



UNIVERSITÀ  
DEGLI STUDI  
DI PADOVA



DIPARTIMENTO  
DI INGEGNERIA  
DELL'INFORMAZIONE

# Lecture 09

## Projects

Thomas Marchioro

November 2, 2023

# How to make a 7/7 project

- 1 Choose a topic (of scientific interest), and find a problem that is suitable for game-theoretic analysis
  - Multiple players, different objectives
- 2 Check what other people have already done on the topic
  - No need for a systematic review, but at least make sure not to reinvent the wheel!
- 3 Start simple, make a lot of assumptions, and then gradually drop them
  - Even simple models can provide good insights on a problem (e.g., Cournot duopoly)
- 4 When possible, run experiments/simulations and evaluate objective metrics (e.g., throughput for networks, monetary cost for power grids)
  - Does the game-theoretic solution lead to good outcomes? Comparison with optimization? Price of Anarchy?

# How to make a 7/7 project

- More tips:
  - Your grade is not proportional to the complexity of your game: focus on a model that accurately describes your problem
  - When investigating related work, do not invest too much time on the math, especially when it is overly complicated: focus on experimental results and takeaways
  - ChatGPT-generated text = 0 points (you can use it to check the grammar, though)
  - Plagiarism = 0 points

# How to make a 7/7 project

- Deliverables:
  - Report: 5–8 pages, double column, 10 pt
- Report sections:
  - Introduction: describe the setting and the problem that you are investigating; explain the core idea of your project
  - Related work: report *few* references that are closely related to your work or that investigate analogous problems
  - Analysis: characterize the game that you are considering, clearly defining players, strategies and payoffs; find NE, subgame-perfect NE, Bayesian NE, etc.; if your analysis results in an algorithm, it should be reported in this section
  - Results: show the obtained results, preferably using plots, tables, etc.; compare them with other works, and/or with other possible solutions (e.g., computing the PoA)
  - Discussion: discuss limitations and/or possible extensions
  - Conclusion: summarize your results in few words

- Automatically accepted topics
  - Anything of scientific interest *and novel*
- Conditionally accepted topics
  - Inflated topics (blockchain, 6G, edge/fog computing) → Lots of game theory works on these topics, you must come up with something really novel/interesting
  - Quantum game theory
  - Board games and videogames → Models must be realistic and lead to algorithms that can actually be implemented (that means no chess, no poker, and no Starcraft)
- Automatically rejected topics
  - Politics and elections
  - Any model that is too scuffed or arbitrary
- **Advice:** Choose a topic that is interesting for you (related to your thesis, previous projects, or personal interests)

- If you are not sure whether your topic is acceptable, just ask
- Different groups can choose the same topic but cannot do the same game-theoretic analysis
- References and examples of previous projects will be uploaded on e-learning

- **Important:** On November 16, 2023, 14:30 there will be a presentation in **classroom Te** about some tabletop games
- These games are valid project topics (automatically accepted)
- Of course, your grade will still depend on the quality of your game-theoretic analysis

- **Group formation and topic selection:** November 20, 2023, 23:59 (Italian time)
- **Project submission:** January 28, 2024, 23:59 (Italian time)
  - E-learning forms will be soon available
  - You can withdraw from the project at any point in time before the deadline and receive the 3-point bonus
  - Once you have withdrawn from a project, you cannot re-join it or join another one



# LoRa networks

Topics: Networks, IoT

- **LoRa**: proprietary modulation designed for energy-constrained devices (e.g., IoT) that need to communicate at long distance (LoRa = long-range)
- LoRa modulation utilizes a technique called “chirp spread spectrum”
- The modulation is parametrized by a number called **spreading factor**  $(SF) \in \{7, 8, \dots, 12\}$ 
  - A low SF means higher data rate  $\rightarrow$  faster transmission, preferable for the transmitting device
  - A higher SF means more reliable transmission (devices that are more distant from the base station must use a higher SF)
  - Multiple devices using the same SF interfere with each other  $\rightarrow$  want to avoid using the same SF as other devices

- *Main reference:* Tolio et al. Spreading factor allocation in LoRa networks through a game theoretic approach. In ICC 2020-2020 IEEE International Conference on Communications (ICC) (pp. 1-6). IEEE.
- **Spreading factor allocation problem:** There are  $N$  devices scattered around a base station, they must decide which SF to use
- If there is only one device, it's easy: just set  $SF=7$
- If there are multiple devices, you need to account for interference

- Optimization model: the base station assigns the SF to each device
- **Game theory model:** the devices decide their own SF according to their belief about the rest of the network
  - *Multiple players:* the devices
  - *Actions:* the spreading factor  $SF \in \{7, 8, \dots, 12\}$
  - *Multiple objectives:* data rate of each device (lower in case of interference)

