# An axiomatic theory for anonymized risk sharing

Ruodu Wang

http://sas.uwaterloo.ca/~wang

Department of Statistics and Actuarial Science
University of Waterloo

INFORMS Annual Meeting, Indianapolis, USA
Oct 15-19, 2022

# Agenda



Based on joint work with
Zhanyi Jiao (Waterloo), Steven Kou (Boston) and Yang Liu (Stanford)

# Risk sharing

- $n$ agents with initial risks $X_1, \dots, X_n \in \mathcal{X}$ (a set of rvs)
- total risk (or asset) $S = \sum_{i=1}^n X_i$

The set of allocations of $S$:

$$\mathbb{A}_n(S) = \left\{ (Y_1, \dots, Y_n) \in \mathcal{X}^n : \sum_{i=1}^n Y_i = S \right\}$$

Two settings

- Collaborative risk sharing: Pareto equilibrium, impossible to strictly improve
- Competitive risk sharing: competitive equilibrium, each agent optimizes their objectives individually

# Risk sharing

To derive an equilibrium

- Collective: requires a central planner who knows preferences of all agents
- Competitive: requires a trading mechanism (e.g., a market) and individual preferences

Preference models: Expected utility, mean-variance, dual utility, RDU, CPT, quantiles, robust/variational preferences, ...

- Difficult to elicit or test
- Allocation to agent $i$ depends on preferences of other agents
- Supplying fake preferences may be rewarding

# Anonymized risk sharing

Anonymized risk sharing mechanisms

- no central planner involved
- no information on preferences revealed
- no identity revealed
- no actual loss/gain revealed
- no irrelevant operations revealed

Examples

- founders stock; Bitcoin mining pool; tontines; P2P insurance; revenue sharing, ...

We take an axiomatic approach

# Setup and axioms

# Setup and axioms

Setup

- $(\Omega, \mathcal{F}, \mathbb{P})$: a probability space
- $\mathcal{X}$: a set of rvs
- $n \geq 3$; $\mathbf{X} = (X_1, \dots, X_n)$; $S^{\mathbf{X}} = \sum_{i=1}^n X_i$

## Risk sharing rules

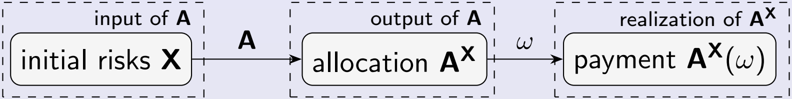
A risk sharing rule is a mapping $\mathbf{A} : \mathcal{X}^n \to \mathcal{X}^n$ satisfying

$$\mathbf{A}^{\mathbf{X}} = (A_1^{\mathbf{X}}, \dots, A_n^{\mathbf{X}}) \in \mathbb{A}_n(S^{\mathbf{X}})$$

for each $\mathbf{X} \in \mathcal{X}^n$.

- Mappings from $\mathcal{X}^n \to \mathcal{X}^n$ are complicated objects
- Risk measures are $\mathcal{X} \to \mathbb{R}$, $\mathcal{X}^n \to \mathbb{R}$ or $\mathcal{X}^n \to \mathbb{R}^n$

# Examples




(i) The identity risk sharing rule

$$\mathbf{A}^{\mathbf{X}}_{\mathrm{id}} = \mathbf{X} \quad \text{for } \mathbf{X} \in \mathcal{X}^n.$$

(ii) The all-in-one risk sharing rule

$$\mathbf{A}^{\mathbf{X}}_{\mathrm{all}} = \left(S^{\mathbf{X}}, 0, \dots, 0\right) \quad \text{for } \mathbf{X} \in \mathcal{X}^n.$$

(iii) The uniform risk sharing rule

$$\mathbf{A}^{\mathbf{X}}_{\mathrm{unif}} = S^{\mathbf{X}} \left(\frac{1}{n}, \dots, \frac{1}{n}\right) \quad \text{for } \mathbf{X} \in \mathcal{X}^n.$$

