Contextually Private Mechanisms

Andreas Haupt

MIT CSAIL

Zoë Hitzig

Harvard Society of Fellows

March 26, 2024

Motivation

In many settings, it is important that the mechanism designer does not learn "too much" about participants.

- Participants have privacy concerns?
- Designer has political worries or legal constraints?

Motivation

In many settings, it is important that the mechanism designer does not learn "too much" about participants.

- Participants have privacy concerns?
- Designer has political worries or legal constraints?

Motivation

In many settings, it is important that the mechanism designer does not learn "too much" about participants.

- Participants have privacy concerns?
- Designer has political worries or legal constraints?

Google's Alleged Scheme to Corner the Online Ad Market

A newly unredacted legal filing sheds light on internal programs that antitrust enforcers argue advantaged Google at the expense of advertisers and publishers.

Google induced advertisers to bid their true value, only to override pre-set AdX floors and … generate unique and custom per-buyer floors **depending on what a buyer had bid in the past.**

State of Texas v. Google

Motivation

In many settings, it is important that the mechanism designer does not learn "too much" about participants.

- Participants have privacy concerns?
- Designer has political worries or legal constraints?

> "In one extreme case, a firm that bid NZ$100,000 paid the second-highest bid of NZ$6… **Politically embarrassing** newspaper headlines resulted, as winners paid prices far below their bids… By revealing the high bidder's willingness to pay, the auction **exposed the government to criticism**, because after the auction everyone knew that the firm valued the license at more than it paid."
>
> **McMillan (1994)**

Motivation

In many settings, it is important that the mechanism designer does not learn "too much" about participants.

- Participants have privacy concerns?
- Designer has political worries or legal constraints?

- **"purpose limitation"**

  Personal data shall be collected for specified, explicit and legitimate purposes and **not further processed in a manner that is incompatible with those purposes**;

- **"data minimisation"**

  Personal data shall be adequate, relevant and **limited to what is necessary in relation to the purposes** for which they are processed;

EU GDPR Article 5(1)

Motivation

In many settings, it is important that the mechanism designer does not learn "too much" about participants.

- Participants have privacy concerns?
- Designer has political worries or legal constraints?

How much is "too much"?

In a **contextually private** mechanism, information revelation is justified by the choice rule.

Motivation

In many settings, it is important that the mechanism designer does not learn "too much" about participants.

- Participants have privacy concerns?
- Designer has political worries or legal constraints?

How much is "too much"?

In a **contextually private** mechanism, information revelation is justified by the choice rule.

Setting.

- Standard mechanism design environments, with and without transfers.
- Dynamic protocols for eliciting agents' reports.

Outline

1. **Definitions**

   Protocols, contextual privacy

2. **Fully contextually private choice rules**

   A necessary condition
   SPA is not contextually private

3. **Maximally contextually private protocols**

   Representation theorem: bi-monotonic protocols
   Maximally contextually private choice rules for SPA

4. **Brief discussion of other results**

   Settings without transfers, characterization for general protocols, incentives, variants.

Set Up

- $N < \infty$ agents
- Private information $\theta_i \in \Theta_i$, $|\Theta_i| < \infty$, profiles $\boldsymbol{\theta} \in \boldsymbol{\Theta}$
- Outcomes $x \in X$
- Preferences over outcomes $u_i : X \times \boldsymbol{\Theta} \to \mathbb{R}$
- Choice rule $\phi : \boldsymbol{\Theta} \to X$, deterministic

Set Up

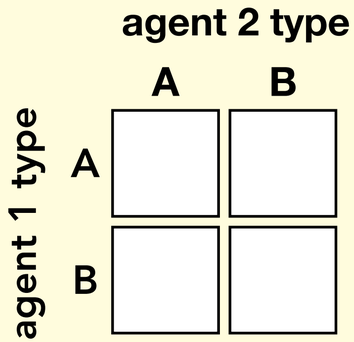
- $N < \infty$ agents
- Private information $\theta_i \in \Theta_i$, $|\Theta_i| < \infty$, profiles $\boldsymbol{\theta} \in \boldsymbol{\Theta}$
- Outcomes $x \in X$
- Preferences over outcomes $u_i : X \times \Theta \to \mathbb{R}$
- Choice rule $\phi : \boldsymbol{\Theta} \to X$, deterministic

The designer learns about the type space through a protocol.

Set Up

- $N < \infty$ agents
- Private information $\theta_i \in \Theta_i$, $|\Theta_i| < \infty$, profiles $\boldsymbol{\theta} \in \boldsymbol{\Theta}$
- Outcomes $x \in X$
- Preferences over outcomes $u_i : X \times \boldsymbol{\Theta} \to \mathbb{R}$
- Choice rule $\phi : \boldsymbol{\Theta} \to X$, deterministic

The designer learns about the type space through a protocol.



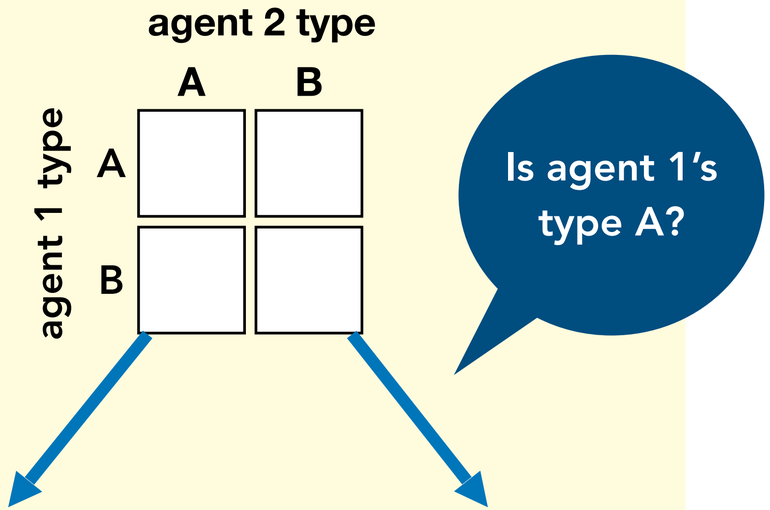
Example. A simple protocol.

- Two agents $N = \{1, 2\}$
- Binary type space $\boldsymbol{\Theta} = \{A, B\}^2$

Set Up

- $N < \infty$ agents
- Private information $\theta_i \in \Theta_i$, $|\Theta_i| < \infty$, profiles $\boldsymbol{\theta} \in \boldsymbol{\Theta}$
- Outcomes $x \in X$
- Preferences over outcomes $u_i : X \times \boldsymbol{\Theta} \to \mathbb{R}$
- Choice rule $\phi : \boldsymbol{\Theta} \to X$, deterministic

The designer learns about the type space through a protocol.



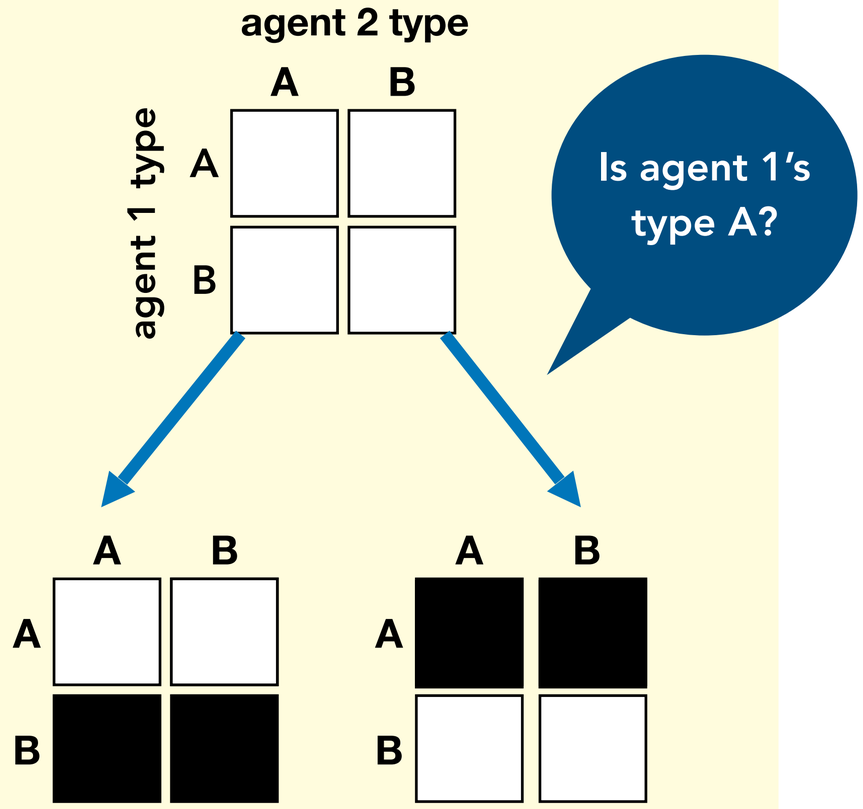
Example. A simple protocol.

- Two agents $N = \{1, 2\}$
- Binary type space $\boldsymbol{\Theta} = \{A, B\}^2$

Set Up

- $N < \infty$ agents
- Private information $\theta_i \in \Theta_i$, $|\Theta_i| < \infty$, profiles $\boldsymbol{\theta} \in \boldsymbol{\Theta}$
- Outcomes $x \in X$
- Preferences over outcomes $u_i : X \times \Theta \to \mathbb{R}$
- Choice rule $\phi : \boldsymbol{\Theta} \to X$, deterministic

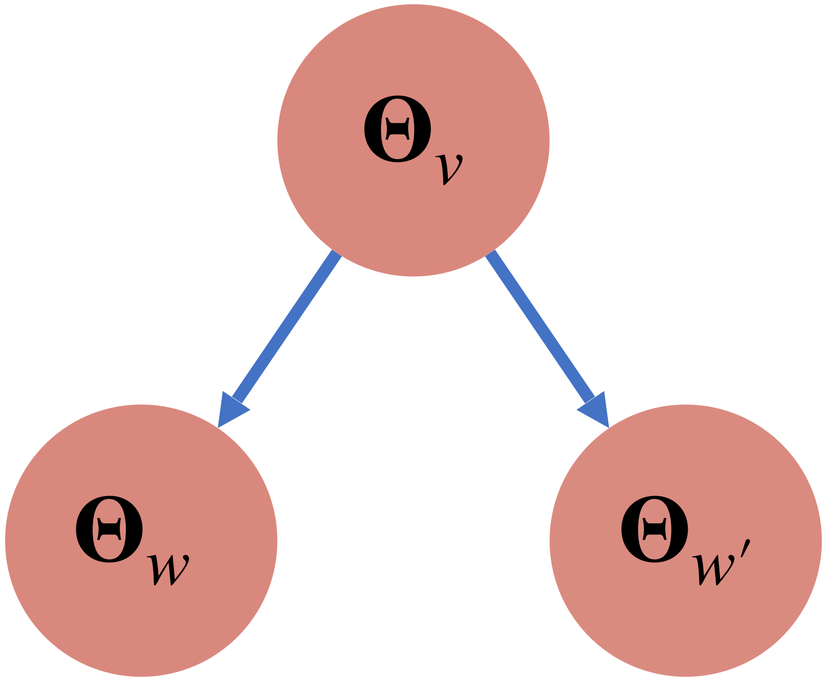
The designer learns about the type space through a protocol.



Example. A simple protocol.

- Two agents $N = \{1, 2\}$
- Binary type space $\boldsymbol{\Theta} = \{A, B\}^2$

Set Up



The designer learns about the type space through a protocol.

Set Up

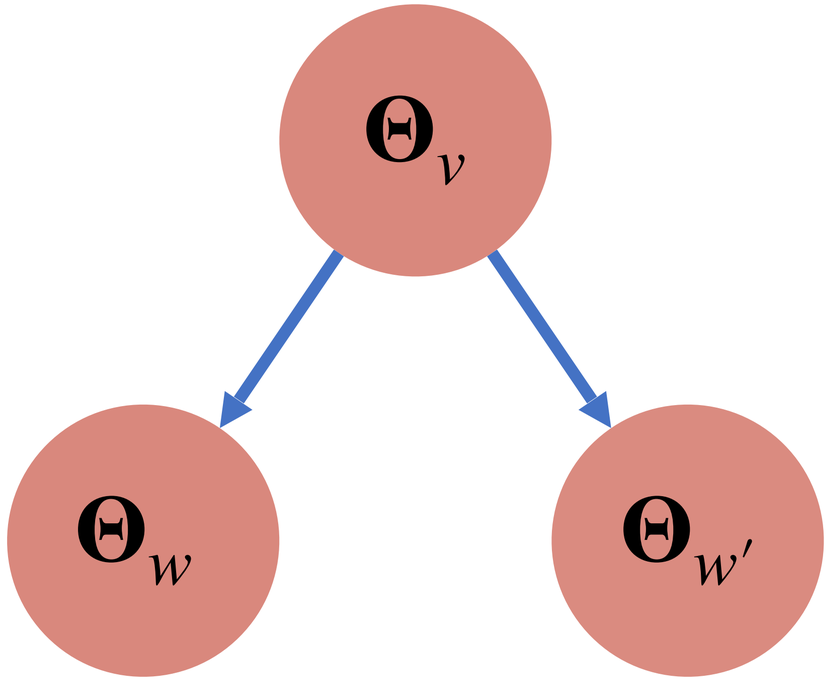
Definition.

A (direct) **protocol** is a directed rooted tree $P = (V, E, r)$ where each node v is labelled with a subset of the type space $\Theta_v \subseteq \Theta$ such that

$$\Theta_r = \Theta \quad \text{and} \quad \bigcup_{w:\,(v,w)\in E} \Theta_w = \Theta_v$$

At the root node all type profiles are possible.

The child nodes (w) form a partition of the parent node (v)



The designer learns about the type space through a protocol.

↪ indirect protocols

Set Up

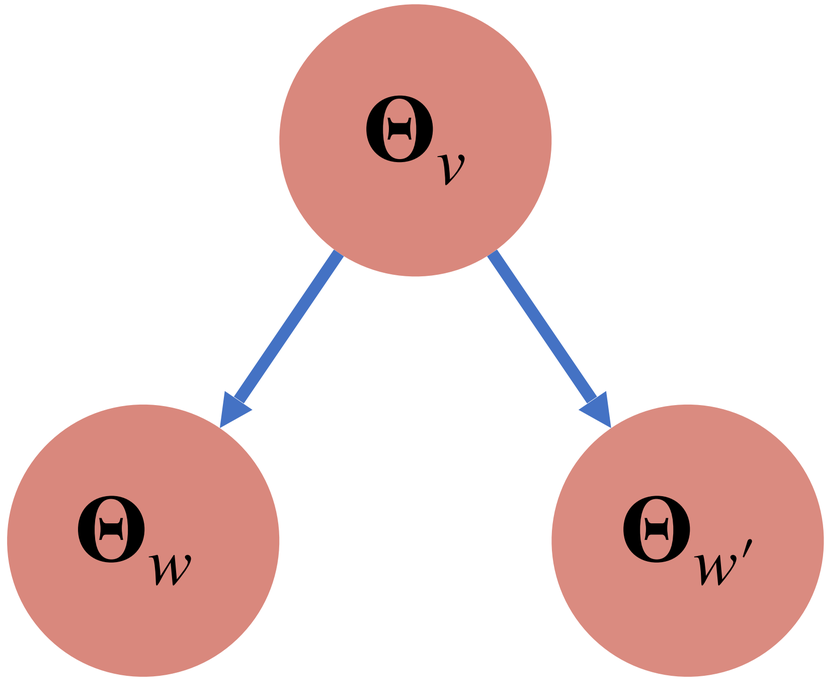
Definition.

A (direct) **protocol** is a directed rooted tree $P = (V, E, r)$ where each node v is labelled with a subset of the type space $\Theta_v \subseteq \Theta$ such that

$$\Theta_r = \Theta \quad \text{and} \quad \bigcup_{w:\,(v,w)\in E} \Theta_w = \Theta_v$$

At the root node all type profiles are possible.

The child nodes (w) form a partition of the parent node (v)



P is a **protocol for choice rule ϕ** if the terminal nodes of P yield enough information to compute the choice rule.

↪ indirect protocols

Set Up

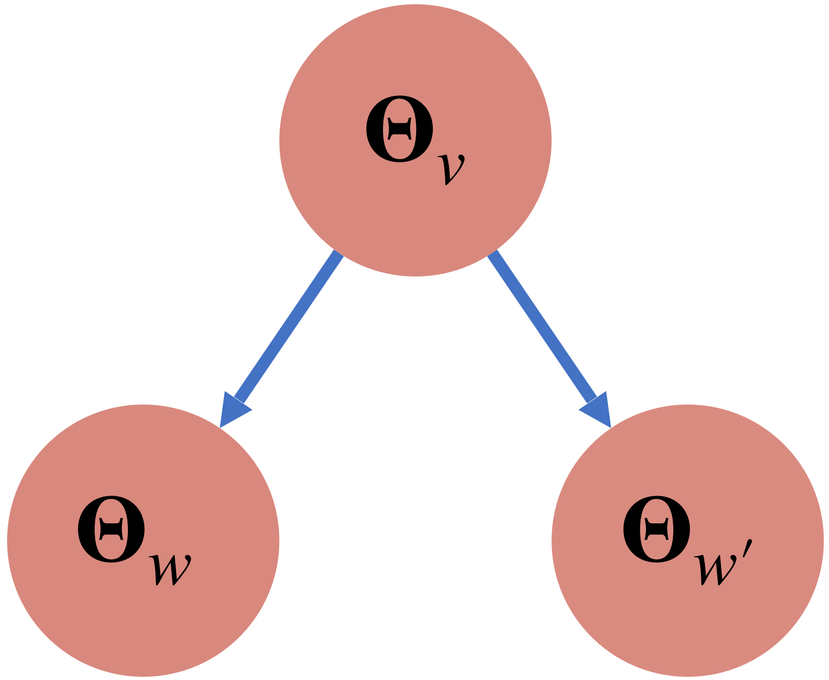
Definition.

A (direct) **protocol** is a directed rooted tree $P = (V, E, r)$ where each node v is labelled with a subset of the type space $\Theta_v \subseteq \Theta$ such that

$$\Theta_r = \Theta \quad \text{and} \quad \bigcup_{w:\,(v,w)\in E} \Theta_w = \Theta_v$$

At the root node all type profiles are possible.

The child nodes (w) form a partition of the parent node (v)



P is a **protocol for choice rule ϕ** if ϕ is measurable with respect to the partition induced by the terminal nodes of P.

↪ indirect protocols

DEFINITIONS

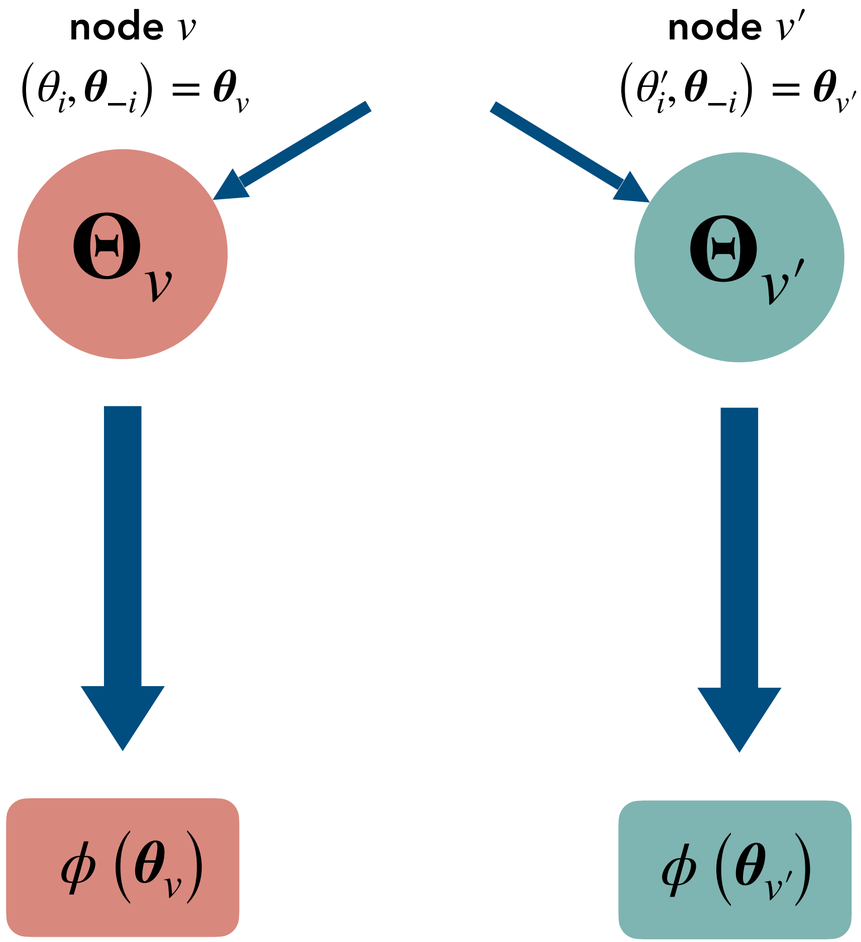
Definition.

There is a **contextual privacy violation** for agent i at profile $\boldsymbol{\theta} = (\theta_i, \boldsymbol{\theta}_{-i})$ under protocol P for choice rule ϕ if there exists a type θ_i' such that

$$(\theta_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_v \in \boldsymbol{\Theta}_v \,, \;\; (\theta_i', \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_{v'} \in \boldsymbol{\Theta}_{v'}$$

but

$$\phi(\boldsymbol{\theta}_v) = \phi(\boldsymbol{\theta}_{v'}).$$



DEFINITIONS

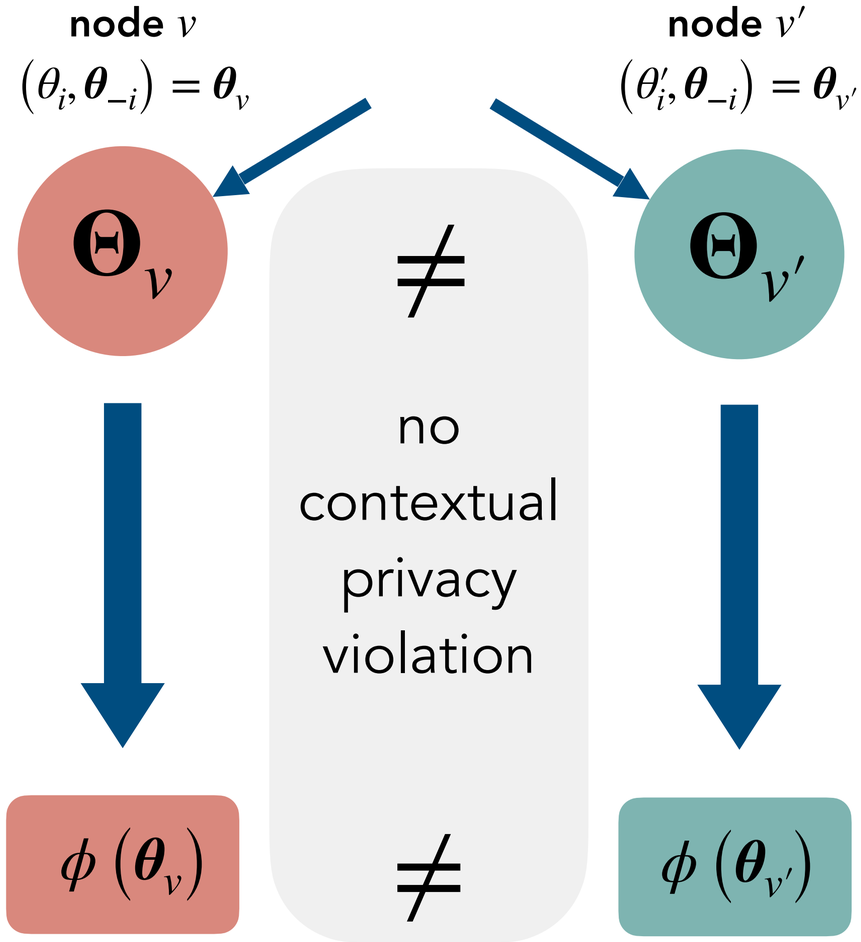
Definition.

There is a **contextual privacy violation** for agent i at profile $\boldsymbol{\theta} = (\theta_i, \boldsymbol{\theta}_{-i})$ under protocol P for choice rule ϕ if there exists a type θ_i' such that

$$(\theta_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_v \in \boldsymbol{\Theta}_v \,, \;\; (\theta_i', \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_{v'} \in \boldsymbol{\Theta}_{v'}$$

but

$$\phi(\boldsymbol{\theta}_v) = \phi(\boldsymbol{\theta}_{v'}).$$



DEFINITIONS

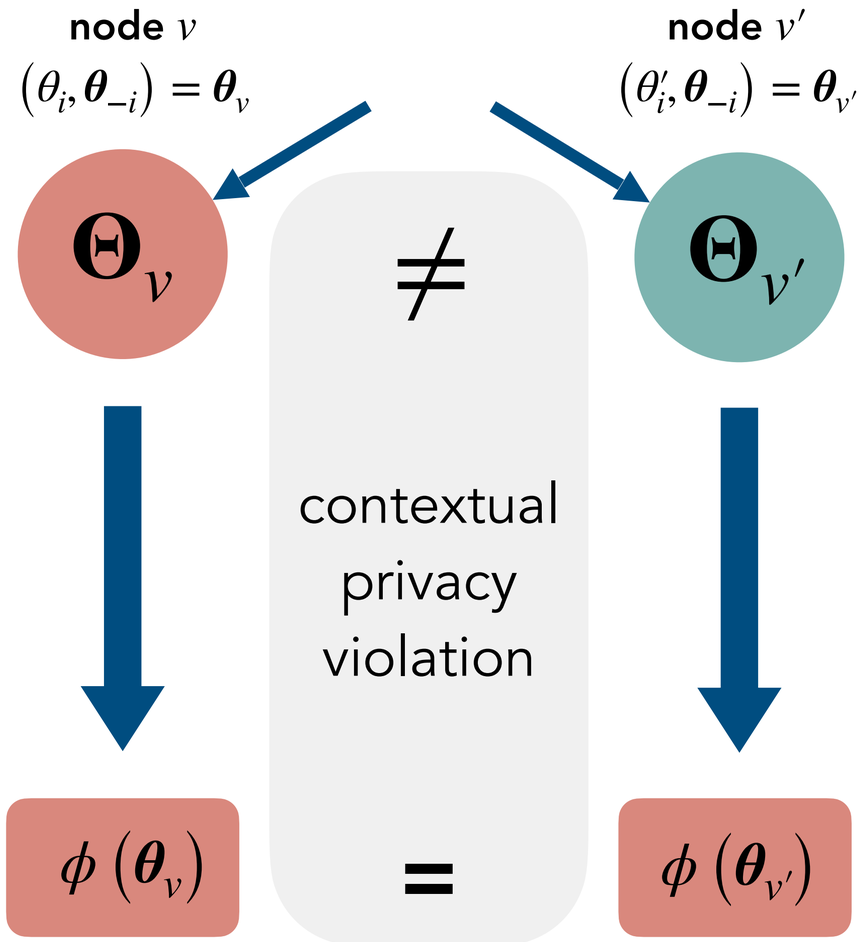
Definition.

There is a **contextual privacy violation** for agent i at profile $\boldsymbol{\theta} = (\theta_i, \boldsymbol{\theta}_{-i})$ under protocol P for choice rule ϕ if there exists a type θ_i' such that

$$(\theta_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_v \in \boldsymbol{\Theta}_v \,, \;\; (\theta_i', \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_{v'} \in \boldsymbol{\Theta}_{v'}$$

but

$$\phi(\boldsymbol{\theta}_v) = \phi(\boldsymbol{\theta}_{v'}).$$



Definitions

Definition.

There is a **contextual privacy violation** for agent i at profile $\boldsymbol{\theta} = (\theta_i, \boldsymbol{\theta}_{-i})$ under protocol P for choice rule ϕ if there exists a type θ_i' such that

$$(\theta_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_v \in \boldsymbol{\Theta}_v \text{ , } (\theta_i', \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_{v'} \in \boldsymbol{\Theta}_{v'}$$

but

$$\phi(\boldsymbol{\theta}_v) = \phi(\boldsymbol{\theta}_{v'}).$$

Why contextual privacy?

1. **Privacy preservation.**
   Agents give up their private information for a reason.
2. **Obliviousness preservation.**
   Designer learns nothing more than what is contained in the outcome.

Definitions

Definition.

There is a **contextual privacy violation** for agent i at profile $\boldsymbol{\theta} = (\theta_i, \boldsymbol{\theta}_{-i})$ under protocol P for choice rule ϕ if there exists a type θ_i' such that

$$(\theta_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_v \in \boldsymbol{\Theta}_v \,, \;\; (\theta_i', \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_{v'} \in \boldsymbol{\Theta}_{v'}$$

but

$$\phi(\boldsymbol{\theta}_v) = \phi(\boldsymbol{\theta}_{v'}).$$

Why contextual privacy?

1. **Privacy preservation.**
   Agents give up their private information for a reason.
2. **Obliviousness preservation.**
   Designer learns nothing more than what is contained in the outcome.

Toward a statistical privacy-implementation frontier:

if designer distinguishes types **at all**

it should make **some** difference.

Definitions

Definition.

There is a **contextual privacy violation** for agent i at profile $\boldsymbol{\theta} = (\theta_i, \boldsymbol{\theta}_{-i})$ under protocol P for choice rule ϕ if there exists a type θ_i' such that

$$(\theta_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_v \in \boldsymbol{\Theta}_v \text{ , } (\theta_i', \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_{v'} \in \boldsymbol{\Theta}_{v'}$$

but

$$\phi(\boldsymbol{\theta}_v) = \phi(\boldsymbol{\theta}_{v'}).$$

Why contextual privacy?