# Simplified game

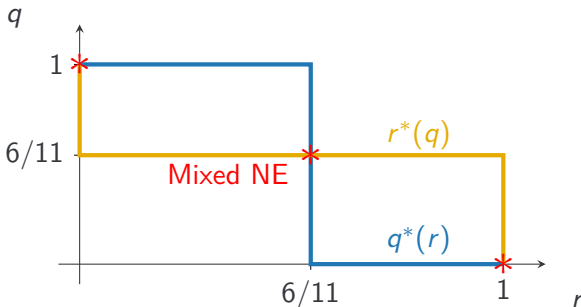
- Assumptions: only 2 devices; both close enough to the base station (can use SF7); if no interference  $\rightarrow$  utility = 13 - SF; if interference  $\rightarrow$  utility = 0
- $N = 2$  devices with  $S_1 = S_2 = \{\text{SF7}, \text{SF8}\}$  (SF9 or higher is strictly dominated)

		Device 2	
		SF7	SF8
Device 1	SF7	0, 0	6, 5
	SF8	5, 6	0, 0

- This becomes a simple **anti-coordination** game

# Simplified game

- $q$  = probability device 1 plays SF7
- $r$  = probability device 2 plays SF7



- **Algorithm:** devices play SF7 with probability  $6/11$ , SF8 with probability  $5/11$

# Dropping some assumptions

- Assumptions: only 2 devices; ~~both close enough to the base station (can use SF7)~~; if no interference  $\rightarrow$  utility =  $13 - \text{SF}$ ; if interference  $\rightarrow$  utility = 0
- Same-distance case (minimum SF is  $\text{SF}_j$  for both)

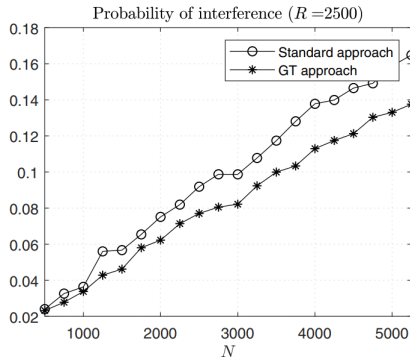
		Device 2	
		SF <sub>j</sub>	SF <sub>j</sub> + 1
Device 1	SF <sub>j</sub>	0, 0	12 - j, 12 - j - 1
	SF <sub>j</sub> + 1	12 - j - 1, 12 - j	0, 0

- Need to handle also other cases (see paper)

- Result of the game-theoretical analysis: algorithm that each device executes locally
- Input: distance from base station
- Output: probability  $p(\text{SF}j)$  associated with each SF
- Devices choose their SF according to  $p$

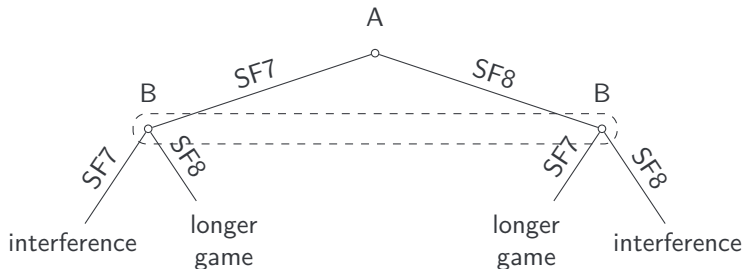


- Publicly available ns-3 simulator for LoRa networks:  
<https://github.com/signetlabdei/lorawan>
- Simulation: game theory algorithm versus baseline approach (use lowest available SF) for variable number of devices ( $N$ )



# What can be improved?

- Previous model is a static game: time dimension is neglected
- One may consider a dynamic game where devices have the option to alternate SF

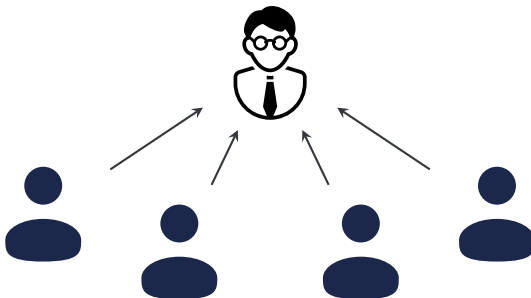


- Many resource allocation problems can be modeled as anti-coordination games
- Players maximize their utility when choosing different options
- Similar to multi-path routing problems, in which nodes prefer to choose different paths
- Analysis of long-term collaboration → Multi-stage or repeated games
- Modeling uncertainty about nodes status → Bayesian games

# Mobile/IoT Crowdsourcing

Topics: Data science, IoT, Privacy

- Organizing large-scale data collection is hard
- Possible solution: **crowdsourcing**, i.e., an organization or research team collects data from volunteers through an online platform



- *Main reference:* Dasari et al., 2020. Game theory in mobile crowdsensing: A comprehensive survey. *Sensors*, 20(7), p.2055.
- Data collected via crowdsourcing: mobile data, IoT data, wearable data
- Main hurdles:
  - **Privacy:** Collected data is often sensitive (location, activity data, lifestyle) → How do users know that they can entrust this information to the data collector?
  - **Quality of data:** In contexts where users receive a reward, they may decide to send inaccurate data or large volumes of data → How does the data collector handle these cases?