# Examples

(iv) The conditional mean risk sharing rule (CMRS)

$$\mathbf{A}^{\mathbf{X}}_{\mathrm{cm}} = \mathbb{E}\left[\mathbf{X} | S^{\mathbf{X}}\right] \quad \text{for } \mathbf{X} \in \mathcal{X}^n \subseteq (L^1)^n.$$

(v) The mean proportional risk sharing rule

$$\mathbf{A}^{\mathbf{X}}_{\mathrm{prop}} = \frac{S^{\mathbf{X}}}{\mathbb{E}[S^{\mathbf{X}}]}\mathbb{E}[\mathbf{X}] \quad \text{for } \mathbf{X} \in \mathcal{X}^n \subseteq (L^1_+)^n.$$

(vi) The covariance risk sharing rule

$$\mathbf{A}^{\mathbf{X}}_{\mathrm{cov}} = \frac{S^{\mathbf{X}} - \mathbb{E}[S^{\mathbf{X}}]}{\mathrm{var}(S^{\mathbf{X}})}\mathrm{cov}(\mathbf{X}, S^{\mathbf{X}}) + \mathbb{E}[\mathbf{X}] \quad \text{for } \mathbf{X} \in \mathcal{X}^n \subseteq (L^2)^n.$$

# Actuarial fairness

**Axiom AF (Actuarial fairness)**

The expected value of each agent's allocation coincides with the expected value of the initial risk, that is,

$$\mathbb{E}[\mathbf{A}^{\mathbf{X}}] = \mathbb{E}[\mathbf{X}] \quad \text{for} \quad \mathbf{X} \in \mathcal{X}^n.$$

- with no information on preferences, actuarial fairness is the most natural requirement
- dates back to at least the 16th century

# Risk fairness

## Axiom RF (Risk fairness)

The allocation to each agent should not exceed their maximum possible loss. That is, for $\mathbf{X} \in \mathcal{X}^n$ and $i \in [n]$, it holds that

$$A_i^{\mathbf{X}} \le \sup X_i.$$

- Pure surplus ($X_i \le 0$) leads to pure surplus allocation
- AF + RF $\Longrightarrow$ $X_i = c$ is a constant, then $A_i^{\mathbf{X}} = c$
- $A_1^{(X,0,\dots,0)} = X$ and $A_j^{(X,0,\dots,0)} = 0$ for $j \neq 1$.
- RF can be alternatively formulated by $A_i^{\mathbf{X}} \ge \inf X_i$

# Risk anonymity

**Axiom RA (Risk anonymity)**

The realized value of the allocation to each agent is determined by that of the total risk. That is, for $\mathbf{X} \in \mathcal{X}^n$,

$$\mathbf{A}^{\mathbf{X}} \text{ is } \sigma(S^{\mathbf{X}})\text{-measurable.}$$

- The knowledge of $\mathbf{X}$ is only used for design but not for settlement
  - once pooled, only the pooled risk matters
- Agents do not need to disclose actual gains/losses
  - e.g., Bitcoin mining pool
- RA holds if $\mathbf{A}^{\mathbf{X}}$ is always comonotonic

# Operational anonymity

**Axiom OA (Operational anonymity)**

The allocation to one agent is not affected if risks of two other agents merge. That is,

$$\mathbf{Y} = \mathbf{X} + X_j\mathbf{e}_i - X_j\mathbf{e}_j \implies A_k^{\mathbf{Y}} = A_k^{\mathbf{X}} \text{ for } k \neq i, j,$$

where $\mathbf{e}_k$ is the unit vector along the $k$-th axis.

- Merging or splitting the risks of some agents will not affect allocation of uninvolved agents
  - Such an operation does not need to be disclosed
  - Two agents may be two accounts of same person or family

# Axiomatic characterization of CMRS

# Axiomatic characterization of CMRS

**Theorem 1**

*Assume $\mathcal{X} = L^1$ or $L^1_+$. A risk sharing rule satisfies Axioms AF, RF, RA and OA if and only if it is CMRS.*

- First result of axiomatic characterization of risk sharing rules
- First axiomatic foundation of CMRS
  - CMRS is popular in many contexts: Landsberger/Meilijson'94; Denuit/Dhaene'12; Denuit/Robert'21; Feng/Liu/Zhang'22, ...