1. **Privacy preservation.**
   Agents give up their private information for a reason.
2. **Obliviousness preservation.**
   Designer learns nothing more than what is contained in the outcome.

Toward a statistical privacy-implementation frontier:

if designer distinguishes types **by x amount**

it should make **y amount** of difference.

Definitions

Definition.

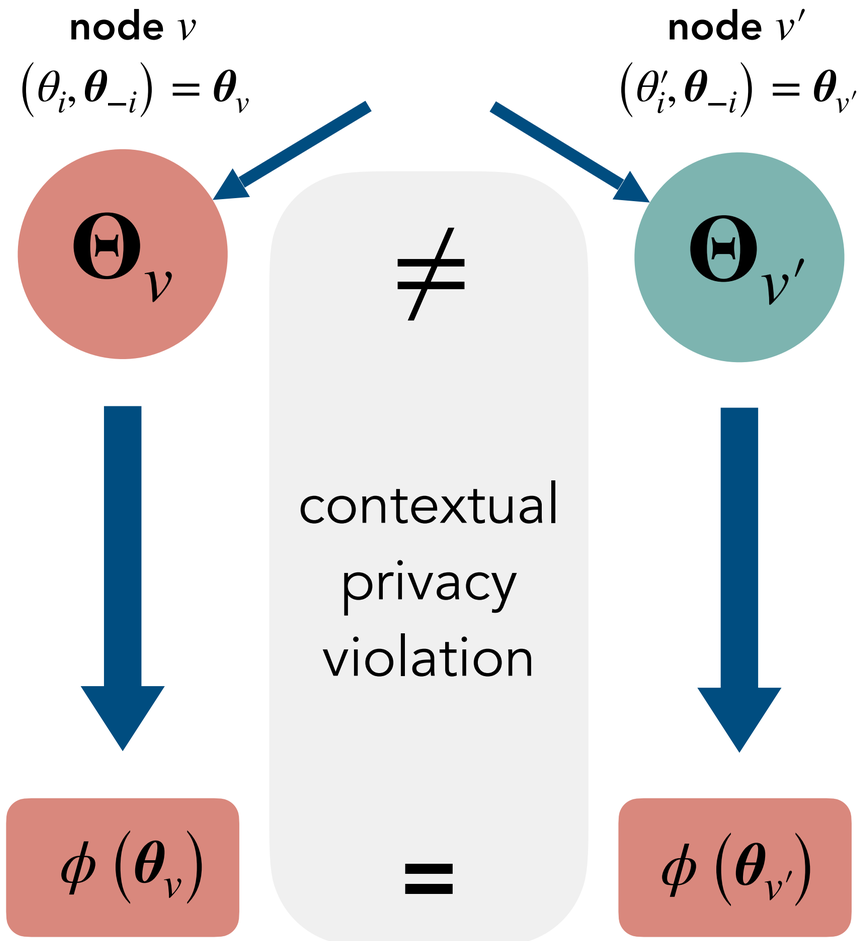
There is a **contextual privacy violation** for agent i at profile $\boldsymbol{\theta} = (\theta_i, \boldsymbol{\theta}_{-i})$ under protocol P for choice rule ϕ if there exists a type θ_i' such that

$$(\theta_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_v \in \boldsymbol{\Theta}_v \text{ , } (\theta_i', \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_{v'} \in \boldsymbol{\Theta}_{v'}$$

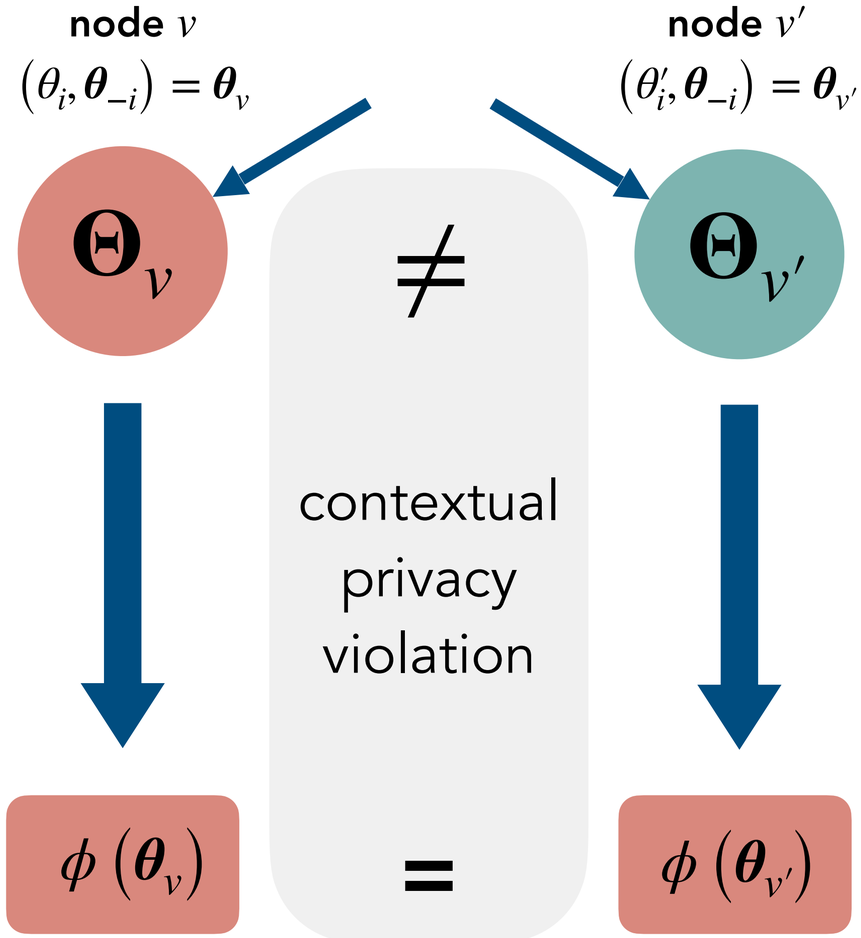
but

$$\phi(\boldsymbol{\theta}_v) = \phi(\boldsymbol{\theta}_{v'}).$$

Denote the **set of contextual privacy violations** produced by P for ϕ, $\Gamma(P, \phi) \subseteq N \times \boldsymbol{\Theta}$.



DEFINITIONS



Denote the **set of contextual privacy violations** produced by P for ϕ, $\Gamma(P, \phi) \subseteq N \times \boldsymbol{\Theta}$.

Definitions

Definition.

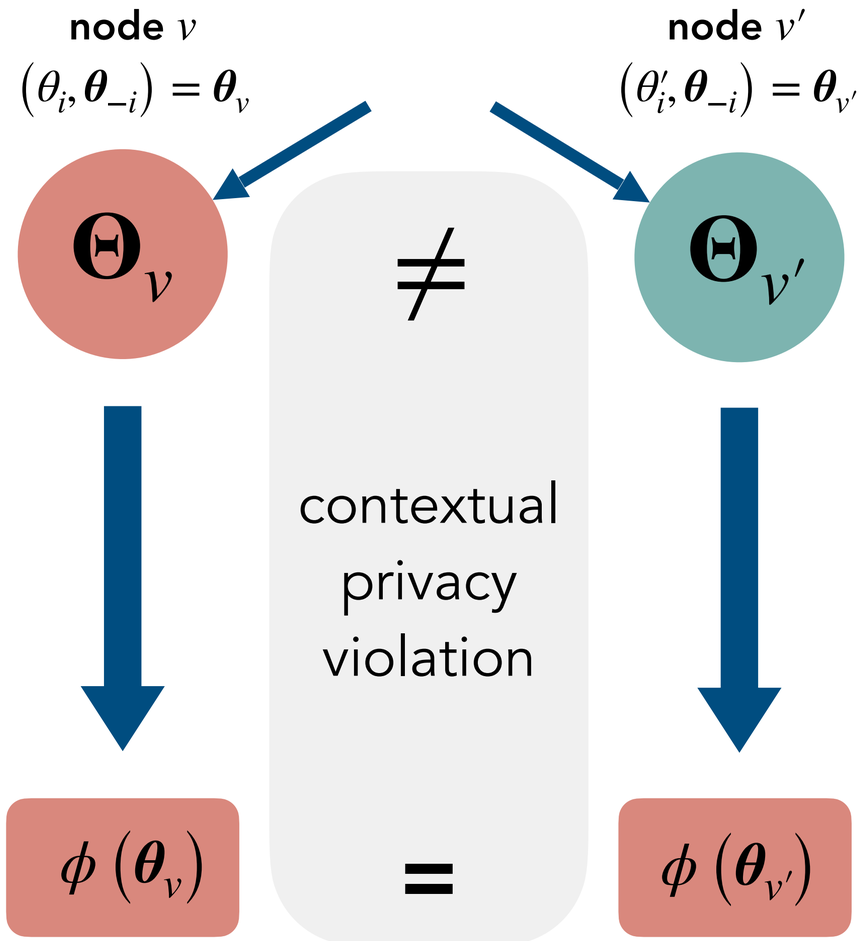
A protocol P for choice rule ϕ is **at least as contextually private** as protocol P' if

$$\Gamma(P, \phi) \subseteq \Gamma(P', \phi).$$

A protocol P is **contextual-privacy equivalent** to P′ if

$$\Gamma(P, \phi) \subseteq \Gamma(P', \phi) \text{ and } \Gamma(P', \phi) \subseteq \Gamma(P, \phi).$$

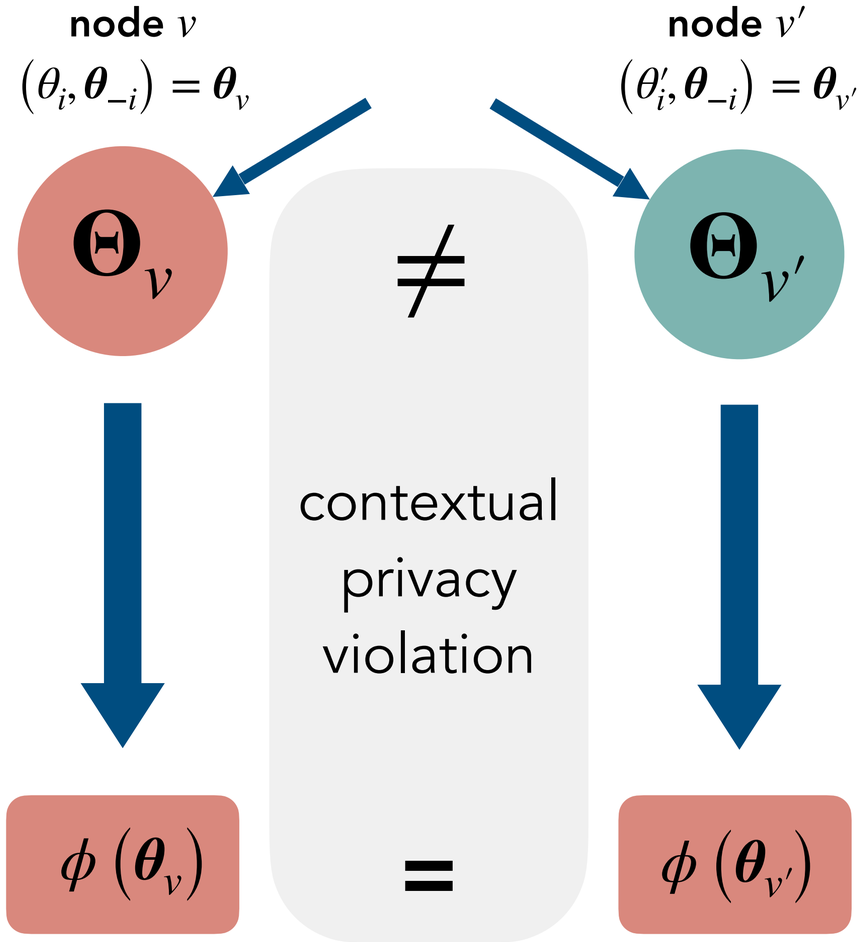
Denote the **set of contextual privacy violations** produced by P for ϕ, $\Gamma(P, \phi) \subseteq N \times \Theta$.



DEFINITIONS

Definition.

A protocol P for choice rule ϕ is **maximally contextually private** if there is no "admissible" protocol P' that is weakly more contextually private.



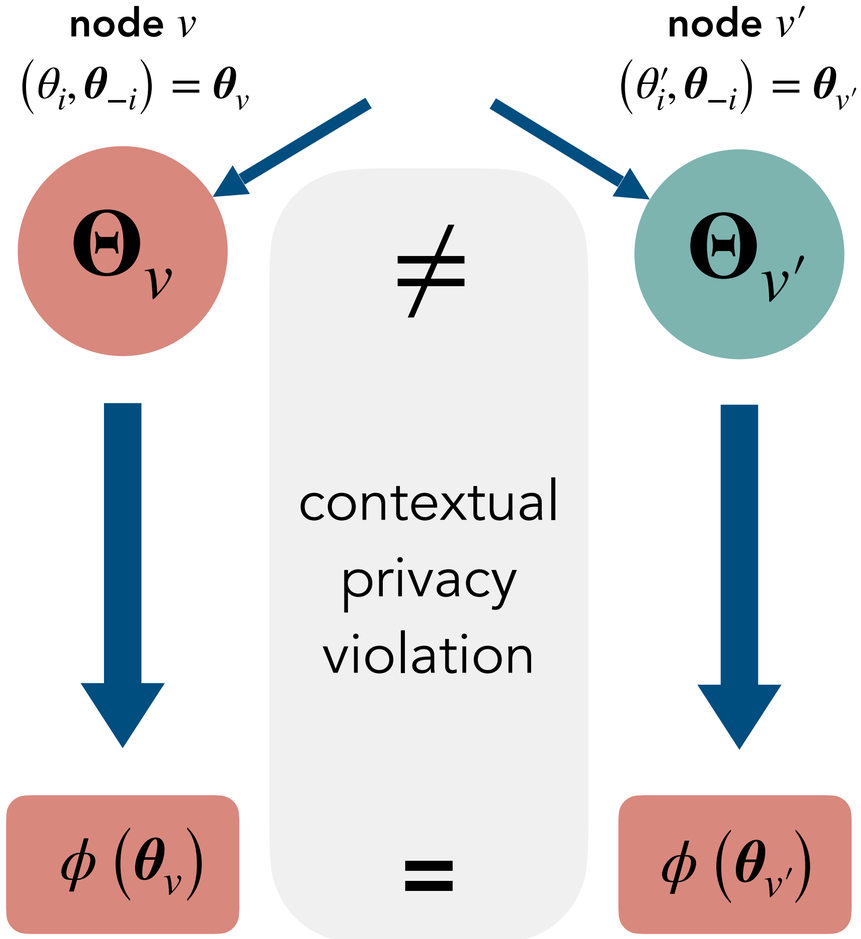
Definitions

Definition.

A protocol P for choice rule ϕ is **maximally contextually private** if there is no "admissible" protocol P' that is weakly more contextually private.

Definition.

A **choice rule ϕ is fully contextually private** if there is an "admissible" protocol P for ϕ that produces no violations.



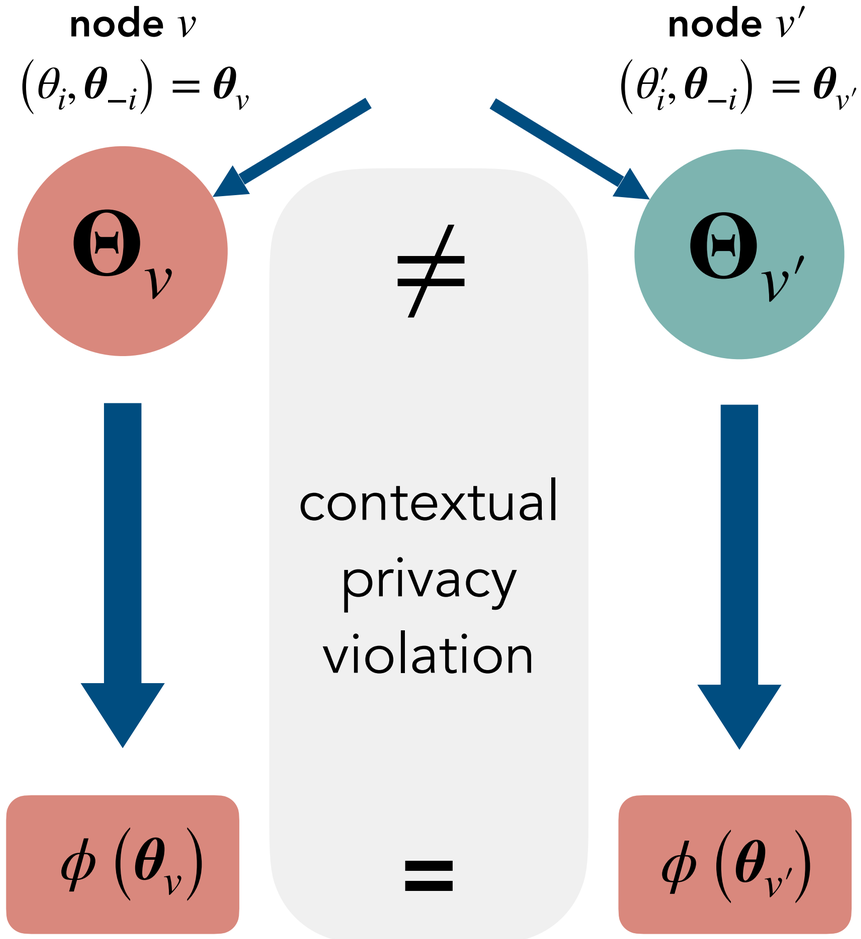
Definitions

Definition.

A protocol P for choice rule ϕ is **maximally contextually private** if there is no **admissible** protocol P' that is weakly more contextually private.

Definition.

A **choice rule ϕ is fully contextually private** if there is an **admissible** protocol P for ϕ that produces no violations.



Which protocols are admissible?

How does the designer physically elicit agents' reports?

ask agents for
one-time reports?

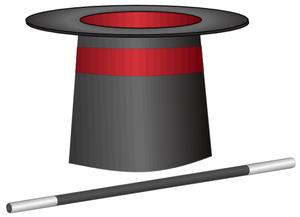
Definition.

A **choice rule ϕ is fully contextually private** if there is an **admissible** protocol P for ϕ that produces no violations.

Which protocols are admissible?

How does the designer physically elicit agents' reports?

ask agents for
one-time reports?



use a magic box?

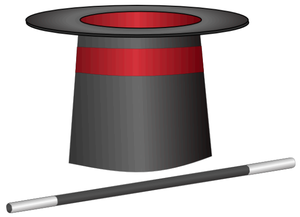
Definition.

A **choice rule ϕ is fully contextually private** if there is an **admissible** protocol P for ϕ that produces no violations.

Which protocols are admissible?

How does the designer physically elicit agents' reports?

ask agents for
one-time reports?



use a magic box?

ask agents for
sequence of reports?

Definition.

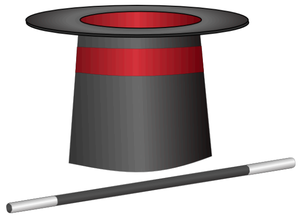
A **choice rule ϕ is fully contextually private** if there is an **admissible** protocol P for ϕ that produces no violations.

DEFINITIONS

Which protocols are admissible?

How does the designer physically elicit agents' reports?

ask agents for one-time reports?



use a magic box?

ask agents for sequence of reports?

Definition.

A **choice rule ϕ is fully contextually private** if there is an **admissible** protocol P for ϕ that produces no violations.

The set of admissible protocols depends on the environment.

1. In the paper: **general results** for an arbitrary fixed class of admissible protocols.

2. Today: a restrictive class of admissible protocols that makes a **minimal assumption.**

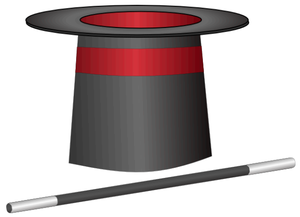
The designer knows something if and only if the agent said it.

DEFINITIONS

Which protocols are admissible?

How does the designer physically elicit agents' reports?

ask agents for one-time reports?



use a magic box?

ask agents for sequence of reports?

The set of admissible protocols depends on the environment.

1. In the paper: **general results** for an arbitrary fixed class of admissible protocols.

2. Today: a restrictive class of admissible protocols that makes a **minimal assumption.**

The designer knows something if and only if the agent said it.

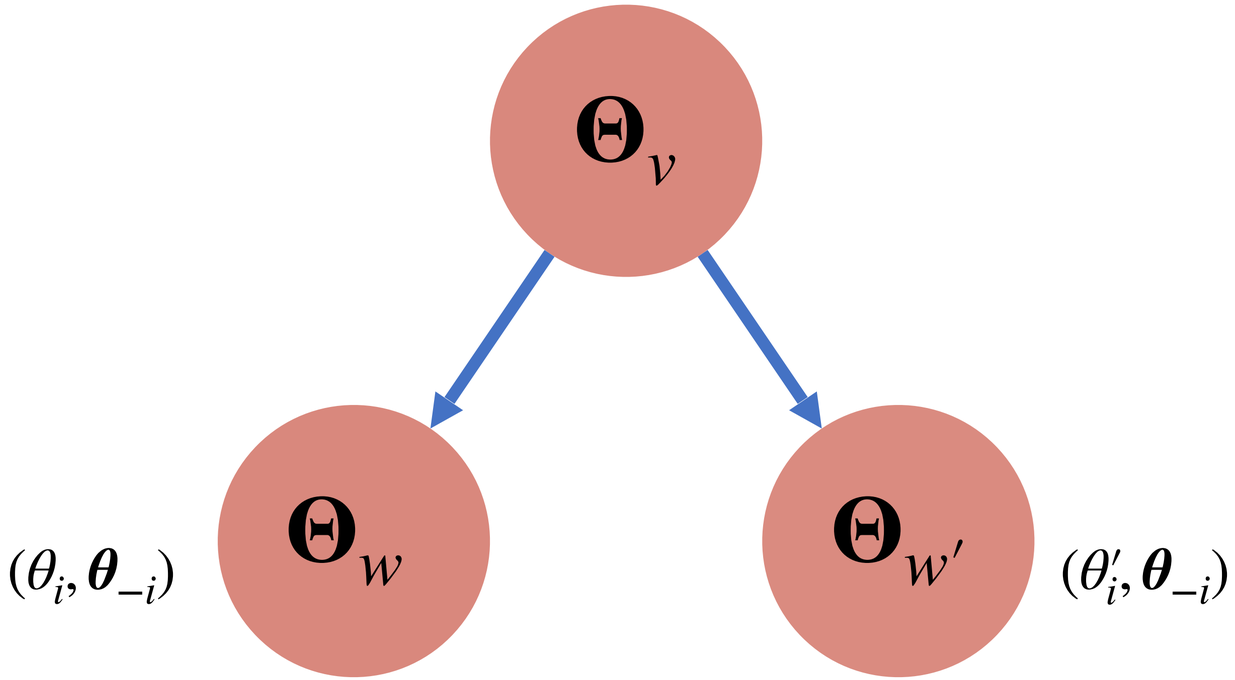
Definition.

A **choice rule ϕ is fully contextually private** if there is an admissible protocol P for ϕ that produces no violations.

This Talk: Restriction on Trusted Protocols

Definition.

A protocol P is **a sequential elicitation protocol** if for all $(v, w), (v, w') \in E$, there is at most one agent i such that $(\theta_i, \boldsymbol{\theta}_{-i}) \in \boldsymbol{\Theta}_w$ and $(\theta_i', \boldsymbol{\theta}_{-i}) \in \boldsymbol{\Theta}_{w'}$.



The set of admissible protocols depends on the environment.

1. In the paper: **general results** for an arbitrary fixed class of admissible protocols.

2. Today: a restrictive class of admissible protocols that makes a **minimal assumption.**

The designer knows something if and only if the agent said it.

Related Literature

Unconditional privacy.

Chor and Kushilevitz (1989), Chor, Gerèb-Graus and Kushilevitz (1994), Ausubel (2004), Brandt (2006), Brandt and Sandholm (2005, 2008), Milgrom and Segal (2020).

We bring unconditional privacy into mechanism design; study settings with and without transfers; study a more general class of protocols.

Auditability, simplicity and credibility.

Li (2017), Akbarpour and Li (2020), Hakimov and Raghavan (2022), Pycia and Ünver (2022), Mackenzie and Zhou (2022), Pycia and Troyan (2023), Grigoryan and Möller (2023).

We introduce an axiom and an order based on how much superfluous information is revealed to the designer.

Communication requirements.

Kushilevitz and Nisan (1997), Nisan and Segal (2006), Segal (2007), Blumrosen, Nisan and Segal (2007), Gonczarowski et al. (2019).

We focus on minimizing superfluous information disclosure whereas these approaches focus on minimizing the number of "bits" communicated.

Related Literature

Unconditional privacy.

Chor and Kushilevitz (1989), Chor, Gerèb-Graus and Kushilevitz (1994), Ausubel (2004), Brandt (2006), Brandt and Sandholm (2005, 2008), Milgrom and Segal (2020).

We bring unconditional privacy into mechanism design; study settings with and without transfers; study a more general class of protocols.

Auditability, simplicity and credibility.

Li (2017), Akbarpour and Li (2020), Hakimov and Raghavan (2022), Pycia and Ünver (2022), Mackenzie and Zhou (2022), Pycia and Troyan (2023), Grigoryan and Möller (2023).

We introduce an axiom and an order based on how much superfluous information is revealed to the designer.

Communication requirements.

Kushilevitz and Nisan (1997), Nisan and Segal (2006), Segal (2007), Blumrosen, Nisan and Segal (2007), Gonczarowski et al. (2019).

We focus on minimizing superfluous information disclosure whereas these approaches focus on minimizing the number of "bits" communicated.

Other approaches to privacy.

Our criterion is sensitive to context: It is…

1. not just about whether or how much info revealed, but how the info revealed is used.

Bayesian privacy.

Eilat, Eliaz and Mu (2021).

Differential privacy.

Dwork (2006), Pai and Roth (2013).

2. agnostic about set of admissible protocols.

Secure multi-party computation.

Bogetoft et al. (2009).

Zero-knowledge proofs.

Canetti, Fiat and Gonczarowski (2023).

Outline

1. **Definitions**

   Protocols, contextual privacy

2. **Fully contextually private choice rules**

   A necessary condition
   SPA is not contextually private

3. **Maximally contextually private protocols**

   Representation theorem: bi-monotonic protocols
   Maximally contextually private choice rules for SPA

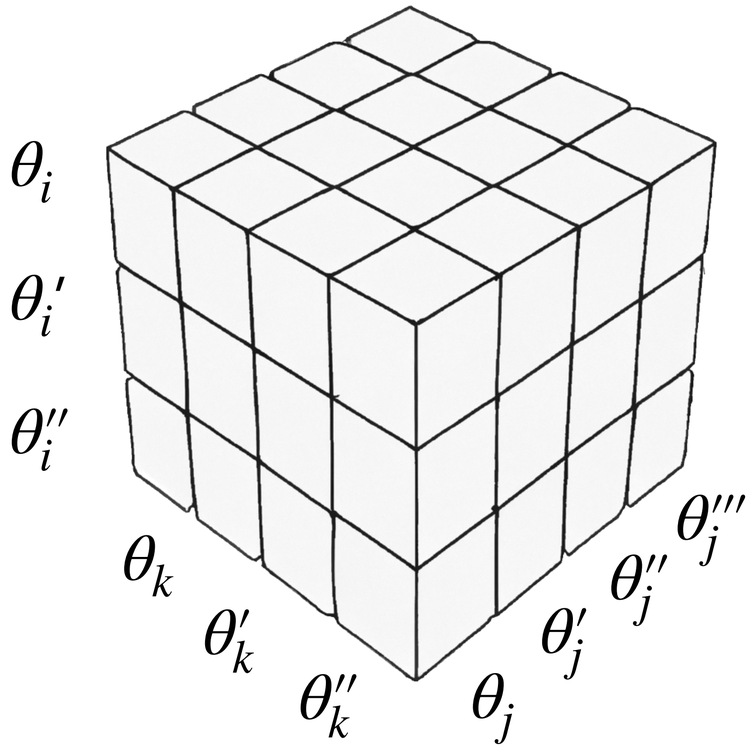
4. **Brief discussion of other results**

   Settings without transfers, characterization for general protocols, incentives, variants.

