

From risk analysis to Adversarial risk analysis

Part VI. Noncooperative games

David Ríos

david.rios@icmat.es

AXA-ICMAT Chair in ARA and Royal Academy of Sciences

DRI. Aalto

Reliability Analysis

How long will a system last under certain operational conditions?

Based on data and prior info...

- Make inferences about parameters present in lifetime models
- Make forecasts about lifetimes

To make decisions about replacement, maintenance, performance, design, configuration,...

Sometimes, several agents in scene: warranties, manufacturer(s)-consumer(s), regulator, security,...

Best HW/SW maintenance policy for a company ERP?

Model HW/SW system (interacting HW and SW blocks)

Forecast block reliabilities (and correlations)

Forecast system reliability

Design maintenance policies

Forecast their impact on reliability (performance, costs,...)

Optimal maintenance policy

Best HW/SW maintenance for the university ERP?

Model HW/SW system (interacting HW and SW blocks)

Forecast block reliabilities (and correlations)

Forecast system reliability

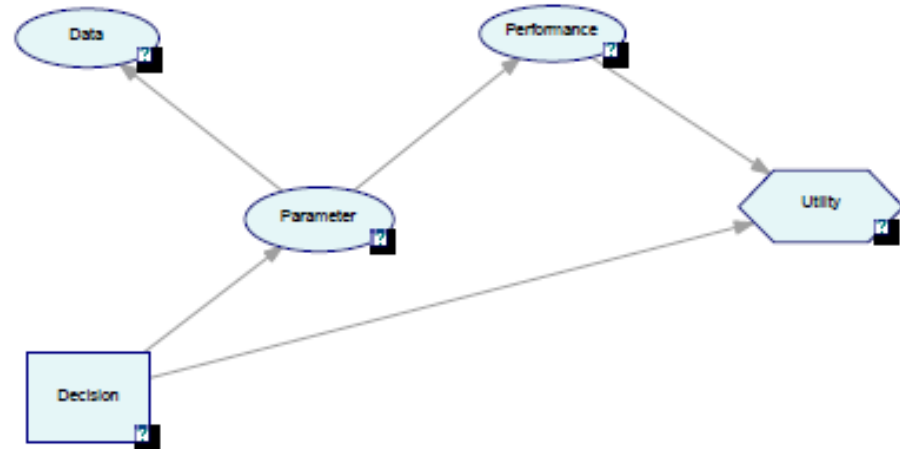
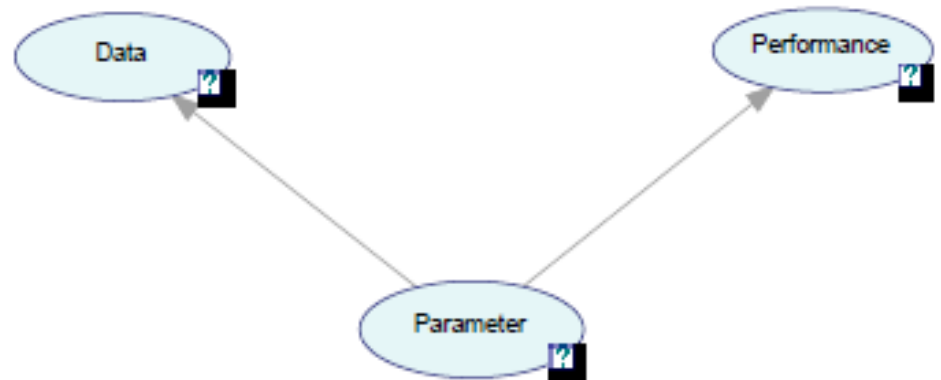
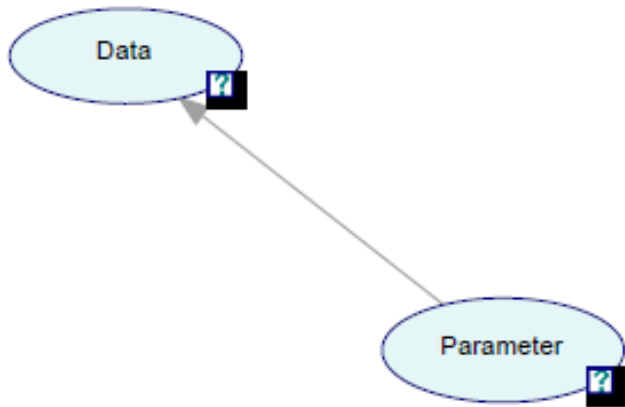
Design maintenance policies

Forecast impact on reliability (performance, costs,...)

