) = \mathbb{P}[\omega = k \mid t_1 = x_1, \ldots, t_n = x_n]$ for any $k \in \Omega$. With each distribution $q \in \Delta(\Omega)$ we associate a partition of $[0,1)$ into m intervals

$$B_k(q) = \left[\sum_{l=0}^{k-1} q(l), \ \sum_{l=0}^{k} q(l) \right), \qquad k = 0, \ldots, m-1.$$

The length of $B_k(q)$ equals the mass assigned by q to $\omega = k$. Let t be a random variable uniformly distributed on $[0,1]$ and independent of $(t_1, \ldots, t_n)$. Consider a new state variable $\omega' \in \Omega$ such that $\omega' = k$ whenever $t \in B_k\big(q(t_1, \ldots, t_n)\big)$. By definition, the joint distributions of $(\omega, t_1, \ldots, t_n)$ and $(\omega', t_1, \ldots, t_n)$ coincide and, therefore, the two structures are equivalent.

The new state ω' is determined by the realizations of $t_1, \ldots, t_n$ and the new signal t. Using Lemma 6, we split the signal t into r_1 and r_2 that are independent of each

[4] We are thankful to Tristan Tomala for suggesting this construction.

other, and where each r_i is independent of t. Note that, by this lemma, we can take r_1 and r_2 to be independent of $(t_1, \ldots, t_n)$. Since each r_i is uninformative of t, the structure $(\omega', (t_1, r_1), (t_2, r_2), t_3, \ldots, t_n)$ where r_1 is revealed to the first agent and r_2 to the second one is a private private structure and is equivalent to $\mathcal{I}$. Since t is a function of r_1 and r_2, the signals $(t_1, r_1), (t_2, r_2), t_3, \ldots, t_n$ determine the state.

It remains to reparameterize the signals of the first two agents so that, instead of being uniform on $[0,1]^2$, they become uniform on $[0,1]$. Consider any bijection $h : [0,1]^2 \to [0,1]$ preserving the Lebesgue measure[5] and define $s_1' = h(t_1, r_1)$, $s_2' = h(t_2, r_2)$, and $s_i' = t_i$ for $i = 3, \ldots, n$. The private private information structure $\mathcal{I}' = (\omega', s_1', s_2', \ldots, s_n')$ is equivalent to $\mathcal{I}$, all the signals are uniform on $[0,1]$, and the realization of signals determines ω'. □

A.3 Proof of Theorem 3

We formulate and prove an extension of Theorem 3 applicable to non-binary sets of states $\Omega = \{0, 1, \ldots, m-1\}$.

Consider a partition of $[0,1]^n$ into m measurable sets $\mathcal{A} = (A_0, \ldots A_{m-1})$. Recall that the structure $\mathcal{I} = (\omega, s_1, \ldots, s_m)$ is said to be associated with a partition $\mathcal{A}$ if all the signals are uniform on $[0,1]$ and $\omega = k$ whenever $(s_1, \ldots s_n) \in A_k$.

We say that two partitions $\mathcal{A} = (A_0, \ldots A_{m-1})$ and $\mathcal{B} = (B_0, \ldots B_{m-1})$ are *equal* if A_k and B_k differ by a set of zero Lebesgue measure for each k. Recall that the projection of a measurable set $A \subseteq [0,1]^n$ on the ith coordinate is denoted by α_i^A (see §5). The notion of sets of uniqueness from §5 extends to partitions as follows.

Definition 9. *A partition $\mathcal{A} = (A_0, \ldots, A_{m-1})$ is a* partition of uniqueness *if for any partition $\mathcal{B} = (B_0, \ldots, B_{m-1})$ such that $\alpha_i^{A_k} = \alpha_i^{B_k}$ for all i and k, it holds that $\mathcal{A} = \mathcal{B}$.*

Theorem 5 (Extension of Theorem 3 to m states)**.** *A private private information structure $\mathcal{I}$ is Pareto optimal if and only if it is equivalent to a structure associated with a partition of uniqueness $\mathcal{A}$.*

Note that in the case of $m = 2$ states, a set A_1 in a partition $\mathcal{A} = (A_0, A_1)$ determines $A_0 = [0,1]^n \backslash A_1$. Hence, $\mathcal{A} = (A_0, A_1)$ is a partition of uniqueness if and only if

[5] Such a bijection exists since both are standard nonatomic spaces. It can be constructed explicitly in the binary representation: $h(x, y) = z$, where $x = 0.x_1x_2x_3x_4x_5x_6\ldots$, $y = 0.y_1y_2y_3y_4y_5y_6\ldots$ and $z = 0.x_1y_1x_2y_2x_3y_3\ldots$.

A_1 is a set of uniqueness. Hence, Theorem 3 is an immediate corollary of its extended version. For an application of the theorem for $m > 2$, see the example contained in Appendix B.2. This example also demonstrates that partitions of uniqueness are not necessary composed of sets of uniqueness for $m > 2$ and, hence, the requirement of a partition to be a partition of uniqueness does not boil down to restrictions on its elements unless $m = 2$.

The proof of the theorem is split in a sequence of lemmas. We say that a private private information structure is *perfect* if the information received by all the agents together is enough to deduce the realization of ω, i.e., there exists a function $f : S_1 \times \ldots \times S_n \to \Omega$ such that $\omega = f(s_1, \ldots, s_n)$. In particular, a structure with signals uniform in $[0, 1]$ is associated with some partition if and only if it is perfect.

The next lemma shows that perfection is necessary for Pareto optimality.

Lemma 7. *If a private private information structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ is equivalent to a structure that is not perfect, then $\mathcal{I}$ is not Pareto optimal.*

The construction of the Pareto improvement resembles the proof of Proposition 2 except for the fact that the newly constructed signal is revealed entirely to one of the agents, thus strictly improving her information (in the Blackwell order), by Corollary 2.

Proof. Without loss of generality, $\mathcal{I}$ itself is imperfect. Let $q : S_1 \times \ldots \times S_n \to \Delta(\Omega)$ be the distribution of ω conditional on $s_1 = x_1, \ldots, s_n = x_n$, i.e., $q(x_1, \ldots, x_n)(k) = \mathbb{P}[\omega = k \mid s_1 = x_1, \ldots, s_n = x_n]$, $k = 0, \ldots, m-1$. Since $\mathcal{I}$ is not perfect, we can find a state $k_0 \in \Omega$ such that the event $\{\omega = k_0\}$ is not always determined by the signals. That is, the random variable $q(s_1, \ldots, s_n)(k_0)$ does not always take values in $\{0, 1\}$. Without loss of generality, we assume that $k_0 = 0$. With each $q \in \Delta(\Omega)$ we associate a partition of $[0, 1) = \bigsqcup_{k \in \Omega} B_k(q)$, where

$$B_k(q) = \big[q(\{0, \ldots, k-1\}),\ q(\{0, \ldots, k\})\big), \qquad k = 0, \ldots, m-1$$

so that the length of $B_k(q)$ equals $q(k)$.

We construct a new equivalent structure with an extra signal t as in the proof of Proposition 2. Let t be a random variable uniformly distributed on $[0, 1]$ and independent of $s_1, \ldots, s_n$. Define a new state ω' as a function of these variables in the following way:

$$\omega' = k \quad \text{whenever} \quad t \in B_k\big(q(s_1, \ldots, s_n)\big).$$

The joint distribution of $(\omega', s_1, \ldots, s_n)$ coincides with that of $(\omega, s_1, \ldots, s_n)$ and, hence, the two structures are equivalent.

To get a Pareto improvement, we reveal the realization of t to the first agent and obtain a private private information structure $\mathcal{I}' = (\omega', (s_1, t), s_2, \ldots, s_n)$. To argue that $\mathcal{I}'$ is indeed a Pareto improvement we need to show that t itself is an informative signal about ω', i.e., the posterior $p(t) \in \Delta(\Omega)$ is not equal to the prior p with a positive probability. It is enough to show $p(t)(k_0)$ takes different values for t in $[0, \varepsilon]$ and in $[1-\varepsilon, 1]$. As we assume without loss of generality that $k_0 = 0$, the interval B_{k_0} is the leftmost one in the partition, and so

$$p(t)(k_0) = p(t)(0) = \mathbb{P}[t < q(s_1, \ldots, s_n)(0) \,|\, t].$$

That is, if we denote by Q the cumulative distribution function of $q(s_1, \ldots, s_n)(0)$, then $p(t)(k_0) = 1 - G(t)$. Since G is a non-constant function on $(0, 1)$ by our assumption on k_0, the induced belief $p(t)(k_0)$ is not a constant. Thus t is informative. By Corollary 2, this implies that the signal (s_1, t) which the first agent receives in $\mathcal{I}'$ strictly dominates the signal s_1 received in $\mathcal{I}$. As the signals of all other agents are the same in the two structures, $\mathcal{I}'$ strictly Pareto dominates $\mathcal{I}$. □

The next step is to show that only structures corresponding to partitions of uniqueness can be Pareto optimal.