A Necessary Condition for Contextual Privacy

Consider a Θ^n matrix in which:

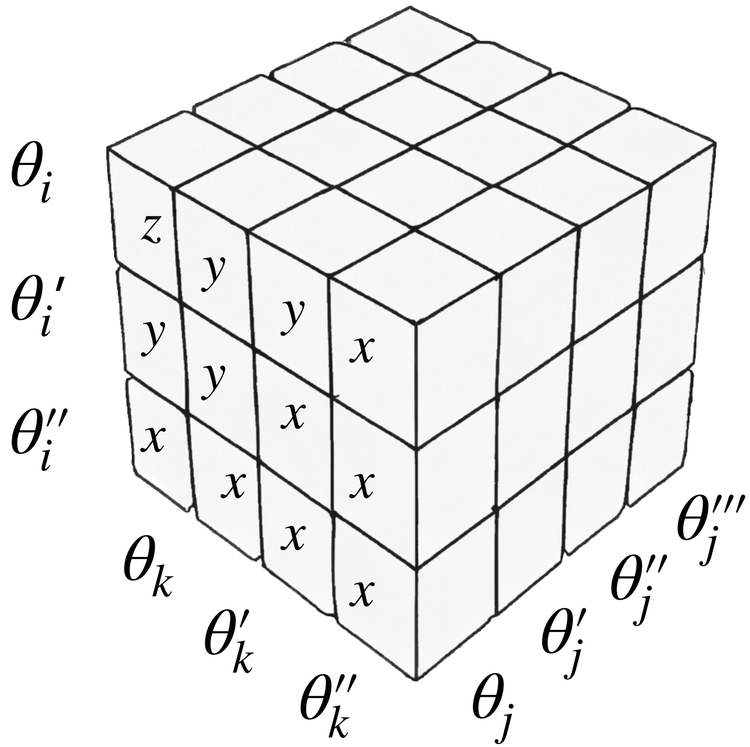
- rows are labelled with possible agent types
- entries correspond to the outcome $\phi(\boldsymbol{\theta})$
- rows labels need not be ordered



A Necessary Condition for Contextual Privacy

Consider a Θ^n matrix in which:

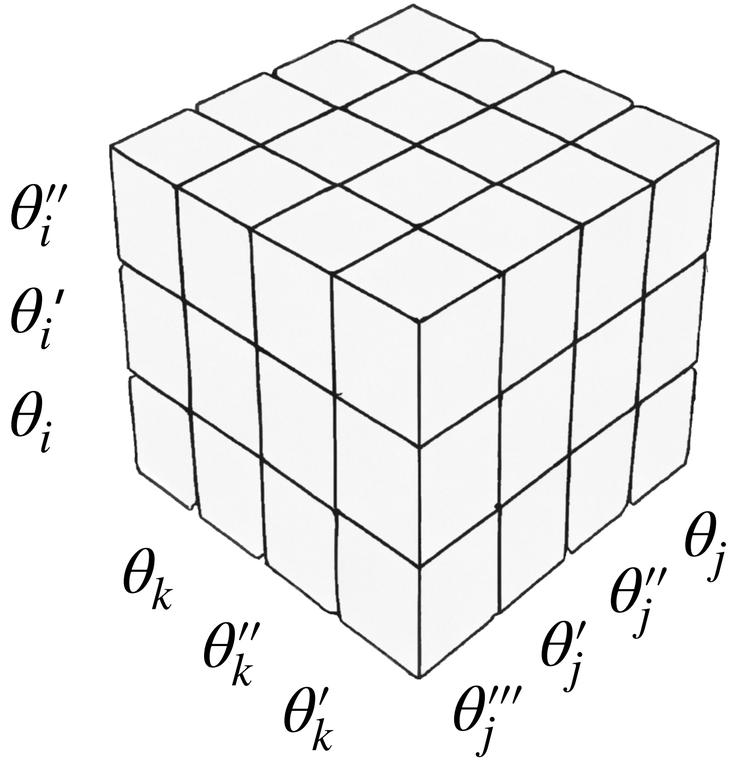
- rows are labelled with possible agent types
- entries correspond to the outcome $\phi(\boldsymbol{\theta})$
- rows labels need not be ordered



A Necessary Condition for Contextual Privacy

Consider a Θ^n matrix in which:

- rows are labelled with possible agent types
- entries correspond to the outcome $\phi(\boldsymbol{\theta})$
- rows labels need not be ordered

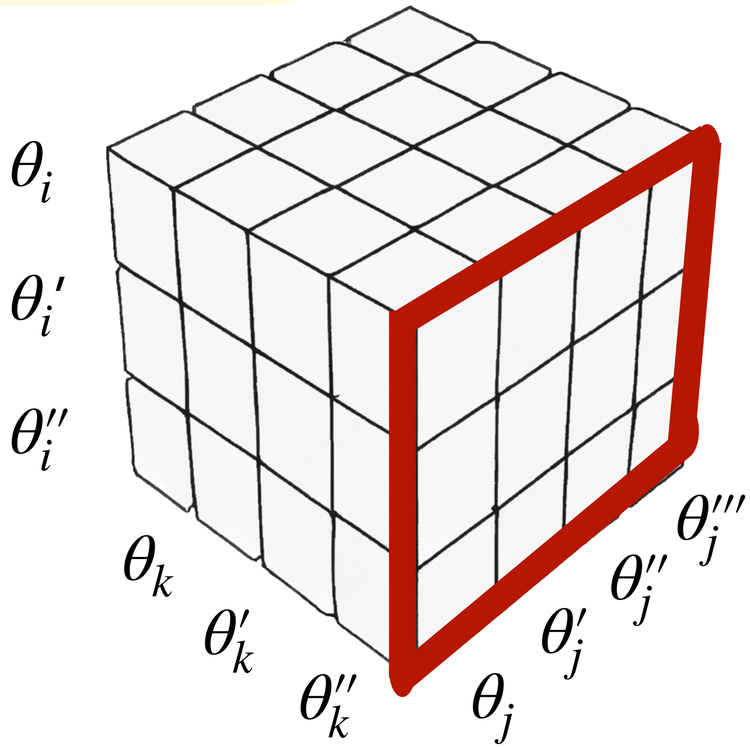


A Necessary Condition for Contextual Privacy

We will state our next result entirely "local" properties of this matrix

Consider a Θ^n matrix in which:

- rows are labelled with possible agent types
- entries correspond to the outcome $\phi(\boldsymbol{\theta})$
- rows labels need not be ordered



Consider "local properties" of this matrix:

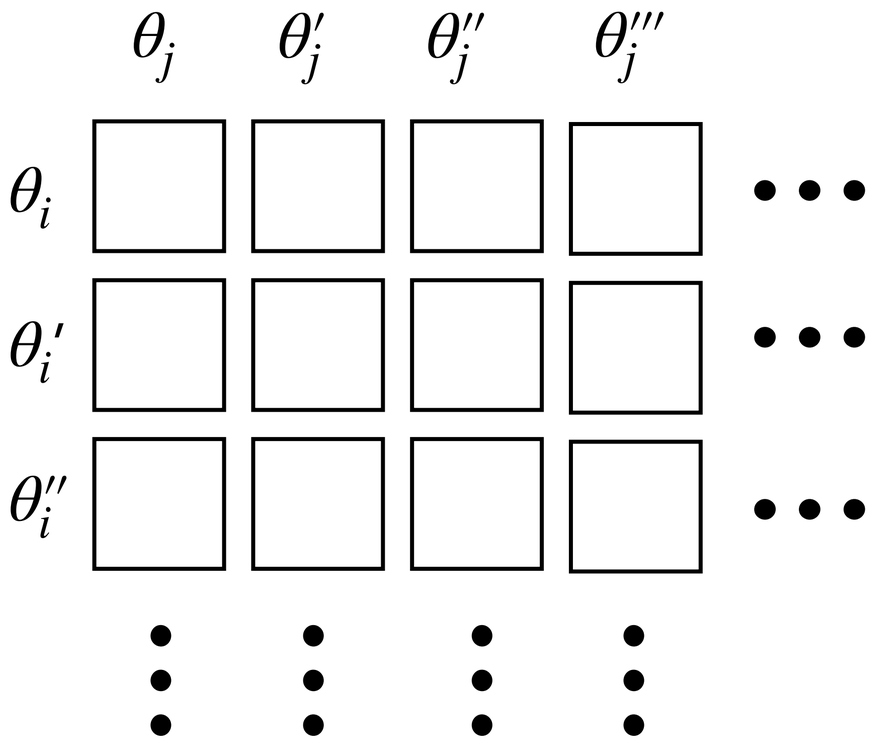
- hold fixed all types $\boldsymbol{\theta}_{-i,-j}$
- select a few types for agents i and j

A Necessary Condition for Contextual Privacy

We will state our next result entirely "local" properties of this matrix

Consider a Θ^n matrix in which:

- rows are labelled with possible agent types
- entries correspond to the outcome $\phi(\boldsymbol{\theta})$
- rows labels need not be ordered



Consider "local properties" of this matrix:

- hold fixed all types $\boldsymbol{\theta}_{-i,-j}$
- select a few types for agents i and j

A Necessary Condition for Contextual Privacy

Individual vs. Collective Pivotality ("Corners Lemma").

If a choice rule ϕ is contextually private, then for all "squares" in the type space,

if three "corners" lead to one outcome

then

the fourth "corner" must also lead to that outcome.

A Necessary Condition for Contextual Privacy

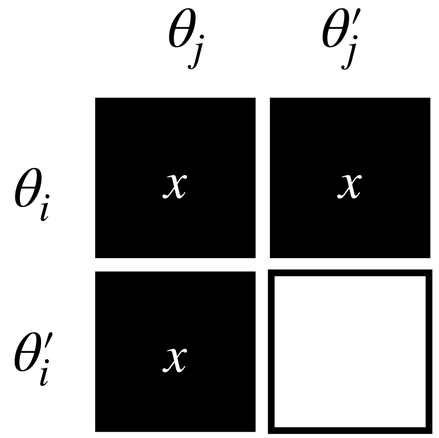
Individual vs. Collective Pivotality ("Corners Lemma").

If a choice rule ϕ is contextually private, then for all "squares" in the type space,

if three "corners" lead to one outcome

then

the fourth "corner" must also lead to that outcome.



A Necessary Condition for Contextual Privacy

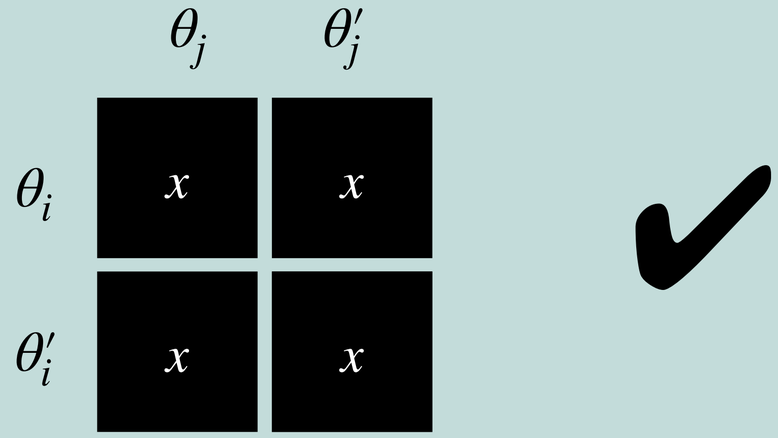
Individual vs. Collective Pivotality ("Corners Lemma").

If a choice rule ϕ is contextually private, then for all "squares" in the type space,

if three "corners" lead to one outcome

then

the fourth "corner" must also lead to that outcome.



A Necessary Condition for Contextual Privacy

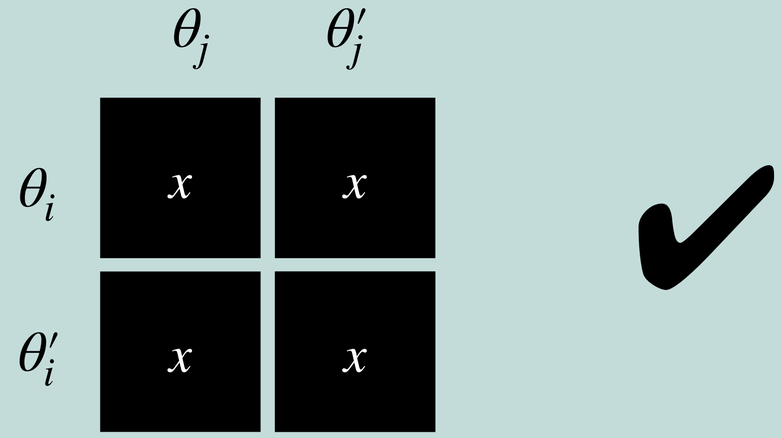
Individual vs. Collective Pivotality ("Corners Lemma").

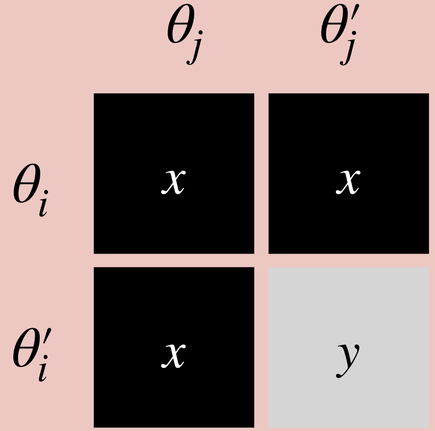
If a choice rule ϕ is contextually private, then for all "squares" in the type space,

if three "corners" lead to one outcome

then

the fourth "corner" must also lead to that outcome.





A Necessary Condition for Contextual Privacy

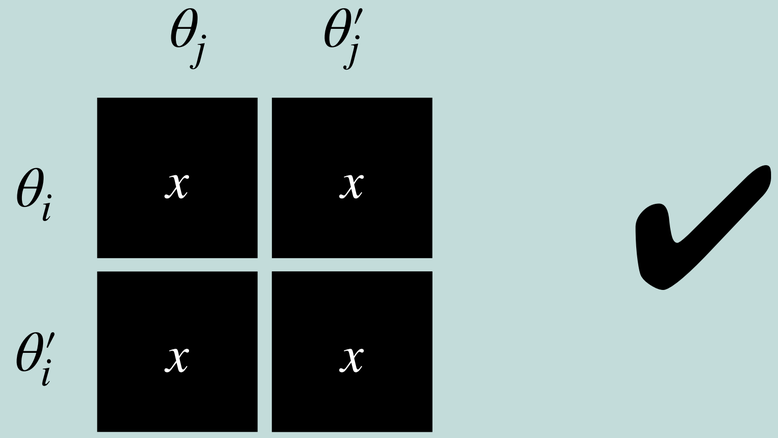
Individual vs. Collective Pivotality ("Corners Lemma").

If a choice rule ϕ is contextually private, then for all agents $i, j \in N$ and all types $\theta_i, \theta_i', \theta_j, \theta_j' \in \Theta$ and all profiles of other agents' types $\boldsymbol{\theta}_{-ij} \in \boldsymbol{\Theta}_{-ij}$,

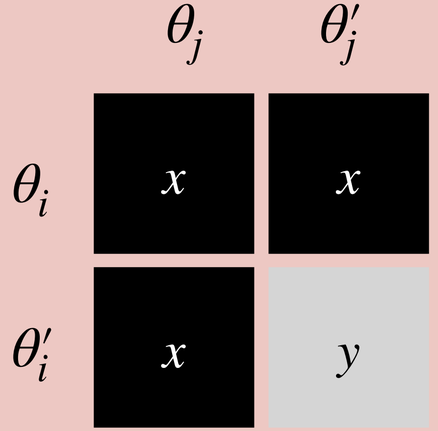
if three "corners" lead to one outcome

then

the fourth "corner" must also lead to that outcome.



✔



✗

A Necessary Condition for Contextual Privacy

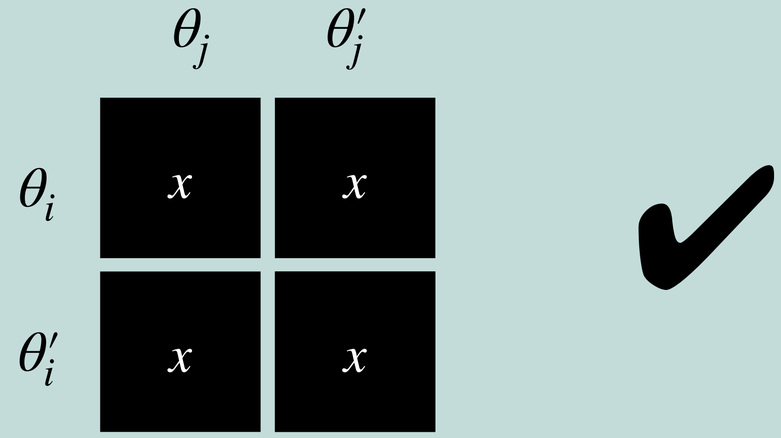
Individual vs. Collective Pivotality ("Corners Lemma").

If a choice rule ϕ is contextually private, then for all agents i, j and all types $\theta_i, \theta_i', \theta_j, \theta_j' \in \Theta$ and all profiles of other agents' types $\boldsymbol{\theta}_{-ij} \in \boldsymbol{\Theta}_{-ij}$,

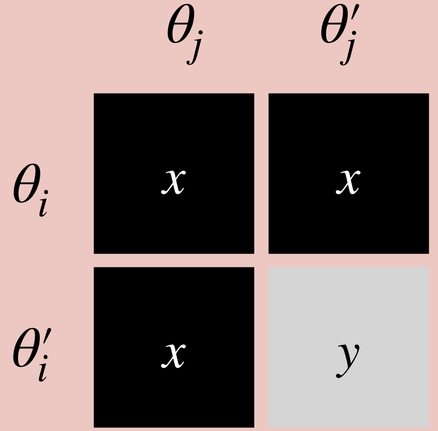
$$\phi(\theta_i, \theta_j, \boldsymbol{\theta}_{-ij}) = \phi(\theta_i', \theta_j, \boldsymbol{\theta}_{-ij}) = \phi(\theta_i, \theta_j', \boldsymbol{\theta}_{-ij}) = x$$

then

the fourth "corner" must also lead to that outcome.



✔



✗

A Necessary Condition for Contextual Privacy

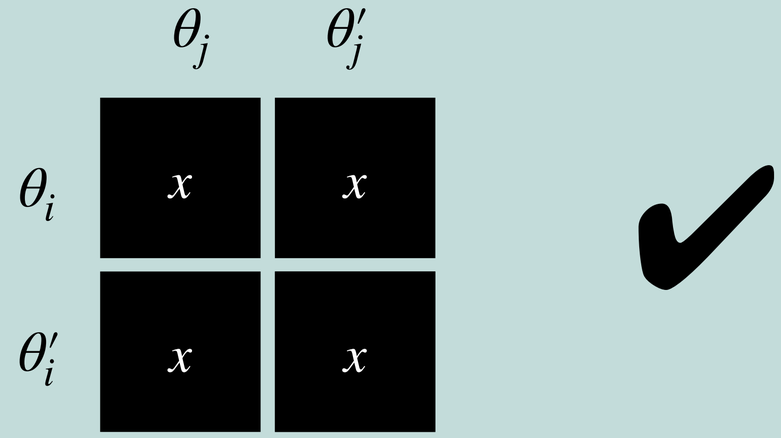
Individual vs. Collective Pivotality ("Corners Lemma").

If a choice rule ϕ is contextually private, then for all agents i, j and all types $\theta_i, \theta_i', \theta_j, \theta_j' \in \Theta$ and all profiles of other agents' types $\boldsymbol{\theta}_{-ij} \in \boldsymbol{\Theta}_{-ij}$,

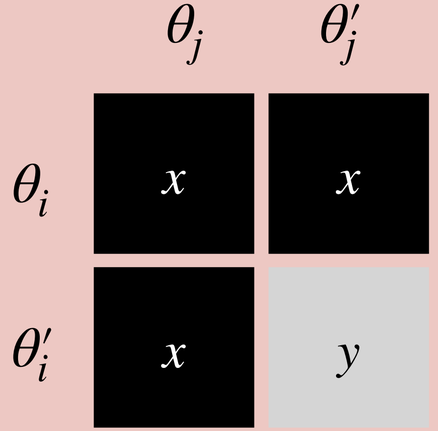
$$\phi(\theta_i, \theta_j, \boldsymbol{\theta}_{-ij}) = \phi(\theta_i', \theta_j, \boldsymbol{\theta}_{-ij}) = \phi(\theta_i, \theta_j', \boldsymbol{\theta}_{-ij}) = x$$

then

$$\phi(\theta_i', \theta_j', \boldsymbol{\theta}_{-ij}) = x.$$



✔



✗

A Necessary Condition for Contextual Privacy

Individual vs. Collective Pivotality ("Corners Lemma").

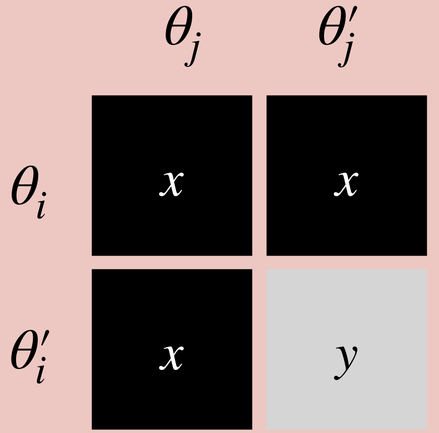
If a choice rule ϕ is contextually private, then for all agents i, j and all types $\theta_i, \theta_i', \theta_j, \theta_j' \in \Theta$ and all profiles of other agents' types $\boldsymbol{\theta}_{-ij} \in \boldsymbol{\Theta}_{-ij}$,

$$\phi(\theta_i, \theta_j, \boldsymbol{\theta}_{-ij}) = \phi(\theta_i', \theta_j, \boldsymbol{\theta}_{-ij}) = \phi(\theta_i, \theta_j', \boldsymbol{\theta}_{-ij}) = x$$

then

$$\phi(\theta_i', \theta_j', \boldsymbol{\theta}_{-ij}) = x.$$

Simplifies search for counterexamples to full contextual privacy.



✗

SPA Is Not Contextually Private

Proposition.

The second-price auction choice rule is not contextually private under sequential elicitation protocols.

Hold fixed the winner.

Consider the second and third highest bids $\underline{\theta} < \overline{\theta}$.

	$\overline{\theta}$	$\underline{\theta}$
$\overline{\theta}$	$p = \overline{\theta}$	$p = \overline{\theta}$
$\underline{\theta}$	$p = \overline{\theta}$	$p = \underline{\theta}$

	θ_j	θ'_j
θ_i	x	x
θ'_i	x	y

✗

SPA Is Not Contextually Private

Proposition.

The second-price auction choice rule is not contextually private under sequential elicitation protocols.

Hold fixed the winner.

Consider the second and third highest bids $\underline{\theta} < \overline{\theta}$.

	$\overline{\theta}$	$\underline{\theta}$
$\overline{\theta}$	$p = \overline{\theta}$	$p = \overline{\theta}$
$\underline{\theta}$	$p = \overline{\theta}$	$p = \underline{\theta}$

	θ_j	θ'_j
θ_i	x	x
θ'_i	x	y

✗

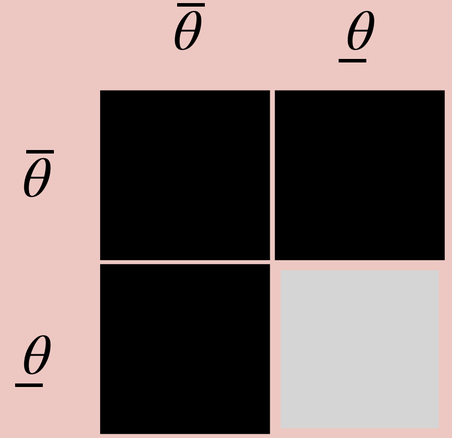
SPA Is Not Contextually Private

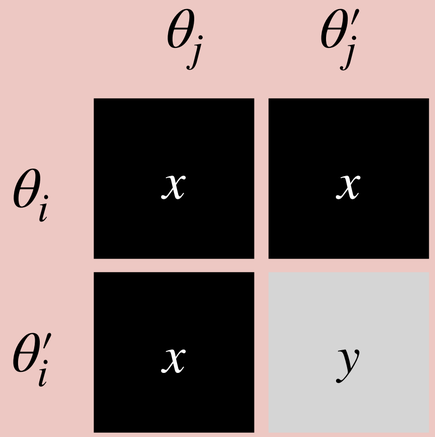
Proposition.

The second-price auction choice rule is not contextually private under sequential elicitation protocols.

Hold fixed the winner.

Consider the second and third highest bids $\underline{\theta} < \overline{\theta}$.



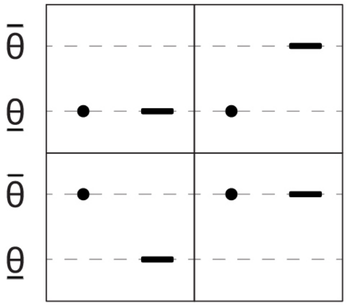


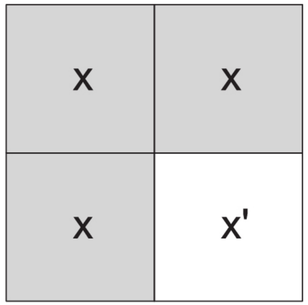
✗

The power of the Corners Lemma

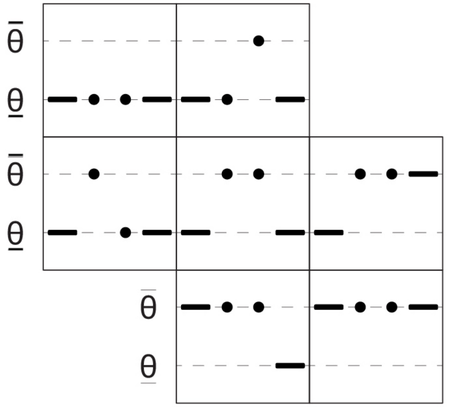
Auctions*

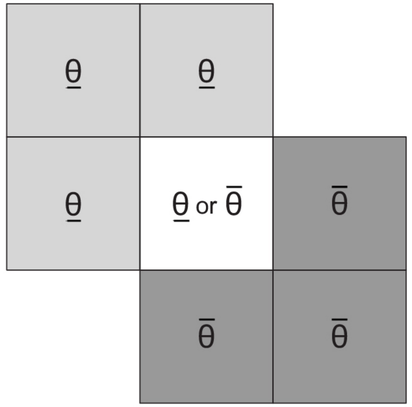
Second Price Auction





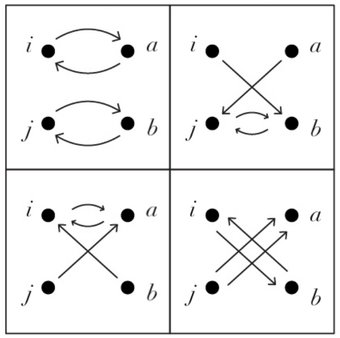
Efficient Double Auction

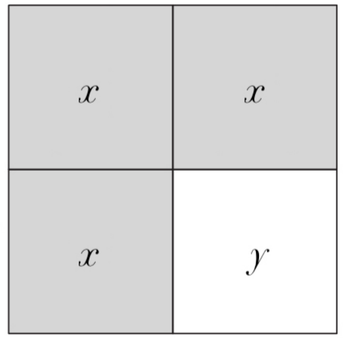




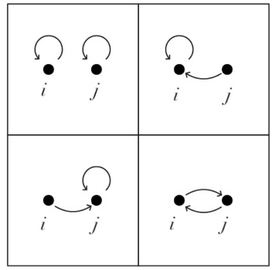
Matching

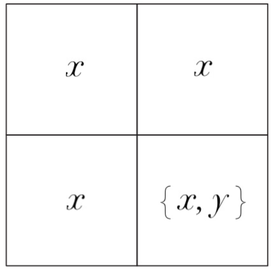
Stability

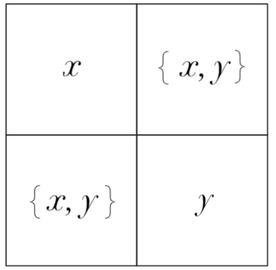


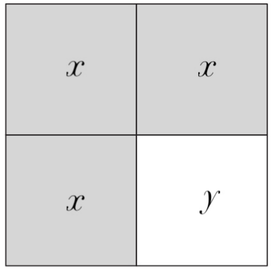


House Assignment









*See paper for more general proofs that don't rely on ties. This counterexample also works for gen. median voting rules.

Outline

1. **Definitions**

   Protocols, contextual privacy

2. **Fully contextually private choice rules**

   A necessary condition
   SPA is not contextually private

3. **Maximally contextually private protocols**

   Representation theorem: bi-monotonic protocols
   Maximally contextually private choice rules for SPA

4. **Brief discussion of other results**

   Settings without transfers, characterization for general protocols, incentives, variants.

Maximal Contextual Privacy in Auctions

Preview of the next result.

When searching for maximally contextually private protocols, we can restrict attention to a much smaller space of protocols.

Maximal Contextual Privacy in Auctions

Preview of the next result.

When searching for maximally contextually private protocols, we can restrict attention to a much smaller space of protocols.

This result will help us show, for instance…

that for the **second-price auction rule**, the

ascending-join and **overdescending-join**

protocols are maximally contextually private.

Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.

Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.

Standard efficient auctions satisfy this property.

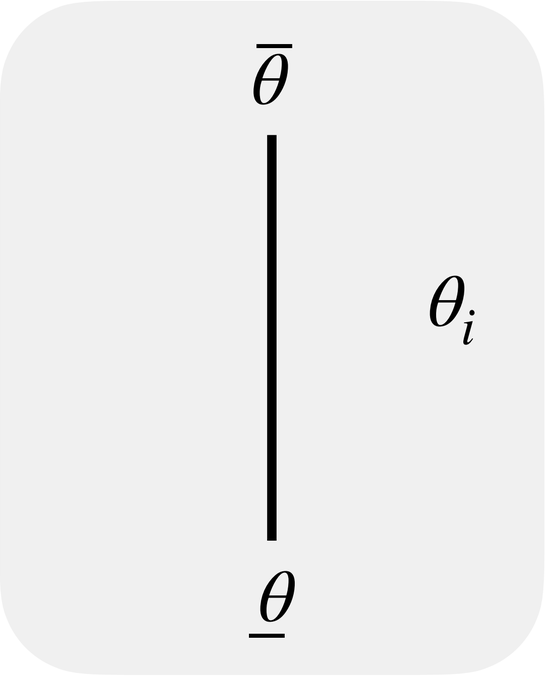
Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.

Fix a profile of other agents' types $\boldsymbol{\theta}_{-i}$.

Vary agent i's type θ_i.



Standard efficient auctions satisfy this property.