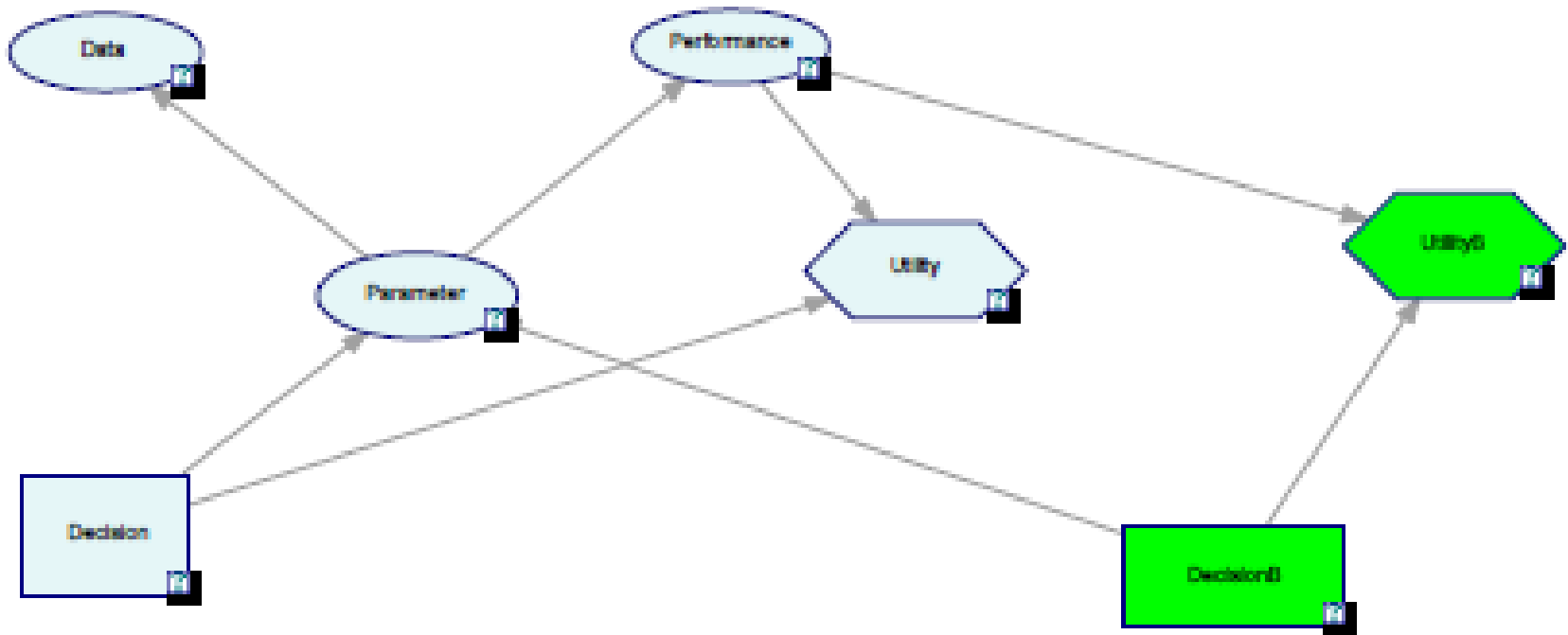
Optimal maintenance policy

NB: What happens with bad guys attacking our system?

Reliability



Reliability



Risk Analysis

What would be the impact over system performance of identified threats?

Based on data and prior info...

- Make forecasts of threat occurrence
- Make forecasts of threat impacts

To make risk management decisions

Sometimes, other agents in scene: security, cybersecurity, competitive marketing, social robotics, auctions,...

Best security resource allocation in a city?

City as a map with cells

Each cell has a value (multiattribute)

For each cell, a predictive model of delictive acts (COMPSTAT, PREDPOL,...)

Allocate security resources (given constraints)

For each cell predict impact of resource allocation

Optimal resource allocation

Best security resource allocation in a city?

City as a map with cells

Each cell has a value (multiattribute)

For each cell, a predictive model of delictive acts (COMPSTAT, PREDPOL,...)

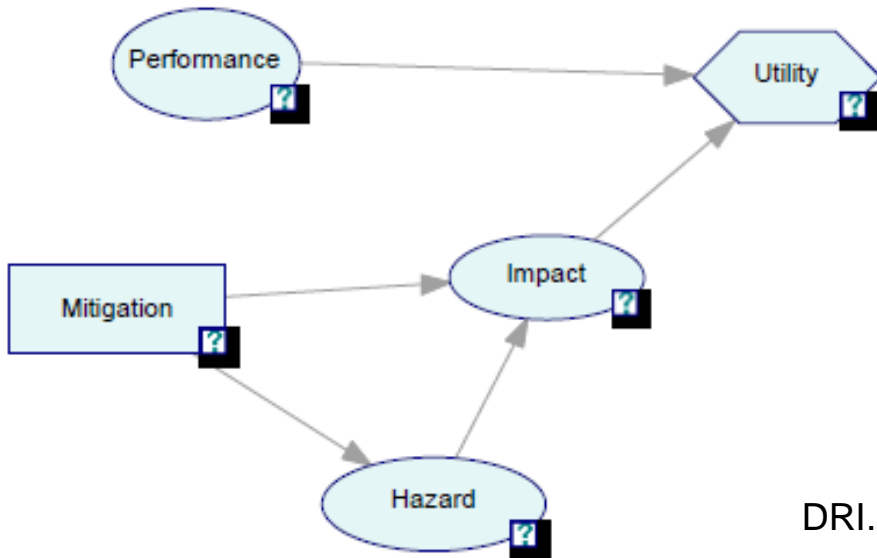
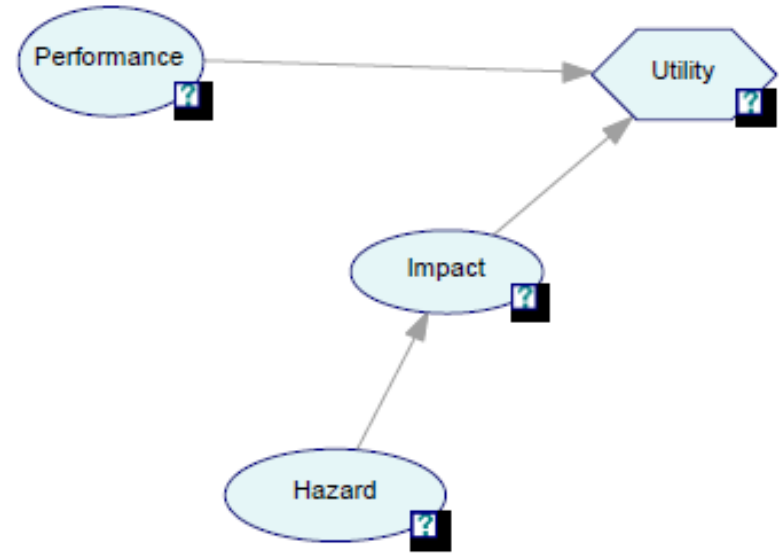
Allocate security resources (given constraints)

