Secure Communication in Networks: Mechanism Design, Games and Cryptography

Tristan Tomala

HEC Paris

GIPSY, Rennes, November 2010

References

- Mechanism design: Myerson, Maskin,....
- Dolev, Dwork, Waarts and Yung, 1993 (ACM). Perfectly Secure Message Transmission.
- Rabin and Ben-Or, 1989 (ACM). Verifiable Secret Sharing and Multiparty Protocols with Honest Majority.
- Shamir, 1979 (ACM). How to share a secret.
- Monderer and Tennenholtz, 1999 (AAAI). Distributed Games: From Mechanisms to Protocols.
- Renou and Tomala, 2009. Mechanism Design and Communication Networks.
- Renault, Renou and Tomala, 2010. Transmitting messages secretly.

Mechanism design

A *social environment* $\mathscr{E}$ is:

- A set of players $N := \{1, \ldots, n\}$;
- A finite set of feasible alternatives A;
- A finite set Θ_i of types of player i;
- A belief $P_i(\cdot|\theta_i)$ over Θ_{-i};
- A utility function $u_i : A \times \Theta \longrightarrow \mathbb{R}$ for each player i.

We assume $P_i(\theta_{-i}|\theta_i) > 0$ for all $(\theta_i, \theta_{-i}) \in \Theta$ and for all $i \in N$.

- The environment has a *worst outcome* if there exists $\underline{a} \in A$ such that for each player i, each type profile θ and each $a \in A \setminus \{\underline{a}\}$, $u_i(\underline{a}, \theta) < u_i(a, \theta)$.

Social choice functions

A social choice function is a mapping $f : \Theta \rightarrow A$.

Such a function is incentive compatible if $\forall i, \theta_i, \theta_i'$,

$$\sum_{\theta_{-i}} u_i(f(\theta_i, \theta_{-i}), \theta_i, \theta_{-i}) P_i(\theta_{-i}|\theta_i) \geq \sum_{\theta_{-i}} u_i(f(\theta_i', \theta_{-i}), \theta_i, \theta_{-i}) P_i(\theta_{-i}|\theta_i)$$

This is an equilibrium outcome of a game of direct communication between the players and the designer.
Examples:
-Dictatorial s.c.f.
-2nd price auction.

Communication networks

- A communication network is a directed graph with $n+1$ vertices representing the n players and the designer (player 0). There is a directed edge ij from player i to player j, if i can send a message to j securely and privately.
- $C(i) = \{j \in N \cup \{0\} : ij \in \mathcal{N}\} = \{\textit{successors of } i\}$
- $D(i) = \{j \in N \cup \{0\} : ji \in \mathcal{N}\} = \{\textit{predecessors of } i\}$

We assume that the network is strongly 1-connected (for each $i \in N$, there exists a directed path from i to 0) and *acyclic*. Each player speaks only once and the designer sends no message.

Mechanisms on communication networks

Given a network $\mathcal{N}$, a mechanism is a pair $\langle (M_{ij})_{ij\in\mathcal{N}}, g\rangle$ where for each edge ij, M_{ij} is the set of messages that player i can send to player j, and $g : \times_{i\in D(0)} M_{i0} \to A$ is the allocation rule. The associated game unfolds as follows.

- Each player i reads the messages he receives from players in $D(i)$. Then he send messages to players in $C(i)$ (he may send different messages to different players).
- The designer reads the messages he receives from players in $D(0)$, and selects an outcome accordingly.

Implementation on a network

Let $\mathbb{P}_{\sigma,\theta}$ be the probability distributions over messages induced by the strategy σ at state θ.

Definition

The mechanism $\langle (M_{ij})_{ij\in\mathcal{N}}, g\rangle$ implements f on $\mathcal{N}$ if there exists a Bayesian-Nash equilibrium σ^* such that:

$$g((m^*_{i0})_{i\in D(0)}) = f(\theta)$$

for all $\theta \in \Theta$ and for all $(m^*_{i0})_{i\in D(0)}$ in the support of $\mathbb{P}_{\sigma^*,\theta}$.

Let $F_{\mathcal{N}}(\mathcal{E})$ be the set of functions partially implementable on $\mathcal{N}$ when the environment is $\mathcal{E}$.

From the revelation principle: $F_{\mathcal{N}}(\mathcal{E}) \subseteq IC$ and $F_{\mathcal{N}^\star}(\mathcal{E}) = IC$ (all players directly connected to 0).

The goal of this project is to give conditions on $\mathcal{N}$ for which $F_{\mathcal{N}}(\mathcal{E}) = IC$, $\forall \mathcal{E}$.

Reformulation: Secret information transmission

A necessary condition for implementation of all IC function is the following.