Lemma 8. *If a private private information structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ is Pareto optimal, then $\mathcal{I}$ is equivalent to a structure associated with a partition of uniqueness.*

Proof. By Proposition 2, we can find a private private information structure $\mathcal{J} = (\omega, t_1, \ldots, t_n)$ equivalent to $\mathcal{I}$ and associated with some partition $\mathcal{A} = (A_0, \ldots, A_{m-1})$ of $[0, 1]^n$.

Let us demonstrate that $\mathcal{A}$ is a partition of uniqueness. Towards a contradiction, assume that there is another partition $\mathcal{A}' = (A'_0, \ldots, A'_{m-1})$ not equal to $\mathcal{A}$ but such that the projections $\alpha_i^{A_k} = \alpha_i^{A'_k}$ for all i and k. So $\mathcal{I}$ is also equivalent to the structure $\mathcal{J}' = (\omega, t'_1, \ldots, t'_n)$ associated with $\mathcal{A}'$.

By Lemma 7, to get a contradiction, it is enough to construct an information structure $\mathcal{I}'$ that is equivalent to $\mathcal{I}$ but not perfect, as this would imply the existence of a strict Pareto improvement. We define $\mathcal{I}'$ as a structure where the joint distribution of the state and signals is a convex combination of the corresponding distributions in $\mathcal{J}$ and $\mathcal{J}'$. Formally, let $s_1', \ldots, s_n'$ be independent random variables each uniformly distributed on $[0, 1]$ and let $\theta \in \{0, 1\}$ be a symmetric Bernoulli random variable independent of $(s_1', \ldots, s_n')$. Define the state ω' as follows:

$$\omega' = k \quad \text{if} \quad \left[\begin{array}{l} (s_1', \ldots, s_n') \in A_k \text{ and } \theta = 0 \\ (s_1', \ldots, s_n') \in A_k' \text{ and } \theta = 1 \end{array} \right. .$$

Since elements of the partitions $\mathcal{A}$ and $\mathcal{A}'$ have the same projections, the posterior induced by observing $t_i = x$ in $\mathcal{J}$ is identical to the one induced by observing $t_i' = x$ in $\mathcal{J}'$. Hence it is again identical to the posterior induced by observing $s_i' = x$ in $\mathcal{I}'$. As the partitions $\mathcal{A}$ and $\mathcal{A}'$ are not equal, there are $k \neq k'$ such that the intersection $A_k \cap A_{k'}'$ has a non-zero Lebesgue measure. Hence, if $(s_1', \ldots, s_n') \in A_k \cap A_{k'}'$, whether $\omega = k$ or $\omega = k'$ is determined by θ. We conclude that, with positive probability, the signals $(s_1', \ldots, s_n')$ do not determine the state, so $\mathcal{I}'$ is not perfect and thus both $\mathcal{I}'$ and $\mathcal{I}$ can be Pareto improved by Lemma 7. $\square$

We see that Pareto optimal structures are contained in those associated with partitions of uniqueness (up to equivalence of information structures). This shows one direction of Theorem 5. It remains to demonstrate that any partition of uniqueness leads to a Pareto optimal structure, i.e., the structures associated to different partitions cannot dominate each other.

For this purpose we need two intermediate steps contained in the next two lemmas. Lemma 9 shows that a garbling of an information structure is never perfect and Lemma 10 implies that imperfect structures cannot be equivalent to those associated with partitions of uniqueness. Recall that for a pair of information structures (ω, t) and (ω, s), the signal t is a garbling of s if, conditional on s, t, and ω are independent. A structure $\mathcal{I} = (\omega, s_1, \ldots, s_n)$ is a garbling of $\mathcal{I}' = (\omega, s_1', \ldots, s_n')$ if each s_i is a garbling of s_i' and each s_i is independent of $(s_j')_{j \neq i}$. The last requirement means that each agent's signal is garbled independently. Note that, by Blackwell's Theorem (Blackwell, 1951, Theorem 12), $\mathcal{I}'$ (weakly) dominates $\mathcal{I}$ if and only if $\mathcal{I}$ is equivalent to a garbling of $\mathcal{I}'$.

Lemma 9. *If $\mathcal{I}$ is a garbling of a private private information structure $\mathcal{I}'$, then $\mathcal{I}$ is not perfect unless $\mathcal{I}$ and $\mathcal{I}'$ are equivalent.*

Proof. Suppose that $\mathcal{I}$ is perfect, and so $\omega = f(s_1, \ldots, s_n)$ for some $f\colon\ S_1 \times \ldots \times S_n \to \Omega$. Our goal is to show that $\mathcal{I}$ is equivalent to $\mathcal{I}'$. For a given realization of s_i, the state ω is a function of the remaining signals s_j, $j \neq i$. Since s_i' and s_j are independent for $i \neq j$, we see that ω is independent of s_i' conditional on s_i. In other words, s_i' is also a garbling of s_i. We conclude that both $\mathcal{I}$ is a garbling of $\mathcal{I}'$ and $\mathcal{I}'$ is a garbling of $\mathcal{I}$, so they are equivalent. □

The next lemma is used to show that imperfect private private information structures cannot correspond to partitions of uniqueness. Before stating it, we will need to introduce the following concept. A *fuzzy partition* is a tuple $(g_0, \ldots, g_m)$ of measurable functions $g_k\colon [0,1]^n \to [0,1]$ such that $\sum_k g_k = 1$. We can identify this tuple with a single function $g\colon [0,1]^n \to \Delta(\Omega)$. The case of a partition is one in which each g_k is the indicator of a set A_k in a partition of $[0,1]^n$. As with partitions, we identify two fuzzy partitions if they agree almost everywhere. We denote the collection of fuzzy partitions by G.

We define the projection of g_k to its ith coordinate by

$$\alpha_i^{g_k}(x_i) = \int_{[0,1]^{n-1}} g_k(x_i, x_{-i})\,\mathrm{d}x_{-i}.$$

When g_k is the indicator of a set A_k, the projection $\alpha_i^{A_k}$ as defined in the main text is equal to the projection of g_k. With each partition $\mathcal{A} = (A_0, \ldots, A_{m-1})$ of $[0,1]^n$ we associate the set

$$G_{\mathcal{A}} = \left\{ g \in G \quad \text{such that} \quad \forall k, i \ \ \alpha_i^{g_k} = \alpha_i^{A_k} \right\}$$

of fuzzy partitions that have the same projections as $\mathcal{A}$.

Lemma 10. *A partition $\mathcal{A} = (A_0, \ldots, A_{m-1})$ of $[0,1]^n$ is a partition of uniqueness if and only $G_{\mathcal{A}}$ is a singleton.*

Note that $G_{\mathcal{A}}$ always contains at least one element, namely, the indicators of the partition $\mathcal{A}$, i.e., $(\mathbb{1}_{A_0}, \ldots, \mathbb{1}_{A_{m-1}}) \in G_{\mathcal{A}}$. The idea behind the lemma is that all extreme points of $G_{\mathcal{A}}$ are indicators of partitions with the same projections as $\mathcal{A}$.

Hence, if $G_{\mathcal{A}}$ is not a singleton it has at least two distinct extreme points, i.e., there is at least one more partition with the same projections as $\mathcal{A}$, which is incompatible with the fact that $\mathcal{A}$ is a partition of uniqueness. This identification of extreme points and indicators has appeared before in the context of sets of uniqueness (see Gutmann et al., 1991).

Proof. First we show that $G_{\mathcal{A}}$ can be treated as a non-empty compact convex subset of a locally convex Hausdorff vector space. Non-emptiness and convexity is straightforward and compactness is to be checked once an appropriate topology is defined.