For each cell predict impact of resource allocation

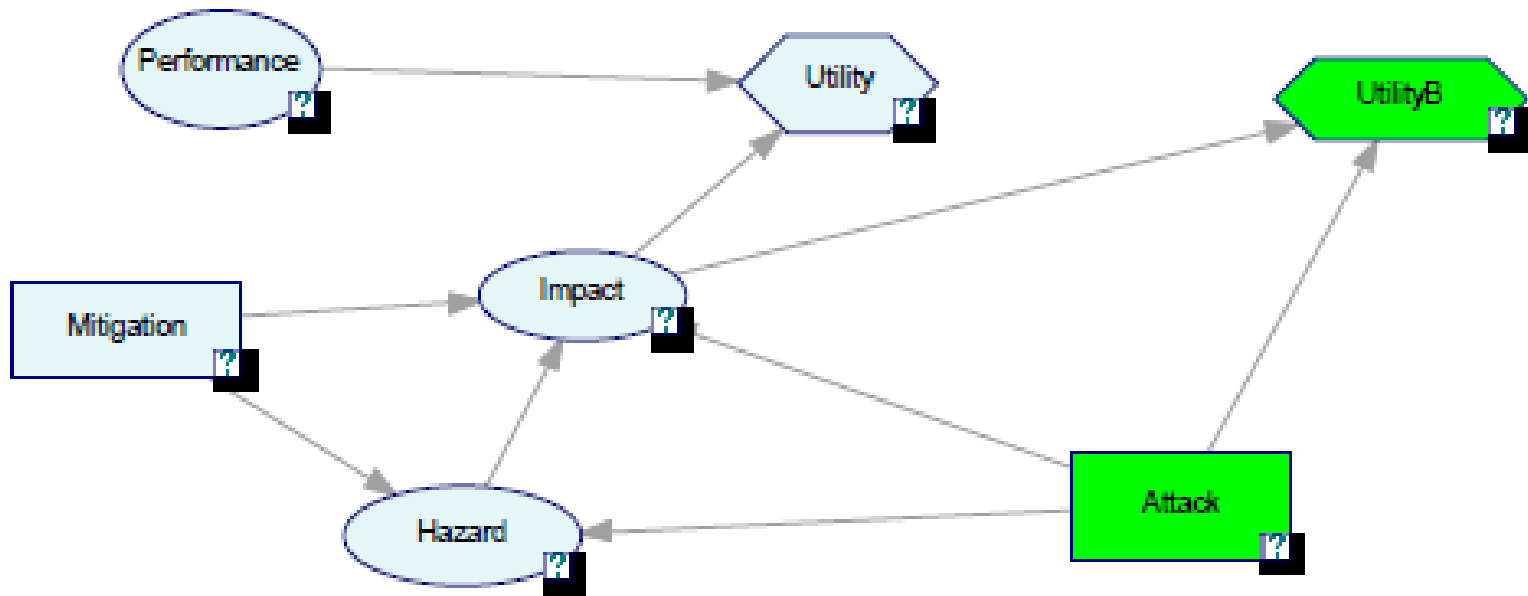
Optimal resource allocation

NB: The bad guys also operate intelligent and organisedly!!!

Risk Analysis



Risk Analysis



Problem

- Need to deal with decision situations with several decision makers.
- **Noncooperative games**
 - **Nasheq**, refinements and variations
 - Decision Analysis/Bayesian approach ->ARA
 - Level-k
 -
- Cooperative games
 - **Bargaining**
 - Group Decision Making
 - Voting
 -
- From competition to cooperation

Games. Basic concepts

- Several decision makers
- My utility depends not only on what I do, but also on what others do
- Conflict and cooperation
- Players, Payoff function
- Game: Set of known rules determining what may be done, their consequences and the associated payoffs

Many variations

- Number of players: 2, 3, ..., n, infinite
- Number of strategies. Finite, Infinite (Discrete, Continuous)
- Payoff function: Zero sum games, Constant sum games, non constant games
- Deterministic, stochastic
- Situation prior to game. Cooperative, Noncooperative
- Representation
 - Normal form. Tables. Simultaneous
 - Extensive form. Trees. Sequential
 - MAIDs
 - Differential games

Basic game concepts through simple examples.

Critical assessment

Two players, two alternatives

- Fixed strategies
- **Common knowledge**
- Simultaneous selection
- No previous discussion

Raiffa, Metcalfe, Richardson (2002)
Heargreaves-Heap, Varoufakis (2006)
Banks, Rios, DRI (2015)

Rothkopf (2007), Lippman, McCardle (2012), D. Wolpert
(2012)

Kadane, Larkey (1982), Raiffa (1982)

Game matrix

	Left	Right
Up	U,L	U,R
Down	D,L	D,R

Game matrix

	Left	Right
Up	3,2	1,5
Down	4,7	3,1

Game matrix: zero sum

	Left	Right
Up	3,-3	-2,2
Down	-4,4	1,-1

Game matrix: zero sum

	Left	Right
Up	3	-2
Down	-4	1

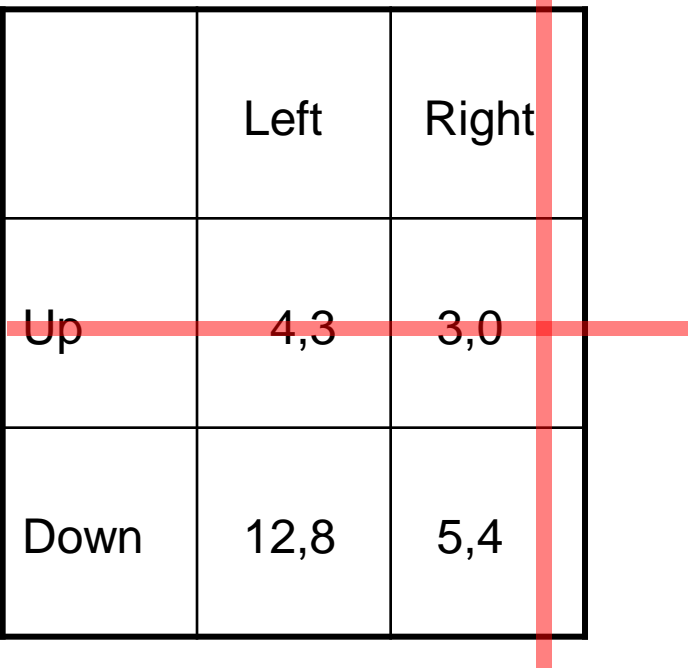
Consider this game...