Definition

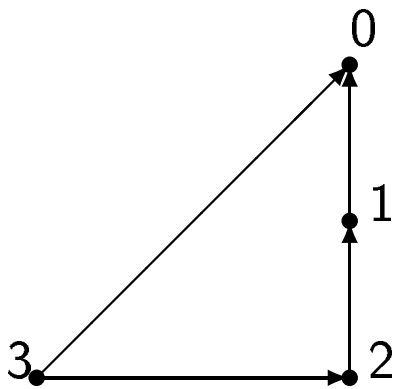
Secret information transmission is possible on the network if there exists a communication protocol such that:
-The designer correctly learns all types,
-No player gets information beyond his own type. I.e. the messages received by j are probabilistically independent from θ_i.

Example: a contribution game (provision of a public good).

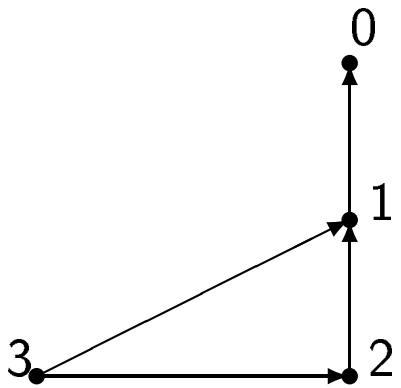
Definition

The communication network $\mathcal{N}$ is *weakly 2-connected* if for each player $i \in N \setminus D(0)$, there exist two disjoint paths (not necessarily directed) π_i^1 and π_i^2 from player i to the designer.

Example 1: A network weakly 2-connected.



Example 2: A network not weakly 2-connected: player 1 "controls" all information.



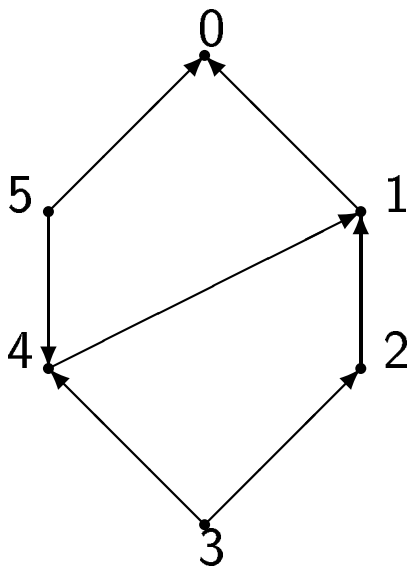
Worst outcome

Theorem (Renou-T09)

-In all environments $\mathscr{E}$ with a worst outcome, $F_{\mathscr{N}}(\mathscr{E}) = IC$ if and only if $\mathscr{N}$ is weakly 2-connected.
-Secret information transmission is possible if and only if $\mathscr{N}$ is weakly 2-connected.

An example

Consider the following network:



- All directed paths from the unique predecessor of 2 (player 3) to the designer, go through player 1.
- Secret information transmission is possible and all IC functions are implementable (under worst outcome).

Probabilistic coding

Assume w.l.o.g. $\Theta_i \subseteq F_2^n \setminus \{0\}$.

- Let X, Y be independent r.v.'s variables in F_2^n. If X is uniformly distributed, so is $X + Y$.
- Let $X_1, \ldots, X_K, \theta$ be independent r.v.'s such that all X_k's are uniformly distributed. Let

$$Y_j \in \text{vect}\{X_1, \ldots, X_K, \theta\}, j = 1, \ldots, J$$

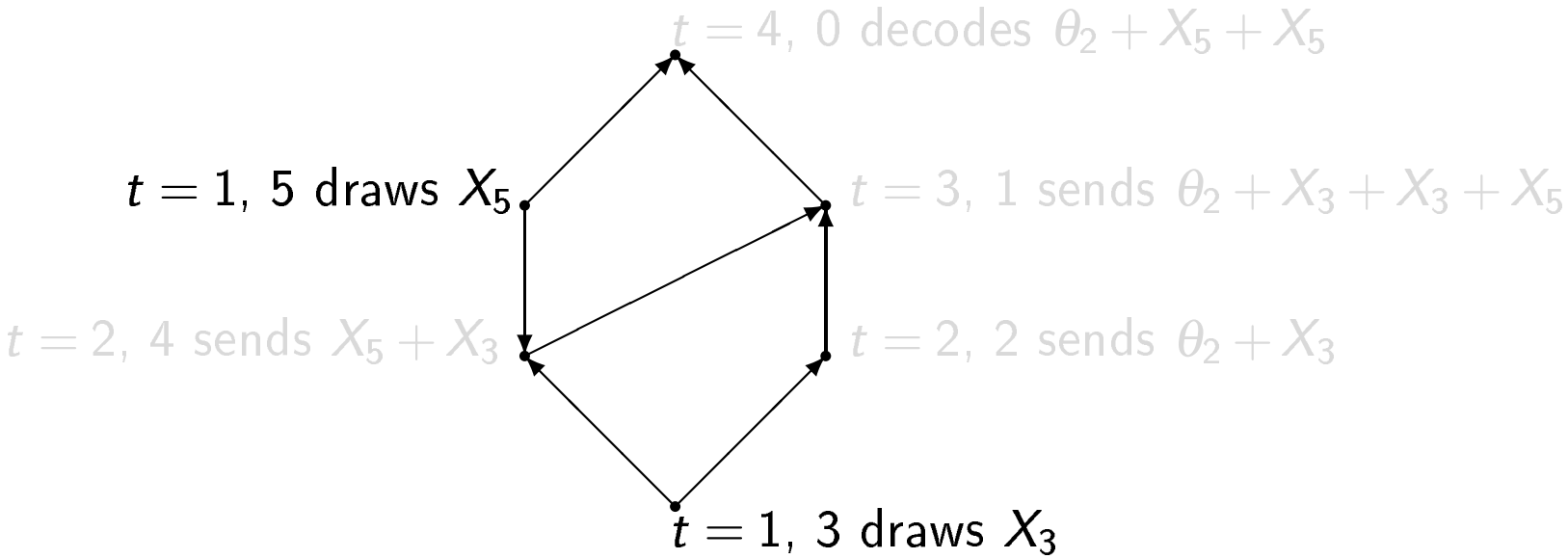
If $\theta \notin \text{vect}\{Y_1, \ldots, Y_J\}$, then $(Y_1, \ldots, Y_J)$ is independent from θ.