Let $M([0,1]^n)$ be the set of all finite signed measures on $[0,1]^n$ endowed with the topology of weak convergence, making it a locally convex Hausdorff topological vector space. We identify a bounded function $g_k\colon [0,1]^n \to \mathbb{R}$ with a measure μ_k on $[0,1]^n$ having the density g_k with respect to the Lebesgue measure, i.e., $\mathrm{d}\mu_k(x_1,\dots,x_n) = g_k(x)\mathrm{d}x_1\dots\mathrm{d}x_n$. Hence, $G_{\mathcal{A}}$ can be identified with a subset of $\Big(M([0,1]^n)\Big)^{\Omega}$. Let $\Delta_{\leqslant}([0,1]^n)$ be the set of sub-probability measures, i.e., non-negative measures μ with $\mu([0,1]^n) \leqslant 1$. The set $\Delta_{\leqslant}([0,1]^n)$ is a compact subset of $M([0,1]^n)$. As $G_{\mathcal{A}}$ is a subset of the compact set $\big(\Delta_{\leqslant}([0,1]^n)\big)^{\Omega}$, compactness of $G_{\mathcal{A}}$ follows from its closedness. To check closedness, we rewrite the conditions defining $G_{\mathcal{A}}$ in an integrated form using as test functions the continuous functions h on $[0,1]^n$. The tuple of measures $(\mu_0,\dots,\mu_{m-1}) \in \Big(M([0,1]^n)\Big)^{\Omega}$ belongs to $G_{\mathcal{A}}$ if and only if

$$\int_{[0,1]^n} \big|h(x_1,\dots,x_n)\big|\mathrm{d}\mu_k \geqslant 0 \tag{8}$$

$$\sum_k \int_{[0,1]^n} h(x_1,\dots,x_n)\mathrm{d}\mu_k = \int_{[0,1]^n} h(x_1,\dots,x_n)\mathrm{d}x_1\dots\mathrm{d}x_n \tag{9}$$

$$\int_{[0,1]^n} h(x_i)\mathrm{d}\mu_k = \int_{[0,1]} h(x_i)\alpha_i^{A_k}(x_i)\mathrm{d}x_i \tag{10}$$

for all $k = 0,\dots,m-1$, $i = 1,\dots,n$, and continuous functions h on $[0,1]^n$ (in the the last condition, h depends on one of the coordinates only). Condition (8) is non-negativity, condition (9) is equivalent to $\sum_k g_k = 1$, and condition (10) corresponds to the equal projections condition $\alpha_i^{g_k} = \alpha_i^{A_k}$. By the definition of the weak topology, integration of a continuous function commutes with taking weak limits. We conclude that $G_{\mathcal{A}}$ contains all its limit points and thus is closed.

By the Krein-Milman theorem, any compact convex subset of a locally convex

Hausdorff vector space is the closed convex hull of its extreme points (see Aliprantis and Border, 2006, Theorem 7.68). Thus $G_{\mathcal{A}}$ is the closed convex hull of its extreme points. Consequently, if $G_{\mathcal{A}}$ is not a singleton, it has at least two distinct extreme points. To prove the lemma, it remains to demonstrate that all extreme points of $G_{\mathcal{A}}$ correspond to partitions. Towards a contradiction, assume that $g = (g_0, \ldots, g_{m-1})$ is an extreme point of $G_{\mathcal{A}}$ but it is not a partition, i.e., there is a state k_0 such that $g_{k_0}(x) \notin \{0, 1\}$ for $x = (x_1, \ldots, x_n)$ in a set of positive Lebesgue measure. Since $\sum_k g_k = 1$, there is $k' \neq k$ such that the set of x where both $g_k(x) > 0$ and $g_{k'}(x) > 0$ has positive measure. Hence, for some $\varepsilon > 0$, the set $D \subseteq [0, 1]^n$ of x such that both $g_k(x) > \varepsilon$ and $g_{k'}(x) > \varepsilon$ also has positive measure. Without loss of generality, we assume that $k = 0$ and $k' = 1$.

By Corollary 2 of Gutmann et al. (1991), for any D of positive measure, there are two disjoint sets $D_1, D_2 \subseteq D$ also of positive measure having the same projections, i.e., $\alpha_i^{D_1} = \alpha_i^{D_2}$ for any $i = 1, \ldots, n$. Hence, the function $a(x) = \varepsilon\big(\mathbb{1}_{D_1}(x) - \mathbb{1}_{D_2}(x)\big)$ has zero projections, is bounded by ε in absolute value, and is equal to zero outside of the set D. For $\sigma \in \{-1, +1\}$, define

$$g_0^\sigma(x) = g_0(x) + \sigma \cdot a(x), \qquad g_1^\sigma(x) = g_1(x) - \sigma \cdot a(x).$$

By definition, g_0^σ and g_1^σ have the same projections as g_0 and g_1, they are non-negative, and $g_0^\sigma + g_1^\sigma = g_0 + g_1$ (hence, $g_0^\sigma + g_1^\sigma + \sum_{k \geqslant 2} g_k = 1$).

We conclude that the two tuples $(g_0^\sigma, g_1^\sigma, g_2, g_3, \ldots, g_{m-1})$, $\sigma \in \{-1, +1\}$, belong to $G_{\mathcal{A}}$. They are not equal to each other as the sets D_1 and D_2 are disjoint. Since the original collection $(g_0, \ldots, g_{m-1})$ is the average of the two constructed ones, it cannot be an extreme point. This contradiction implies that all the extreme points of $G_{\mathcal{A}}$ correspond to partitions and completes the proof. □

Relying on the last two lemmas, we can demonstrate that any structure associated with a partition of uniqueness is Pareto optimal.

Lemma 11. *Let $\mathcal{I}$ be a private private information structure equivalent to a structure associated with a partition of uniqueness, then $\mathcal{I}$ is Pareto optimal.*

Proof. Without loss of generality, $\mathcal{I} = (\omega, s_1 \ldots, s_n)$ is itself a structure associated with a partition of uniqueness $\mathcal{A} = (A_, \ldots, A_{m-1})$ of $[0, 1]^n$.

Towards a contradiction, assume that there is a private private information structure $\mathcal{J}$ strictly dominating $\mathcal{I}$. By Blackwell's theorem, $\mathcal{I}$ is equivalent to some garbling of $\mathcal{J}$ denoted by $\mathcal{I}' = (\omega, s'_1, \ldots, s'_n)$. By Lemma 9, $\mathcal{I}'$ is not perfect. Let $t_i = p(s'_i) \in \Delta(\Omega)$ be the posterior belief induced by s'_i and $\mu_i \in \Delta(\Delta(\Omega))$ be its distribution. Consider the structure $\mathcal{I}'' = (\omega, t_i, \ldots, t_n)$. It is equivalent to $\mathcal{I}'$ (and hence to $\mathcal{I}$) by Lemma 2. As t_i is a function of s'_i and $\mathcal{I}'$ is not perfect, $\mathcal{I}''$ cannot be perfect either (this is also a consequence of the fact that $\mathcal{I}''$ is a garbling of $\mathcal{J}$).

Let $f\colon \Delta(\Omega) \times \ldots \times \Delta(\Omega) \to \Delta(\Omega)$ be the conditional distribution of ω given the realized signals $t_1, \ldots, t_n$. This function is defined μ-everywhere with $\mu = \mu_1 \times \ldots \times \mu_n$. As $\mathcal{I}''$ is not perfect, there is a state $k_0 \in \Omega$ such that $f_{k_0} \notin \{0, 1\}$ on a set of positive μ-measure.

Choose a fuzzy partition $g\colon\ [0,1]^n \to \Delta(\Omega)$ so that the following identity holds almost surely[6]

$$g(s_1, \ldots, s_n) = f\big(p(s_1), \ldots, p(s_n)\big).$$

The distributions of posteriors $(p(s_1), \ldots, p(s_n))$ and $(p(t_1), \ldots, p(t_n))$ both coincide with μ as the structures $\mathcal{I}$ and $\mathcal{I}''$ are equivalent. Hence, $g_{k_0} \neq \{0, 1\}$ on a set of positive Lebesgue measure, i.e., g does not correspond to a partition. On the other hand, g has the same projections as the partition $\mathcal{A}$. Indeed, let us compute $\alpha_i^{g_k}(x)$:

$$\begin{aligned}
\alpha_i^{g_k}(x) &= \mathbb{E}[g_k(s_1, \ldots, s_n) \mid s_i = x] \\
&= \mathbb{E}[g_k(s_1, \ldots, s_{i-1}, x, s_{i+1}, \ldots, s_n)] \\
&= \mathbb{E}[f_k(p(s_1), \ldots, p(s_{i-1}), q, p(s_{i+1}), \ldots, p(s_n))],
\end{aligned}$$

where q is the posterior induced by $s_i = x$. Since the distribution of $p(s_j)$ is identical to that of t_j,

$$\begin{aligned}
\alpha_i^{g_k}(x) &= \mathbb{E}[f_k(t_1, \ldots, t_{i-1}, q, t_{i+1}, \ldots, t_n)] \\
&= \mathbb{E}[f_k(t_1, \ldots, t_n) \mid t_i = q] \\
&= q(k),
\end{aligned}$$

[6]To construct such a g, define $h_i\colon [0,1] \to \Delta(\Omega)$ by $h_i(x_i)(k) = \mathbb{P}[\omega = k \mid s_i = x_i]$. That is, h_i is the map that assigns to each signal realization the induced posterior, so that $p(s_i) = h_i(s_i)$ holds as an equality of random variables. Then let $g\colon\ [0,1]^n \to \Delta(\Omega)$ be given by $g(x_1, \ldots, x_n) = f(h_1(x_1), \ldots, h_n(x_n))$.

where in the last equality we rely on the fact that the belief induced by t_i coincides with t_i. Since q is the posterior induced by $s_i = x$, the posterior $q(k)$ is equal to $\alpha_i^{A_k}(x)$.