Maximal Contextual Privacy in Auctions

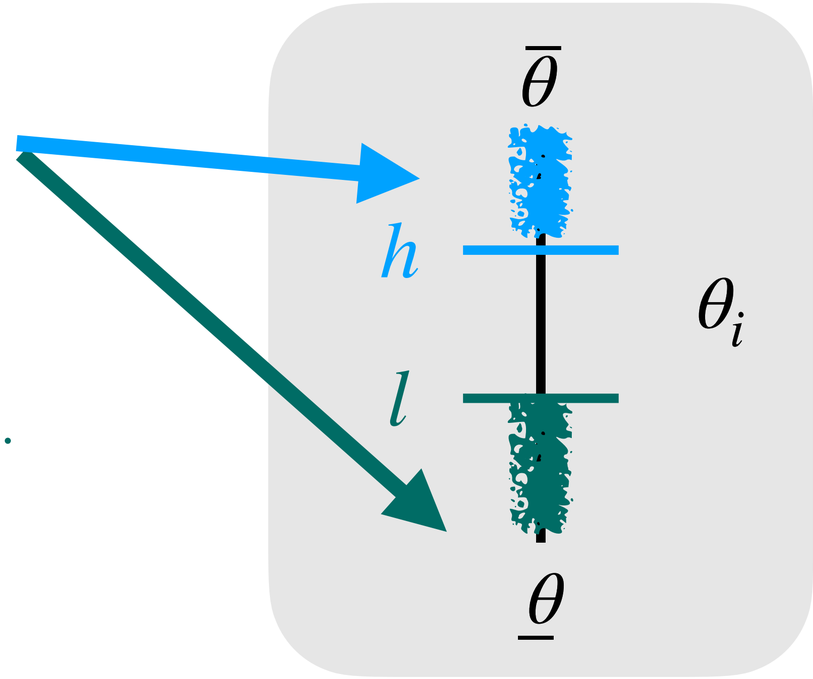
Theorem.

If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.

Fix a profile of other agents' types $\boldsymbol{\theta}_{-i}$.

Vary agent i's type θ_i.

$\phi(\theta_i, \boldsymbol{\theta}_{-i})$ is constant outside of an internal interval $[l\ , h] \cap \Theta_i$.



Standard efficient auctions satisfy this property.

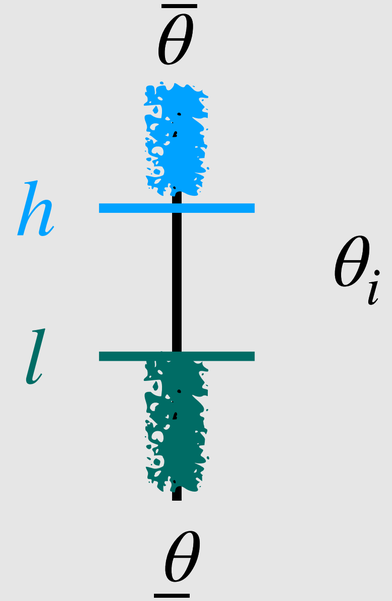
Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.

Definition.

A choice rule ϕ satisfies the **interval pivotality property** if for all agents $i \in N$ and all profiles of other agents $\boldsymbol{\theta}_{-i} \in \boldsymbol{\Theta}_{-i}$, there is one interval $[l\ ,\ h] \cap \Theta_i$ outside which $\phi(\theta_i, \boldsymbol{\theta}_{-i})$ is constant, inside which $\phi(\theta_i, \boldsymbol{\theta}_{-i})$ is injective.



Standard efficient auctions satisfy this property.

Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.

Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.

Definition.

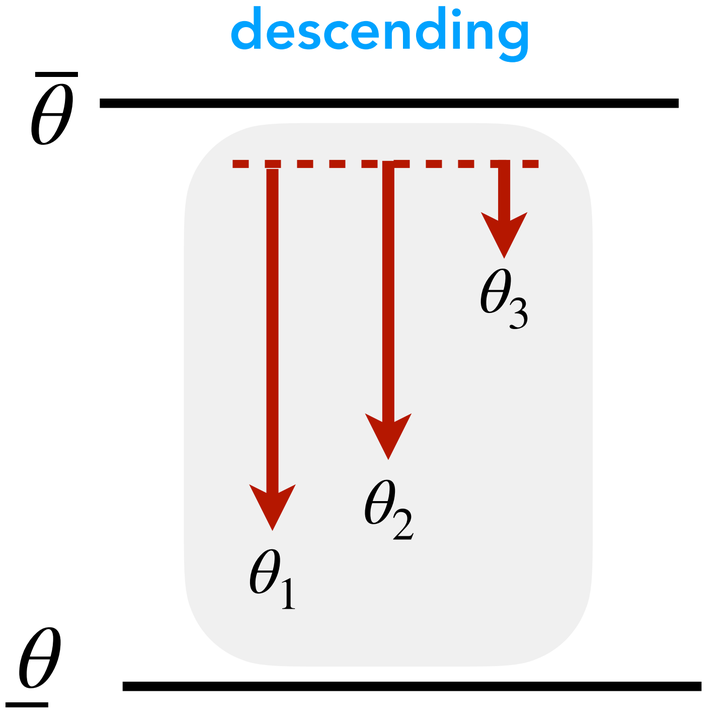
A protocol P is **bi-monotonic** if

1. all queries are "threshold queries", and
2. for each agent, the answer to the first query determines whether subsequent queries are monotonically increasing or decreasing in the threshold.

Maximal Contextual Privacy in Auctions

Theorem.

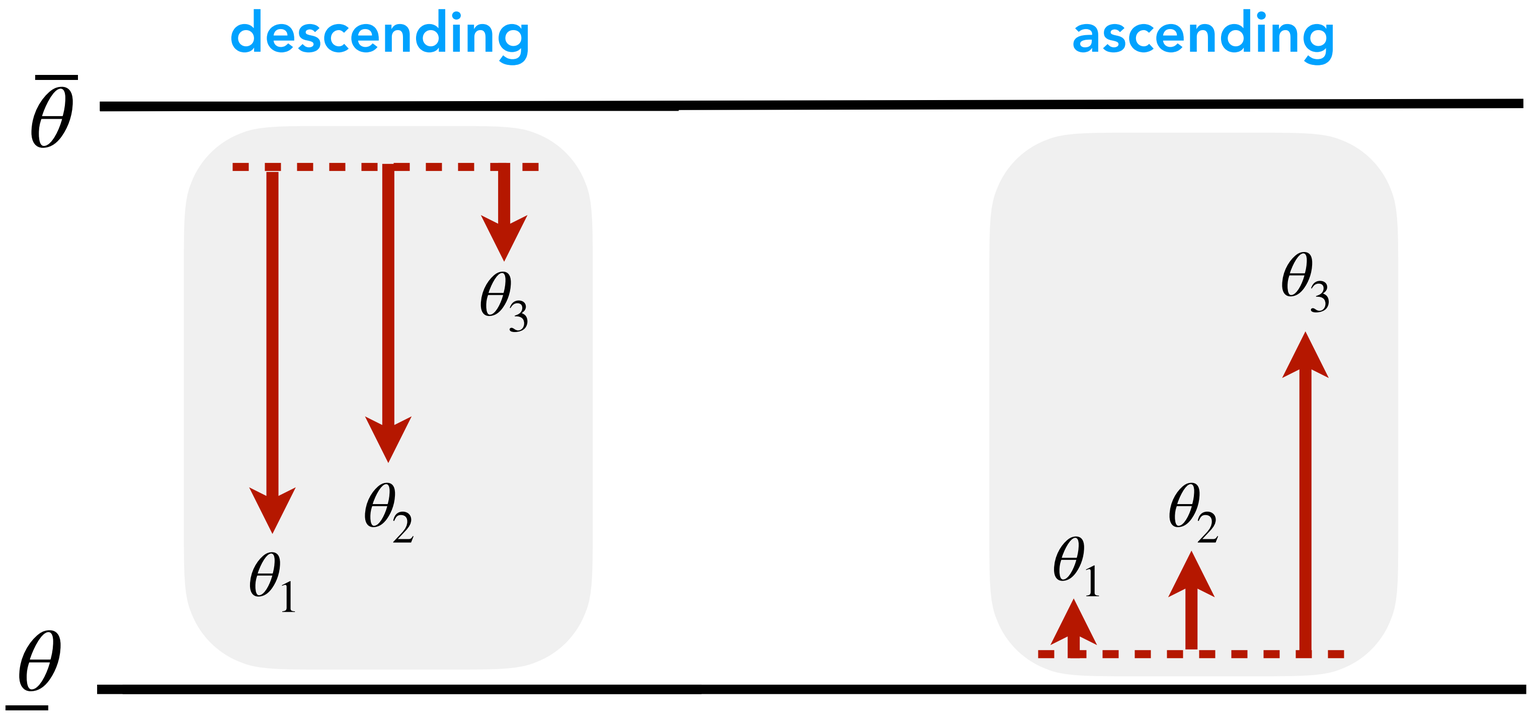
If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.



Maximal Contextual Privacy in Auctions

Theorem.

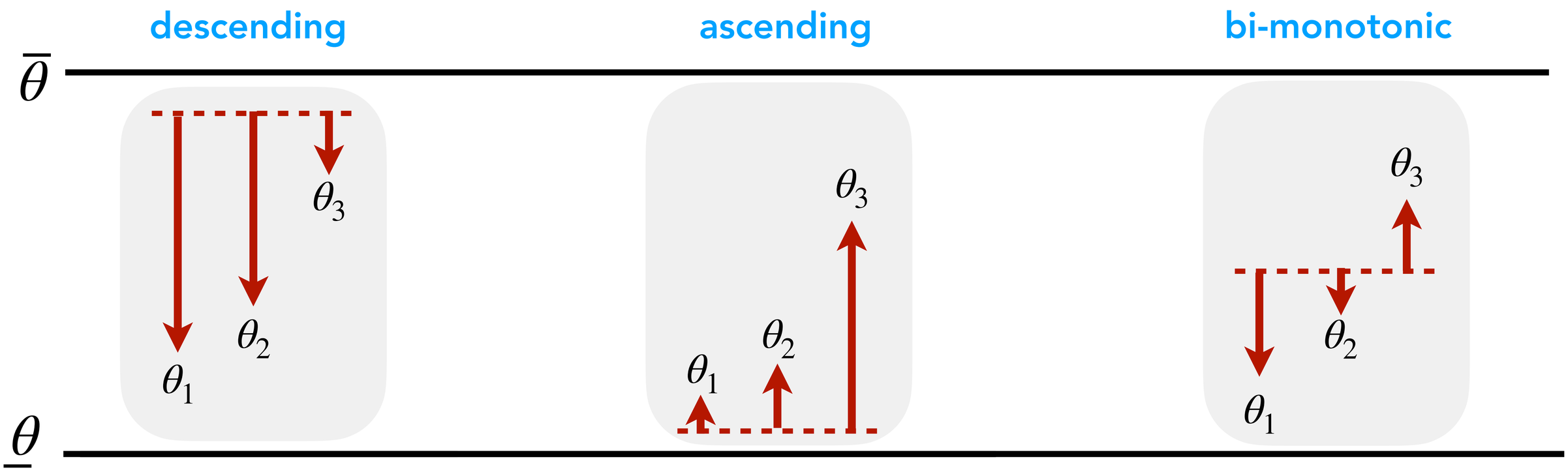
If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.



Maximal Contextual Privacy in Auctions

Theorem.

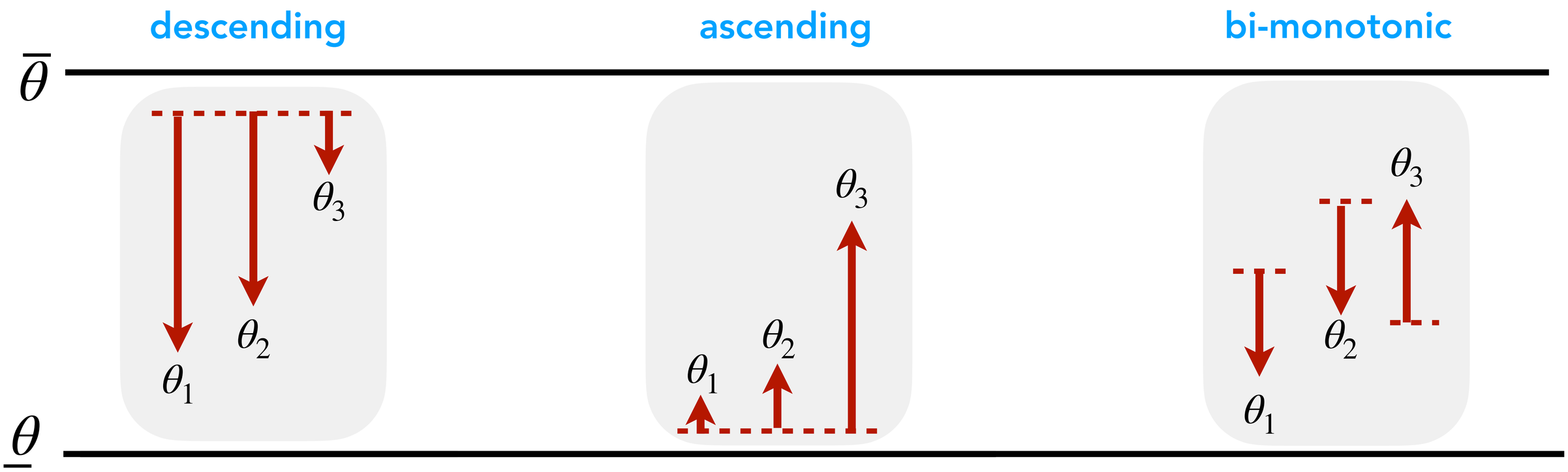
If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.



Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **"interval pivotality property"**, then any protocol for ϕ is contextual-privacy equivalent to a **"bi-monotonic"** protocol.

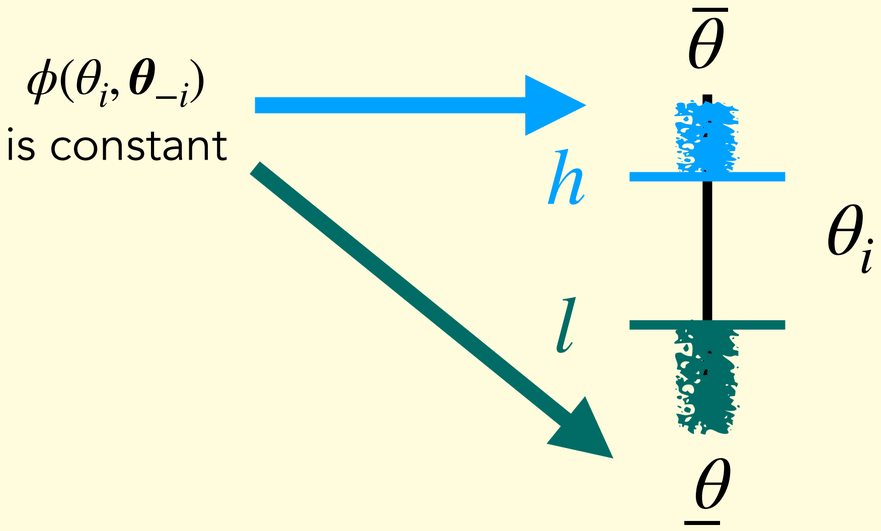


Maximal Contextual Privacy in Auctions

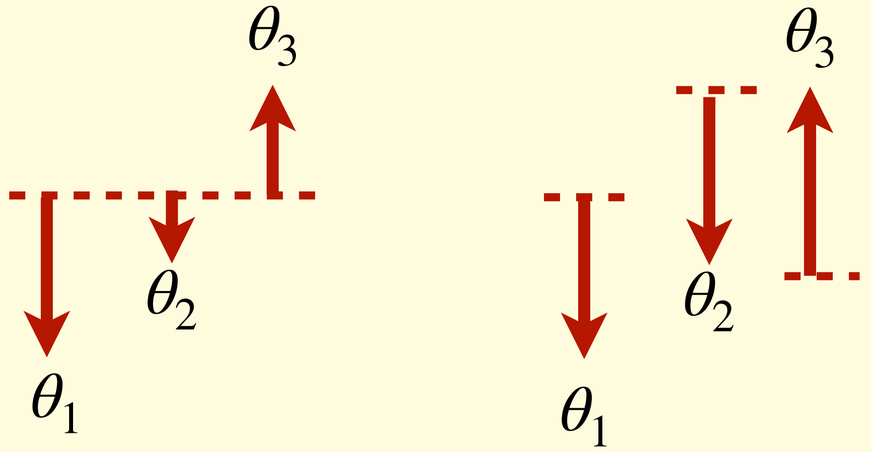
Theorem.

If a choice rule ϕ satisfies the **interval pivotality property**, then any protocol for ϕ is contextual privacy equivalent to a **bi-monotonic protocol**.

choice rule with interval pivotality



bi-monotonic protocol



Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **interval pivotality property**, then any protocol for ϕ is contextual privacy equivalent to a **bi-monotonic protocol**.

Proof idea.

Show that any protocol P for ϕ that is not bi-monotonic can be transformed into a protocol that is at least as contextually private as P and also bi-monotonic.

Step 1. **Inject threshold queries** between highest and lowest types separated at node v.

Step 2. **Fill in gaps** between threshold queries.

Step 3. **Delete redundant queries**.

Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **interval pivotality property**, then any protocol for ϕ is contextual privacy equivalent to a **bi-monotonic protocol**.

Theorem.

The **ascending-join** protocol and the **overdescending-join** protocol are **maximally contextually private** protocols for the second-price auction.

Maximal Contextual Privacy in Auctions

Theorem.

If a choice rule ϕ satisfies the **interval pivotality property**, then any protocol for ϕ is contextual privacy equivalent to a **bi-monotonic protocol**.

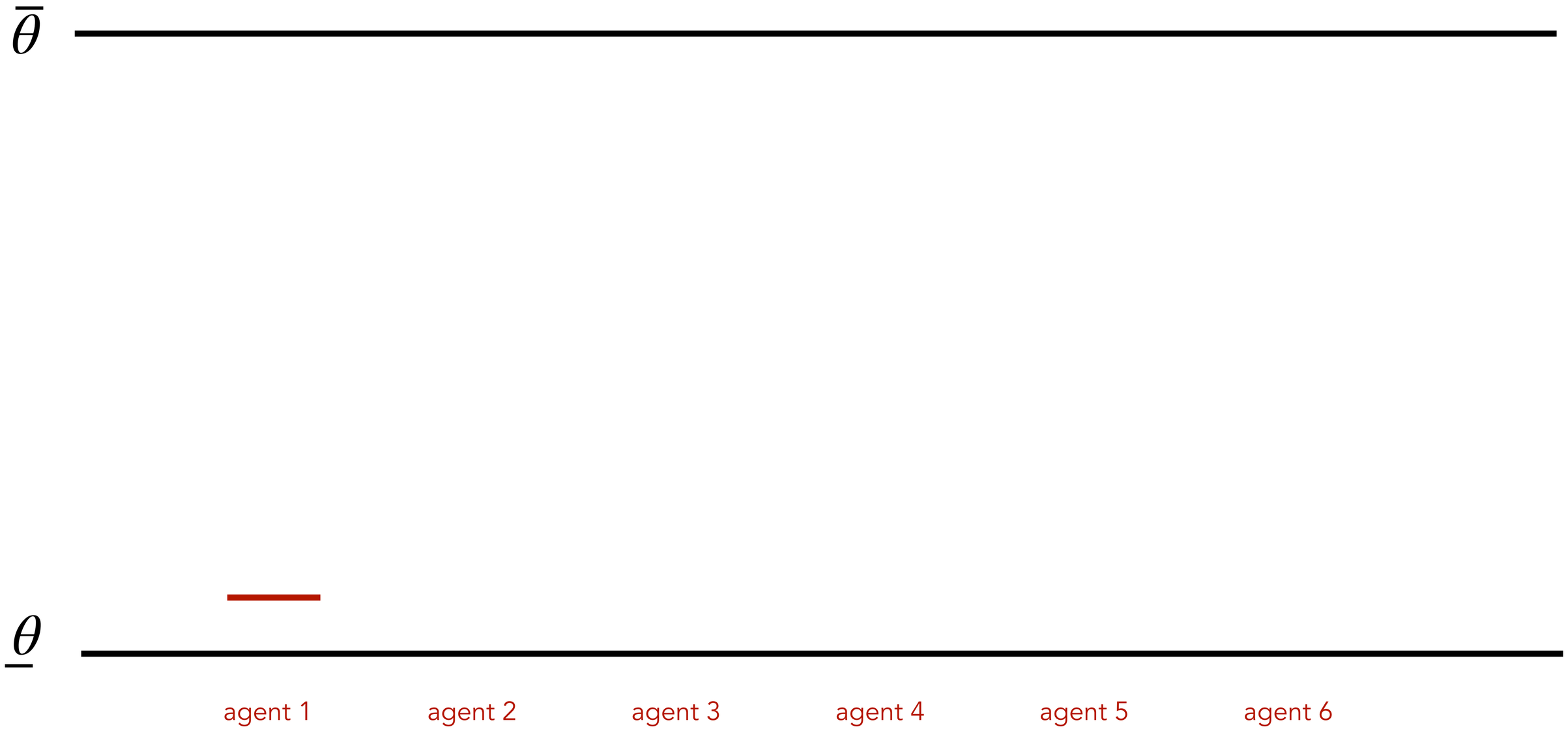
Theorem.

The **ascending-join** protocol and the **overdescending-join** protocol are **maximally contextually private** protocols for the second-price auction.

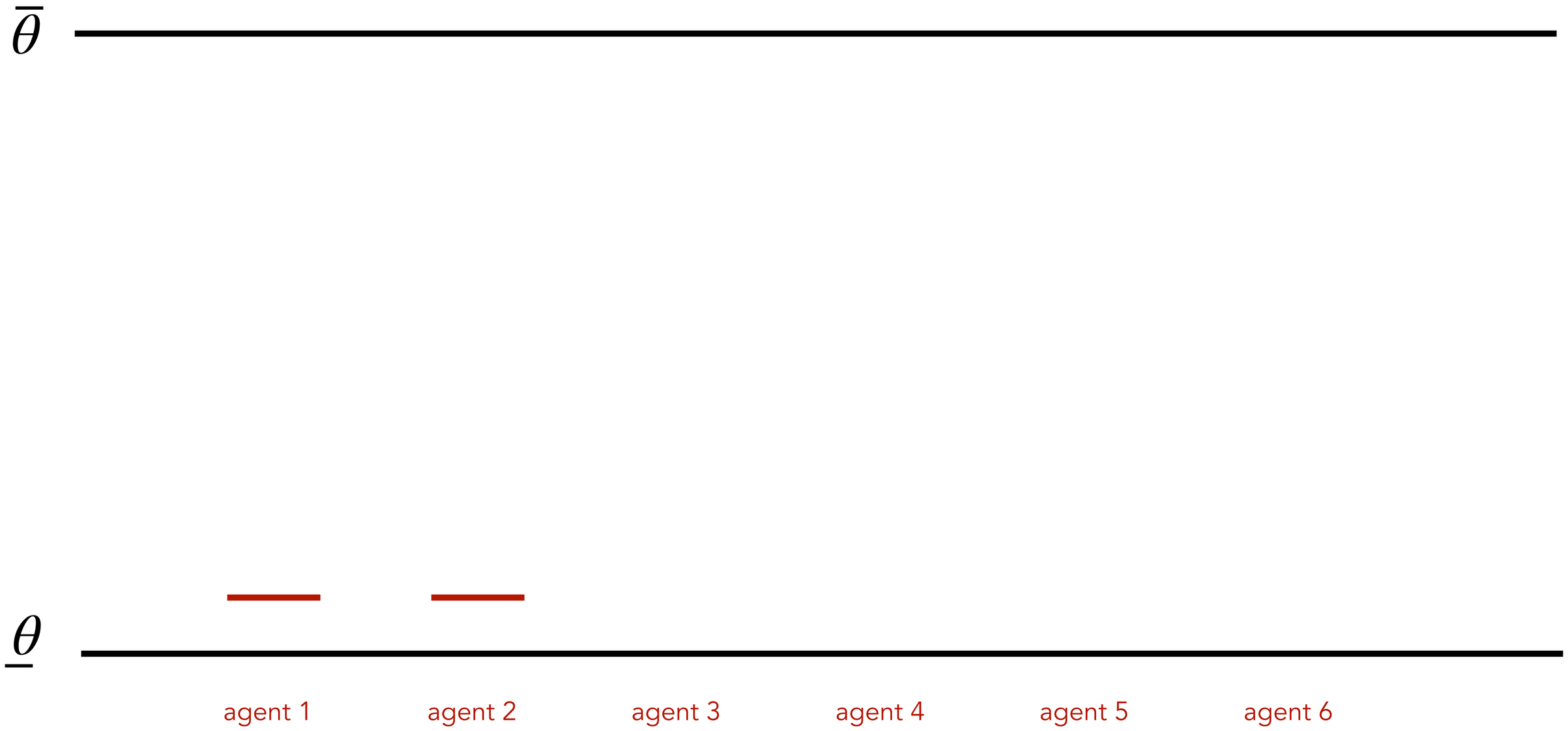
Maximally contextually private protocols trade off privacy of different agents.

For choice rules that have a "price," delay asking as much as possible.

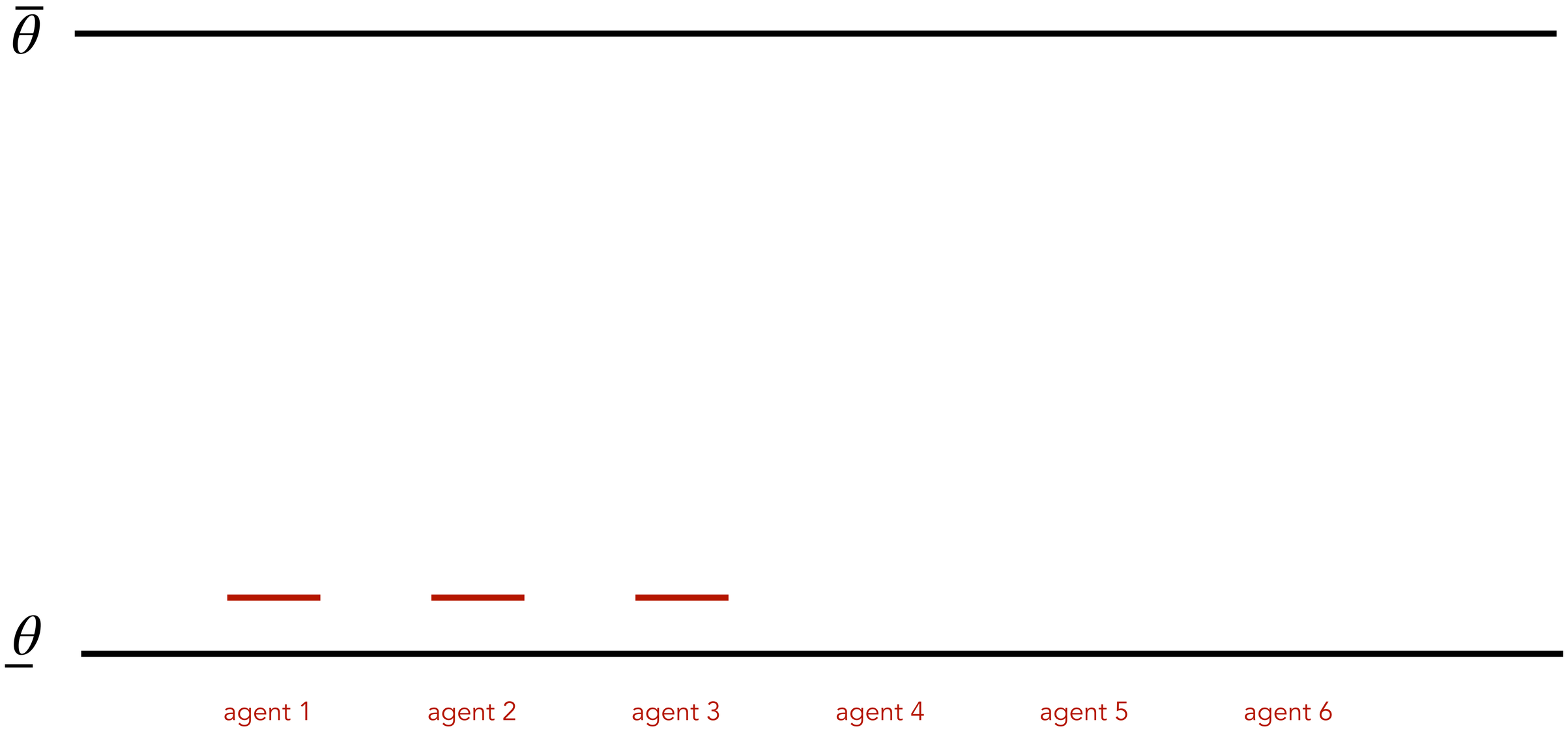
Ascending Protocol Is Not Maximally Contextually Private