An example

The protocol for transmitting θ_2 is the following.

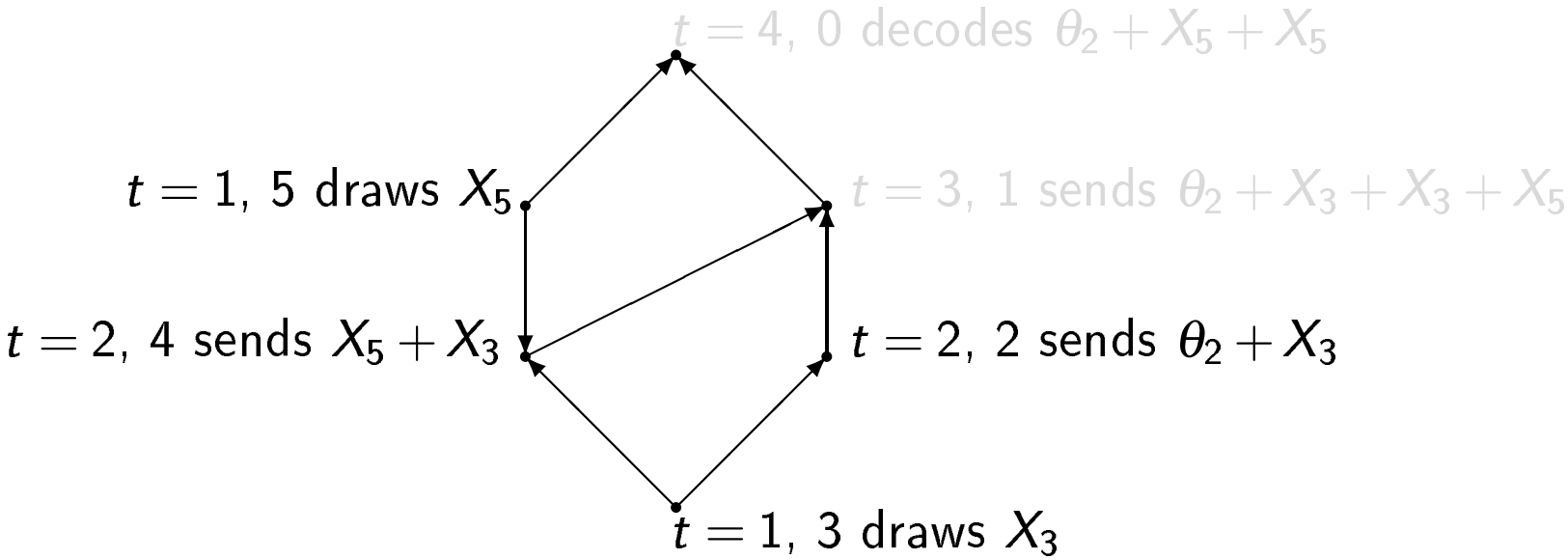
An example

The protocol for transmitting θ_2 is the following.