We thus constructed g not equal to $(\mathbb{1}_{A_0}, \ldots, \mathbb{1}_{A_{m-1}})$ but having the same projections. By Lemma 10, the partition $\mathcal{A} = (A_0, \ldots, A_{m-1})$ cannot be a partition of uniqueness. This contradiction shows that no structure can dominate the one associated with a partition of uniqueness, i.e., such structures are Pareto optimal. $\square$

The proof of Theorem 5 is now immediate.

Proof of Theorem 5. By Lemma 8, for each Pareto optimal $\mathcal{I}$, we can find an equivalent structure associated with a partition of uniqueness $\mathcal{A} = (A_0, \ldots, A_{m-1})$. By Lemma 11, any structure admitting such an equivalent representation is Pareto optimal. $\square$

A.4 Proof of Theorem 4

Proof. Lorentz (1949)'s characterization of two-dimensional sets of uniqueness uses the idea of a *non-increasing rearrangement* $\grave{\varphi}$ of a function $\varphi : [0,1] \to [0,1]$. The function $\grave{\varphi}$ is defined almost everywhere by the following two properties: it is non-increasing on $[0,1]$ and, for any $q \in [0,1]$, the lower-contour sets $\{t \in [0,1] : \varphi(t) \leqslant q\}$ and $\{t \in [0,1] : \grave{\varphi}(t) \leqslant q\}$ have the same Lebesgue measure. A non-increasing rearrangement exists and moreover is unique (as an element of $L^\infty([0,1])$).

Lorentz (1949) proved that $A \subseteq [0,1]^2$ is a set of uniqueness if and only if the non-increasing rearrangements of its two projections are inverses of each other, i.e.,

$$\grave{\alpha}_1^A = \left(\grave{\alpha}_2^A\right)^{-1}. \tag{11}$$

Formally, if the inverse $\left(\grave{\alpha}_2^A\right)^{-1}(t)$ is not unique for some t, the equality (11) is to be understood as the inclusion: $\grave{\alpha}_2^A(t) \in \left(\grave{\alpha}_1^A\right)^{-1}(t)$.

Let us demonstrate that the characterization from Theorem 4 is equivalent to the original characterization of Lorentz (1949). That is, we need to check that a set A is a rearrangement of an upward-closed set if and only if the condition (11) holds. Note that for any downward-closed[7] set B, its image under the map $x_1 \mapsto 1 - x_1$

[7] A set $B \subseteq [0,1]^2$ is downward-closed if, with each point (x_1, x_2), it contains all the points $(x_1', x_2') \in [0,1]^2$ such that $x_1' \leqslant x_1$ and $x_2' \leqslant x_2$.

and $x_2 \mapsto 1 - x_2$ is upward-closed. Hence, it is enough to check the equivalence between (11) and the existence of a downward-closed rearrangement of A.

Suppose that A is a rearrangement of a downward-closed set B. Towards showing that (11) holds, note that any downward-closed set B can be represented through its projections in two symmetric ways: $B = \{x_2 \leqslant \alpha_1^B(x_1)\}$ and $B = \{x_1 \leqslant \alpha_2^B(x_2)\}$ up to a zero-measure set. Hence,

$$\alpha_2^B = (\alpha_1^B)^{-1}. \tag{12}$$

Since B is downward-closed, its projections are non-increasing. Moreover, the sets $\{t \in [0,1] : \alpha_i^B(t) \leqslant q\}$ and $\{t \in [0,1] : \alpha_i^A(t) \leqslant q\}$ have the same measure for any i and q as B is a rearrangement of A. Thus $\alpha_i^B = \grave{\alpha}_i^A$ and we obtain (11) from (12).

Now assume that the condition (11) is satisfied and construct the downward-closed set B as follows:

$$B = \{(x_1, x_2) \in [0,1]^2 : x_2 \leqslant \grave{\alpha}_1^A(x_1)\}.$$

By the definition, the projection α_1^B equals $\grave{\alpha}_1^A$. For any downward closed set, the projections satisfy the identity (12) and thus

$$\alpha_2^B = \left(\alpha_1^B\right)^{-1} = \left(\grave{\alpha}_1^A\right)^{-1} = \grave{\alpha}_2^A,$$

where the last equality follows from (11). Hence, for any i and q, the measure of $\{\alpha_i^B(t) \leqslant q\}$ coincides with that of $\{\grave{\alpha}_i^A(t) \leqslant q\}$ and thus with the measure of $\{\alpha_i^A(t) \leqslant q\}$. We conclude that B is a downward-closed rearrangement of A. □

A.5 Proof of Theorem 1

First, we show that the conjugate of a cumulative distribution function on $[0,1]$ is also a cumulative distribution function.

Claim 2. *The conjugate $\hat{F}$ is a cumulative distribution function. Furthermore, it has the same mean: $\int x \,\mathrm{d}\hat{F}(x) = \int x \,\mathrm{d}F(x)$.*

Proof. To show that $\hat{F}$ is a cumulative distribution function it suffices to show that it is weakly increasing, right-continuous, that $\hat{F}(0) \geqslant 0$, and that $\hat{F}(1) = 1$.

We first note that F^{-1} is weakly increasing, by its definition at x as the minimum of the preimage of $[x, \infty)$ under F. Hence $\hat{F}$ is also weakly increasing.

To see that $\hat{F}$ is right continuous, let $\lim_k x_k = x \in [0,1]$, with $x_k \leqslant x$. Then

$$\begin{aligned}\lim_k F^{-1}(x_k) &= \lim_k \min\{y \,:\, F(y) \geqslant x_k\} \\ &= \min\{y \,:\, F(y) \geqslant x\} \\ &= F^{-1}(x)\end{aligned}$$

where the penultimate equality follows from the fact that F is right-continuous. Hence F^{-1} is left-continuous, and so $\hat{F}$ is right-continuous.

It is immediate from the definitions that $\hat{F}(0) \geqslant 0$ and $\hat{F}(1) = 1$, and thus F is a cumulative distribution function. Finally, the expectations of F and $\hat{F}$ are identical since the shape under F (whose measure is equal to its expectation), given by $\{(x,y) \in [0,1]^2 \,:\, y \leqslant F(x)\}$ is congruent to the shape under $\hat{F}$, since one maps to the other by the measure preserving map $(x,y) \mapsto (1-y, 1-x)$. □

Now, we prove Theorem 1.

Proof. First, suppose $\mathcal{I}$ is Pareto optimal. By Theorem 3, $\mathcal{I}$ is equivalent to some structure $\mathcal{I}'$ associated with a set of uniqueness A. By Theorem 4, A is a rearrangement of an upward-closed set A', whose associated structure $\mathcal{I}''$ must also be equivalent to $\mathcal{I}$. We show that the two agents' posterior belief distributions induced by $\mathcal{I}''$ are conjugates of each other.

Define $\tilde{h} : [0,1] \to [0,1]$ by $\tilde{h}(x_1) = \inf\{x_2 : (x_1, x_2) \in A'\}$. We have that $\tilde{h}$ is a decreasing function since A is upward-closed. Define a left-continuous version of $\tilde{h}$ as $h(x) = \lim_{z \to x^-} \tilde{h}(z)$. For any $q \in [0,1]$, in the structure associated with A', up to a measure-zero set of signals, agent 1 has a belief lower or equal to q after observing the signal x_1 if and only if $h(x_1) \geqslant 1-q$, so the cumulative distribution function of agent 1's posterior belief is $F_1(q) = \max\{x_1 : h(x_1) \geqslant 1-q\}$. For agent 2, note that his posterior belief after any signal lower than $x_2 = h(1-q)$ is lower or equal to q, while his belief at higher signals are strictly higher than q. So, the cumulative distribution function of agent 2's posterior belief is $F_2(q) = h(1-q)$. Note that $F_2^{-1}(1-q) = \min\{y : h(1-y) \geqslant 1-q\} = 1 - \max\{x_1 : h(x_1) \geqslant 1-q\} = 1 - F_1(q)$, so F_1 and F_2 are conjugates.