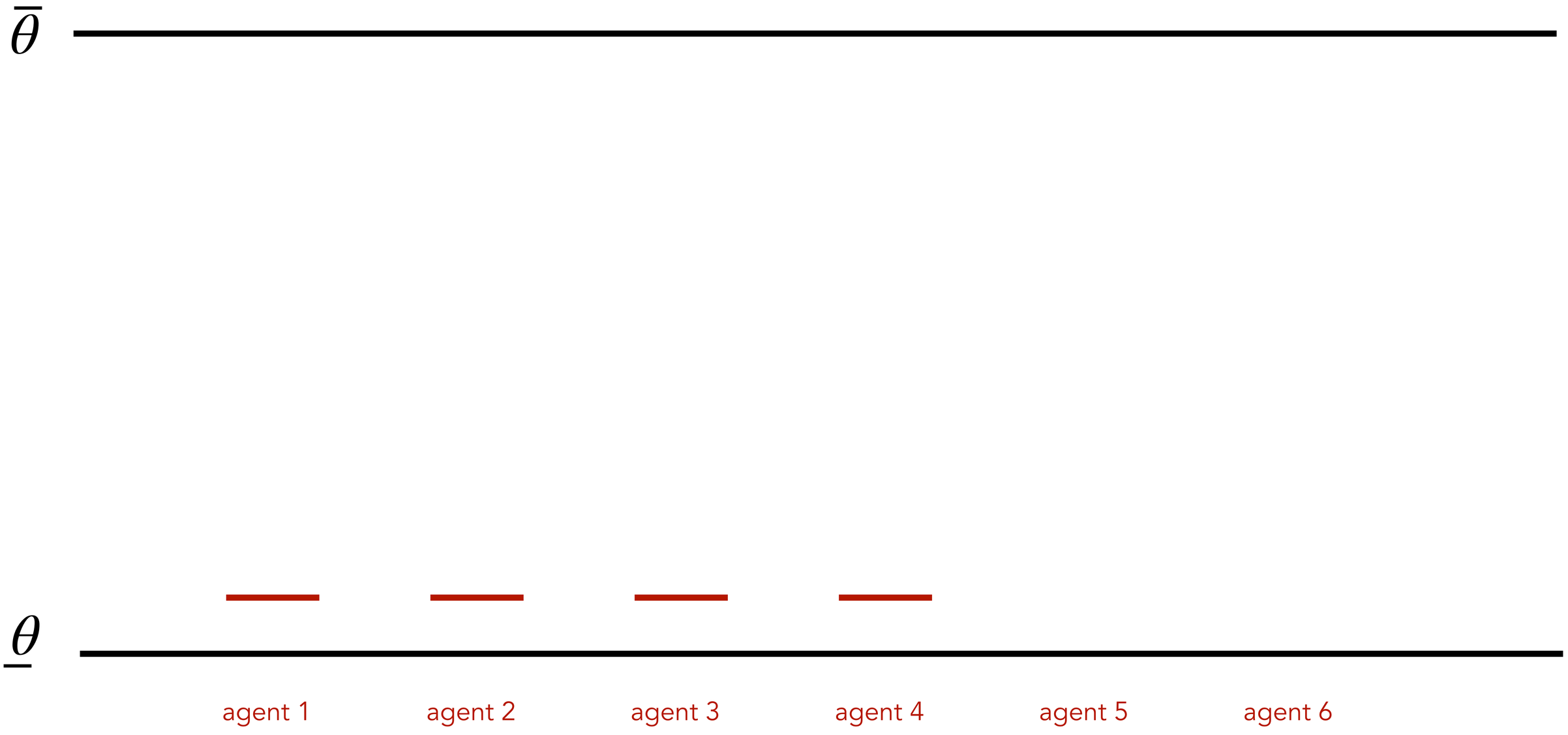
Ascending Protocol Is Not Maximally Contextually Private



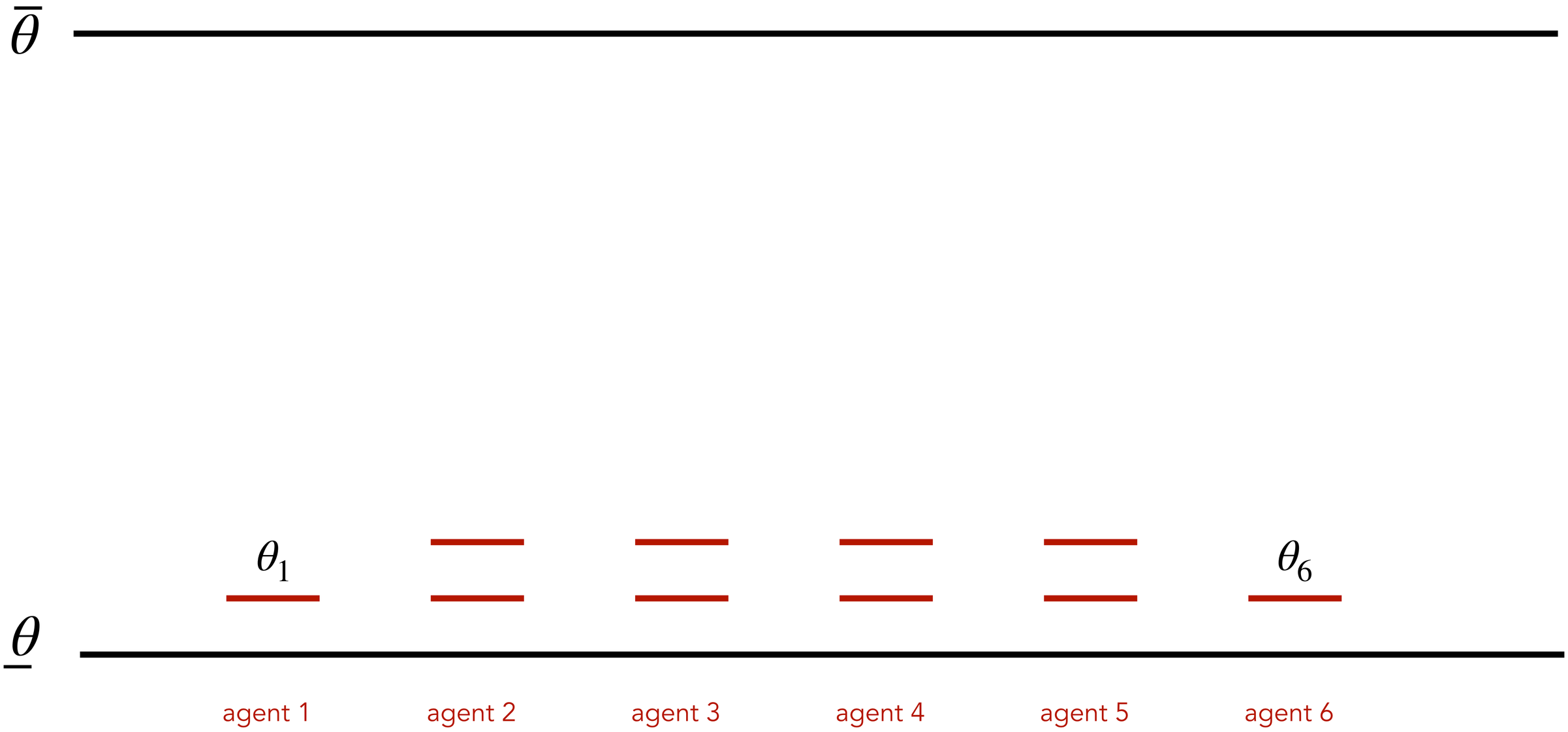
Ascending Protocol Is Not Maximally Contextually Private



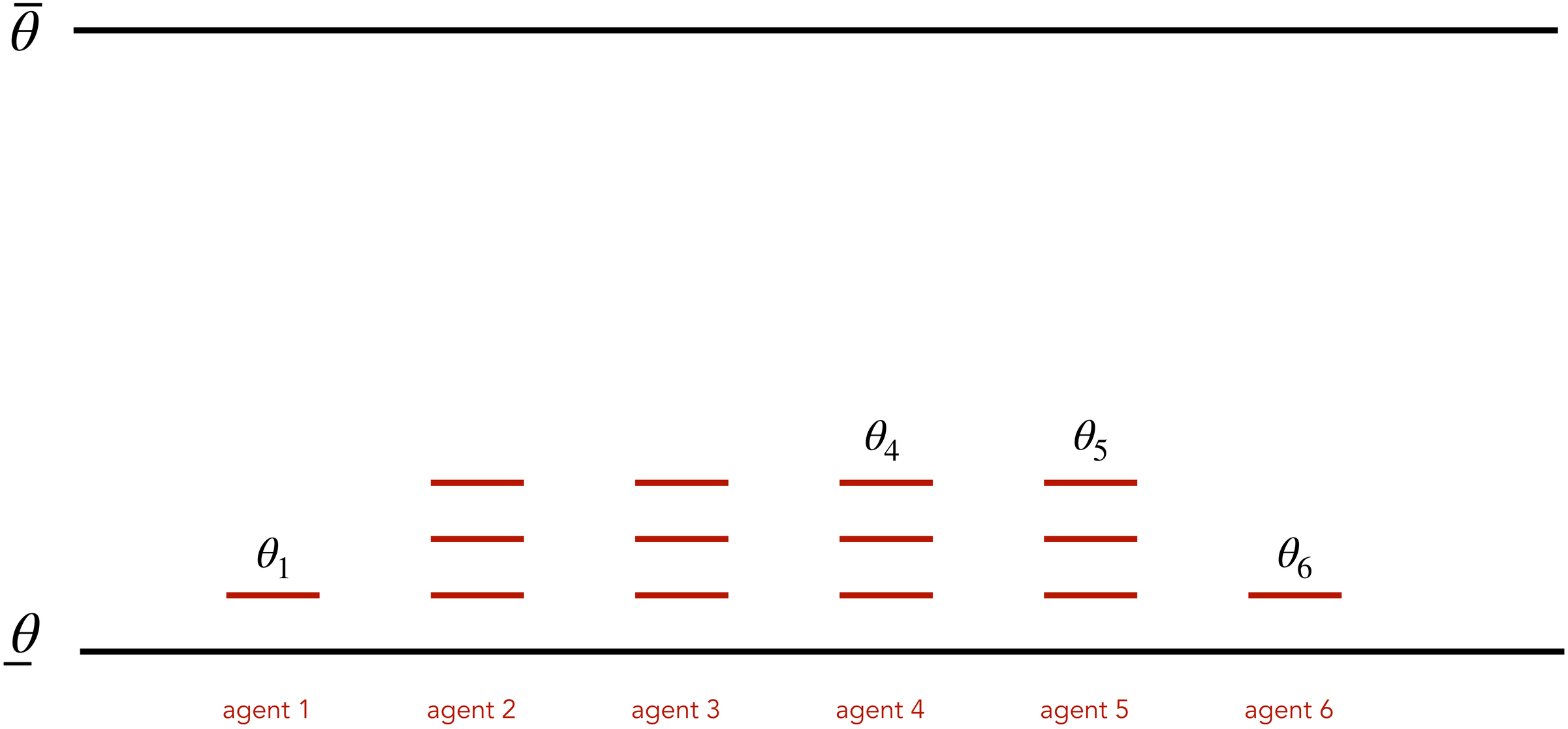
Ascending Protocol Is Not Maximally Contextually Private



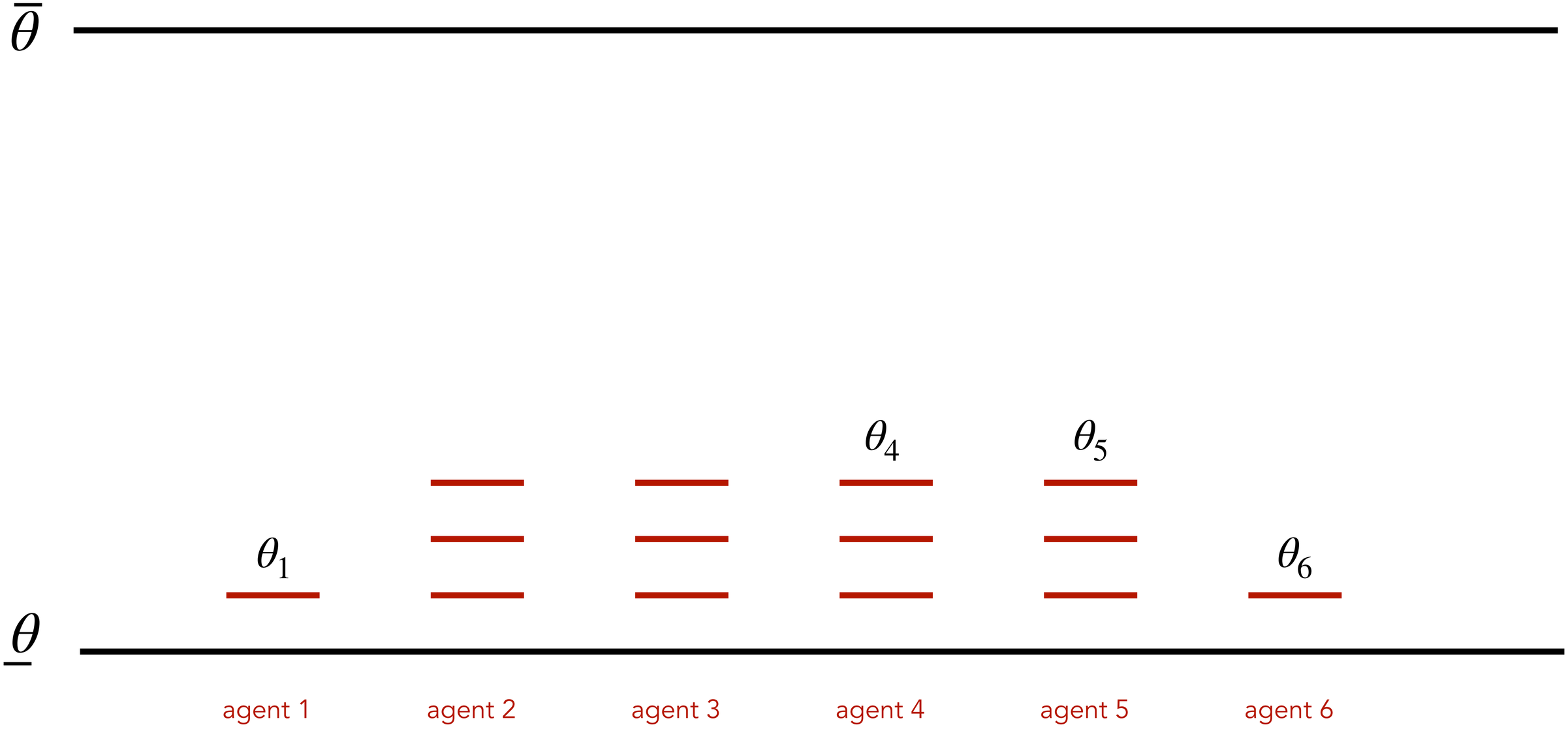
Ascending Protocol Is Not Maximally Contextually Private



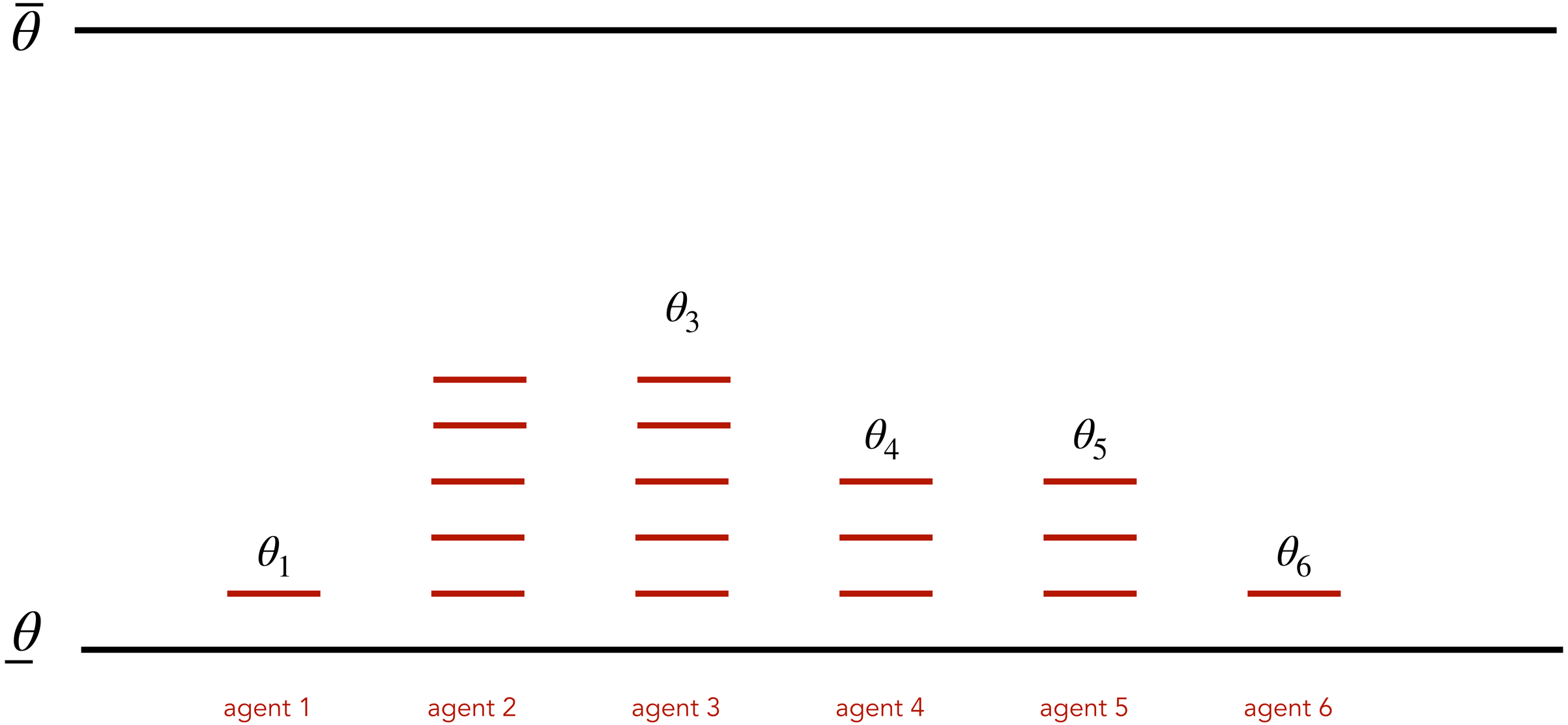
Ascending Protocol Is Not Maximally Contextually Private



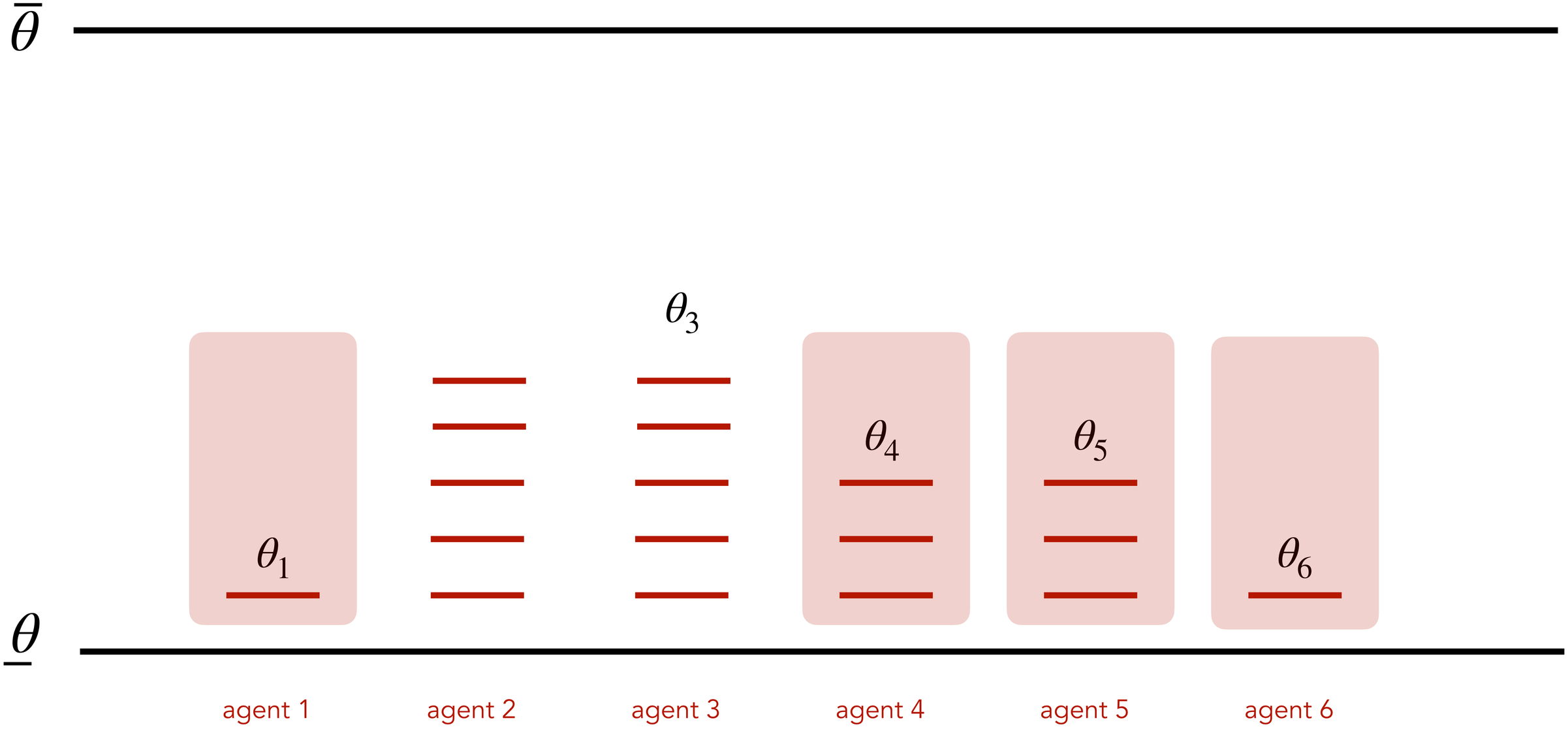
Ascending Protocol Is Not Maximally Contextually Private



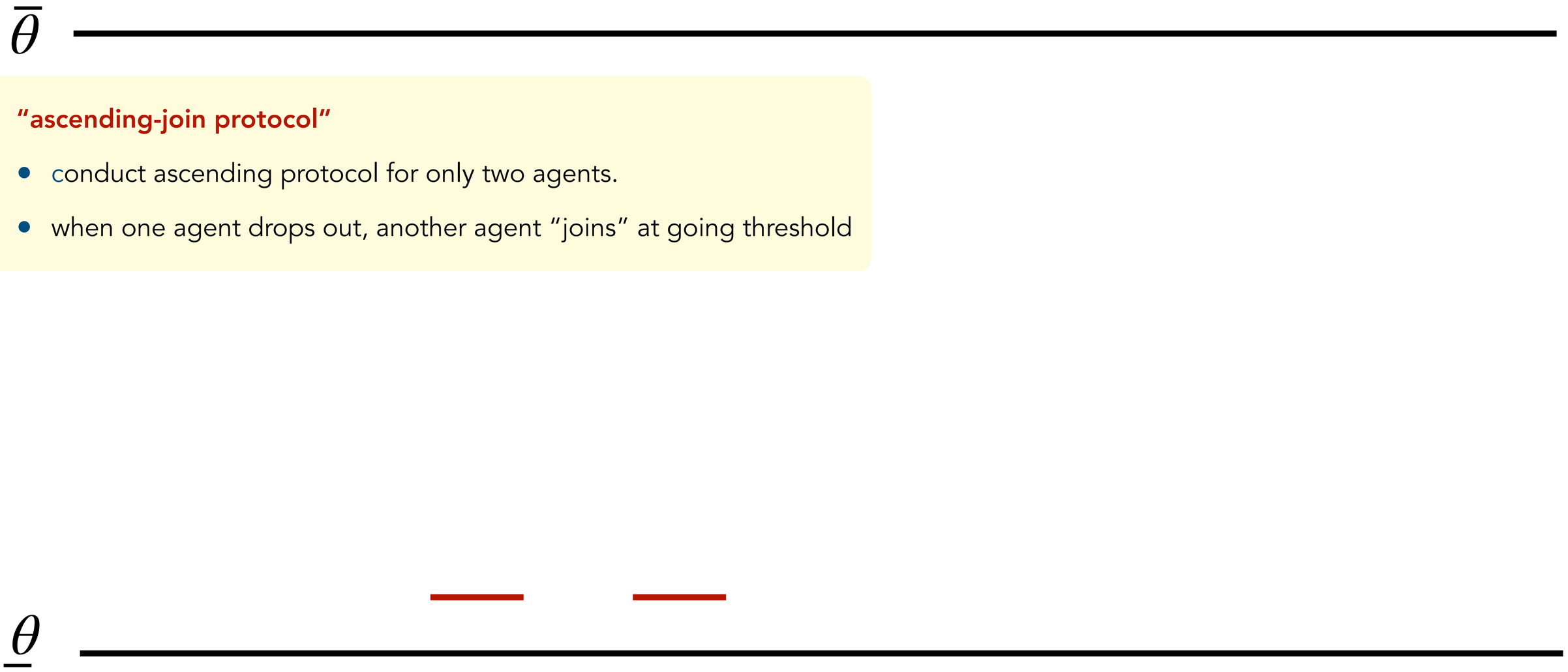
Ascending Protocol Is Not Maximally Contextually Private



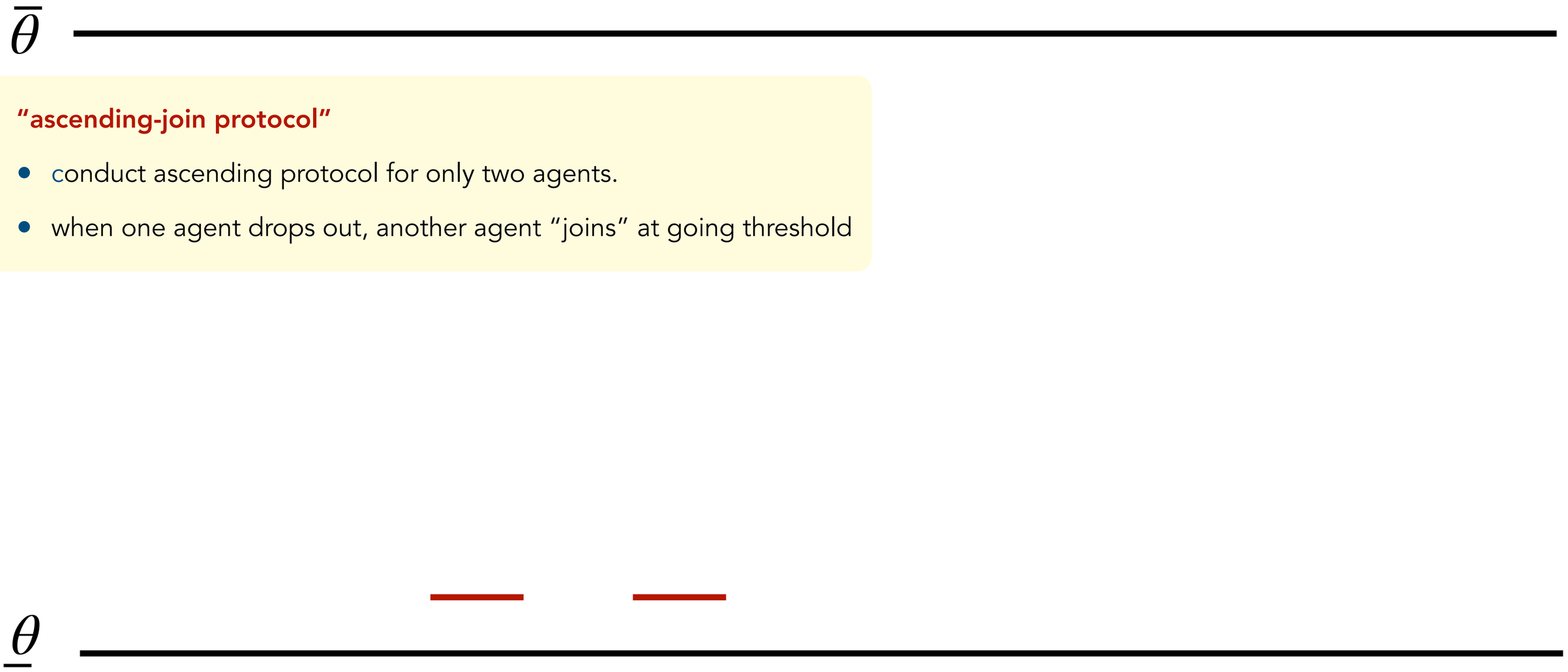
Ascending Protocol Is Not Maximally Contextually Private