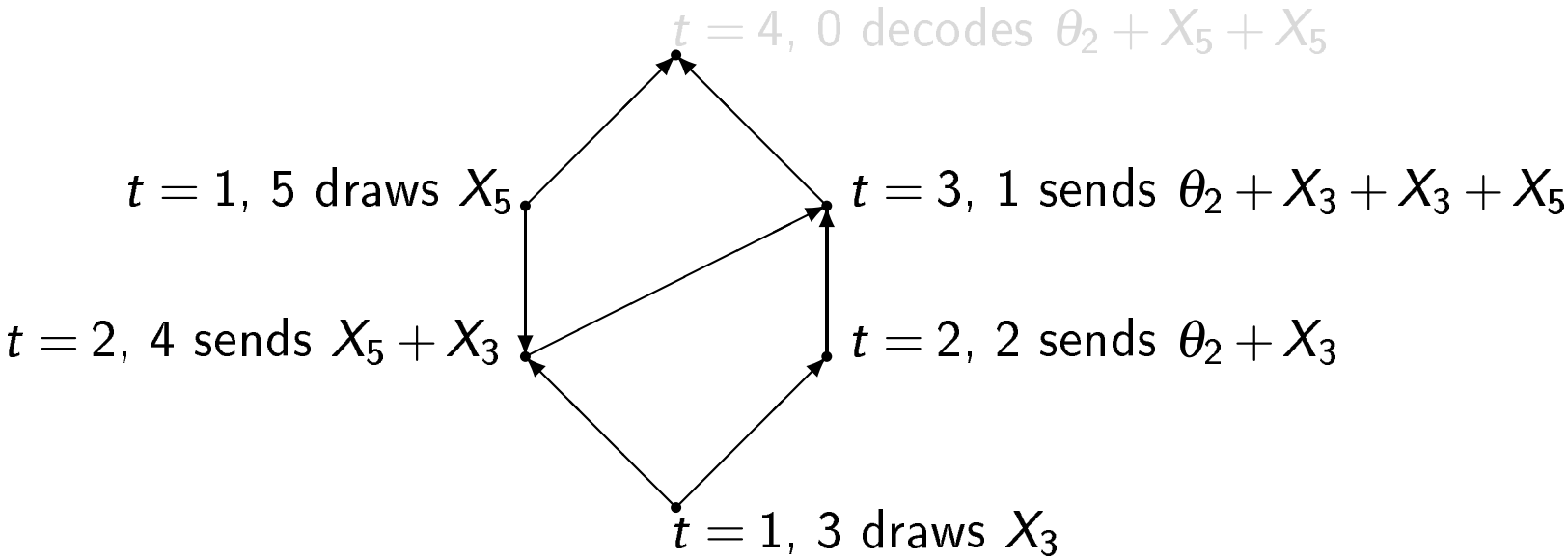
An example

The protocol for transmitting θ_2 is the following.



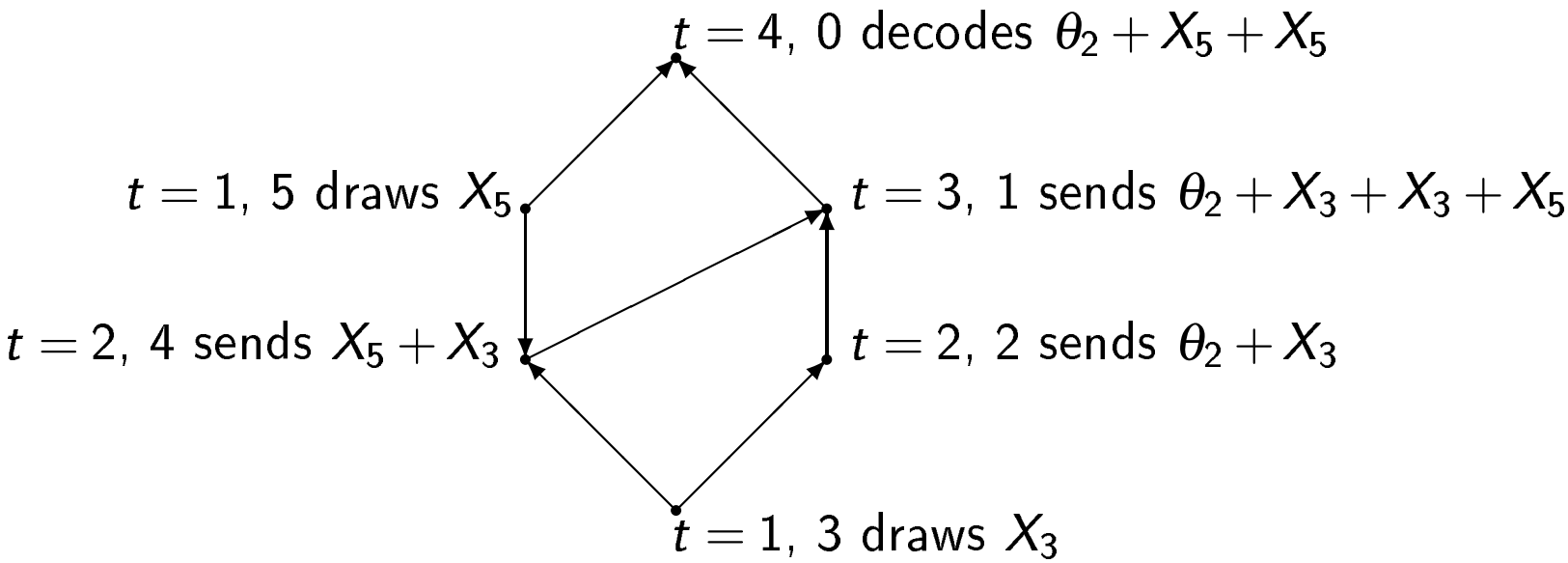
An example

The protocol for transmitting θ_2 is the following.