Conversely, suppose the distributions of $p(s_1)$ and $p(s_2)$ in a private private information structure $\mathcal{I}$ are conjugates. Write $\tilde{F}_1$ and $\tilde{F}_2$ for the cumulative distribution functions of $p(s_1)$ and $p(s_2)$, and consider the set $A \subseteq [0,1]^2$ where $(x_1, x_2) \in A$ if and only if $x_2 \geqslant \tilde{F}_2(1 - x_1)$. We show that the structure associated with A is equivalent to $\mathcal{I}$; Figure 4 illustrates the construction. Let $\tilde{h}(x) = \tilde{F}_2(1 - x)$, and define a left-continuous version of $\tilde{h}$ as $h(x) = \lim_{z \to x^-} \tilde{h}(z)$. For the structure associated with A, by the same argument as above, the distribution function of agent 2's posterior belief is $F_2(q) = h(1 - q) = \tilde{F}_2(q)$. The distribution function of agent 1's posterior belief, by the same argument as above, is $F_1(q) = \max\{x_1 : h(x_1) \geqslant 1 - q\} = 1 - \min\{x_2 : \tilde{F}_2(x_2) \geqslant 1 - q\} = 1 - \tilde{F}_2^{-1}(1 - q)$. Using the hypothesis that $\tilde{F}_1$ and $\tilde{F}_2$ are conjugates, $1 - \tilde{F}_2^{-1}(1 - q) = \tilde{F}_1(q)$. So, the structure associated with A is equivalent to $\mathcal{I}$. Because $x_1 \mapsto \tilde{F}_2(1 - x_1)$ is a decreasing function, the set A is upward-closed. Using Theorem 3 and Theorem 4, $\mathcal{I}$ is Pareto optimal. □

A.6 Proof of Theorem 2

Proof. We are given (ω, s_1) and aim to construct a new signal $s_2^\star$ independent of s_1 and such that any other signal s_2 independent of s_1 is dominated by $s_2^\star$.

As usual, $p(s_1)$ is the belief induced by s_1. We sample $s_2^\star$ uniformly from the interval $[1 - p(s_1), 1]$ if the state is $\omega = 1$ and from $[0, 1 - p(s_1)]$ if $\omega = 0$. Hence, conditioned on s_1, the constructed signal is distributed uniformly on $[0, 1]$ and so $s_2^\star$ is independent of s_1. Denote by F the cumulative distribution function of $p(s_1)$ and compute the belief induced by $s_2^\star$. The conditional probability of $\omega = 1$ given $s_2^\star = t$ is equal to $\mathbb{P}[1 - p(s_1) \leqslant t]$. Hence, $p(s_2^\star) = 1 - F(1 - s_2^\star)$. Thus the distribution function $F^\star$ of $p(s_2^\star)$ is given by

$$F^\star(x) = \mathbb{P}[p(s_2^\star) \leqslant x] = \mathbb{P}[1 - F(1 - s_2^\star) \leqslant x] = \mathbb{P}\big[s_2^\star \leqslant 1 - F^{-1}(1 - x)\big],$$

where F^{-1} is defined as in (1). Since $s_2^\star$ is uniformly distributed on $[0, 1]$, we get

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

where $\hat{F}$ is the conjugate of F.

We conclude that $(\omega, s_1, s_2^\star)$ is a private private information structure and the distributions of posteriors induced by s_1 and $s_2^\star$ are conjugates. Thus $(\omega, s_1, s_2^\star)$ is Pareto optimal by Theorem 1, and $s_2^\star$ is an optimal private disclosure.

Now, let us show that any s_2 independent of s_1 is weakly dominated by $s_2^\star$. If (ω, s_1, s_2) is itself Pareto optimal, then, by Theorem 1, the cumulative distribution function of beliefs induced by s_2 is $\hat{F}$ and thus s_2 is equivalent to $s_2^\star$. Hence, it suffices to consider the case where $\mathcal{I} = (\omega, s_1, s_2)$ is not Pareto optimal. Let μ_1 and μ_2 be the distributions of beliefs induced by s_1 and s_2, respectively. Below we will verify that there is a Pareto optimal structure $\mathcal{I}' = (\omega, s_1', s_2')$ that dominates $\mathcal{I}$ and the distribution of $p(s_1')$ coincides with μ_1, i.e., only the second signal becomes more informative. Then, by Theorem 1, the distribution of beliefs induced by s_2' is the conjugate of μ_1. Hence, s_2' is equivalent to $s_2^\star$ and we conclude that $s_2^\star$ must also dominate s_2.

We verify the existence of a Pareto optimal structure $\mathcal{I}' = (\omega, s_1', s_2')$ such that $p(s_1')$ is distributed according to μ_1 and s_2' dominates s_2. Consider the set $\mathcal{M}(\mu_1)$ of distributions μ_2' of beliefs such that the pair (μ_1, μ_2') is feasible, i.e., there is a private private information structure inducing these distributions. In particular, μ_2 belongs to $\mathcal{M}(\mu_1)$. By Lemma 3, $\mathcal{M}(\mu_1)$, as a closed subset of the feasible pairs $\mathcal{M}$, is compact in the weak topology. As the Blackwell order is continuous in the weak topology (see the proof of Lemma 4), there is a maximal element $\mu_2' \in \mathcal{M}(\mu_1)$ dominating μ_2. Let $\mathcal{I}' = (\omega, s_1', s_2')$ be the private private information structure inducing the pair of distributions (μ_1, μ_2'). The structure $\mathcal{I}'$ must be Pareto optimal. Else, by Lemma 9, there is an equivalent structure $\mathcal{I}'' = (\omega, s_1'', s_2'')$ where the signals do not determine the state. Then, by the construction from Lemma 7, there exists an informative signal t independent of s_1'' and s_2''. By revealing t to the second agent, we obtain a strict Pareto improvement of $\mathcal{I}''$ where the distribution of beliefs induced by the first signal remains fixed, but the distribution of beliefs induced by the second signal is improved to μ_2'''. So we have $\mu_2''' \in \mathcal{M}(\mu_1)$ and μ_2''' strictly dominates μ_2', which contradicts the maximality of μ_2' in $\mathcal{M}(\mu_1)$. This contradiction implies the existence of the structure $\mathcal{I}'$ and completes the proof. $\square$

A.7 Proof of Proposition 1

Proof. Denote the indirect utility of agent $i \in \{1, 2\}$ by $U_i(q) = \sup_{a_i \in A_i} \big((1-q) \cdot u_i(a_i, 0) + q \cdot u_i(a_i, 1)\big)$. Since each u_i is bounded from above, the indirect utilities are continuous convex functions. The social welfare for a private private information structure $\mathcal{I} = (\omega, s_1, s_2)$ can be rewritten as follows:

$$W(\mathcal{I}) = \mathbb{E}\big[U_1\big(p(s_1)\big) + U_2\big(p(s_2)\big)\big],$$

where, as usual, $p(s_i)$ is the belief induced by the signal s_i. By the convexity of U_i the welfare is monotone in the Blackwell order, and is therefore always maximized by a Pareto optimal structure.

Let $\mathcal{I}$ be a Pareto optimal structure. By Theorem 1, the distributions of posteriors $p(s_1)$ and $p(s_2)$ are conjugates. Denote the distribution of $p(s_1)$ by μ, which can be an arbitrary measure on $[0,1]$ with mean equal to the prior p. Denote the set of all such measures by $\Delta_p([0,1])$. The choice of $\mu \in \Delta_p([0,1])$ determines the distribution $\hat{\mu}$ of $p(s_2)$. Thus, to maximize welfare over $\mathcal{I}$ it is enough to find $\mu \in \Delta_p([0,1])$ maximizing the functional

$$w(\mu) = \int_{[0,1]} U_1(q)\mathrm{d}\mu(q) + \int_{[0,1]} U_2(q)\mathrm{d}\hat{\mu}(q).$$

Below we check that $w(\mu)$ is convex and continuous in the weak topology. Hence, by Bauer's principle, the optimum is attained at an extreme point of $\Delta_p([0,1])$. It is well-known that the extreme points of this set are measures with the support of size at most two: see, e.g., Winkler (1988). Since the optimal μ is supported on at most two points, its conjugate $\hat{\mu}$ is supported on at most three points (see the discussion after Theorem 1) and we conclude that there is an optimal structure $\mathcal{I}$ where s_1 takes at most two values and s_2 takes at most three values.