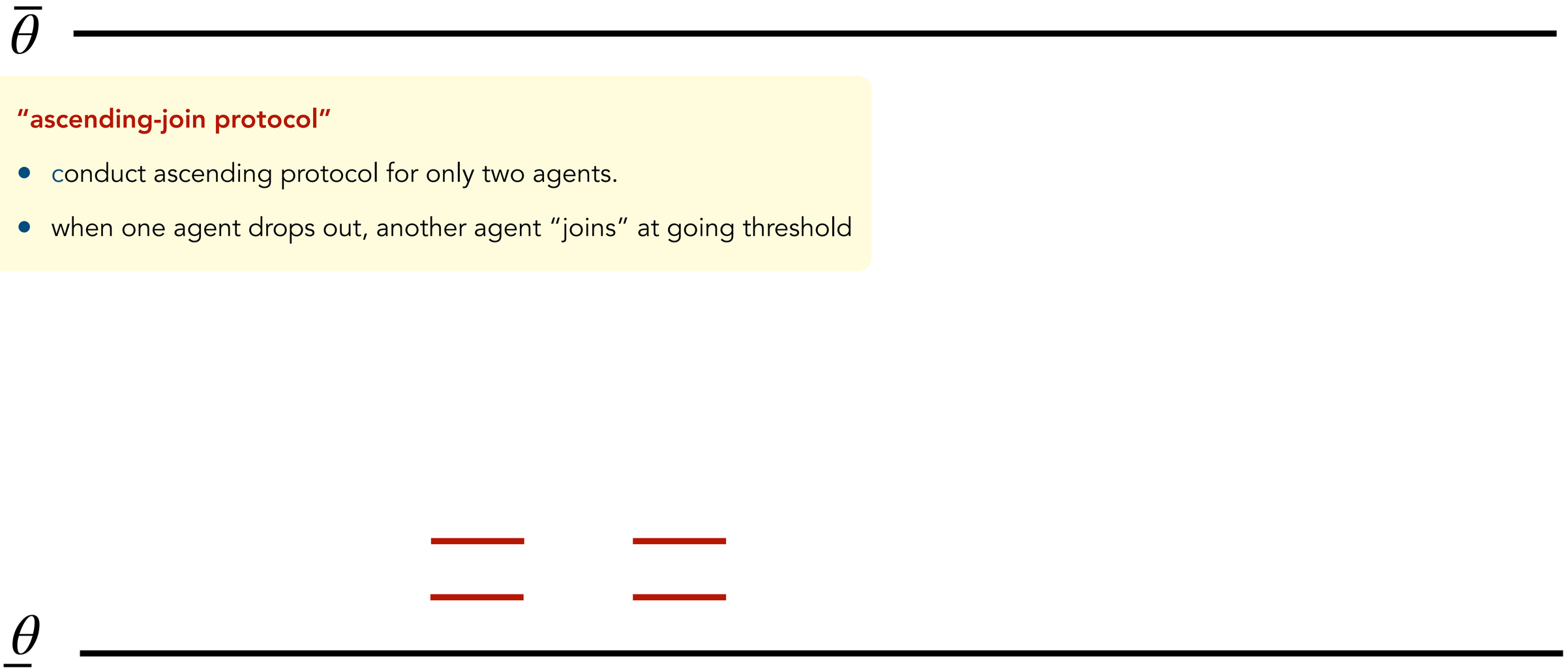
A Maximally Contextually Private Protocol



A Maximally Contextually Private Protocol



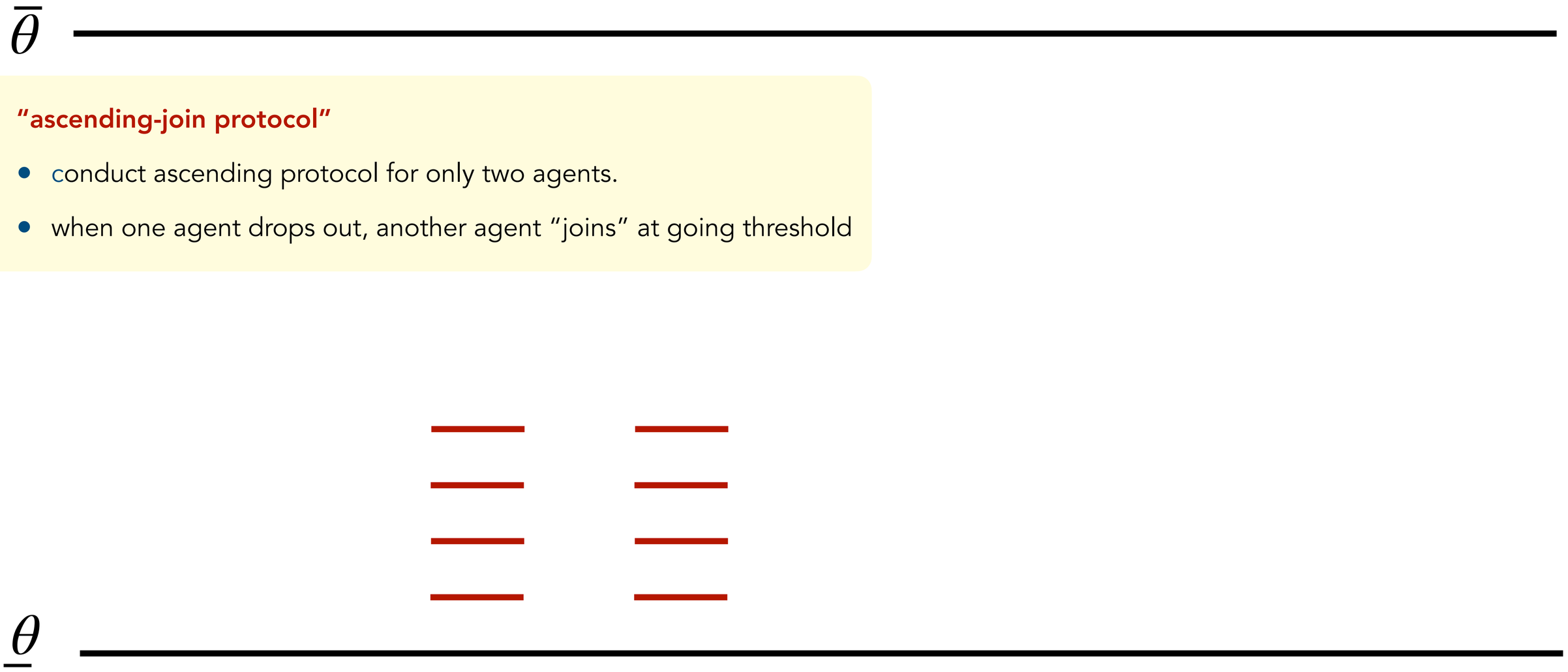
A Maximally Contextually Private Protocol



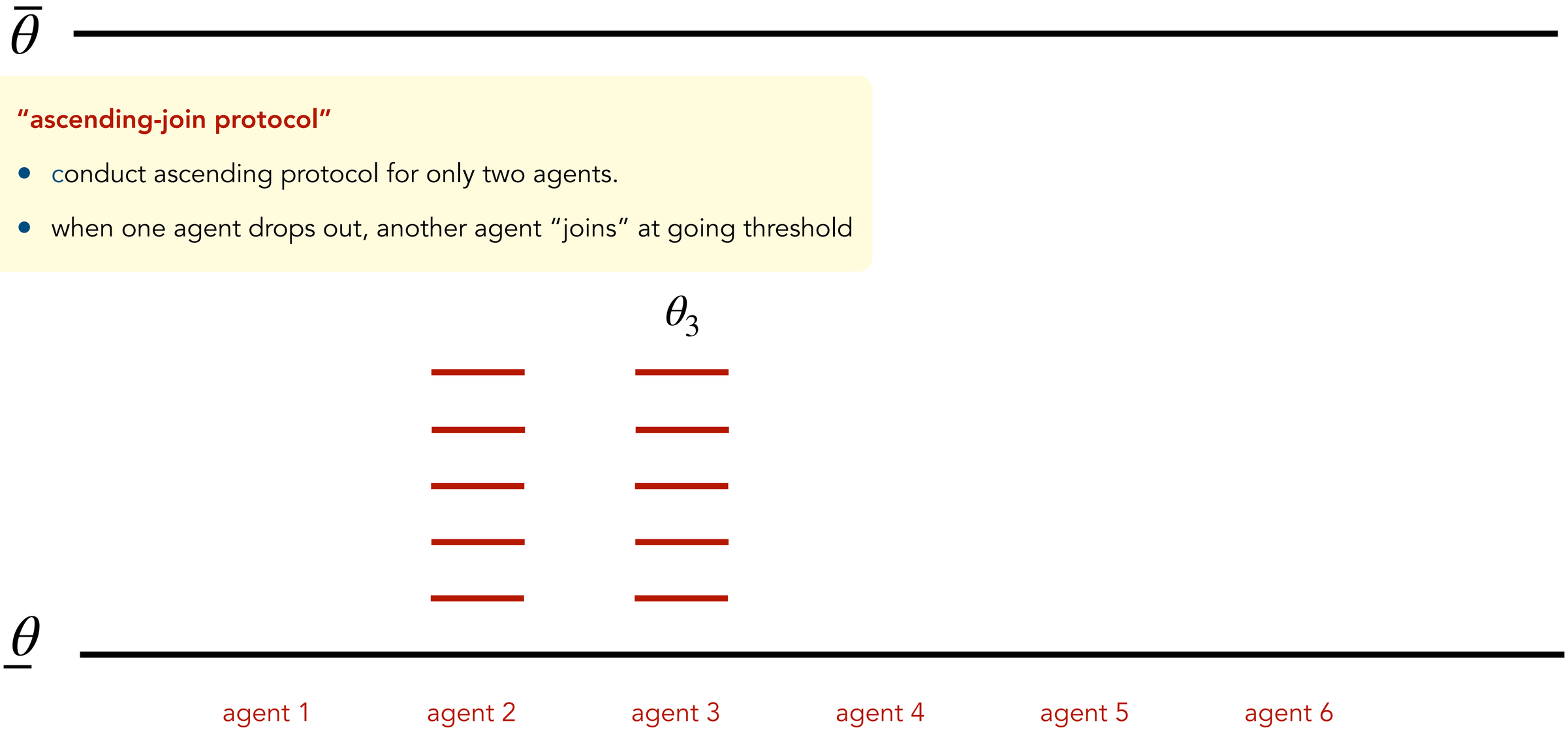
"ascending-join protocol"

- conduct ascending protocol for only two agents.
- when one agent drops out, another agent "joins" at going threshold

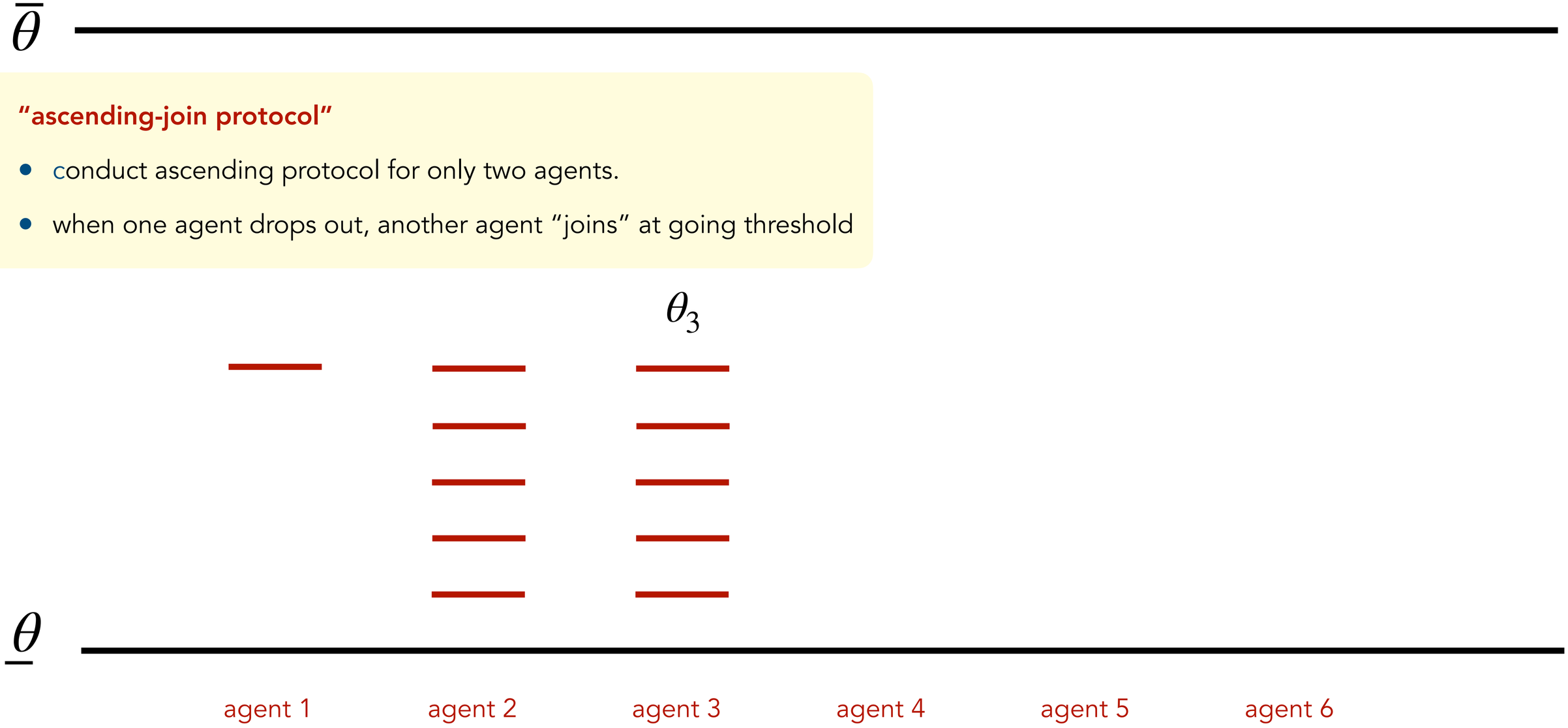
A Maximally Contextually Private Protocol



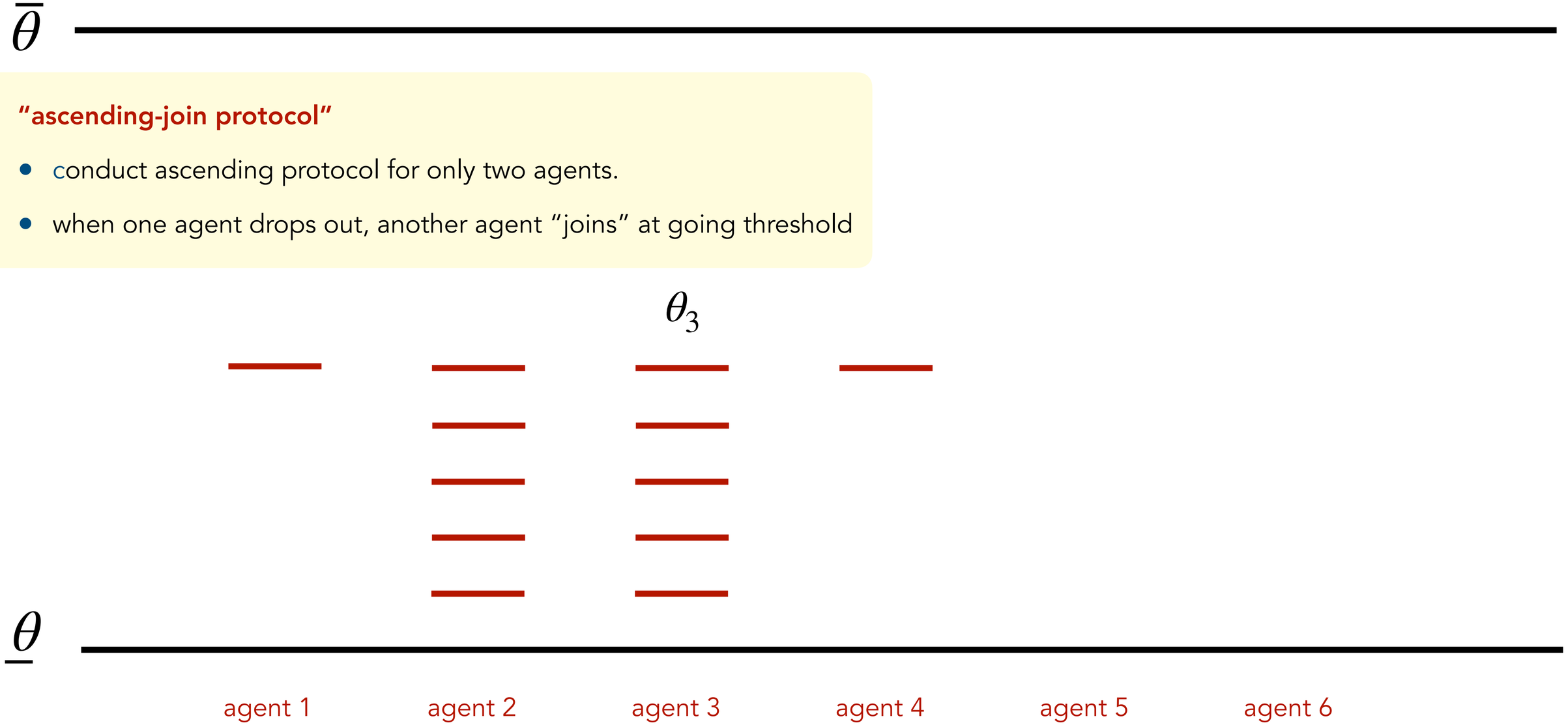
A Maximally Contextually Private Protocol



A Maximally Contextually Private Protocol



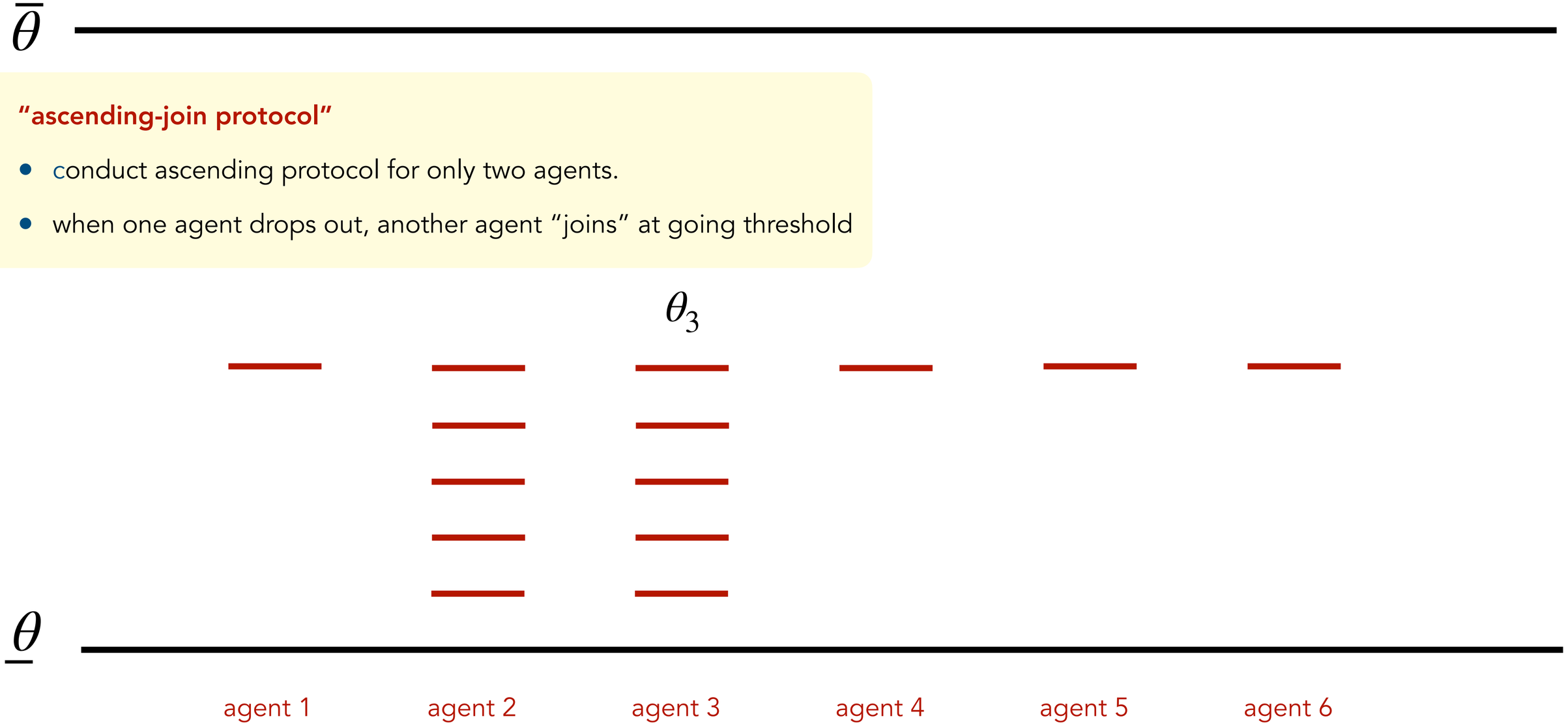
A Maximally Contextually Private Protocol



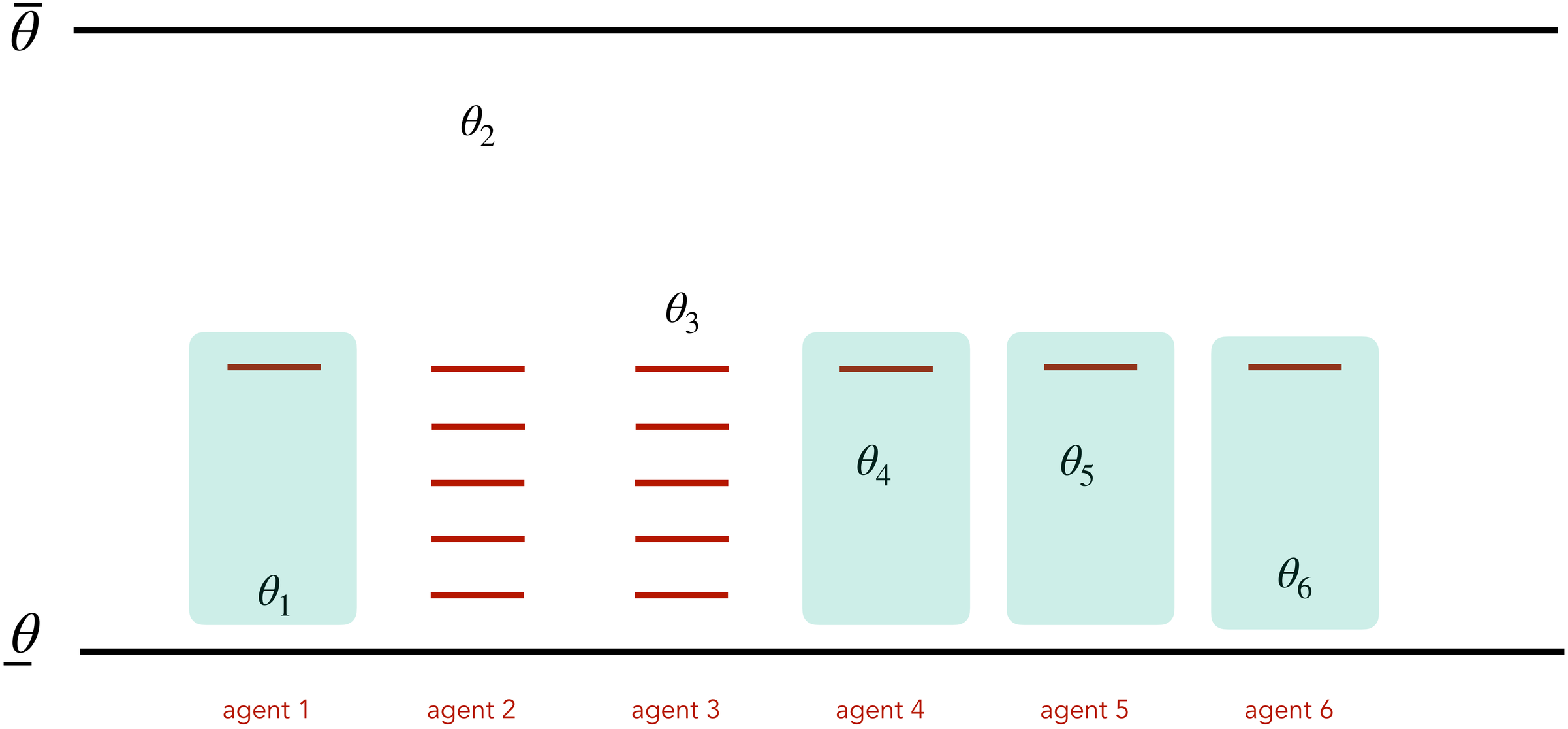
A Maximally Contextually Private Protocol

"ascending-join protocol"

- conduct ascending protocol for only two agents.
- when one agent drops out, another agent "joins" at going threshold



A Maximally Contextually Private Protocol



Ascending Protocol Improvement?

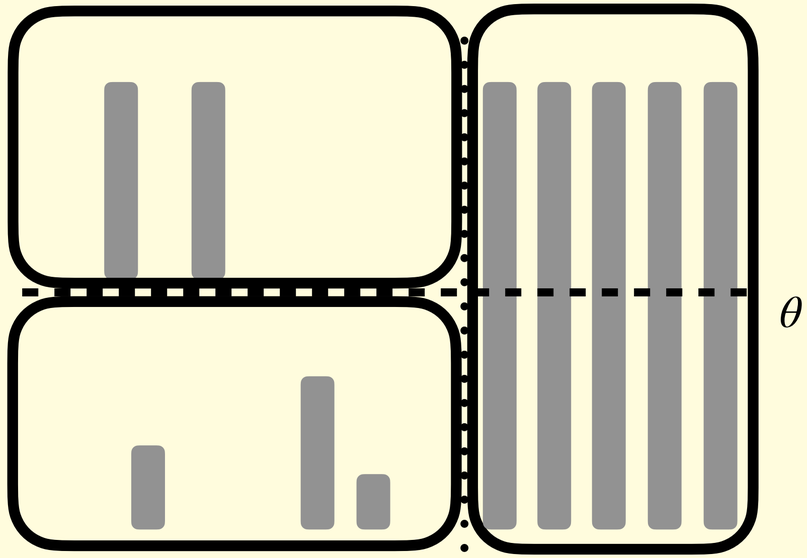
Theorem.

The **ascending-join** protocol is a **maximally contextually private** protocol for the second-price auction. It protects the winner and low-priority losers.

Proof idea.

Construct the protocol by induction.

- Bimonotonicity reduces to a choice of (i) threshold to start each agent ask and (ii) order in which to ask agents.
- Show that at every stage there is exactly one query that either leads into a "protective information state" or termination.



protective information state

Outline

1. **Definitions**

   Protocols, contextual privacy

2. **Fully contextually private choice rules**

   A necessary condition
   SPA is not contextually private

3. **Maximally contextually private protocols**

   Representation theorem: bi-monotonic protocols
   Maximally contextually private choice rules for SPA

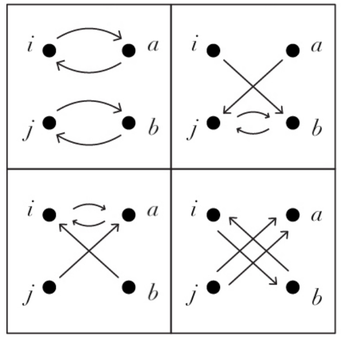
4. **Brief discussion of other results**

   Settings without transfers, characterization for general protocols, incentives, variants.

Impossibility Results In Assignment Domains

Matching

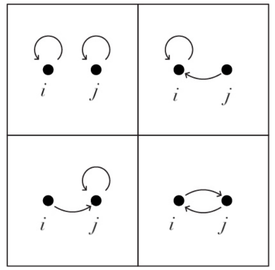
Stability



x	x
x	y

House Assignment

Efficiency + IR



x	x
x	$\{x, y\}$

x	$\{x, y\}$
$\{x, y\}$	y

x	x
x	y

Proposition.

There is no stable matching rule that is contextually private.

Proposition.

There is no efficient, individually rational and contextually private choice rule.

Additional Results

Theorem. Characterization of contextually private choices rules.

For any "non-adaptive protocol", a social choice function ϕ is contextually private

if and only if

there is no **generalized corner** $\tilde{\Theta} \subseteq \Theta$ such that any "non-trivial" query could separate two type profiles that lead to the same outcome.

Proposition. Incentives in (maximally)-contextually private auction protocols.

- **Ascending** and **ascending-join** protocols for second-price auction rule are obviously DSIC implementable.
- **Over-descending** protocol for second-price auction rule is DSIC implementable.
- **Descending** protocol for first-price auction rule has an equilibrium equivalent to the BNE in a static auction.

Conclusion

Today.

- **Defined contextual privacy.**
  - The designer only learns what they need to know to compute the choice rule.
- **Looked for contextually private choice rules.**
  - SPA ✗
  - Individual vs Collective Pivotality (Corners Lemma).
- **Characterized maximally contextually private protocols.**

  Maximally contextually private protocols…
  - are bi-monotonic.
  - trade off the privacy of different agents.

Conclusion

Today.

- **Defined contextual privacy.**
  - The designer only learns what they need to know to compute the choice rule.
- **Looked for contextually private choice rules.**
  - SPA ✗
  - Individual vs Collective Pivotality (Corners Lemma).
- **Characterized maximally contextually private protocols.**

  Maximally contextually private protocols…
  - are bi-monotonic.
  - trade off the privacy of different agents.

Tomorrow?

Contextual privacy and IC?

Privacy-implementation frontier?

Other restrictions on protocols?

Conclusion

Today.

- **Defined contextual privacy.**
  - The designer only learns what they need to know to compute the choice rule.
- **Looked for contextually private choice rules.**
  - SPA ✗
  - Individual vs Collective Pivotality (Corners Lemma).
- **Characterized maximally contextually private protocols.**

  Maximally contextually private protocols…
  - are bi-monotonic.
  - trade off the privacy of different agents.

Tomorrow?

Contextual privacy and IC?

Privacy-implementation frontier?

Other restrictions on protocols?