An example

The protocol for transmitting θ_2 is the following.



Detering deviations

This allows secret information transmission. To ensure implementation under worst outcome, the designer must *detect* deviations.

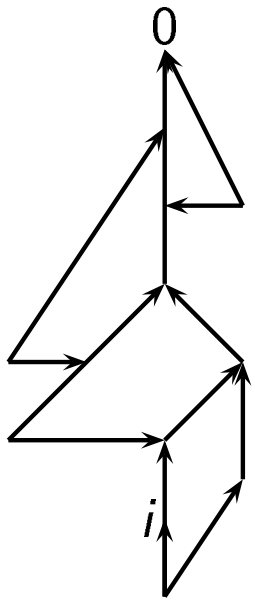
- Authentication scheme (check-vectors in Rabin and Ben-or).
  Assume strong 2-connectedness.
  - Sender draws keys A, B, C, D, X and sets $Y = X + \theta$, $U = AX + B$, $V = CY + D$.
  - Sender sends (X, U, C, D) on one path and (Y, V, A, B) on the other.
  - Receiver checks $U = AX + B$ and $V = CY + D$. If he accepts, he decodes $\theta = X + Y$. Otherwise, he punishes.
  The probability to tamper with the message AND to pass the test is small.

Detering deviations

- Without strong 2-connectedness (as in example), run in parallel a large number independent copies of the previous protocol and let the Sender (player 2): -select one of these protocols at random, -input his type in the selected protocol, -input 0 in all others. Receiver accepts if exactly one protocol has a non-zero output and punishes otherwise.

The general proof

We show that a directed graph which is acyclic, strongly 1-connected and weakly 2-connected contains subgraphs of the type:



Secret information transmission: general case

Fix a sender i and the receiver 0. Let k be an integer.

Definition

k-Secret information transmission from i to 0 is possible on the network if there exists a communication protocol such that:
- 0 correctly learns θ_i,
- For every $S \subseteq N \setminus i$, $|S| \leq k$, the joint messages received by S are probabilistically independent from θ_i.

Information transmission against an "honest but curious" adversary.

Secret information transmission: general case

Assume that the graph is strongly 1-connected. The graph is $k+1-C(i,0)$ if there are $k+1$ disjoint undirected paths from i to 0.

Theorem (Renault-Renou-T10)

k-Secret information transmission from i to 0 is possible IFF $i \in D(0)$ or the graph is $k+1-C(i,0)$.

The condition is clearly necessary.

Secret information transmission: general case

Secret sharing

Let θ be a random variable in F_2^n.
For each n, there exists $Y_1, \ldots, Y_n$ such that:

- $\theta = \sum_{i=1}^{n} Y_i$,
- For each i, $(Y_j)_{j \neq i}$ is independent from θ.

Draw $Y_1, \ldots, Y_{n-1}$ i.i.d. uniform and set $Y_n := \theta + \sum_{i=1}^{n-1} Y_i$.

More generally, k-secret sharing between n-players (Shamir) is such that no coalition of size k can decode and any coalition of size $k+1$ can. Efficient algorithm draws a random polynomial f of degree k in F_p and informs player i of $f(i)$ (p is a prime $p > n$).

Secret information transmission: general case

Sufficiency: Assume that the digraph is acyclic and consider the following protocol.

- Player i computes $s_i = \sum_{k \in C(i)} m_{ki}(+\theta_i)$.
- Share s_i in n_i pieces $Y_1, \ldots, Y_{n_i}$ and sends the ℓ-th piece to the ℓ-th successor (i has n_i successors).

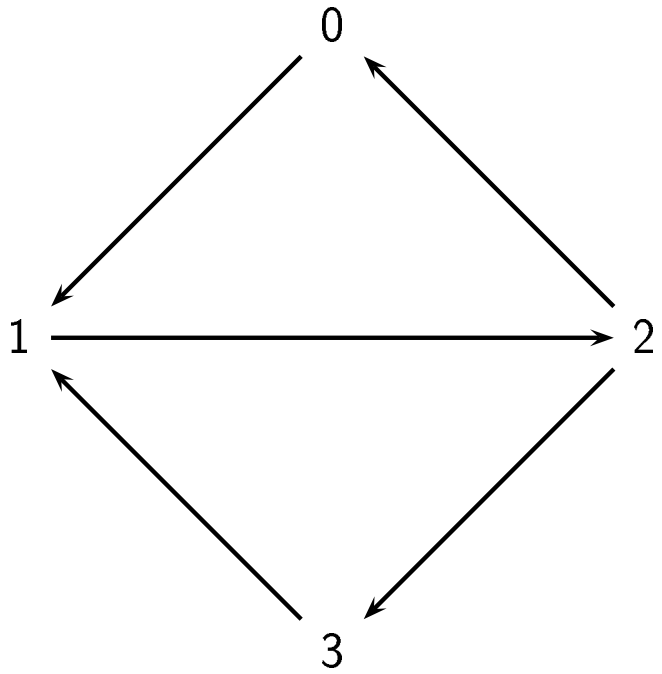
Claim 1.