It remains to check that $w(\mu)$ is convex and continuous in the weak topology. For the first integral, this is immediate: it is linear in μ (hence, convex) and continuous thanks to the continuity of the integrand. To show that the two properties hold for the second integral, we rewrite it through the cumulative distribution function F of μ. Assuming first that F is a bijection $[0,1] \to [0,1]$, we obtain

$$\int_{[0,1]} U_2(q)\mathrm{d}\hat{\mu}(q) = \int_{[0,1]} U_2(q)\mathrm{d}\left(1 - F^{-1}(1-q)\right) = \int_{[0,1]} U_2\big(1 - F(t)\big)\mathrm{d}t, \tag{13}$$

by changing the variable $q = 1 - F(t)$ in the second equality. Let us show that the identities (13) hold even without the assumption that F is a bijection. Since any continuous function on $[0,1]$ can be approximated by a linear combination of indicators $\mathbb{1}_{[0,a]}$ in the sup-norm, it is enough to prove that

$$\int_{[0,1]} \mathbb{1}_{[0,a]}(q)\mathrm{d}\hat{\mu}(q) = \int_{[0,1]} \mathbb{1}_{[0,a]}\big(1 - F(t)\big)\mathrm{d}t$$

or, equivalently, that

$$\hat{F}(a) = \lambda\big(\{t \in [0,1] : 1 - F(t) \leqslant a\}\big), \tag{14}$$

where λ stands for the Lebesgue measure. By the monotonicity of F, the set from the right-hand side of (14) is an interval $[t_a, 1]$ where $t_a = \min\{t : F(t) \geqslant 1 - a\}$, i.e., $t_a = F^{-1}(1-a)$ as defined in §4. We conclude that (14) holds as it is equivalent to the equality $\hat{F}(a) = 1 - F^{-1}(1-a)$ defining the conjugate distribution and thus (13) holds as well.

Since U_2 is convex, we conclude that $\int_{[0,1]} U_2\big(1 - F(t)\big)\mathrm{d}t$ is a convex function of F and, hence, of μ. To show the continuity, note that the weak convergence $\mu_k \to \mu$ implies the convergence of $F_k(q) \to F(q)$ for all points q of continuity of F (see Aliprantis and Border, 2006, Theorem 15.3). Since any monotone function is continuous almost everywhere with respect to the Lebesgue measure, the sequence of functions $U_2\big(1 - F_k\big)$ converges almost everywhere in $[0,1]$ and is bounded thanks to boundedness of U_2. The Lebesgue dominated convergence theorem implies that $\int_{[0,1]} U_2\big(1 - F_k(t)\big)\mathrm{d}t$ converges to $\int_{[0,1]} U_2\big(1 - F(t)\big)\mathrm{d}t$. We conclude that the second integral in $w(\mu)$ is a convex continuous function of μ. Thus the functional $w(\mu)$ is itself continuous and convex. □

A.8 Proof of Proposition 3

Proof. We have $I(\omega; (s_1, \ldots, s_n)) \leqslant H(p)$, so this result follow from Lemma 1. □

A.9 Proof of Proposition 4

Proof. We have $I(\omega; (s_1, \ldots, s_n)) \leqslant H(p)$, so it suffices to show that

$$\sum_i I(\omega; s_i) \leqslant I(\omega; (s_1, \ldots, s_n)) - \frac{\ln 2}{8} \sum_{i<j} I(\omega; s_i) I(\omega; s_j). \tag{15}$$

Similarly to the proof of Lemma 1, the result for general n follows from the result for $n = 2$ via an inductive argument. Indeed, assume that the statement holds for

$n \leqslant n_0$ with $n_0 \geqslant 2$ and show that it holds for $n = n_0 + 1$ as well:

$$\begin{aligned}
&I\Big(\omega\,;\,\big(s_1,\ldots,s_{n_0},s_{n_0+1}\big)\Big)\\
&= I\Big(\omega\,;\,\big((s_1,\ldots,s_{n_0}),s_{n_0+1}\big)\Big)\\
&\geqslant I\Big(\omega\,;\,\big(s_1,\ldots,s_{n_0}\big)\Big) + I(\omega\,;\,s_{n_0+1}) + \frac{\ln 2}{8} I\Big(\omega\,;\,\big(s_1,\ldots,s_{n_0}\big)\Big)\cdot I(\omega\,;\,s_{n_0+1}),
\end{aligned}$$

where we applied the two-signal version of (15) for the pair of signals $(s_1,\ldots,s_{n_0})$ and s_{n_0+1}. Estimating $I(\omega\,;\,s_1,\ldots,s_{n_0})$ from below via the n_0-signal version of (15), we get

$$\begin{aligned}
&I\Big(\omega\,;\,\big(s_1,\ldots,s_{n_0},s_{n_0+1}\big)\Big)\\
&\geqslant \sum_{i=1}^{n_0} I\big(\omega\,;\,s_i\big) + \frac{\ln 2}{8}\sum_{1\leqslant i<j\leqslant n_0} I\big(\omega\,;\,s_i\big)\cdot I\big(\omega\,;\,s_j\big) + I(\omega\,;\,s_{n_0+1}) +\\
&\quad + \frac{\ln 2}{8} I(\omega\,;\,s_{n_0+1})\cdot\left(\sum_{i=1}^{n_0} I\big(\omega\,;\,s_i\big) + \frac{\ln 2}{8}\sum_{1\leqslant i<j\leqslant n_0} I\big(\omega\,;\,s_i\big)\cdot I\big(\omega\,;\,s_j\big)\right)
\end{aligned}$$

Eliminating all the cubic terms from the second line can only decrease the right-hand side and leads to inequality (15) for $n = n_0 + 1$:

$$I\Big(\omega\,;\,\big(s_1,\ldots,s_{n_0},s_{n_0+1}\big)\Big) \geqslant \sum_{i=1}^{n_0+1} I\big(\omega\,;\,s_i\big) + \frac{\ln 2}{8}\sum_{1\leqslant i<j\leqslant n_0+1} I\big(\omega\,;\,s_i\big)\cdot I\big(\omega\,;\,s_j\big).$$

It thus remains to prove the result for $n = 2$. We aim to show that

$$I(\omega\,;\,s_1) + I(\omega\,;\,s_2) - I(\omega\,;\,s_1,s_2) \leqslant -\frac{\ln 2}{8} I(\omega\,;\,s_1)\cdot I(\omega\,;\,s_2). \tag{16}$$

Since (16) is symmetric with respect to the states, we can assume that the state $\omega = 1$ is more likely, i.e., $p \geqslant 1/2$ without loss of generality.

Denote the left-hand side of (16) by Δ and the posterior probabilities of the high state by $p_i = \mathbb{P}[\omega = 1\,|\,s_i]$ and $p_{12} = \mathbb{P}[\omega = 1\,|\,s_1,s_2]$. By the martingale property, $\mathbb{E}[p_{12}\,|\,s_i] = p_i$ and $\mathbb{E}[p_i] = p$. Thanks to the martingale property, we can represent

$I(\omega\,;\,s_i)$ as follows:

$$I(\omega\,;\,s_i) = \mathbb{E}\left[p_{12}\log_2\left(\frac{p_i}{p}\right) + (1-p_{12})\log_2\left(\frac{1-p_i}{1-p}\right)\right],$$

where p_i outside of the logarithm was replaced by p_{12}. Hence,

$$\Delta = \mathbb{E}\left[p_{12}\log_2\left(\frac{p_1\cdot p_2}{p_{12}\cdot p}\right) + (1-p_{12})\log_2\left(\frac{(1-p_1)(1-p_2)}{(1-p_{12})(1-p)}\right)\right].$$

By the concavity of the logarithm, a convex combination of logarithms is at most the logarithm of the convex combination. Therefore,

$$\Delta \leqslant \mathbb{E}\left[\log_2\left(\frac{p_1 p_2}{p} + \frac{(1-p_1)(1-p_2)}{(1-p)}\right)\right].$$

Denote the centred posteriors by $\bar{p}_1 = p_1 - p$ and $\bar{p}_2 = p_2 - p$. The right-hand side simplifies to

$$\mathbb{E}\left[\log_2\left(\frac{p_1\cdot p_2}{p} + \frac{(1-p_1)(1-p_2)}{(1-p)}\right)\right] = \mathbb{E}\left[\log_2\left(1 + \frac{\bar{p}_1\cdot\bar{p}_2}{p(1-p)}\right)\right].$$

Note that $\frac{\bar{p}_1\cdot\bar{p}_2}{p(1-p)}$ belongs to the interval $\left[-1, \frac{1-p}{p}\right]$. By the assumption that $p \geqslant 1/2$, this interval is contained in $[-1,1]$. Consider the function $f(x) = \log_2(1+x)$. By the Taylor formula, for any $x \in [-1,1]$,

$$f(x) = f(0) + f'(0)\cdot x + \frac{f''(y)}{2}x^2$$

for some y between 0 and x. Computing the derivatives, we get

$$f(x) = \frac{1}{\ln 2}x + \frac{1}{2\ln 2}\frac{-1}{(1+y)^2}x^2 \leqslant \frac{1}{\ln 2}x - \frac{1}{8\ln 2}x^2,$$

where in the last inequality we used the fact that $y \in [-1,1]$. We conclude that

$$\mathbb{E}\left[\log_2\left(1 + \frac{\bar{p}_1\cdot\bar{p}_2}{p(1-p)}\right)\right] \leqslant \frac{1}{\ln 2}\mathbb{E}\left[\frac{\bar{p}_1\cdot\bar{p}_2}{p(1-p)}\right] - \frac{1}{8\ln 2}\mathbb{E}\left[\left(\frac{\bar{p}_1\cdot\bar{p}_2}{p(1-p)}\right)^2\right].$$