Thanks!

zhitzig@g.harvard.edu

That's It

Comments?

haupt@mit.edu
zhitzig@g.harvard.edu

Indirect Protocols

- $N < \infty$ agents
- Private information $\theta_i \in \Theta$, $|\Theta| < \infty$, profiles $\boldsymbol{\theta} \in \boldsymbol{\Theta}$
- Outcomes $x \in X$
- Preferences over outcomes $u_i : X \to \mathbb{R}$
- Choice rule $\phi : \boldsymbol{\Theta} \to X$, deterministic
- Universal message set M
- Set of **elicitation technologies** $S \subseteq \{f : M^n \to \tilde{M}\}$

Learn everything

$\text{id} : M^n \to \tilde{M} := M^n$

$\mathbf{m} \mapsto \mathbf{m}$

Learn agent i's msg

$\text{proj}_i : M^n \to \tilde{M} := M$

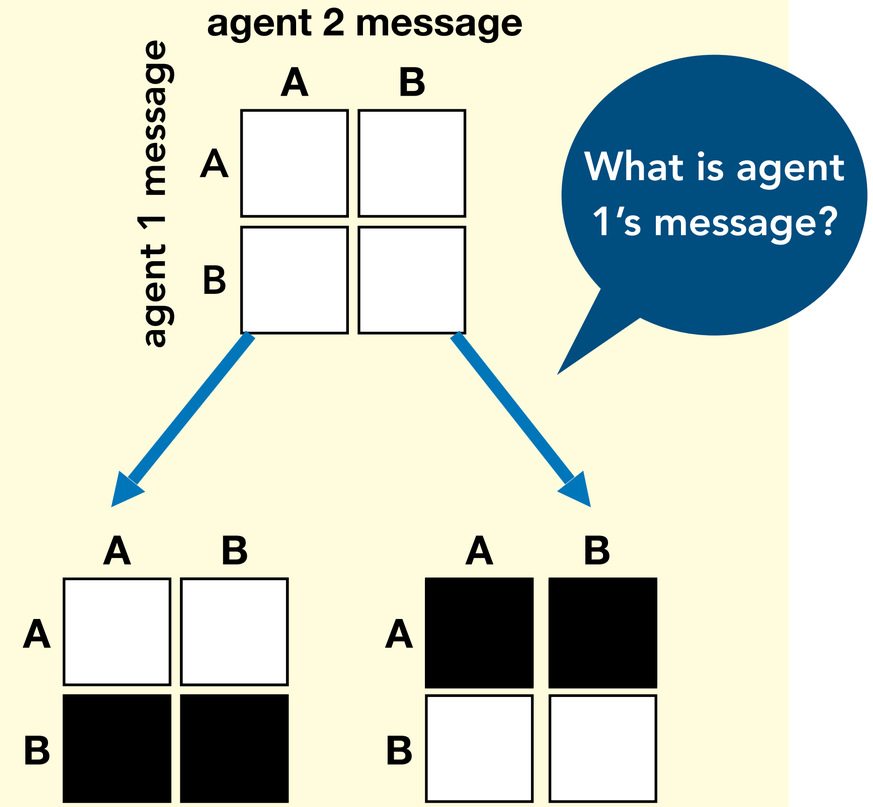
$\mathbf{m} \mapsto m_i$

Count msgs

$\text{count} : M^n \to \tilde{M} := \mathbb{N}^M$

$\mathbf{m} \mapsto (|\{i : m_i = m\}|)_{m \in M}$

↪ back



Example. A simple protocol.

- Two agents $N = \{1, 2\}$
- Type space $\Theta = \{1,2,3\}$
- Message space $M = \{A, B\}$

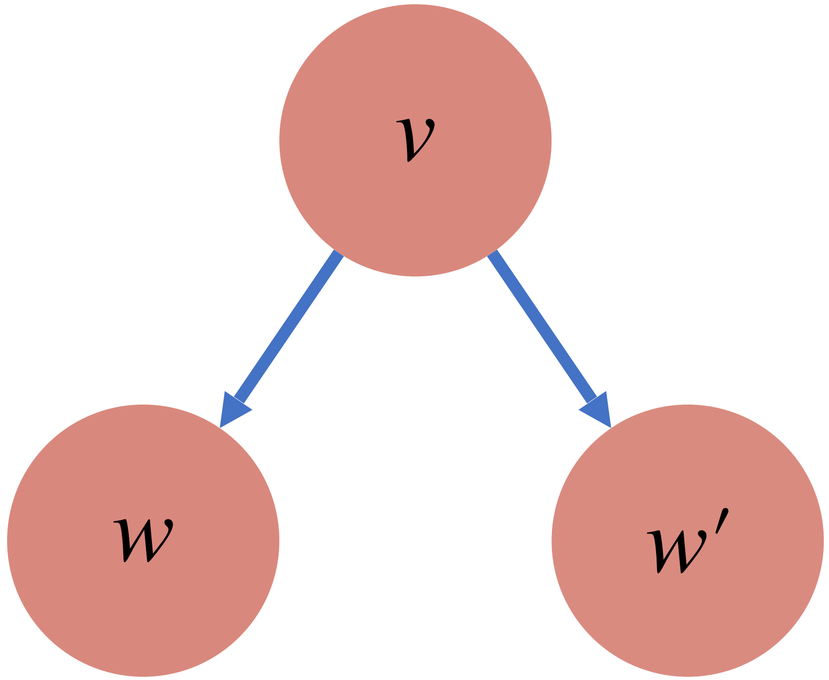
TECHNOLOGIES

Indirect Protocols

Definition.

A (direct) **protocol** is an extensive-form game in which agents repeatedly submit **messages** $\mathbf{m} \in M^n$ from a set M according to reporting strategies $(\sigma_1, \sigma_2, \ldots, \sigma_n)$. A node v must be a function of the responses of the technology,

$$(f_w(\mathbf{m}_w))_{w \in \text{ancestor}(v)}.$$



The designer learns about the types through a protocol.

Indirect Protocols

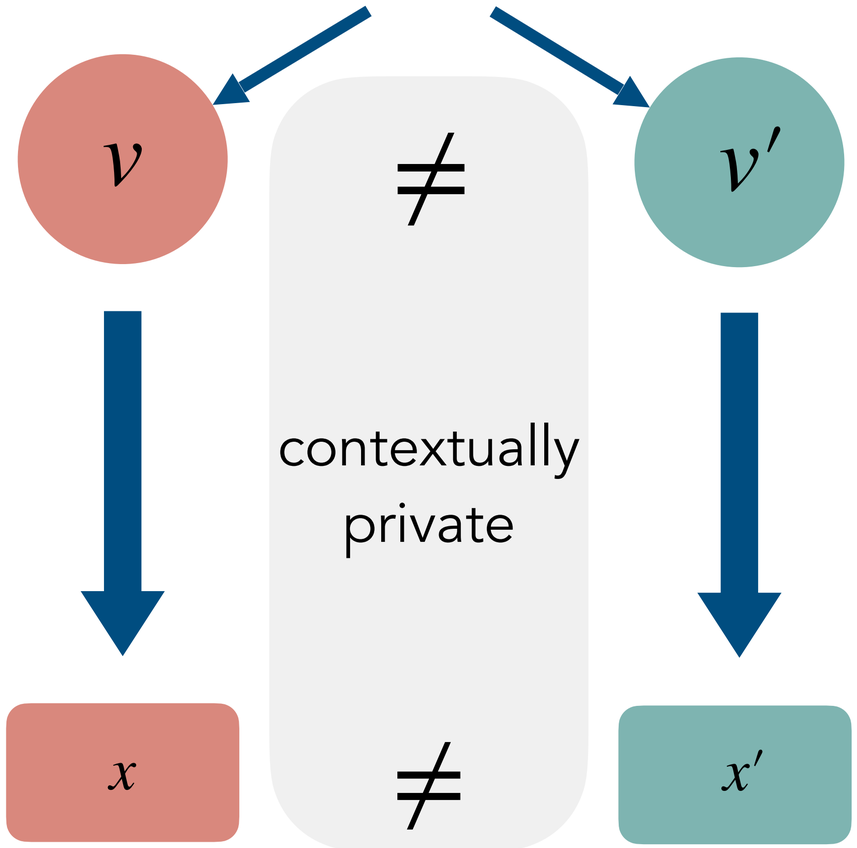
Definition.

A **protocol P is contextually private** if a unilateral change in messages $(m_i, \mathbf{m}_{-i})$, $(m_i', \mathbf{m}_{-i})$ that P "distinguishes" lead to different outcomes

$$x(m_i, \mathbf{m}_{-i}) \neq x(m_i, \mathbf{m}_{-i}).$$

Definition.

A **social choice function ϕ is contextually private** if there are reporting strategies $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_n)$ such that $(P, \boldsymbol{\sigma})$ "implement" ϕ and P is contextually private.



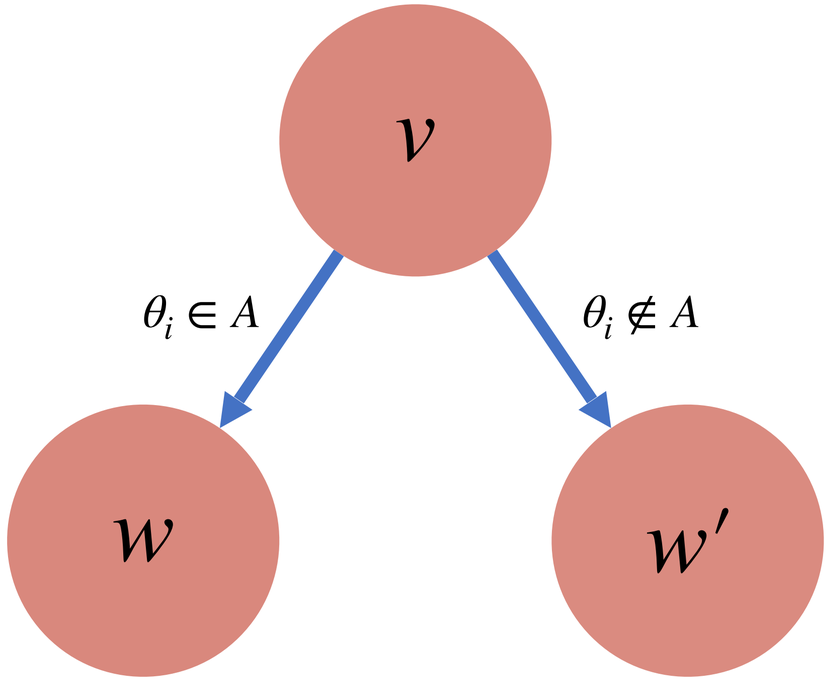
Indirect Protocols

Definition.

Let $S_{\mathrm{SE}} = \{\pi \circ \mathrm{proj}_i \mid \pi\colon \Theta_i \to \Theta_i\}$, the sequential elicitation technology.

Proposition.

Let $M \supseteq \Theta$. For every S_{SE}-protocol P for ϕ with strategy $\boldsymbol{\sigma}$ there exists a contextual privacy equivalent protocol P' for ϕ with strategy $\sigma_i\colon (\theta_i, h) \mapsto \theta_i$.



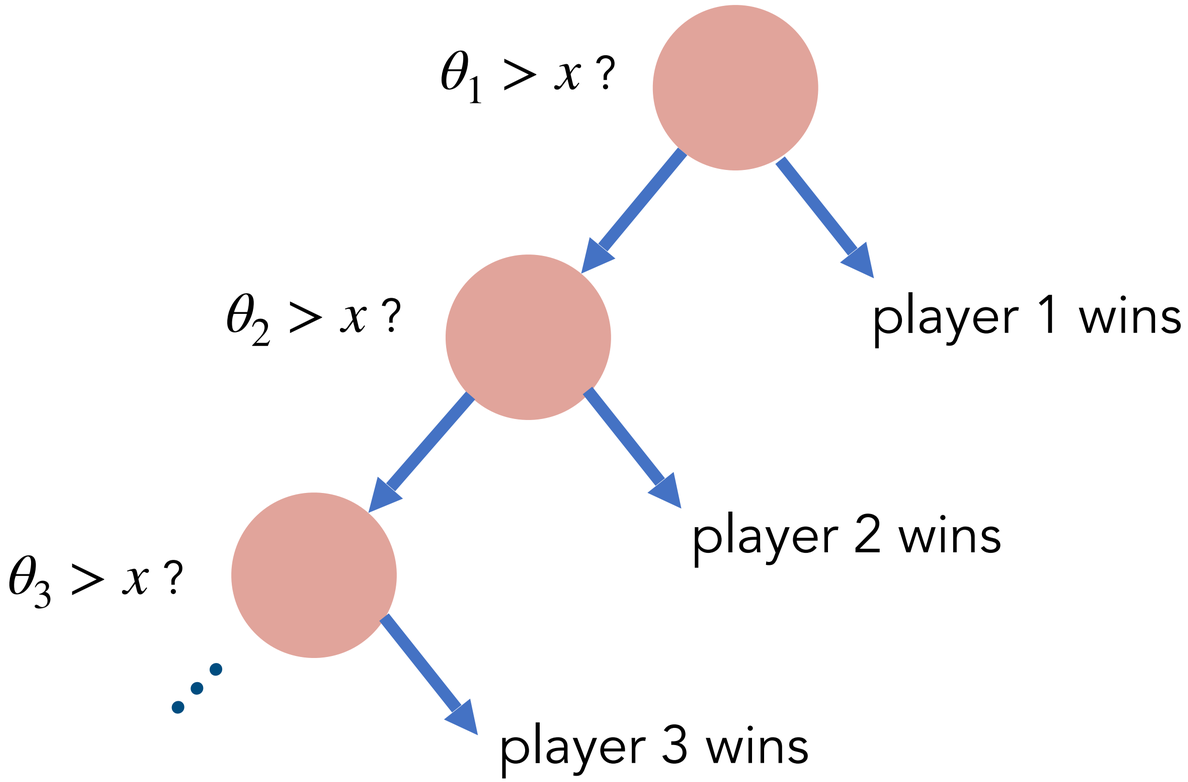
S_{SE} is necessary for this result to hold. Consider, e.g., counting.

FPA Is Contextually Private

Proposition.

The first-price auction choice rule is contextually private under sequential elicitation protocols, with a descending ("Dutch") protocol.

Illustration of proof.



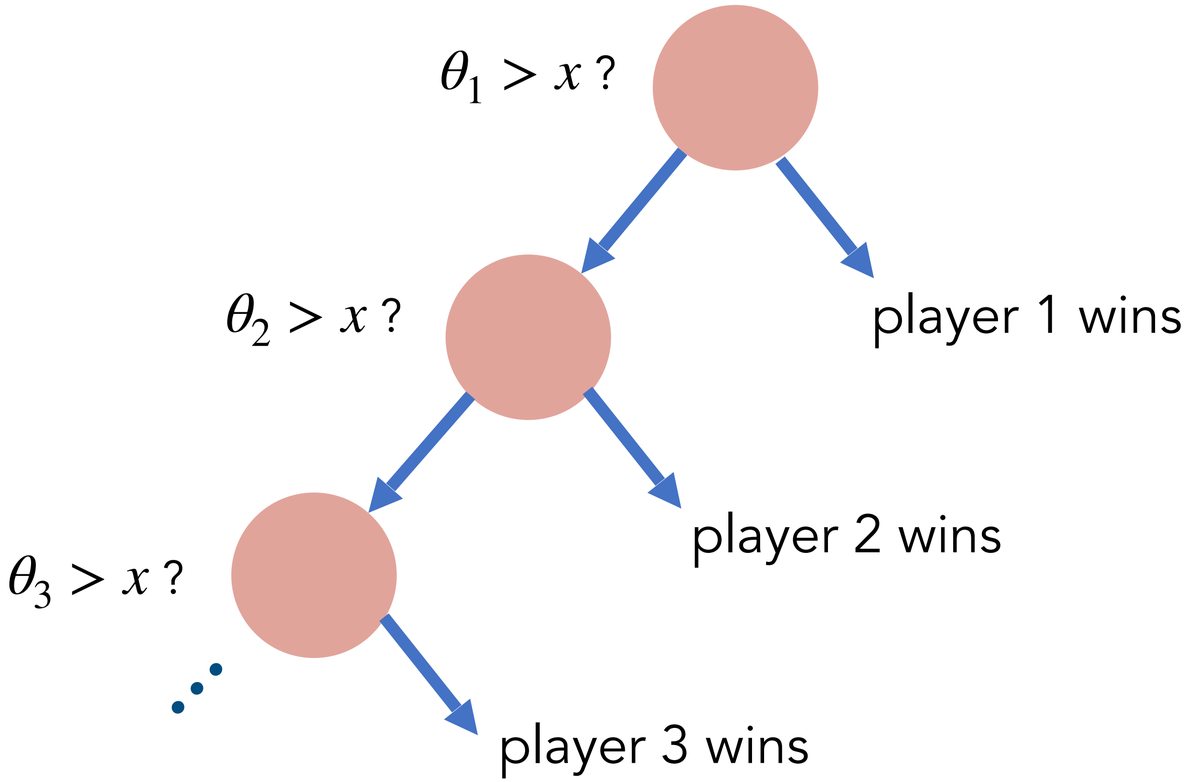
FPA Is Contextually Private

Proposition.

The first-price auction choice rule is contextually private under sequential elicitation protocols, with a descending ("Dutch") protocol.

Illustration of proof.

If at any point, one agent had answered "yes" instead of "no," the outcome would be different.



VARIANTS

Definition.

A protocol P is **individually** contextually private if all type profiles at distinct terminal nodes v, v' that differ for agent i

$$(\theta_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_v \in \boldsymbol{\Theta}_v \,, \;\; (\theta'_i, \boldsymbol{\theta}_{-i}) = \boldsymbol{\theta}_{v'} \in \boldsymbol{\Theta}_{v'}$$

lead to different outcomes for agent i

$$\phi_i(\boldsymbol{\theta}_v) \neq \phi_i(\boldsymbol{\theta}_{v'}).$$

Proposition.

ϕ is individually contextually private if and only if it is non-bossy and contextually private.

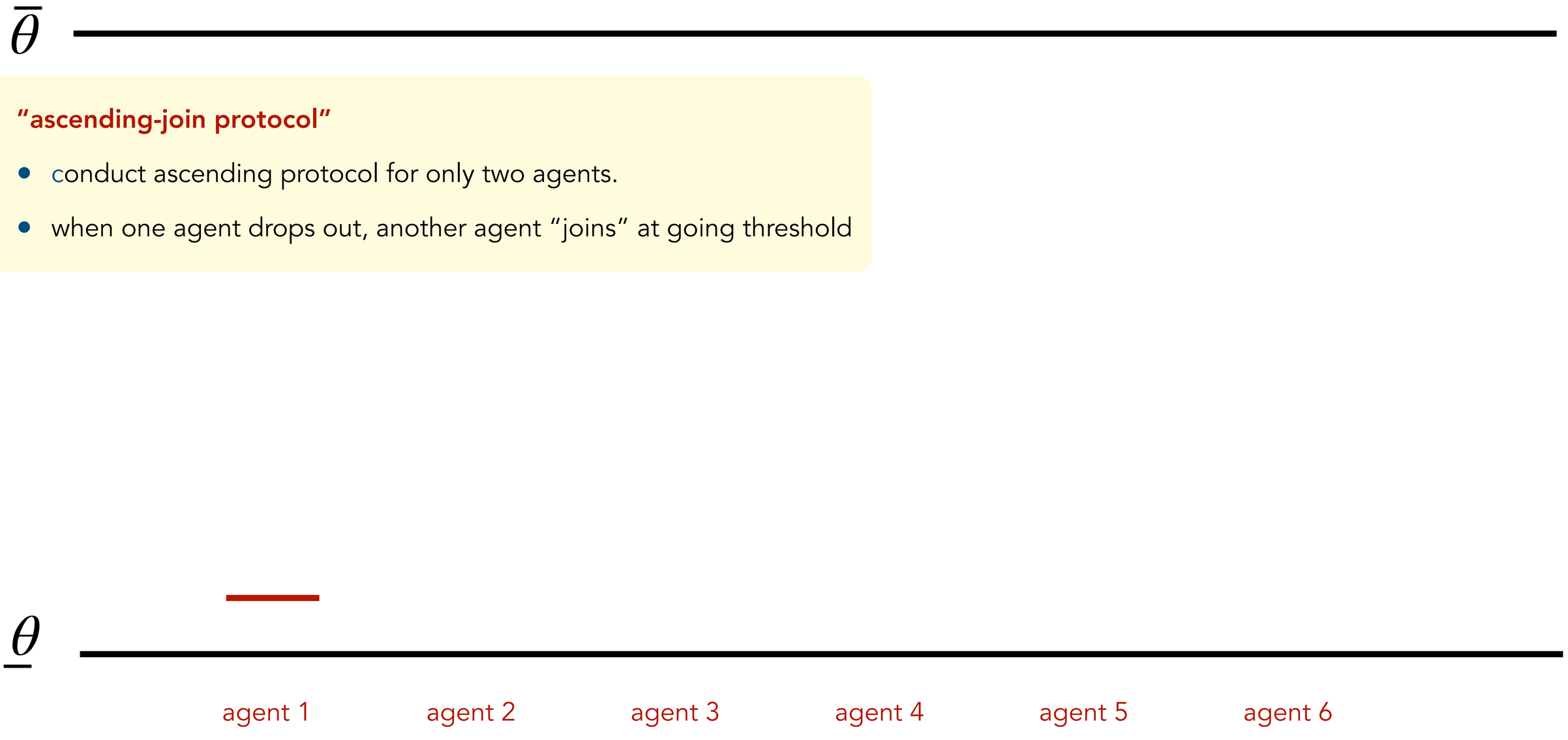
ϕ is non-bossy if

$$\phi_i(\theta_i, \boldsymbol{\theta}_{-i}) = \phi_i(\theta'_i, \boldsymbol{\theta}_{-i})$$

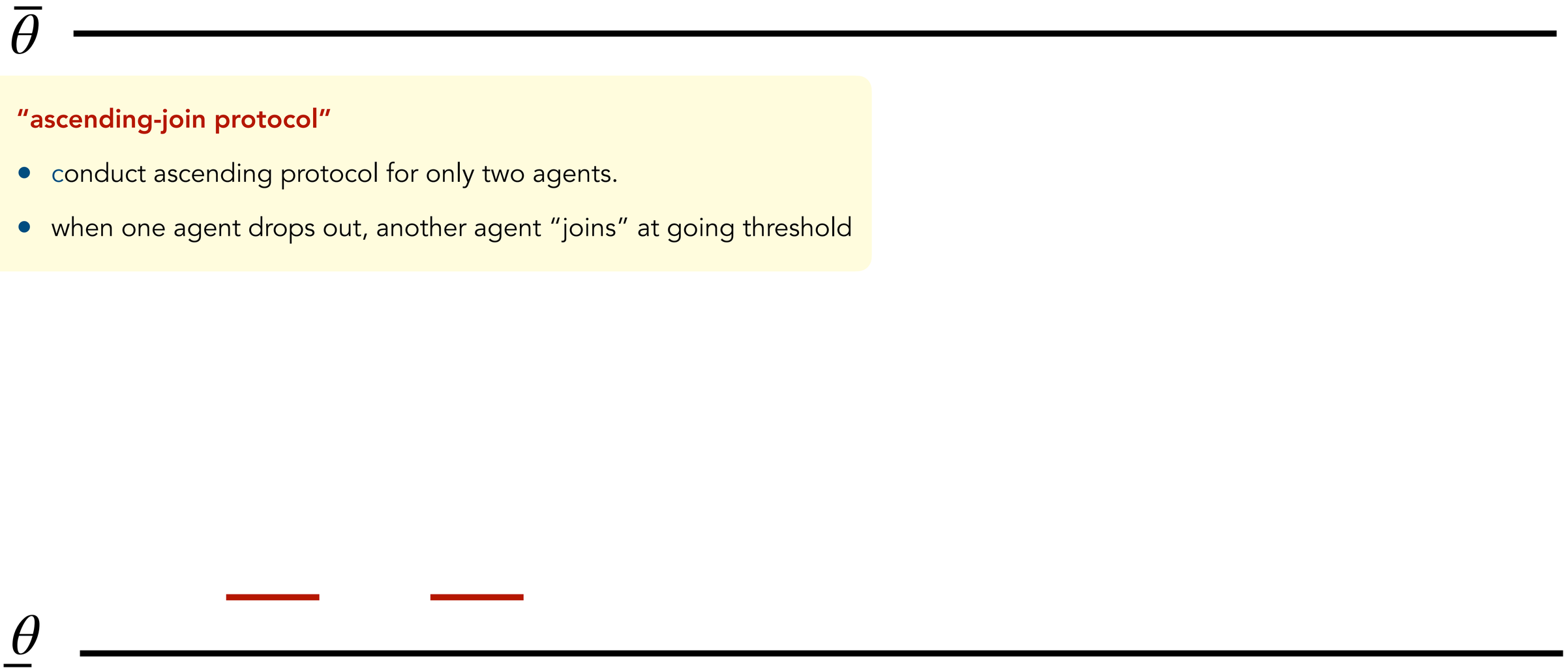
implies

$$\phi(\theta_i, \boldsymbol{\theta}_{-i}) = \phi(\theta'_i, \boldsymbol{\theta}_{-i}) \,.$$

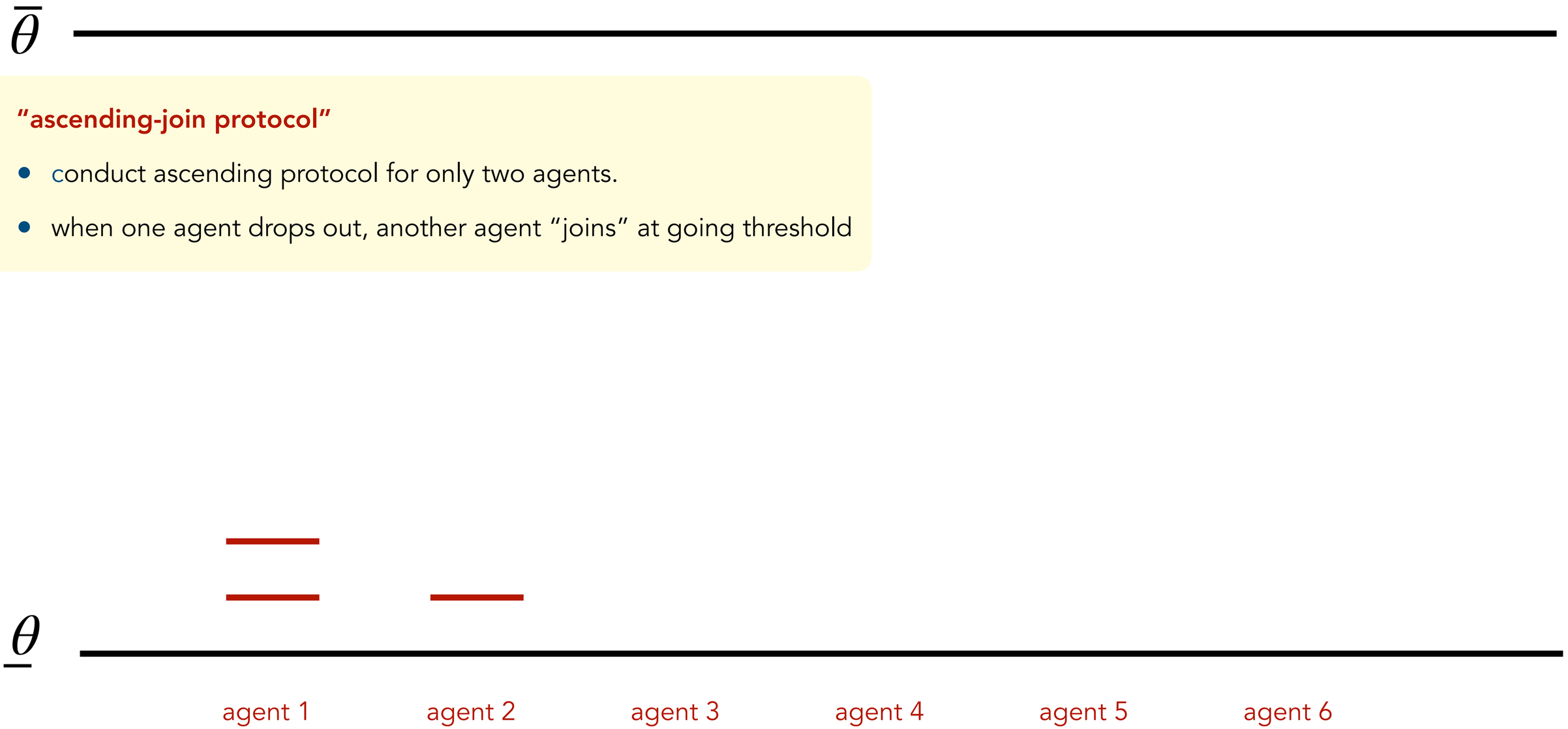
A Maximally Contextually Private Protocol



A Maximally Contextually Private Protocol



A Maximally Contextually Private Protocol



A Maximally Contextually Private Protocol

$\overline{\theta}$

"ascending-join protocol"

- conduct ascending protocol for only two agents.
- when one agent drops out, another agent "joins" at going threshold

$\underline{\theta}$

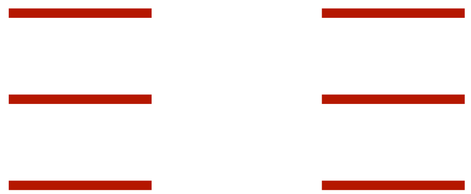
agent 1 agent 2 agent 3 agent 4 agent 5 agent 6

A Maximally Contextually Private Protocol

$\overline{\theta}$

"ascending-join protocol"

- conduct ascending protocol for only two agents.
- when one agent drops out, another agent "joins" at going threshold



$\underline{\theta}$

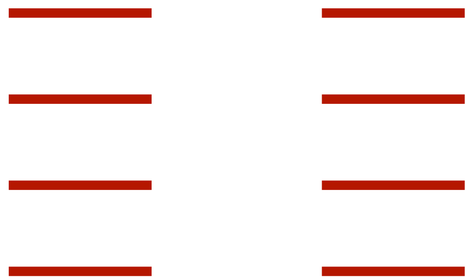
agent 1 agent 2 agent 3 agent 4 agent 5 agent 6

A Maximally Contextually Private Protocol

$\overline{\theta}$

"ascending-join protocol"