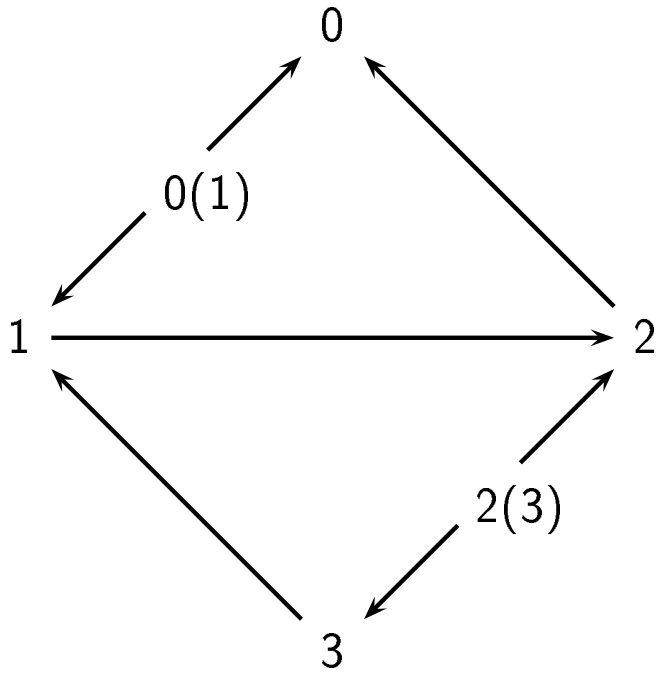
$$s_0 := \sum_{k \in D(0)} m_{k0} = \theta_i$$

Claim 2. If $|S| \leq k$, the joint messages received by S are independent from θ_i.

Dispensing with acyclicity

If the graph is strongly 1-connected a weakly 2-connected, all results go through. We associate an acyclic graph as follows:





Common independent beliefs and private values

Theorem

In all environments $\mathscr{E}$ with common independent beliefs and private values, $F_{\mathscr{N}}(\mathscr{E}) = IC$ if and only if the network $\mathscr{N}$ is weakly 2-connected.

Consider the following network.

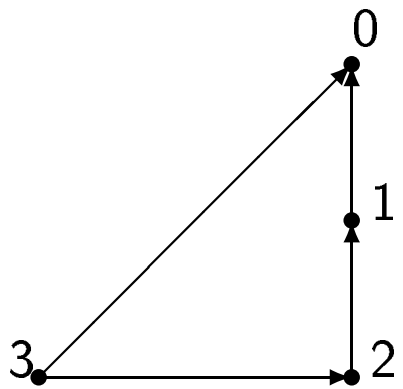
We show how to implement the dictatorial s.c.f. of player 2.

Common independent beliefs and private values

Theorem

In all environments $\mathscr{E}$ with common independent beliefs and private values, $F_{\mathscr{N}}(\mathscr{E}) = IC$ if and only if the network $\mathscr{N}$ is weakly 2-connected.

Consider the following network.



We show how to implement the dictatorial s.c.f. of player 2.

Assume that $\Theta_2 = \{a, b\}$ and $P(\theta_2 = a) = p$. The protocol (i.e., mechanism and strategies) is the following:

- Player 3 draws an encoding key y uniformly on $[0,1]$, and sends it to player 2 and the designer.
- Player 2 of type a draws x uniformly on $[0,p)$ and sends $z = x + y \bmod_{01}$ to player 1.
- Player 2 of type b draws x' uniformly on $(p,1]$ and sends $z = x' + y \bmod_{01}$ to player 1.
- Players 1 forwards his message to the designer.
- The designer computes $\hat{x} = (z - y) \bmod_{01}$ and decodes $\theta_2' = a\mathbf{1}_{\{\hat{x} \in [0,p)\}} + b\mathbf{1}_{\{\hat{x} \in [p,1]\}}$.

$\theta_2' =^d \theta_2$ under unilateral deviation of player 1 or 3.

Assume that $\Theta_2 = \{a, b\}$ and $P(\theta_2 = a) = p$. The protocol (i.e., mechanism and strategies) is the following:

- Player 3 draws an encoding key y uniformly on $[0,1]$, and sends it to player 2 and the designer.
- Player 2 of type a draws x uniformly on $[0,p)$ and sends $z = x + y \bmod_{01}$ to player 1.
- Player 2 of type b draws x' uniformly on $(p,1]$ and sends $z = x' + y \bmod_{01}$ to player 1.
- Players 1 forwards his message to the designer.
- The designer computes $\hat{x} = (z - y) \bmod_{01}$ and decodes $\theta_2' = a\mathbf{1}_{\{\hat{x} \in [0,p)\}} + b\mathbf{1}_{\{\hat{x} \in [p,1]\}}$.

