How Turing machines play

- Infinitely repeated games
- Cooperation with encrypted communication
- Correlated equilibria

Olivier Grossner: Repeated games played by cryptographically sophisticated players

Impression

- An exploration of a game theorist into cryptography and complexity theory
- Open points in communication: authentication?
- Role of a mediator - existing or not?
- Trusted Turing machines?
- Applicability to finitely repeated games?

Goal of the paper

Assumptions:

- Players are represented by polynomial Turing machines
- There exists a trapdoor function

Result: A correlated strategy can be built without private communication (?), by using a public correlation device.

Compared to previous presentations about getting rid of the mediator:

- More players than two can play
- No specific encryption scheme is used.
- However, one player has a central role.

Example

A and B want to meet with out C. There are L possible meeting points.

- A and B cannot talk with each other. The probability for success:

$$\frac{1}{L} \cdot \frac{L-1}{L}$$

- A and B can talk through a private phone line.

$$\Rightarrow \frac{L-1}{L}$$

- A and B exchange public messages. C has unbounded computational power.
- A and B exchange encrypted public messages, and C cannot break the cryptosystem.

Basic idea

- A deterministic polynomial Turing machine calculates the equilibrium profiles for each step. The players obey this machine.
- Main problem: Punishing a deviator.
- Means: A probabilistic Turing machine calculates actions for all the honest players after one deviated. One player sends encrypted actions to the honest players. (Correlated strategy against the deviator).
- The deviator is computationally bounded, cannot understand what the others are up to, and cannot win.

Repeated games

- Repeated game: extensive game with perfect information and simultanious moves (Osborne and Rubinstein)
- Infinite: The game goes towards an infinite history of action profiles.
- Non-discounted: While comparing sequences of action profiles, all the past actions are equally valued.
  (Discounting: the oldest decisions in the history become less important)

Game theoretic results

- *Feasible payoff*: a convex combination of payoff profiles
- The worst payoff other players than i can force to him by using mixed strategies: $\bar{v}^i$ (so called minmax)
  $\Rightarrow$ *individually rational* payoffs are those that are at least as good as the worst for all the players
- Folk Theorem: the set of equilibrium payoffs of the infinite repetition of a strategic game with no discounting is the intersection of feasible and individually rational payoffs.
- Similar definitions and results for correlated strategies: $\underline{v}^i$ (correlated minmax), correlated individually rational payoffs, Folk Theorem for correlated equilibrium payoffs...

Turing machines

Each Turing machine has

- Input tapes (IT), computation tape (CT), output tape (OT)
- One IT has the time t coded in unary, another IT has information about the history of the game.
- For each Turing machine, there exists a polynomial $P(t)$ that bounds the computation.
- Playing: action phase, observation phase
- A probabilistic Turing machine has a stochastic transition function.

Playing...

Theorem: the closure of equilibrium payoffs is the intersection of feasible payoffs and correlated individual payoffs

- The equilibrium payoff is

$$v = \Sigma_{a \in A} p_a g(a),$$

  where p_a is the probability of the action profile a. A is the infinite history of action profiles. $g(a)$ is the payoff.

- A deterministic Turing machines outputs periodically elements $a_t \in A$ according to the frequencies (p_a).

- Honest playing: play minmax against a_t. (?)

Punishing

Player i has deviated at time t_0.

- All the players have Turing machines that implement a trapdoor function (generate encryption and decryption keys and perform encryption and decryption)
- At each stage $t \geq t_0 + 1$, the honest players generate an encryption key and announce it at their output tapes.
- A coordinator, player i, encrypts the next action for each player and announces the result in its output tape.
- All players but i are informed after stage $t + 1$ of the profile of actions to be played at stage $t + 2$.
- Correlated minmax is the best i can guarantee against the others.

Trapdoor functions

A trapdoor function doesn't give any information about the message once encrypted. A k-trapdoor function doesn't give any information about the message encrypted independently with k different keys.

Proposition: Every trapdoor function is a k-trapdoor function for all k.

Remarks

- Public communication + assumptions of modern cryptography $\Rightarrow$ the equilibrium payoffs of a infinitey repeated game without discounting are the correlated equilibrium payoffs.
- Claim: Doesn't hold for
  - finitely repeated games
    (the limitation on computational power is only effective when t tends to ∞. (?))
  - infinitely repeated games with discounting
- Further work: correlation through the actions? finite number of messages?