- What if you play rows?
- What if you play columns?

	Left	Right
Up	4,3	3,0
Down	12,8	5,4

Dominance

	Left	Right
Up	4,3	3,0
Down	12,8	5,4

A 2x2 payoff matrix is shown. The columns are labeled 'Left' and 'Right', and the rows are labeled 'Up' and 'Down'. The payoffs are: (Up, Left) = 4,3; (Up, Right) = 3,0; (Down, Left) = 12,8; (Down, Right) = 5,4. A red vertical line is drawn through the 'Right' column, and a red horizontal line is drawn through the 'Up' row, intersecting at the (Up, Right) cell.

The doom of rationality

Social dilemmas

	Left	Right
Up	5,5	-5,10
Down	10,-5	-2,-2

Prisoner's dilemma (years in prison)

	No Conf	Conf
No Conf	1,1	5,0
Conf	0,5	3,3

A social dilemma in cybersecurity

	Company B invests in IT security	Company B does not invest in IT security
Company A invests in IT security	Both incur security costs Low security risks	A incurs security costs Relatively high security risk
Company A does not invest in IT security	B incurs security costs Relatively high security risk DRI. Aalto	Equilibrium:A,B avoid costs High security risk

The negotiator's dilemma

		Levante	
		Be open and sincere	Hide info or lead in wrong direction
I N T E L E S A	Be open and sincere	Both have modest gains	Small gains for Intelesa; large gains for Levante
	Hide info or lead in wrong direction	Small gains for Levante; large gains for Intelesa	None gains. Negos may fail

The arms race (60-80)

- Each country stocking or reducing arms
 - Both realise economic sacrifices due to arms race
 - Both prefer military superiority to equality
1. Inferiori
 2. Race (equal, economic constraints)
 3. Mutual disarming
 4. Superiority

Arms race (60-80)

	USRR Disarm	Arm
USA Disarm	3,3	1,4
Arm	4,1	2,2

Consider this game...

- What if you play rows?
- What if you play columns?

	Left	Right
Up	0,2	5,4
Down	10,3	3,8

Iterated dominance

	Left	Right
Up	0,2	5,4
Down	10,3	3,8

Iterated dominance

	Left	Right
Up	0,2	5,4
Down	10,3	3,8

Consider this game

	Left	Right
Up	4,3	10,6
Down	12,8	5,4

Nash equilibria

	Left	Right
Up	4,3	10,6
Low	12,8	5,4

Nash equilibria. Which one?

	Left	Right
Up	4,3	8,10
Low	12,6	5,4

Nash equilibria. Best response

	C1	C2	C3
F1	1,4	2,2	2,3
F2	3,1	1,5	4,1
F3	2,0	3,4	1,2

Nash equilibria. Best response

	C1	C2	C3
F1	1,4x	2,2	2,3
F2	3,1	1,5	4,1
F3	2,0	3,4	1,2

Nash equilibria. Computation

	C1	C2	C3
F1	1,4x	2,2	2,3
F2	3,1	1,5x	4,1
F3	2,0	3,4x	1,2

Nash equilibria. Computation

	C1	C2	C3
F1	1,4 x	2,2	2,3
F2	x3,1	1,5x	x4,1
F3	2,0	x3,4x	1,2

Nash equilibria. Existence

	C1	C2
F1	-1,1	1,-1
F2	1,-1	-1,1

Nash equilibria. Existence

	C1	C2
F1	-1,1X	X1,-1
F2	X1,-1	-1,1X

Nash equilibria. Existence

	qC1	(1-q)C2
pF1	-1,1	1,-1
(1-p)F2	1,-1	-1,1

Mixed strategies

p for row F1

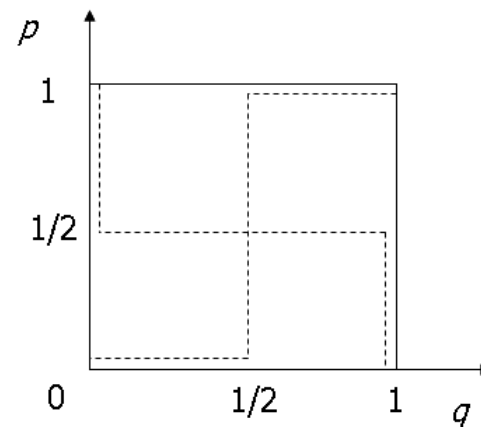
q for column C1

For row player

$$p^*(1-2q)+(1-p)^*(2q-1)=2p+2q-4pq-1$$

Best response calculation $p=1/2$

$q=1/2$



Consider this game

- Now one of the agents chooses first
- Two Nash eq (F1,C2), (F2, C1)
- If row goes first. Choose F2. Column, C1
- If column goes first. Choose C2. Row, F1

	C1	C2
F1	0,0	1,2
F2	2,1	0,0

Formal concepts

There are n agents:

- Alternative set for each agent:

$$S_i, \quad i \in \{1, \dots, n\}$$

- Alternatives for each agent: $s_i \in S_i$
- Evaluation for each agent

Let $(s_1, \dots, s_i, \dots, s_n)$ combination of strategies :

$u_i(s_1, \dots, s_i, \dots, s_n)$ the utility that i -th agent perceives.

- **Game in normal form:** Specifies the set of strategies S_1, \dots, S_n and the utility functions u_1, \dots, u_n .
- Denote the game through $G = \{S_1, \dots, S_n; u_1, \dots, u_n\}$.

Formal concepts. Nondominated strategy

- Nondominated solution:
Game in normal form, s_i' and s_i'' strategies for i -th agent. s_i' is **dominated** by strategy s_i'' if for every combination $(s_1, \dots, s_{i-1}, s_{i+1}, \dots, s_n)$:
$$u_i(s_1, \dots, s_{i-1}, s_i', s_{i+1}, \dots, s_n) < u_i(s_1, \dots, s_{i-1}, s_i'', s_{i+1}, \dots, s_n)$$
- Rational players do not use dominated strategies.

