Game Theory

A game consists of a set of (rational/selfish) players, set of actions & strategies (i.e., the way of choosing actions), and finally a pay-off (utility) function, which is used by each player to compute his utility/gain before selecting an action.

1. cooperative games → player collaborate & split the total utility among themselves.
2. non_cooperative games → players cannot form agreements to coordinate their behavior, in other words, any cooperation must be self_enforcing.

prisoners' dilemma well-known non-cooperative game

1. Two players P_1 & P_2
2. Actions: Confess / keep Quiet → strategies
3. payoffs/utility: +1 : Free
   - 0 : Jail for one year
   - −1 : Jail for two years
   - −2 : Jail for three years

ideal

P_1 \ P_2	C: Quiet	D: Confess
C: Quiet	0 , 0	−2 , +1
D: Confess	+1 , −2	−1 , −1

→ Cooperation → keep Quiet
Defection → Confess

* which is not ideal
* Nash Equilibrium

①

	P2	
row cooperation →	0,0	-2,+1
	+1,-2	-1,-1

→ Therefor P2 will defeat (confess)

P_1: what if I cooperate

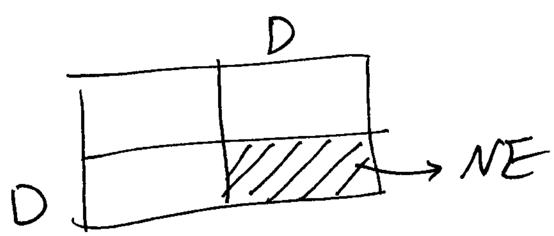
②

	0,0	-2,+1
row defection →	+1,-2	-1,-1

P2

→ Therefor P2 will defeat (confess) again

P_1 : what if I defeat



$\boxed{NE\ \#}$ No matter if P_1 cooperates / defeats, P_2 will alway defeat. Similarly, no matter if P_2 cooperates / defeats, P_1 will also defeat all the time (because the payoff matrix is symmetric)

$\boxed{Def\#1}$: Let $\mathcal{A} \overset{\text{def}}{=} \mathcal{A}_1 \times \cdots \times \mathcal{A}_n$ be an action profile for n players where $\mathcal{A}_i$ denotes the set of possible actions of player P_i.
A game $\Gamma = (\mathcal{A}_i, u_i)$ for $1 \leqslant i \leqslant n$ consists of $\mathcal{A}_i$ and a utility function $u_i : \mathcal{A} \longmapsto \mathbb{R}$ for each player P_i.
We refer to a vector of actions $\vec{a} = (a_1, \ldots a_n) \in \mathcal{A}$ as an outcome of the game.

Def #2 The utility function u_i illustrates the preferences of player P_i over different outcomes. We say P_i <u>prefers</u> outcome $\vec{a}$ to $\vec{a}'$ iff $u_i(\vec{a}) > u_i(\vec{a}')$, and he <u>weakly prefers</u> outcome $\vec{a}$ to $\vec{a}'$ iff $u_i(\vec{a}) \geq u_i(\vec{a}')$

In order to allow the players to follow randomized strategies, we define σ_i as a probability distribution over A_i for a player P_i.

$P_1 : (C, D)$

This means P_i samples $a_i \in A_i$ according to σ_i.

↳ A strategy is said to be a <u>pure-strategy</u> if each σ_i assigns probability "1" to a certain action. Otherwise, it's said to be <u>mixed-strategy</u>.

let $\vec{\sigma} = (\sigma_1, \dots, \sigma_n)$ be the vector of players' strategies.

$$(\sigma_i', \vec{\sigma}_{-i}) \overset{\text{def}}{=} (\sigma_1, \dots, \sigma_{i-1}, \sigma_i', \sigma_{i+1}, \dots, \sigma_n)$$

only P_i will change his strategy

all the other players will use the same strategies that they had previously.

Def 3# # A vector of strategies $\vec{\sigma}$ is a Nash Equilibrium if for all i and any $\sigma_i' \neq \sigma_i$, it holds that

just for one player

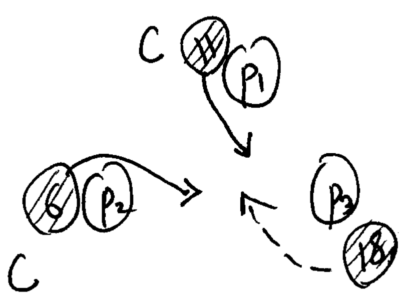
$$u_i(\sigma_i', \vec{\sigma}_{-i}) \leq u_i(\vec{\sigma})$$

Vectors

This means no one gains any advantage by deviating from the protocol as long as the other players follow the protocol (rules of the game).

Introducing $\boxed{\text{Rational Secret Sharing}}$ $\longrightarrow$ STOC'04

$f(x) = 3 + 2x + x^2 \xrightarrow{\mathbb{Z}_{27}} t = 3$ three shares are enough for secret recovery



C: reveal your share at the recovery phase

D: otherwise

D $\longrightarrow$ detective player learns the secret

$\left.\begin{array}{l}\vec{a}\\ \vec{a}'\end{array}\right\}$ Two imaginary outcomes

$l_i(\vec{a})$ is a bit defining whether P_i has learned secret or not

$l_i = 1$ (learned) or $\emptyset$ (not learn)

$\delta(\vec{a}) = \sum_i l_i(\vec{a})$ $\longleftarrow$ * how many players have learned the secret

Utility assumptions

1 $\quad$ 0

P_i:

$l_i(\vec{a}) > l_i(\vec{a}') \Longrightarrow u_i(\vec{a}) > u_i(\vec{a}')$

$\underset{1/0}{l_i(\vec{a})} = \underset{1/0}{l_i(\vec{a}')}$ and $\delta(\vec{a}) < \delta(\vec{a}') \Longrightarrow u_i(\vec{a}) > u_i(\vec{a}')$

less # of players learn the secret