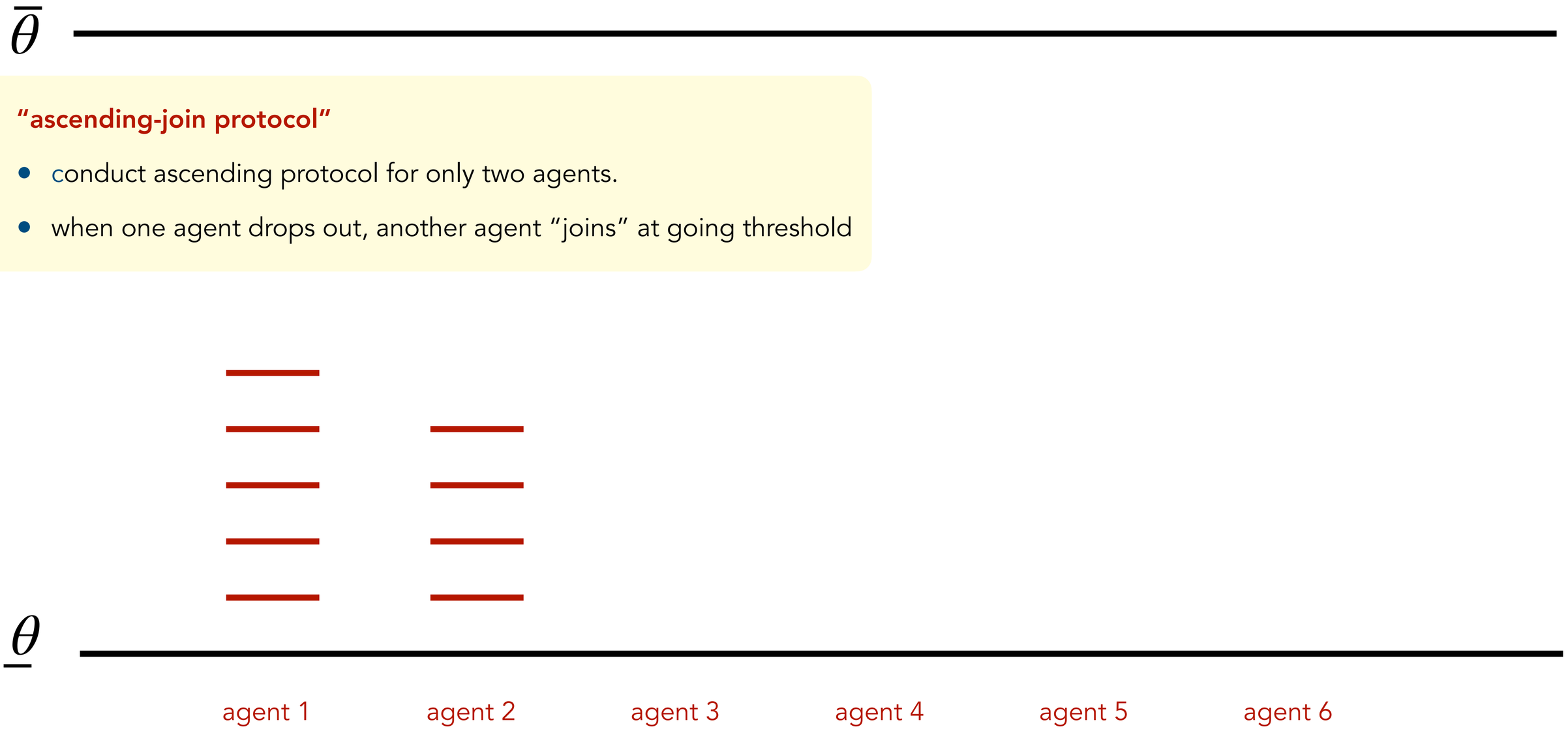
- conduct ascending protocol for only two agents.
- when one agent drops out, another agent "joins" at going threshold



$\underline{\theta}$

agent 1 agent 2 agent 3 agent 4 agent 5 agent 6

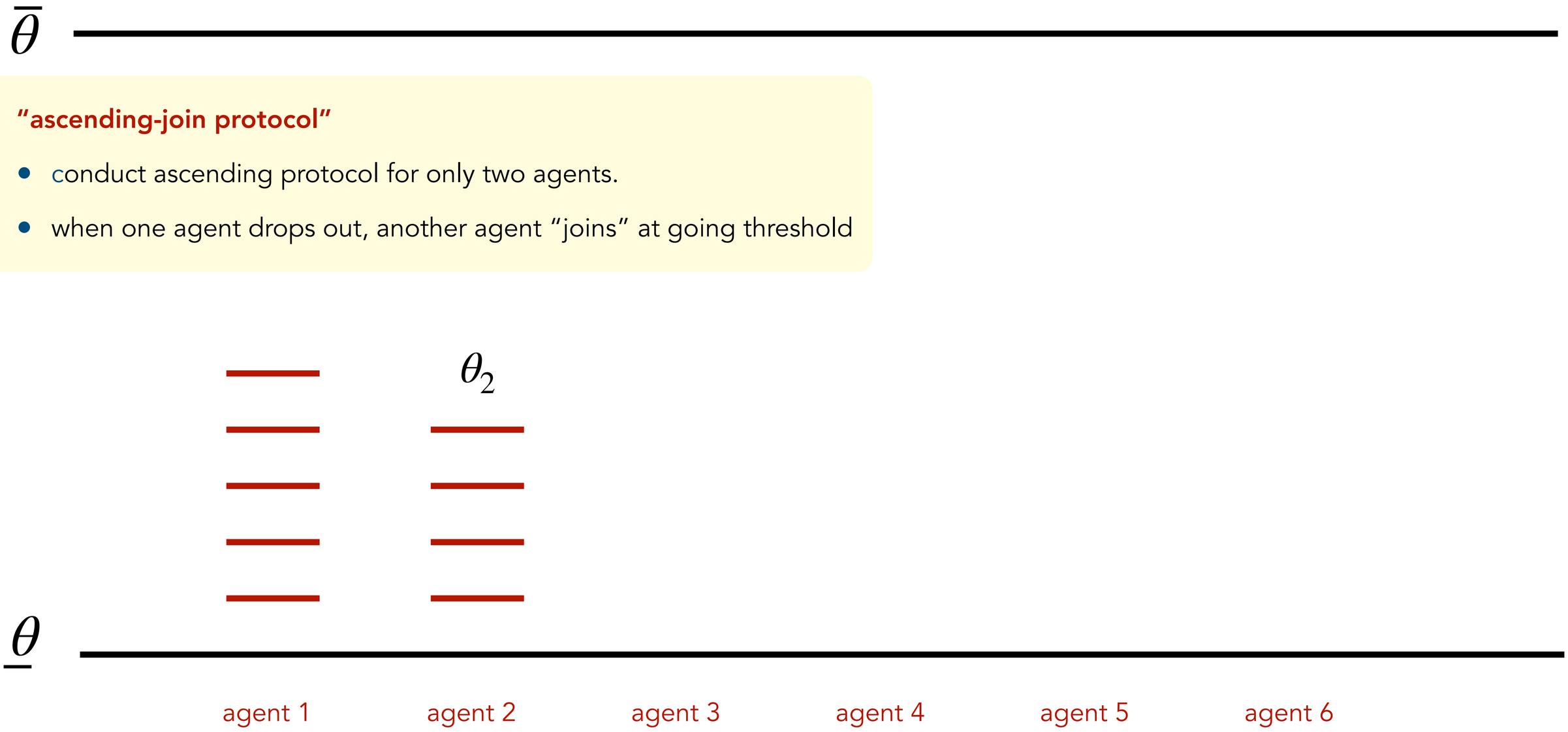
A Maximally Contextually Private Protocol



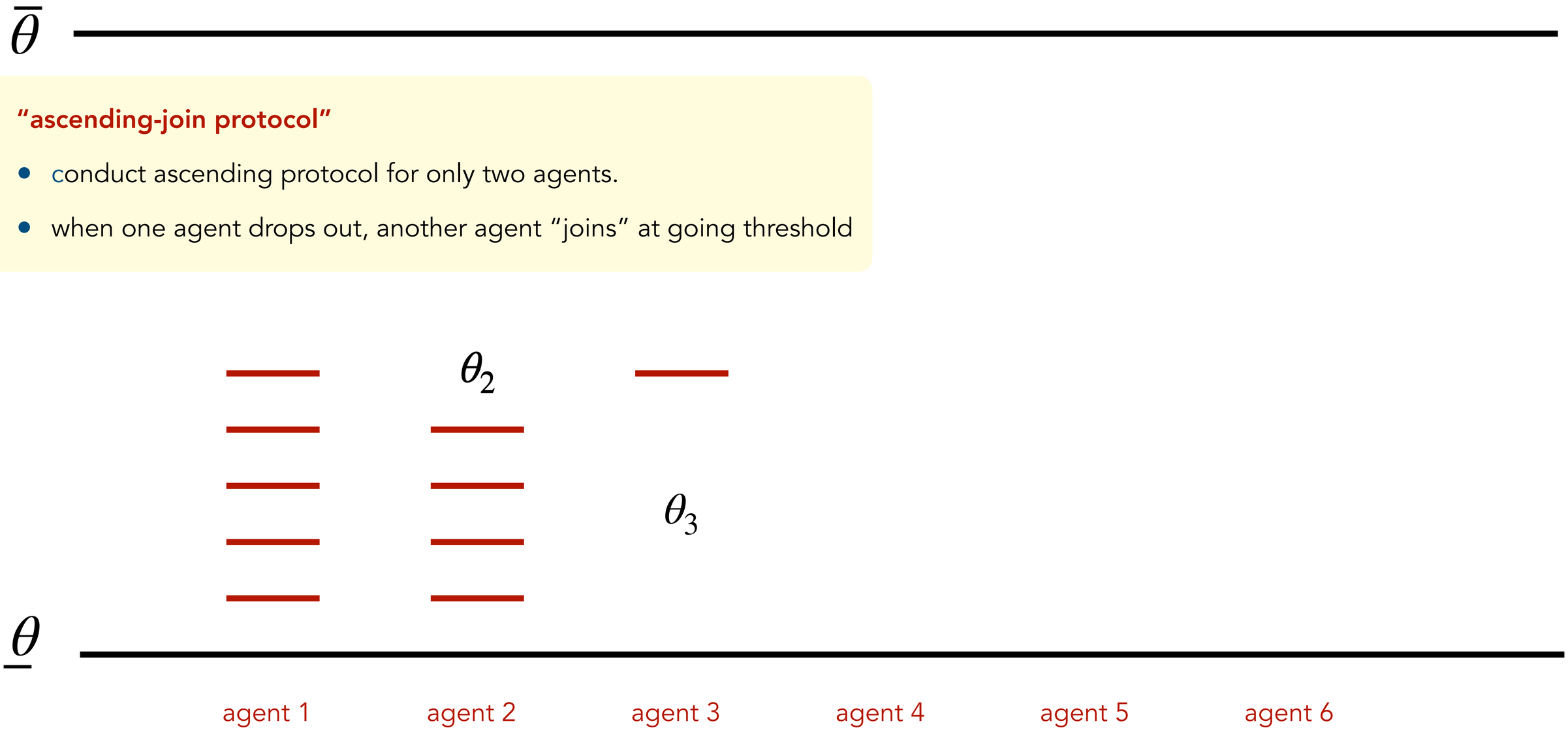
"ascending-join protocol"

- conduct ascending protocol for only two agents.
- when one agent drops out, another agent "joins" at going threshold

A Maximally Contextually Private Protocol



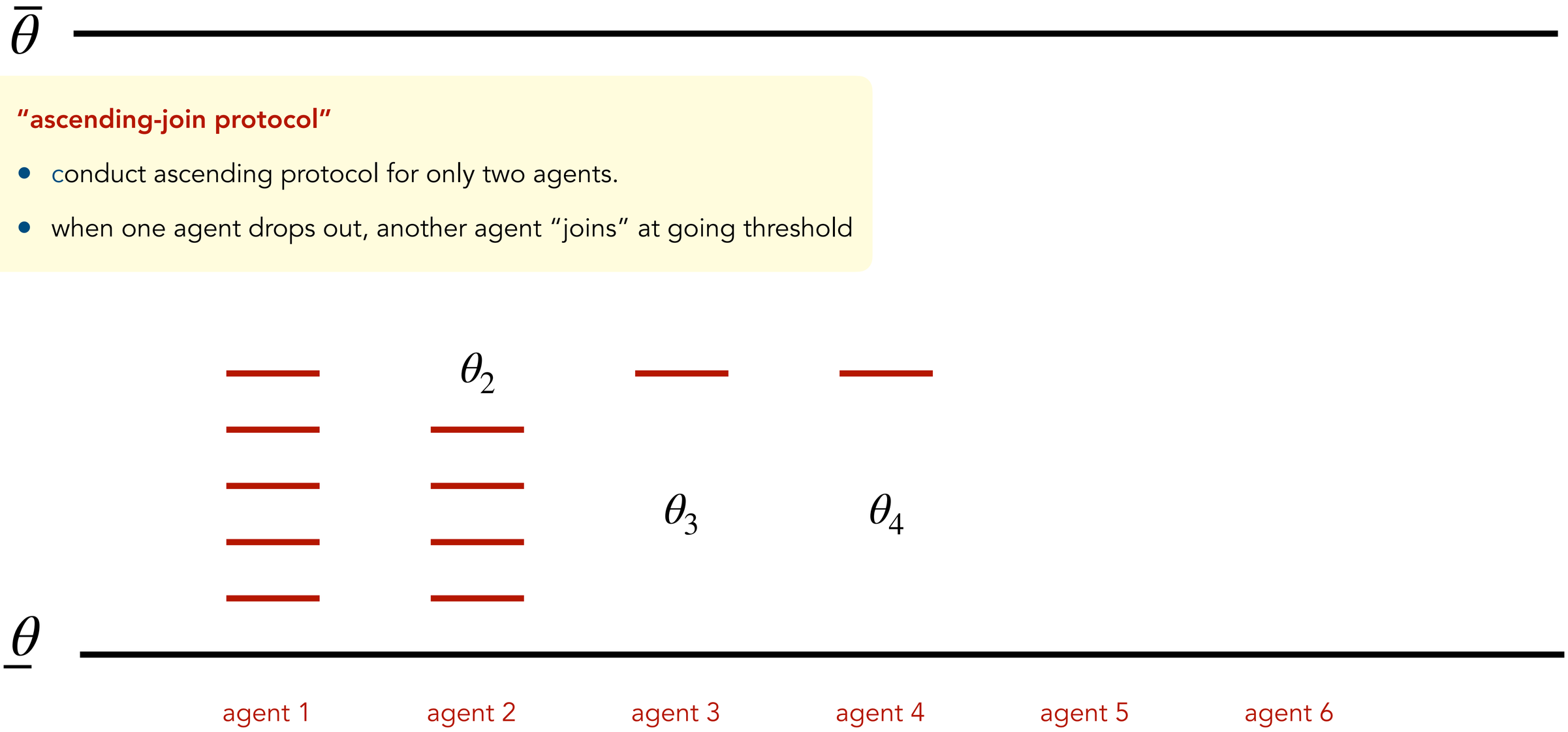
A Maximally Contextually Private Protocol



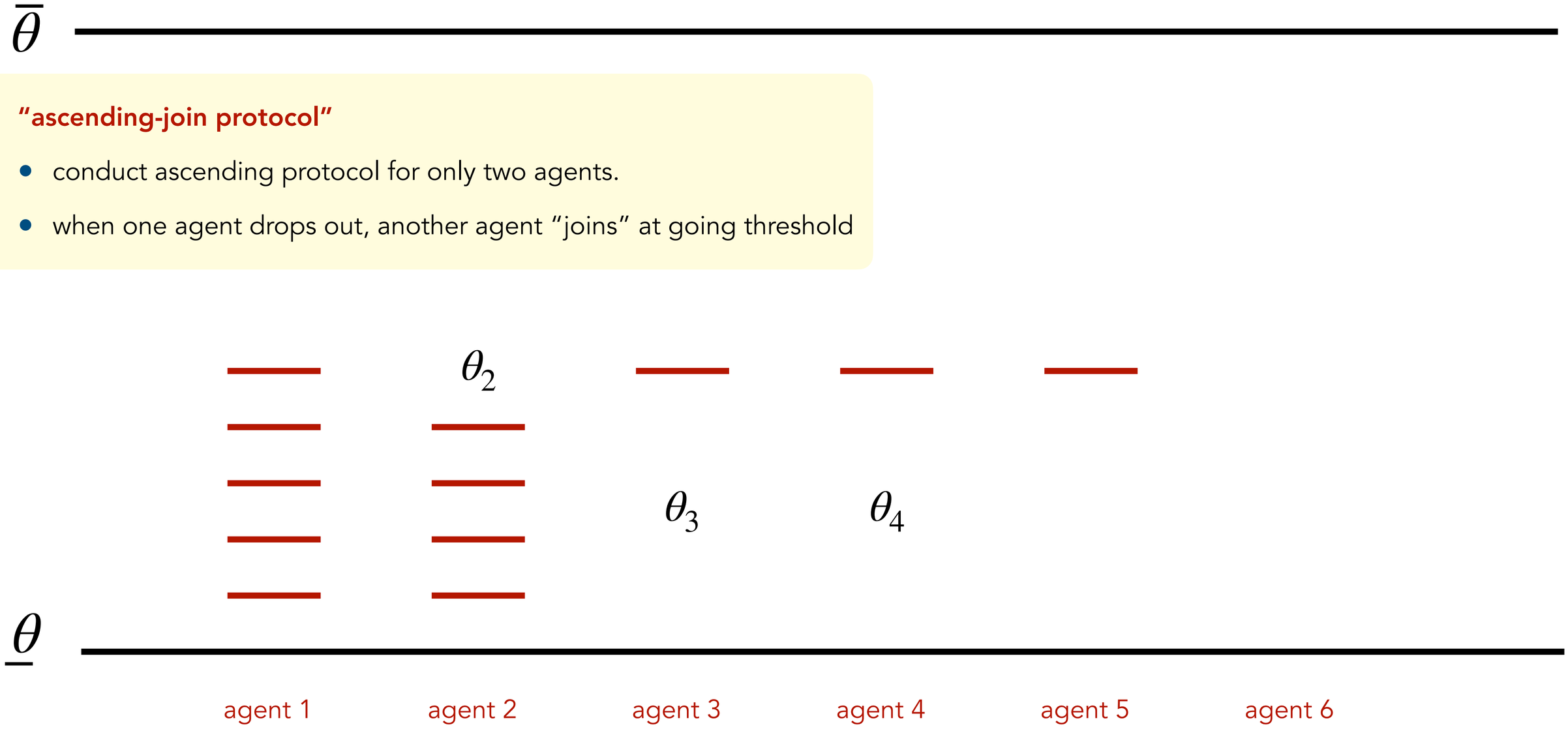
"ascending-join protocol"

- conduct ascending protocol for only two agents.
- when one agent drops out, another agent "joins" at going threshold

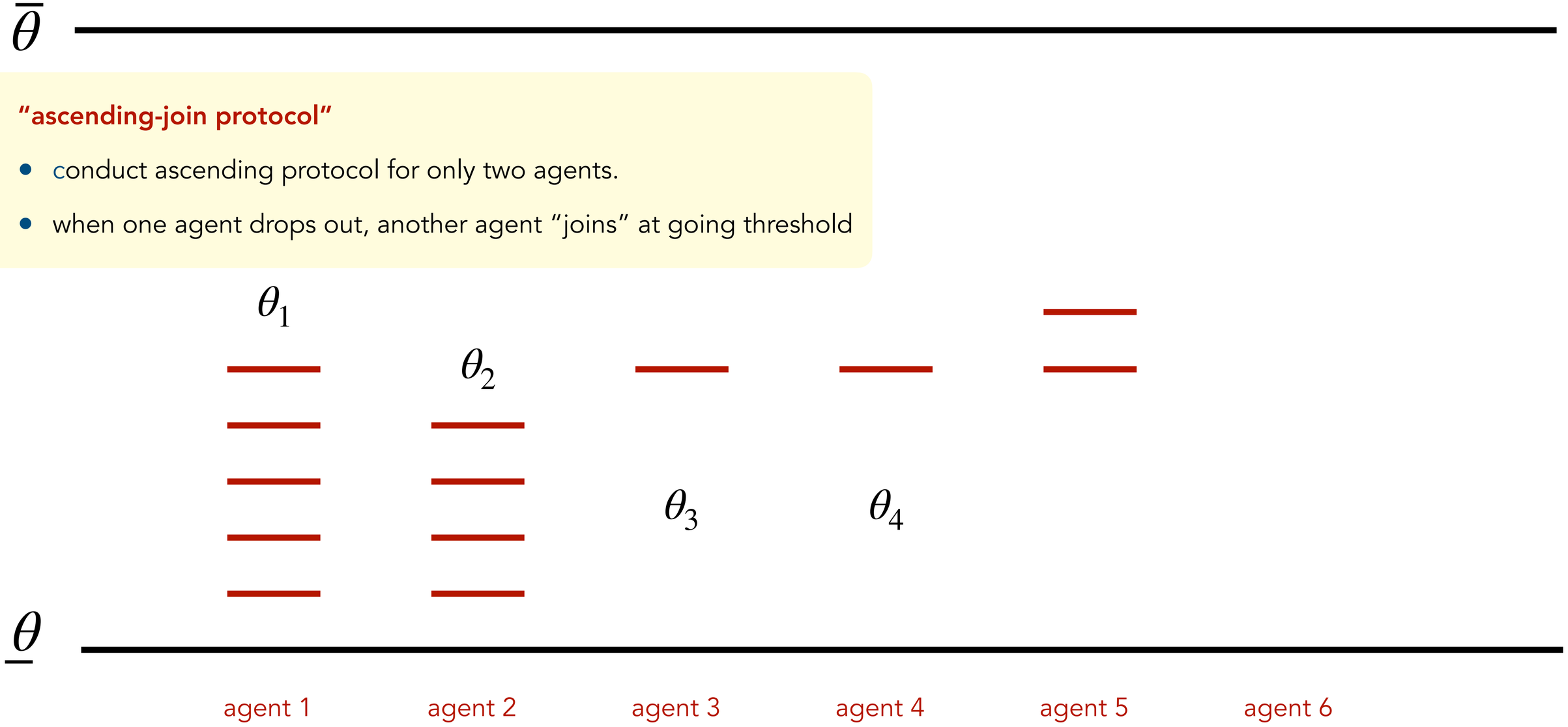
A Maximally Contextually Private Protocol



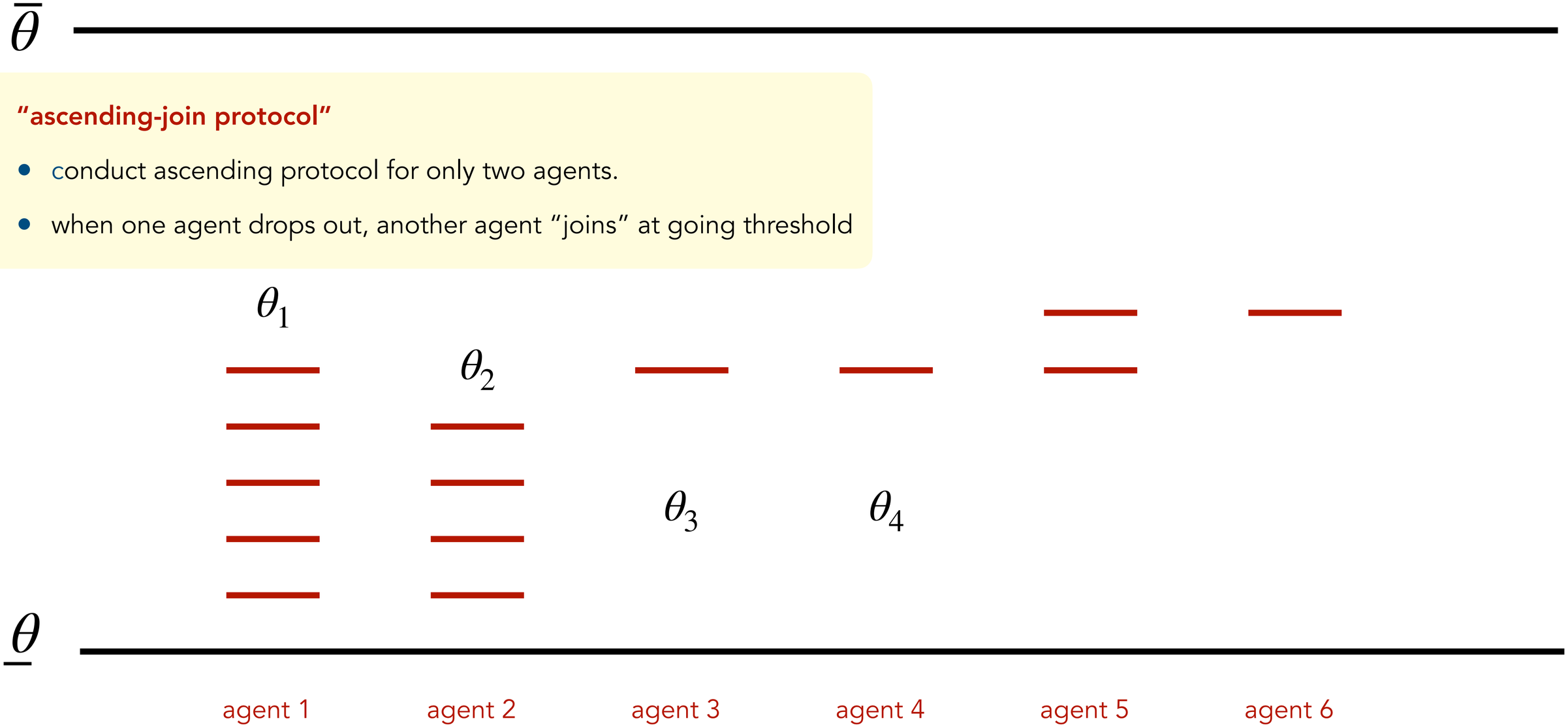
A Maximally Contextually Private Protocol



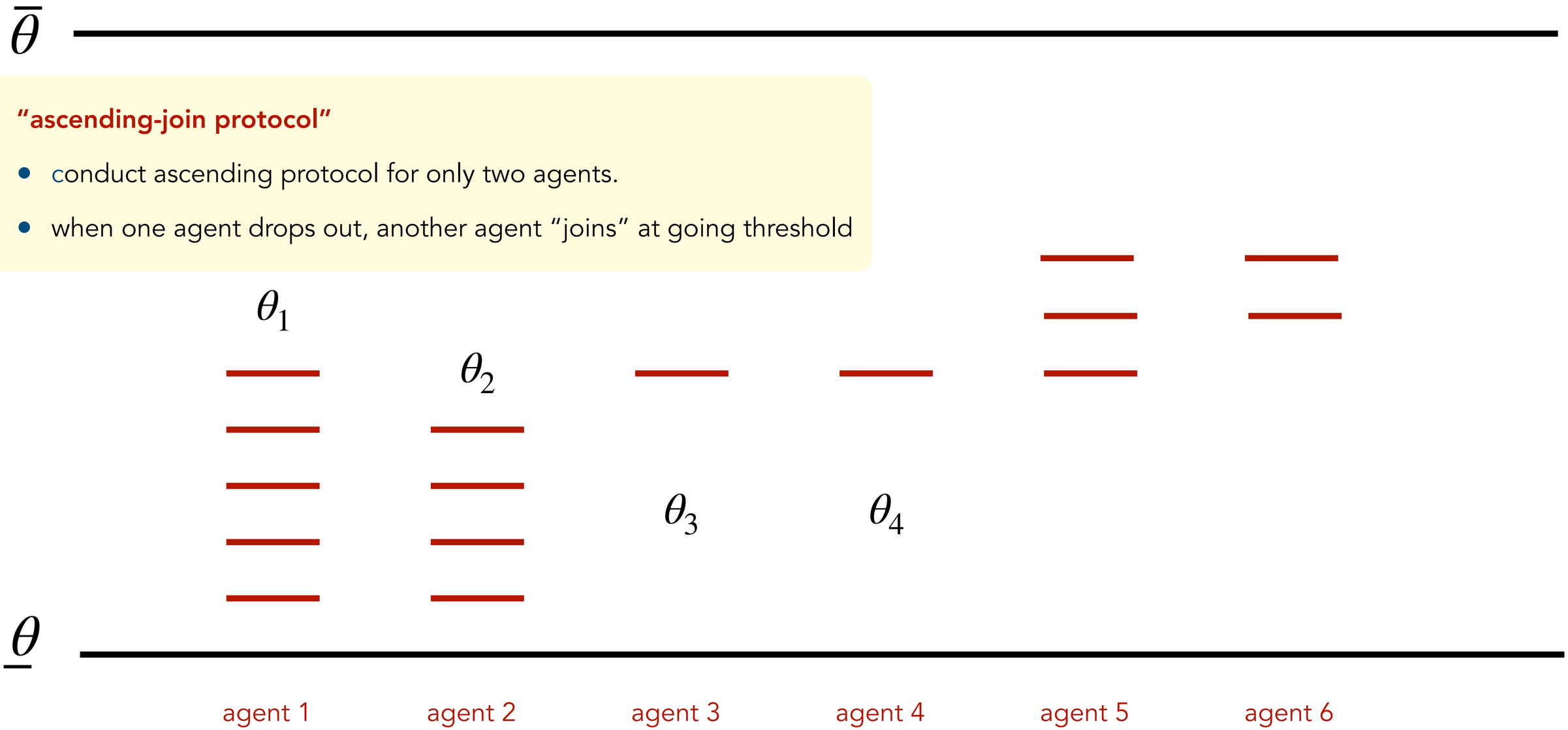
A Maximally Contextually Private Protocol



A Maximally Contextually Private Protocol



A Maximally Contextually Private Protocol



A Maximally Contextually Private Protocol