Formal concepts. Nash eq

- Nash eq:

s_1^*, \dots, s_n^* form a Nash eq if s_i^* is *i-th* best response to the other $n - 1$ agents ($s_1^*, \dots, s_{i-1}^*, s_{i+1}^*, \dots, s_n^*$):

$$u_i(s_1^*, \dots, s_{i-1}^*, s_i^*, s_{i+1}^*, \dots, s_n^*) \geq u_i(s_1^*, \dots, s_{i-1}^*, s_j, s_{i+1}^*, \dots, s_n^*)$$

for each $s_j \in S_j$; i.e solution of

$$\begin{aligned} & \max u_i(s_1^*, \dots, s_{i-1}^*, s_j, s_{i+1}^*, \dots, s_n^*) \\ & \text{s.t. } s_j \in S_j \end{aligned}$$

No agent has incentives to abandon it unilaterally

Nash eq as crossing of best responses

Formal concepts. Mixed strategies

- Best response of agent i to agent j mixed strategy.
 - J pure strategies in S_1 , K pure strategies in S_2
 - $S_1 = \{s_{11}, \dots, s_{1J}\}$, $S_2 = \{s_{21}, \dots, s_{2K}\}$.
 - Agent 1 believes agent 2 will use (s_{21}, \dots, s_{2K}) with probs $p_2 = (p_{21}, \dots, p_{2K})$, expected utility of agent 1 if he uses $p_1 = (p_{11}, \dots, p_{1J})$ is

$$v_1(p_1, p_2) = \sum_{j=1}^J p_{1j} \left[\sum_{k=1}^K p_{2k} u_1(s_{1j}, s_{2k}) \right] = \sum_{j=1}^J \sum_{k=1}^K p_{1j} \cdot p_{2k} u_1(s_{1j}, s_{2k}),$$

- Same with agent 2.
- (p_1^*, p_2^*) is Nash eq if

$$v_1(p_1^*, p_2^*) \geq v_1(p_1, p_2^*)$$

$$v_2(p_1^*, p_2^*) \geq v_2(p_1^*, p_2)$$

Formal concepts. Results

- In a normal form game $G = \{S_1, \dots, S_n; u_1, \dots, u_n\}$, if S_i is finite for each i , there is at least one Nash eq, possibly with mixed strategies.
- G game whose strategy sets are open intervals with payoff functions twice differentiable

If a profile (s_1^*, \dots, s_n^*) satisfies, for each agent i ,

$$\frac{\partial u_i(s_1^*, \dots, s_n^*)}{\partial s_i} = 0$$

and

$$\frac{\partial^2 u_i(s_1^*, \dots, s_n^*)}{\partial^2 s_i} < 0$$

then it is a Nash eq.

Assessment

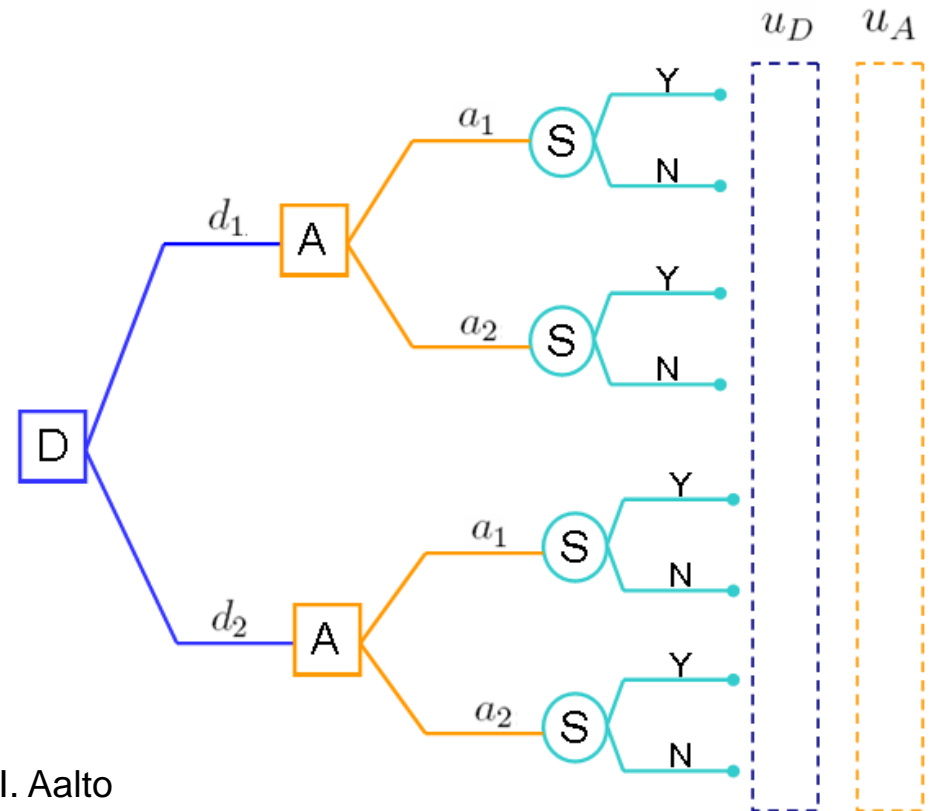
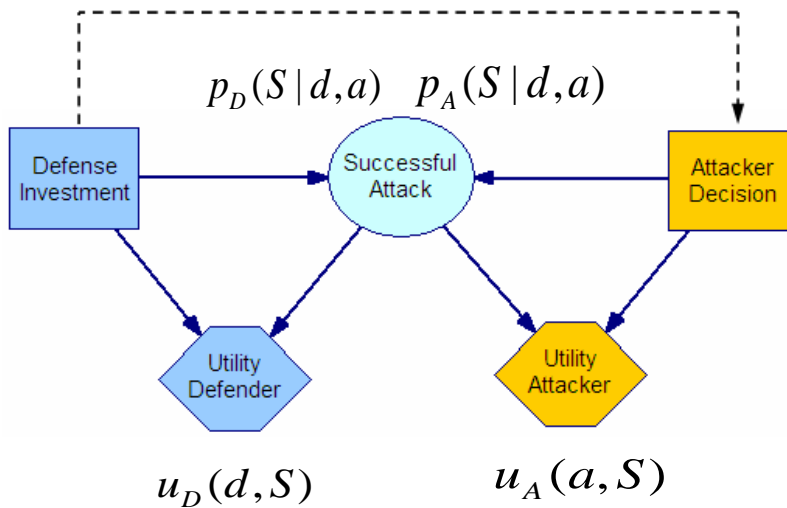
Nasheq very important. Many applications in economics, political science, biology, risk analysis, reliability analysis,.... But some criticisms