# A new characterization of conditional expectation

## Theorem 2

*For a random variable $S$ on $(\Omega, \mathcal{F}, \mathbb{P})$ and $\mathcal{G} = \sigma(S)$, let $\phi : L^1(\Omega, \mathcal{F}, \mathbb{P}) \to L^1(\Omega, \mathcal{G}, \mathbb{P})$. The equality $\phi(X) = \mathbb{E}[X|S]$ holds for all $X \in L^1(\Omega, \mathcal{F}, \mathbb{P})$ if and only if $\phi$ satisfies the following properties:*

(a) $\phi(t) = t$ *for all* $t \in \mathbb{R}$;

(b) $\phi(X + Y) = \phi(X) + \phi(Y)$ *for all* $X, Y$;

(c) $\phi(Y) \geq \phi(X)$ *if* $Y \geq X$;

(d) $\phi(S) = S$;

(e) $\mathbb{E}[\phi(X)] = \mathbb{E}[X]$ *for all* $X$.

# Independence of axioms

**Proposition 1**

*Axioms AF, RF, RA and OA are independent.*

- RF, RA and OA, but not AF: $\mathbf{A}^{\mathbf{X}}_{Q\text{-cm}} = \mathbb{E}^{Q}[\mathbf{X}|S^{\mathbf{X}}]$ for $Q \neq \mathbb{P}$
- AF, RA and OA, but not RF:

$$\mathbf{A}^{\mathbf{X}}_{\mathrm{ma}} = \left(S^{\mathbf{X}} - \mathbb{E}[S^{\mathbf{X}}], 0, \dots, 0\right) + \mathbb{E}[\mathbf{X}]$$

- AF, RF and OA, but not RA: $\mathbf{A}^{\mathbf{X}}_{\mathrm{id}} = \mathbf{X}$
- AF, RF and RA, but not OA:

$$\mathbf{A}^{\mathbf{X}} = \mathbf{A}^{\mathbf{X}}_{\mathrm{all}} \text{ if } \mathbf{X} \text{ is standard Gaussian and } \mathbf{A}^{\mathbf{X}} = \mathbf{A}^{\mathbf{X}}_{\mathrm{cm}} \text{ otherwise}$$

# Universal improvement

- Convex order $X \leq_{\mathrm{cx}} Y$: $\mathbb{E}[u(X)] \leq \mathbb{E}[u(Y)]$ for all convex $u$

**Property UI (Universal improvement)**

The allocation improves the initial risk in convex order. That is, $A_i^{\mathbf{X}} \leq_{\mathrm{cx}} X_i$ for all $i \in [n]$ and $\mathbf{X} \in \mathcal{X}^n$.

**Proposition 2**

*Property UI implies Axioms RF and AF.*

**Corollary 1**

*Assume $\mathcal{X} = L^1$ or $L^1_+$. A risk sharing rule satisfies Axioms RA and OA and Property UI if and only if it is CMRS.*

# Comonotonicity

## Properties CM, CP and ZP

- CM (Comonotonicity): For $\mathbf{X} \in \mathcal{X}^n$, $\mathbf{A}^{\mathbf{X}}$ is comonotonic.
- CP (Constant preserving): For $\mathbf{X} \in \mathcal{X}^n$ and $i \in [n]$, if $X_i = c \in \mathbb{R}$, then $A_i^{\mathbf{X}} = c$.
- ZP (Zero preserving): For $\mathbf{X} \in \mathcal{X}^n$ and $i \in [n]$, if $X_i = 0$, then $A_i^{\mathbf{X}} = 0$.

$$\text{UI} \implies \text{AF} + \text{RF} \implies \text{CP} \implies \text{ZP}; \qquad \text{CM} \implies \text{RA}.$$