Since the expectation of the product is the product of expectations for the independent random variables $\bar{p}_1$ and $\bar{p}_2$,

$$\frac{1}{\ln 2}\mathbb{E}\left[\frac{\bar{p}_1 \cdot \bar{p}_2}{p(1-p)}\right] - \frac{1}{8\ln 2}\mathbb{E}\left[\left(\frac{\bar{p}_1 \cdot \bar{p}_2}{p(1-p)}\right)^2\right] = -\frac{1}{8p^2(1-p^2)\ln 2}\mathrm{Var}[p_1] \cdot \mathrm{Var}[p_2].$$

It remains to lower-bound the variance by the mutual information. The Kullback–Leibler divergence between Bernoulli random variables with success probabilities p and x is defined as follows: $D_{\mathrm{KL}}(x||p) = x\log_2\left(\frac{x}{p}\right) + (1-x)\log_2\left(\frac{1-x}{1-p}\right)$. Then $I(\omega\,;\,s_i) = \mathbb{E}[D_{\mathrm{KL}}(p_i||p)]$. Applying the inequality $\ln t \leqslant t-1$ to both logarithms and taking into account that $\log_2 t = \frac{1}{\ln 2}\ln t$, we obtain

$$D_{\mathrm{KL}}(x||p) \leqslant \frac{1}{\ln 2}\left(x\cdot\left(\frac{x}{p}-1\right) + (1-x)\cdot\left(\frac{1-x}{1-p}-1\right)\right) = \frac{1}{p(1-p)\ln 2}(x-p)^2$$

for $x \in [0,1]$. Therefore,

$$\mathrm{Var}[p_i] \geqslant (p(1-p)\ln 2)\cdot I(\omega\,;\,s_i).$$

Thus we obtain

$$-\frac{1}{8p^2(1-p^2)\ln 2}\mathrm{Var}[p_1]\cdot\mathrm{Var}[p_2] \leqslant -\frac{\ln 2}{8}\cdot I(\omega\,;\,s_1)\cdot I(\omega\,;\,s_2)$$

and conclude that

$$\Delta \leqslant -\frac{\ln 2}{8}\cdot I(\omega\,;\,s_1)\cdot I(\omega\,;\,s_2),$$

which is equivalent to the desired inequality (16). □

A.10 Proof of Proposition 5

Proof. As in the proof of Proposition 3, we show a stronger statement:

$$\sum_i \bar{I}(\omega; s_i) \leqslant \bar{I}(\omega; (s_1, \ldots, s_n)).$$

This implies the statement of Proposition 5 since $\bar{H}$ is concave, and so, as with mutual information, $\bar{I}(\omega; (s_1, \ldots, s_n)) \leqslant \bar{H}(p)$.

Applying the definition of $\bar{I}$, and using the martingale property $\mathbb{E}[p(s_i)] = \mathbb{E}[p(s_1, \ldots, s_n)] =$

p, what we want to prove is that

$$\sum_i \sum_{k \in \Omega} \mathbb{E}\big[[p(s_i)(k) - p(k)]^2\big] \leqslant \sum_k \mathbb{E}\big[[p(s_1, \ldots, s_n)(k) - p(k)]^2\big].$$

In fact, we prove an even stronger statement, showing that the inequality holds already for each $k \in \Omega$ separately, rather than only when summed over Ω.

To this end, fix k, and denote the centered posteriors by $\bar{p}_i = p(s_i)(k) - p(k)$, so that $\bar{p}_i$ is a zero-mean bounded random variable. Likewise denote $\bar{p} = p(s_1, \ldots, s_n)(k) - p(k)$. We want to prove that $\mathbb{E}[\bar{p}^2] \geqslant \sum_i \mathbb{E}[\bar{p}_i^2]$.

Let V be the vector space of zero-mean random variables spanned by $\{\bar{p}, \bar{p}_1, \ldots, \bar{p}_n\}$. As a subspace of L^2, it is endowed with the inner product given by the expectation of the product.

Since the structure is private private, $\mathbb{E}[\bar{p}_i \cdot \bar{p}_j] = \mathbb{E}[\bar{p}_i] \cdot \mathbb{E}[\bar{p}_j] = 0$ for $i \neq j$. That is, the vectors $\{\bar{p}_1, \ldots, \bar{p}_n\}$ are orthogonal. Hence, $V = \operatorname{span}\{\bar{q}, \bar{p}_1, \ldots, \bar{p}_n\}$ for some $q \in V$ that is orthogonal to each $\bar{p}_i$ (note that $q = 0$ is allowed and corresponds to the case where $\bar{p}$ can be represented as a linear combination of $\bar{p}_i$). Since $\bar{p} \in V$, we can write

$$\bar{p} = \alpha q + \sum_i \alpha_i \bar{p}_i$$

for some scalars $\alpha, \alpha_1, \ldots, \alpha_n$. By the martingale property, $\mathbb{E}[\bar{p} \,|\, \bar{p}_i] = \bar{p}_i$, and so $\mathbb{E}[(\bar{p} - \bar{p}_i) \cdot p_i] = 0$. That is, $\bar{p} - \bar{p}_i$ is orthogonal to $\bar{p}_i$. Hence $\alpha_i = 1$, and

$$\bar{p} = \alpha q + \sum_i \bar{p}_i.$$

Since $\{\bar{q}, \bar{p}_1, \ldots, \bar{p}_n\}$ are orthogonal,

$$\mathbb{E}\big[\bar{p}^2\big] = \alpha^2 \mathbb{E}\big[q^2\big] + \sum_i \mathbb{E}\big[\bar{p}_i^2\big],$$

and in particular $\mathbb{E}[\bar{p}^2] \geqslant \sum_i \mathbb{E}[\bar{p}_i^2]$.

$\square$

Note that we used the assumption that the structure is private private only inasmuch as it implies that posteriors of different agents are uncorrelated.

B Further Examples and Results

B.1 Comparative Statics along the Pareto Frontier

In this section we state and prove the following proposition.

Proposition 6. *Consider two Pareto optimal private private information structures* (ω, s_1, s_2) *and* (ω, t_1, t_2) *with binary state* ω*. If* t_1 *dominates* s_1*, then* t_2 *is dominated by* s_2*.*

Proof. Since (ω, s_1, s_2) is Pareto optimal, the signal s_2 can be seen as an optimal private disclosure corresponding to (ω, s_1). By Theorem 2, such s_2 dominates any other signal s_2' independent of s_1. Hence, to conclude that s_2 dominates t_2, it is enough to demonstrate that there is a private private information structure (ω, s_1', s_2') such that s_1' is equivalent to s_1 and s_2' is equivalent to t_2. By the assumption, t_1 dominates s_1 and, therefore, the signal s_1 is equivalent to some garbling s_1' of t_1. Putting $s_2' = t_2$, we get the desired private private information structure (ω, s_1', s_2') and deduce that t_2 is dominated by s_2. □

B.2 Non-Uniqueness of Optimal Private Disclosures for Non-Binary States

Theorem 2 shows that when the state is binary, there is a unique optimal private disclosure $s_2^\star$ for each s_1. In this section we show that this does not hold for non-binary states.

Consider the case of $\Omega = \{0, 1, 2\}$ where $\omega \in \Omega$ is distributed according to the prior $p = \left(1/4, 1/2, 1/4\right)$. The signal s_1 is binary: if $\omega = 2$ then $s_1 = 1$, if $\omega = 0$ then $s_1 = 0$, and if $\omega = 1$ then $s_1 \in \{0, 1\}$ equally likely. The induced beliefs $p(s_1)$ are equal to either $\left(1/2, 1/2, 0\right)$ or $\left(0, 1/2, 1/2\right)$, each with probability $1/2$.

To construct an optimal disclosure $s_2^\star$ we first build an auxiliary private private information structure (ω, t_1, t_2), associated with the partition of $[0, 1]^2$ into three sets A_0, A_1, and A_2 depending on a parameter $\beta \in [0, 1/2]$, as depicted in Figure 8. The pair of signals (t_1, t_2) is uniformly distributed on $[0, 1]^2$ and the state ω equals k whenever the pair of signals belongs to A_k. Since the area of A_1 is twice the area of A_0 and A_2, and since the latter two areas are equal, ω has the right distribution $p = \left(1/4, 1/2, 1/4\right)$.