$\theta_2' =^d \theta_2$ under unilateral deviation of player 1 or 3.

Assume that $\Theta_2 = \{a, b\}$ and $P(\theta_2 = a) = p$. The protocol (i.e., mechanism and strategies) is the following:

- Player 3 draws an encoding key y uniformly on $[0,1]$, and sends it to player 2 and the designer.
- Player 2 of type a draws x uniformly on $[0,p)$ and sends $z = x + y \bmod_{01}$ to player 1.
- Player 2 of type b draws x' uniformly on $(p,1]$ and sends $z = x' + y \bmod_{01}$ to player 1.
- Players 1 forwards his message to the designer.
- The designer computes $\hat{x} = (z - y) \bmod_{01}$ and decodes $\theta_2' = a\mathbf{1}_{\{\hat{x} \in [0,p)\}} + b\mathbf{1}_{\{\hat{x} \in [p,1]\}}$.

$\theta_2' =^d \theta_2$ under unilateral deviation of player 1 or 3.

Pure equilibria

Let $F^p_{\mathcal{N}}(\mathcal{E})$ be the set of functions partially implementable by *pure equilibria* on $\mathcal{N}$ when the environment is $\mathcal{E}$.

Theorem

$F^p_{\mathcal{N}}(\mathcal{E}) = IC^p$ *for all* $\mathcal{E}$ *if and only if* $D(0) = N$.

If $\exists i \notin D(0)$, we construct an incentive compatible social choice function and a utility profile such that:

- Each player $j \neq i$ has an incentive to lie about his own type, given the type of player i,
- the social choice depends on each player's type.

E.g. a contribution game.

Then, at a pure equilibrium, some player $j \neq i$ learns (something about) the type of player i.

Pure equilibria

Let $F^p_{\mathcal{N}}(\mathscr{E})$ be the set of functions partially implementable by *pure equilibria* on $\mathcal{N}$ when the environment is $\mathscr{E}$.

Theorem

$F^p_{\mathcal{N}}(\mathscr{E}) = IC^p$ *for all* $\mathscr{E}$ *if and only if* $D(0) = N$.

If $\exists i \notin D(0)$, we construct an incentive compatible social choice function and a utility profile such that:

- Each player $j \neq i$ has an incentive to lie about his own type, given the type of player i,
- the social choice depends on each player's type.

E.g. a contribution game.

Then, at a pure equilibrium, some player $j \neq i$ learns (something about) the type of player i.

Pure equilibria

Let $F^p_{\mathcal{N}}(\mathcal{E})$ be the set of functions partially implementable by *pure equilibria* on $\mathcal{N}$ when the environment is $\mathcal{E}$.

Theorem

$F^p_{\mathcal{N}}(\mathcal{E}) = IC^p$ *for all* $\mathcal{E}$ *if and only if* $D(0) = N$.

If $\exists i \notin D(0)$, we construct an incentive compatible social choice function and a utility profile such that:

- Each player $j \neq i$ has an incentive to lie about his own type, given the type of player i,
- the social choice depends on each player's type.

E.g. a contribution game.

Then, at a pure equilibrium, some player $j \neq i$ learns (something about) the type of player i.

Pure equilibria

Let $F^p_{\mathcal{N}}(\mathcal{E})$ be the set of functions partially implementable by *pure equilibria* on $\mathcal{N}$ when the environment is $\mathcal{E}$.

Theorem

$F^p_{\mathcal{N}}(\mathcal{E}) = IC^p$ *for all* $\mathcal{E}$ *if and only if* $D(0) = N$.

If $\exists i \notin D(0)$, we construct an incentive compatible social choice function and a utility profile such that:

- Each player $j \neq i$ has an incentive to lie about his own type, given the type of player i,
- the social choice depends on each player's type.

E.g. a contribution game.

Then, at a pure equilibrium, some player $j \neq i$ learns (something about) the type of player i.

Pure equilibria

Let $F^p_{\mathcal{N}}(\mathcal{E})$ be the set of functions partially implementable by *pure equilibria* on $\mathcal{N}$ when the environment is $\mathcal{E}$.

Theorem

$F^p_{\mathcal{N}}(\mathcal{E}) = IC^p$ *for all* $\mathcal{E}$ *if and only if* $D(0) = N$.

If $\exists i \notin D(0)$, we construct an incentive compatible social choice function and a utility profile such that:

- Each player $j \neq i$ has an incentive to lie about his own type, given the type of player i,
- the social choice depends on each player's type.

E.g. a contribution game.

Then, at a pure equilibrium, some player $j \neq i$ learns (something about) the type of player i.

Pure equilibria

Let $F^p_{\mathcal{N}}(\mathcal{E})$ be the set of functions partially implementable by *pure equilibria* on $\mathcal{N}$ when the environment is $\mathcal{E}$.

Theorem

$F^p_{\mathcal{N}}(\mathcal{E}) = IC^p$ *for all* $\mathcal{E}$ *if and only if* $D(0) = N$.