- Common knowledge assumption
- Multiple equilibria, with difficulties to distinguish among them
- Social dilemmas, with many practical implications
- Not always useful for decision support to a party
 - Sometimes useful to communicate before game starts. Sometimes not, to avoid threats.
 - Sometimes move first. Sometimes wait.
 -
 - Useful, to forecast the game result... if we know the participants' preferences
- Behavioral GT. Stahl, Wilson (1995), Camerer (2003), Gintis (2009) DRI. Aalto

- GT solutions to some stylised risk and reliability problems
- Subgame perfect equilibrium, Bayes-Nasheq,...
- MAIDs and Game Trees

Sequential game

- Two intelligent players
 - Defender and Attacker. D knows A's judgements
- Sequential moves
 - Def, then Attacker



Standard GT Analysis

Expected utilities at node S

$$\psi_D(d, a) = p_D(S = 0|d, a) u_D(d, S = 0) + p_D(S = 1|d, a) u_D(d, S = 1)$$

$$\psi_A(d, a) = p_A(S = 0 | d, a) u_A(a, S = 0) + p_A(S = 1 | d, a) u_A(a, S = 1)$$

Best Attacker's decision at node A

$$a^*(d) = \operatorname{argmax}_{a \in \mathcal{A}} \psi_A(d, a)$$

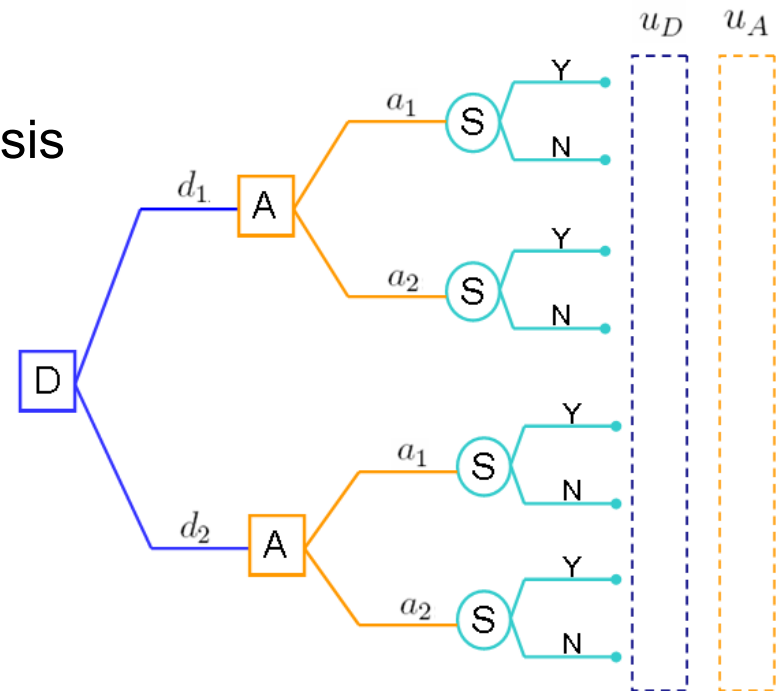
Assuming Defender knows Attacker's analysis

Defender's best decision at node D

$$d^* = \operatorname{argmax}_{d \in \mathcal{D}} \psi_D(d, a^*(d))$$

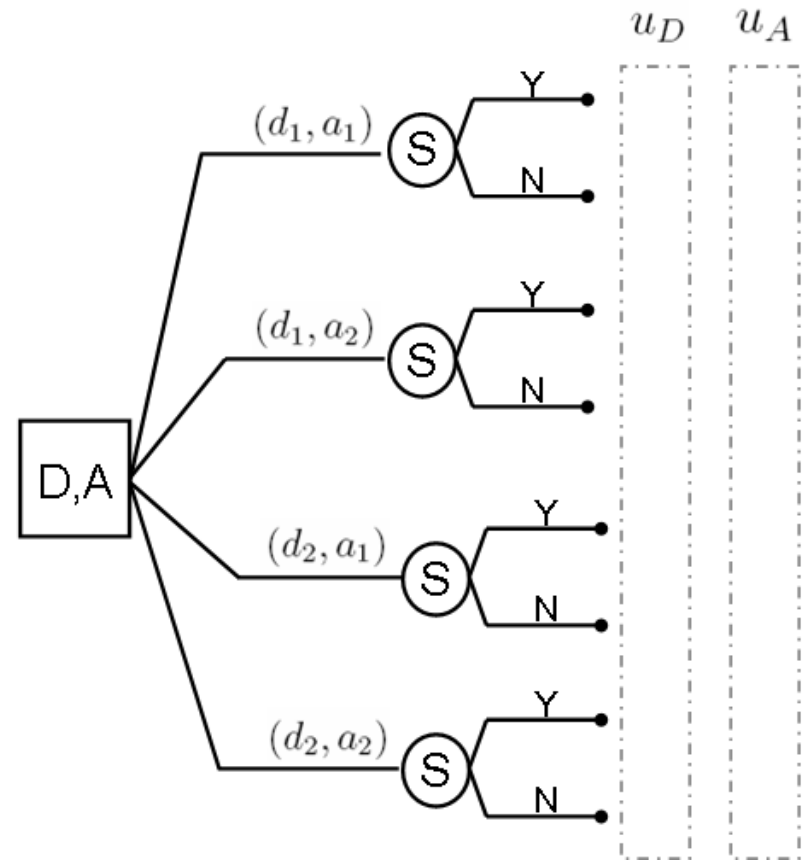
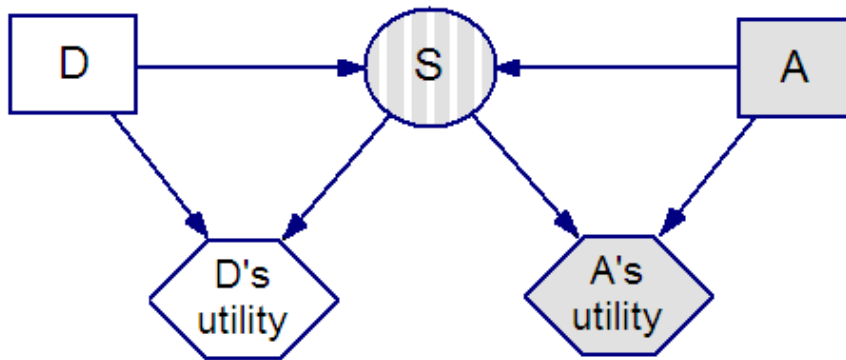
Solution: $(d^*, a^*(d^*))$