Let us check that the signal t_1 is equivalent to s_1, i.e., it induces the same posterior distribution. Indeed, if the realization of t_1 belongs to $[0, 1/2]$, half of each vertical

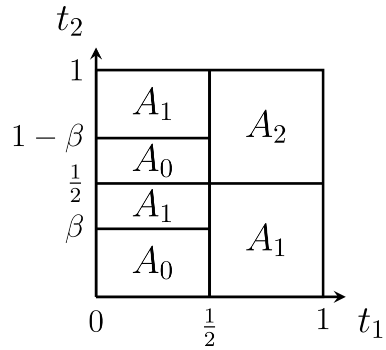

Figure 8: In the private private information structure associated with the partition (A_0, A_1, A_2), the signal t_1 induces the same distribution of posteriors as s_1. For any parameter $\beta \in [0, 1/2]$, this partition is a partition of uniqueness and, hence, we get a one-parametric family of non-equivalent optimal disclosures given by the signal t_2.

slice of the square is covered by A_0 and half by A_1, and so the induced posterior is $p(t_1) = \big(1/2, 1/2, 0\big)$ with probability $1/2$. Similarly, for $t_1 \in [1/2, 1]$, we get $p(t_1) = \big(0, 1/2, 1/2\big)$ also with probability $1/2$.

Let us check that for different values of β we obtain non-equivalent disclosures. For this purpose, we compute the distribution of posteriors induced by t_2. Note that t_2 is equivalent to a signal $s_2^\star$ taking four different values corresponding to different pairs of sets (A_i, A_j) intersected by the horizontal slice of the square. We get the following distribution of posteriors:

$$p(s_2^\star) = \begin{cases} \big(0, 1/2, 1/2\big) & \text{with probability } \beta \\ \big(1/2, 0, 1/2\big) & \text{with probability } 1/2 - \beta \\ \big(0, 1, 0\big) & \text{with probability } 1/2 - \beta \\ \big(1/2, 1/2, 0\big) & \text{with probability } \beta \end{cases}$$

For different values of β we get different distributions, i.e., the constructed disclosures are not equivalent.

It remains to show that for any value of β, the signal $s_2^\star$ is an optimal private disclosure. To this end we check that the partition (A_0, A_1, A_2) is a partition of uniqueness (as defined in Appendix A.3). Therefore, by Theorem 5, the information structure (ω, t_1, t_2) is Pareto optimal. Thus t_2 is an optimal private disclosure and so is $s_2^\star$ as it is equivalent to t_2.

To show that (A_0, A_1, A_2) is a partition of uniqueness, we rely on the following elementary but useful general observation: if in a partition $(A_0, \ldots, A_{m-1})$ of $[0,1]^n$ all sets except for possibly one are sets of uniqueness, then the partition itself is a partition of uniqueness. In our example, the set A_2 is upward-closed and hence is a set of uniqueness by Theorem 4. The set A_0 is a rearrangement of an upward-closed set (since it can be made upward-closed via a measure-preserving reparametrization of the axes) and so is a set of uniqueness by the same theorem. Thus the partition (A_0, A_1, A_2) is a partition of uniqueness and $s_2^\star$ is an optimal disclosure for any value of β.

The partition (A_0, A_1, A_2) provides an interesting example of the fact that a partition of uniqueness is not necessary composed of sets of uniqueness. Indeed, for $\beta \neq 0$, the set A_1 is not a set of uniqueness as it has the same marginals as the set obtained by the reflection of A_1 with respect to the vertical line $t_1 = 1/2$.

B.3 Representing Private Private Signals for Binary ω as Sets

To simplify notation, in this section we consider the case of $n = 2$ agents and a binary state $\omega \in \Omega = \{0, 1\}$. Nevertheless, the same ideas apply more generally to finitely many agents and possible values of the state. By Proposition 2, any private private information structure $\mathcal{I}$ is equivalent to a structure associated with some set $A \subseteq [0,1]^2$, which we denote by $\mathcal{I}_A = (\omega, s_1, s_2)$. In this section, we show how to construct $\mathcal{I}_A$ given $\mathcal{I}$. We begin with the case where $\mathcal{I}$ is uninformative and describe $\mathcal{I}_A$ for any prior $p = \mathbb{P}[\omega = 1]$. Relying on this construction, we then describe how to construct $\mathcal{I}_A$ for any $\mathcal{I}$ with a finite number of possible signal values.

Recall that in $\mathcal{I}_A$, the signals (s_1, s_2) are uniformly distributed on $[0,1]^2$, the state is $\omega = \mathbb{1}_A(s_1, s_2)$, and A is some measurable subset of $[0,1]^2$ with Lebesgue measure $\lambda(A) = p$ so that $p = \mathbb{P}[\omega = 1]$. Recall that the distribution of posteriors induced by $\mathcal{I}_A$ can be computed as follows: The conditional probability of the high state given that agent i receives a signal $s_i = t$ is exactly $\alpha_i^A(t)$, the one-dimensional Lebesgue measure of the cross-section $\{(y_1, y_2) \in A : y_i = t\}$. In other words, $\alpha_i^A(s_i)$ is i's posterior corresponding to s_i and the induced distribution of posteriors μ_i is the image of the uniform distribution under the map α_i^A, i.e., $\mu_i([0,t])$ equals the Lebesgue measure of $\{x_i \in [0,1] : \alpha_i^A(x_i) \leqslant t\}$.

Example 1 (Non-informative signals). Consider a private private information structure $\mathcal{I}$, where both agents receive completely uninformative signals, i.e., the induced posteriors are equal to the prior p almost surely.

To find an equivalent structure $\mathcal{I}_A$, we need to construct a set $A = A_p \subseteq [0,1]^2$ such that the Lebesgue measure of all its projections equals p. To this end, let Y be any subset of $[0,1]$ with measure p (e.g., $[0,p]$), and let

$$A = \left\{(x_1, x_2) \in [0,1]^2 \,:\, \lfloor x_1 + x_2 \rfloor \in Y\right\},$$

where $\lfloor x \rfloor$ is the fractional part of $x \in \mathbb{R}$. It is easy to see that A indeed has the desired property.

It turns out that the construction of an information structure $\mathcal{I}_{A_p}$ representing completely uninformative signals can be used to find a representation for any information structure with a finite number of possible signal values.

Example 2 (Arbitrary finite number of signal values). Let $\mathcal{I} = (\omega, s_1, s_2)$ be a private private information structure with $n = 2$ agents and finite signal spaces S_1 and S_2. Our goal is to construct a set $A \subseteq [0,1]^2$ such that the structure $\mathcal{I}_A$ associated with A is equivalent to $\mathcal{I}$.

For each agent $i \in \{1,2\}$, consider a disjoint partition of $[0,1]$ into intervals A_{s_i}, $s_i \in S_i$, so that the length of each A_{s_i} coincides with the probability that the signal $s_i \in S_i$ is sent under $\mathcal{I}$. Let $q(s_1, s_2) \in [0,1]$ be the conditional probability of $\{\omega = 1\}$ given signals (s_1, s_2).

Recall that, in Example 1, we constructed a set $A_p \subseteq [0,1]^2$ such that its projection to each of the coordinates has a constant density p. Now we construct A by pasting the appropriately rescaled copy of $A_{q(s_1,s_2)}$ into each rectangle $A_{s_1} \times A_{s_2}$. Denote by $T_{[a,b]\times[c,d]}$ an affine map $\mathbb{R}^2 \to \mathbb{R}^2$ that identifies $[0,1]^2$ with $[a,b] \times [c,d]$:

$$T_{[a,b]\times[c,d]}(x_1, x_2) = \big(a + (b-a)x_1,\ c + (d-c)x_2\big).$$

We define A as the following disjoint union:

$$A = \bigsqcup_{s_1 \in S_1,\, s_2 \in s_2} T_{A_{s_1} \times A_{s_2}}\Big(A_{q(s_1,s_2)}\Big).$$

Let $s_i' \in [0,1]$ be a signal received by an agent i in $\mathcal{I}_A$. The signal s_i' falls into A_{s_i} with the same probability that i receives the signal s_i in $\mathcal{I}$. By construction, the conditional probability of $\{\omega = 1\}$ given s_i' is constant over each interval A_{s_i} and coincides with the posterior $p_i(s_i)$ that i gets under $\mathcal{I}$. We conclude that $\mathcal{I}$ and $\mathcal{I}_A$ induce the same distribution of posteriors and so are equivalent.