If $\exists i \notin D(0)$, we construct an incentive compatible social choice function and a utility profile such that:

- Each player $j \neq i$ has an incentive to lie about his own type, given the type of player i,
- the social choice depends on each player's type.

E.g. a contribution game.

Then, at a pure equilibrium, some player $j \neq i$ learns (something about) the type of player i.

Pure equilibria

Let $F^p_{\mathcal{N}}(\mathcal{E})$ be the set of functions partially implementable by *pure equilibria* on $\mathcal{N}$ when the environment is $\mathcal{E}$.

Theorem

$F^p_{\mathcal{N}}(\mathcal{E}) = IC^p$ *for all* $\mathcal{E}$ *if and only if* $D(0) = N$.

If $\exists i \notin D(0)$, we construct an incentive compatible social choice function and a utility profile such that:

- Each player $j \neq i$ has an incentive to lie about his own type, given the type of player i,
- the social choice depends on each player's type.

E.g. a contribution game.

Then, at a pure equilibrium, some player $j \neq i$ learns (something about) the type of player i.

Pure equilibria

Let $F^p_{\mathcal{N}}(\mathcal{E})$ be the set of functions partially implementable by *pure equilibria* on $\mathcal{N}$ when the environment is $\mathcal{E}$.

Theorem

$F^p_{\mathcal{N}}(\mathcal{E}) = IC^p$ *for all* $\mathcal{E}$ *if and only if* $D(0) = N$.

If $\exists i \notin D(0)$, we construct an incentive compatible social choice function and a utility profile such that:

- Each player $j \neq i$ has an incentive to lie about his own type, given the type of player i,
- the social choice depends on each player's type.

E.g. a contribution game.

Then, at a pure equilibrium, some player $j \neq i$ learns (something about) the type of player i.

Secure communication

Implementation of all IC functions in all environments is more demanding.

Definition

SECURE information transmission is possible on the network if there exists a communication protocol such that:
-The designer correctly learns all types, even under unilateral deviation (RELIABLE),
-No player gets information beyond his own type, even under unilateral deviaton (SECRET).

This is a necessary and sufficient condition for implementation of all IC functions in all environments.
Strong 3-connectedness is sufficient with continuous mechanisms. Strong 4-connectedness is sufficient with finite mechanisms.

Secure communication in 2-way networks

Dolev et al. characterize k-secure communication in 2-way networks, i.e. undirected graphs. Fix a sender and a receiver.

Theorem (DDWY93)

k-secure communication between the sender and the receiver is possible IFF the (undirected) graph is $k+1$-connected between sender and receiver.

The protocol for $k = 1$

Assume that there are 3 disjoint path from sender to receiver, through player 1, player 2 and player 3 respectively.

- Sender draws X, X_1, X_2, X_3, X', X'_1, X'_2, X'_3 and sends:
  $(X_1 + X, X_2, X_3)$, $(X'_1 + X', X'_2, X'_3)$ to player 1
  $(X_1, X_2 + X, X_3)$, $(X'_1, X'_2 + X', X'_3)$ to player 2
  $(X_1, X_2, X_3 + X)$, $(X'_1, X'_2, X'_3 + X')$ to player 3.
  The message to player 1 *(resp. 2, 3) conveys no information on* (X, X'). *On another hand, the pooled messages of any two players reveal both* X *and* X'.

The protocol for $k = 1$, ctd.

Denote the messages received by receiver:
$(y_1, x_2(1), x_3(1))$, $(y_1', x_2'(1), x_3'(1))$ from player 1
$(x_1(2), y_2, x_3(2))$, $(x_1'(2), y_2', x_3'(2))$ from player 2
$(x_1(3), x_2(3), y_3)$, $(x_1'(3), x_2'(3), y_3')$ from player 3.

- If $x_1(2) = x_1(3)(= X_1)$, $x_2(1) = x_2(3)(= X_2)$ and $x_3(1) = x_3(2)(= X_3)$, then sender computes $y_1 + X_1$, $y_2 + X_2$ and $y_3 + X_3$. Under unilateral deviation, at least two of these values coincide $(= X)$. Then receiver broadcasts OK and sender broadcasts back $X + \theta$.
- Otherwise there exists i such that $x_i(j) \neq x_j(k)$ (with $\{i, j, k\} = \{1, 2, 3\}$). In this case j contradicts k.

The protocol for $k = 1$, ctd.

- If j contradicts the two other players, then sender recognizes j as deviating. Then $x_i(k) = X_k$ and $x_i(k) + y_k = X$. Then receiver broadcasts OK and sender broadcasts back $X + \theta$.
- If j contradicts only one player k then receiver does not know who of j and k is deviating. He broadcasts $(x_i(j), x_i(k))$. Sender compares $x_i(j)$ and $x_i(k)$ with X_i. If $x_i(j) \neq X_i$ (and $x_i(k) = X_i$), sender broadcasts $\{j\}$ and $X' + \theta$. Receiver computes $X' = y'_i + x_k(i)$ and finds out θ.