## Proposition 3

*Assume $\mathcal{X} = L^1$. There is no risk sharing rule satisfying Axiom OA and Properties CM and ZP.*

# An example: Bitcoin mining pool

# An example: Bitcoin mining pool

Bitcoin mining pool for one block

- $n$ miners in a mining pool
- $P > 0$: (random) monetary value of the next block
- Initial risk vector $\mathbf{X} = P(\mathbb{1}_{D_1}, \dots, \mathbb{1}_{D_n})$ representing contributions
  - $D_i$: the event that miner $i$ issues the block
  - $D_1, \dots, D_n$ are disjoint; $D = \bigcup_{i=1}^n D_i$
  - $\mathbb{P}(D_i)$: the contribution (hashes tried) of miner $i$ divided by that of all miners in the world
- $\mathcal{B}_n = \{P(\mathbb{1}_{D_1}, \dots, \mathbb{1}_{D_n}) : D_1, \dots, D_n \subseteq \Omega \text{ disjoint and } \perp P\}$

# Bitcoin mining pool

A reward sharing rule is a mapping $\mathbf{A} : \mathcal{B}_n \to \mathcal{X}^n$ satisfying

- $\mathbf{A}^{\mathbf{X}} = \mathbb{A}_n(S^{\mathbf{X}})$ for each $\mathbf{X} \in \mathcal{B}_n$
- $A_i^{\mathbf{X}} = A_j^{\mathbf{X}}$ for $i, j \in [n]$ with $\mathbb{P}(D_i) = \mathbb{P}(D_j)$
    - The computational contributions $\mathbb{P}(D_1), \dots, \mathbb{P}(D_n)$ of each miner are used instead of the random events $D_1, \dots, D_n$

Interpretation of the axioms

- AF: no miner gets less (or more) than initial contribution in expectation
- RF: no negative reward ($A_i^{\mathbf{X}} \geq \inf X_i = 0$)
- RA: reward does not depend on who solved the block
- OA: safe against merging/Sybel attacks

# Rewarding sharing rule

## Proposition 3

Assume $P \in \mathcal{X} = L^1$ and $P > 0$. A reward sharing rule $\mathbf{A} : \mathcal{B}_n \to \mathcal{X}^n$ satisfies Axioms RA, RF, AF and OA if and only if it is specified by

$$A_i^{\mathbf{X}} = \frac{\mathbb{P}(D_i)}{\mathbb{P}(D)} P \mathbb{1}_D, \quad i \in [n], \ \mathbf{X} = P(\mathbb{1}_{D_1}, \dots, \mathbb{1}_{D_n}) \in \mathcal{B}_n, \tag{1}$$

which is CMRS (because $\mathbb{E}[P\mathbb{1}_{D_i} | P\mathbb{1}_D] = P\mathbb{1}_D \mathbb{P}(D_i)/\mathbb{P}(D)$).

- The axiomatic theory of Leshno/Strack'20 rationalizes the proportional (in probability) reward rule for home miners
- Our theory rationalizes the proportional (in monetary value) reward rule for pooled miners

# An example: A pool of three miner

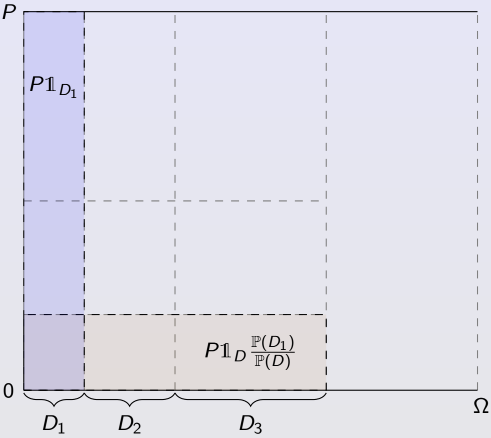



Figure: Purple: miner 1's payoff as a home miner; orange: miner 1's payoff in a pool of 3 miners

# Thank you

Thank you for your kind attention

https://arxiv.org/abs/2208.07533