Nasheq. Subgame
perfect equilibrium



Simultaneous games

- Decisions are made without knowing each other's decisions



Game Theory Analysis

- Common knowledge

- Each knows expected utility of every pair (d, a) for both of them
- Nash equilibrium: (d*, a*) satisfying

$$\psi_D(d^*, a^*) \geq \psi_D(d, a^*) \quad \forall d \in \mathcal{D}$$

$$\psi_A(d^*, a^*) \geq \psi_A(d^*, a) \quad \forall a \in \mathcal{A}$$

- When some information is not common knowledge

- Private information
 - Type of Defender and Attacker

$$\tau_D \in T_D \longrightarrow u_D(d, s, \tau_D) \quad p_D(S \mid d, a, \tau_D)$$

$$\tau_A \in T_A \longrightarrow u_A(d, s, \tau_D) \quad p_A(S \mid d, a, \tau_D)$$

- Common prior over private information $\pi(\tau_D, \tau_A)$
- Model the game as one of incomplete information

Bayes Nash Equilibrium

– Strategy functions

- Defender $d : \tau_D \rightarrow d(\tau_D) \in \mathcal{D}$
- Attacker $a : \tau_A \rightarrow a(\tau_A) \in \mathcal{A}$

– Expected utility of (d,a)

- for Defender, given her type $\psi_D(d(\tau_D), a, \tau_D) =$
$$= \int \left[\sum_{s \in S} u_D(d(\tau_D), s, \tau_D) p_D(S = s \mid d(\tau_D), a(\tau_A), \tau_D) \right] \pi(\tau_A \mid \tau_D) d\tau_A$$

- Similarly for Attacker, given his type $\psi_A(d, a(\tau_A), \tau_A)$

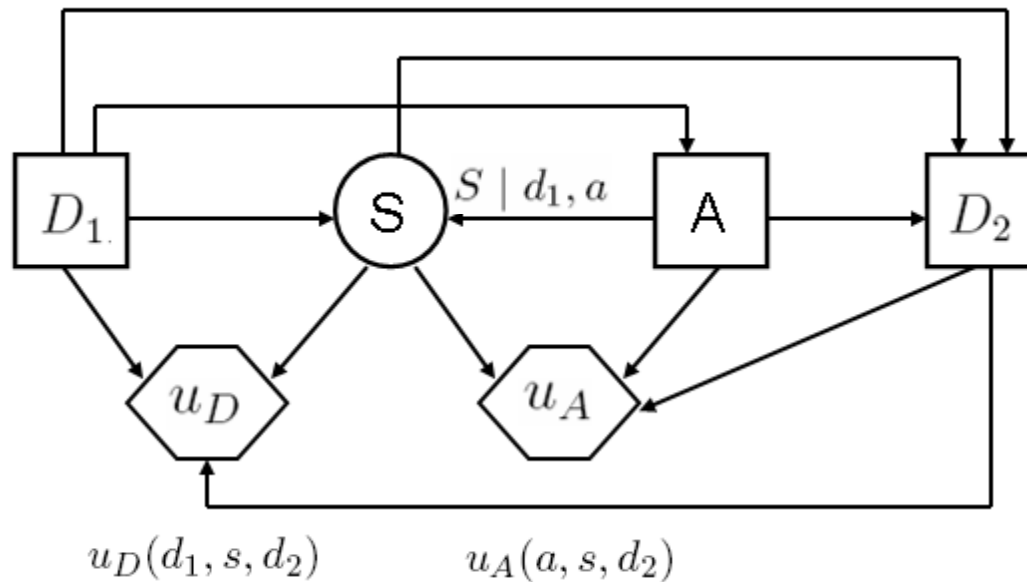
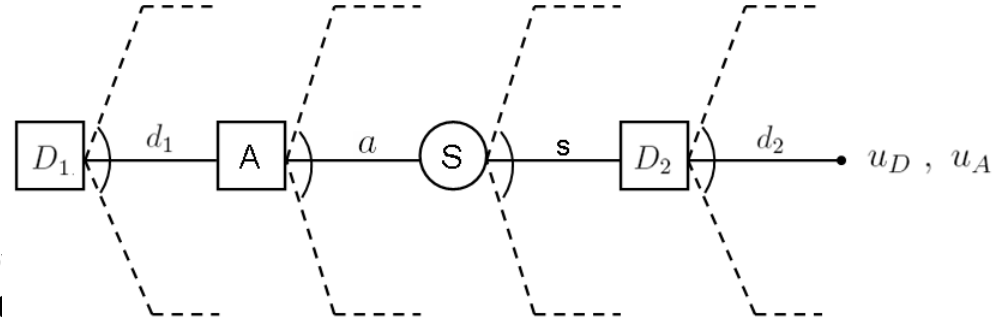
– Bayes-Nash Equilibrium (d^*, a^*) satisfying

$$\psi_D(d^*(\tau_D), a^*, \tau_D) \geq \psi_D(d(\tau_D), a^*, \tau_D) \quad \forall d : \tau_D \rightarrow d(\tau_D)$$

$$\psi_A(d^*, a^*(\tau_A), \tau_A) \geq \psi_A(d^*, a(\tau_A), \tau_A) \quad \forall a : \tau_A \rightarrow a(\tau_A)$$

Sequential Defend–Attack–Defend model

- Two intelligent players
 - Defender and Attacker
- Sequential moves
 - First, Defender moves
 - Afterwards, Attacker knowing Defender's move
 - Afterwards, Defender again responding to attack



Standard Game Theory

Analysis

- Under common know. of utilities and probs

- At node D_2

$$d_2^*(d_1, s) = \operatorname{argmax}_{d_2 \in \mathcal{D}_2} u_D(d_1, s, d_2)$$

- Expected utilities at node S

$$\psi_D(d_1, a) = \int u_D(d_1, s, d_2^*(d_1, s)) p_D(s | d_1, a) ds$$

$$\psi_A(d_1, a) = \int u_A(a, s, d_2^*(d_1, s)) p_A(s | d_1, a) ds$$

- Best Attacker's decision at node A

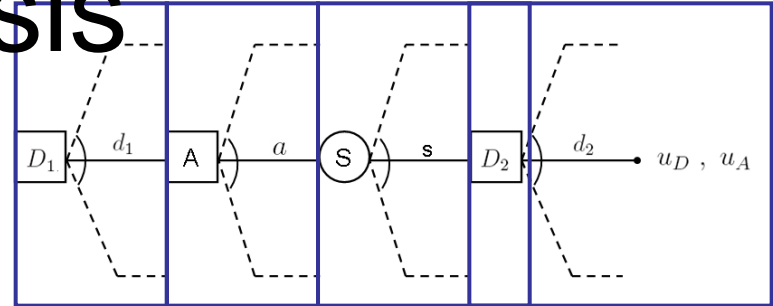
$$a^*(d_1) = \operatorname{argmax}_{a \in \mathcal{A}} \psi_A(d_1, a)$$

- Best Defender's decision at no D_1

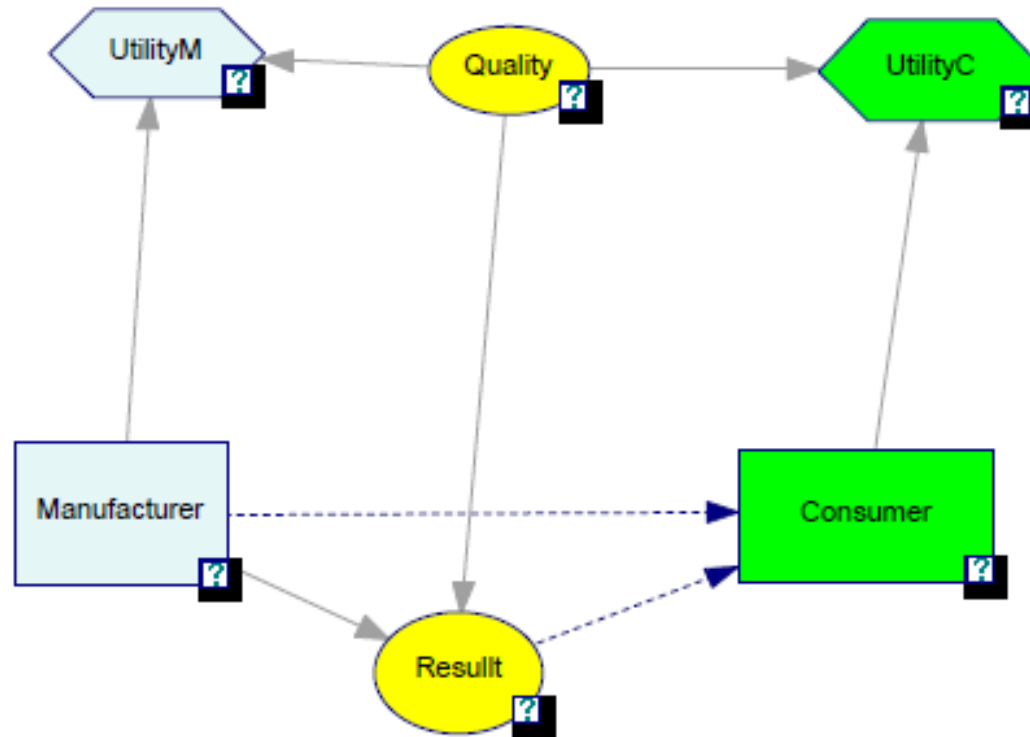
$$d_1^* = \operatorname{argmax}_{d_1 \in \mathcal{D}_1} \psi_D(d_1, a^*(d_1))$$

- Nash Solution:

$$d_1^* \in \mathcal{D}_1 \quad a^*(d_1^*) \in \mathcal{A} \quad d_2^*(d_1^*, s) \in \mathcal{D}_2$$



A reliability example



A reliability example

1. Inverting the arc θ - D and computing, by Bayes' formula,

$$p_C(\theta|d, n) \propto p_C(\theta)p_C(d|\theta, n).$$

2. Computing the expected utilities, to reduce node Θ ,

$$\psi_C(n, d, c) = \int u_C(c, \theta)p_C(\theta|d, n)d\theta.$$

3. Computing the optimal decision c , given d and n ,

$$c^*(d, n) = \arg \max_{c \in \{A, R\}} \psi_C(d, n, c).$$

1. Computing the expected utilities, to eliminate node C ,

$$\psi_M(n, d, \theta) = \sum_{c \in \{A, R\}} u_M(c, n, \theta)p_M(c|d, n).$$

2. Computing the expected utilities, to reduce node D ,

$$\psi_M(n, \theta) = \int \psi_M(n, d, \theta)p_M(d|\theta, n) dd.$$

3. Computing the expected utilities, to reduce node Θ ,

$$\psi_M(n) = \int \psi_M(n, \theta)p_M(\theta) d\theta.$$

4. Finally, computing her optimal decision through

DRI. Aalto

$$n^* = \arg \max \psi_M(n).$$