# Toy example

- Game between user and data collector
- User has possible strategies: donate (D) or not (N) his/her data
- Data collector has possible strategies: use privacy-preserving algorithms (P) or use standard algorithm (S)
  - Standard algorithms give higher utility  $K$  to the data collector but may lead to privacy leaks with probability  $q$ ; privacy-preserving algorithms give lower utility  $k$
  - The user receives a reward  $r$  in exchange for their data; however, privacy leaks cause a loss in utility  $-\ell$

		Data collector	
		P	S
User	D	$r, k$	$r - \ell, K$
	N	$0, 0$	$0, 0$

# Toy example

- Numerical example:  $K = 2$ ,  $k = 1$ ,  $r = 1$ ,  $\ell = 2$

		Data collector	
		P	S
User	D	1, 1	-1, 2
	N	0, 0	0, 0

- In this case, there is only one NE
- However, cooperation may be enforced via repetition of the game (we will see this later in the course)
- Intuition: building a good reputation to increase payoff on the long term



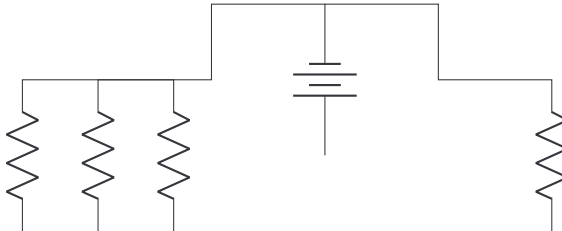
# Power grids (smart and non-smart)

Topics: Electrical engineering

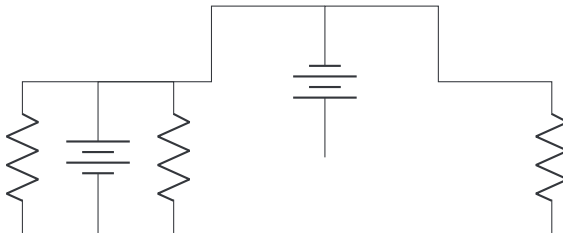
# Power grid



- **Traditional grid model:** centralized distribution network (generator) that produces alternate current powering the whole network



- **Modern power grid:** some of the consumers are also generators (solar panels, wind turbines, etc.)
- This may lead to interference with the central distribution
- Sometimes power *curtailment* is necessary (central distribution pays solar panel owners to limit production)



- **Smart grid:** decentralized distribution network where
  - power usage and loss are monitored by sensors
  - multiple power sources (micro-grids) communicate with each other
  - automatic decisions are possible
- current use cases: retailers profiling their customers
- ideal use case: automatic handling of conflicts and power loss

- **Possible games** (*main reference*: Saad et al., 2012. Game-theoretic methods for the smart grid: An overview of microgrid systems, demand-side management, and smart grid communications. IEEE Signal Processing Magazine, 29(5), pp.86-105.):
  - Cooperative games between micro-grids to minimize power loss  
→ are coalitions sustainable?
  - (Bayesian) non-cooperative games between consumers → selfish consumption may lead to power outages
- Remark: In these applications, strategy sets are typically continuous (how much energy to buy, sell, etc.) → NE are found as stationary points as in the Cournot duopoly
- You may use PandaPower for simulations:  
<http://www.pandapower.org/>

# Network intrusion detection and response

Topics: security, networks

- Network **intrusion detection** consists in the task of identifying ongoing attacks within a network (reconnaissance, phishing, malware, DoS, etc.)
  - NID is not an exact science, you have uncertainty in the detection
- Network **intrusion response** is how attacks are handled
  - You cannot just block all traffic and interrupt all services (that would be the perfect DoS)



- An intrusion detection game is an adversarial game between an attacker (hacker) and a defender (the target network/company)
- However, it is not necessarily a zero-sum game: the defender wants not only to protect itself from the attack, but also to maintain the usual activity
  - Utility function can be application-specific
- Simplest case: the attacker chooses between different types of attack, some easier to detect than others; the defender decides on the policy to adopt, it could be a conservative policy or a relaxed policy

- More possible games (*main reference*: Kiennert et al., 2018. A survey on game-theoretic approaches for intrusion detection and response optimization. ACM Computing Surveys (CSUR), 51(5), pp.1-31.):
  - Resource allocation → Which nodes in the network should be monitored?
  - Response optimization → React immediately, or wait and collect information on the attacker?

- Tips for a more realistic model:
  - Rather than a generic network, think of a specific target for an attacker (a bank? a factory? a hospital?)
  - Different networks may have different vulnerabilities and may be targeted by different types of attack
  - E.g., see: Hu et al., 2020. Optimal decision making approach for cyber security defense using evolutionary game. IEEE Transactions on Network and Service Management, 17(3), pp.1683-1700.
  - Once you have decided on a target, you can use knowledge-bases like Mitre Att&ck (<https://attack.mitre.org/>) to research common attacks used against similar targets

# Shapley value and data/feature selection

Topics: machine learning, data science

- In machine learning, we may encounter the following problems:
  - Too many features, need to determine which ones are important (feature selection)
  - Different data sources, need to estimate their individual value (data valuation)
- The Shapley value allows to estimate the value of features or data sources
- Game-theoretic intuition: consider a coalition of  $n$  players (features or data sources); the Shapley value of player  $i$  is its marginal contribution to the coalition

- Consider a coalition  $C = \{1, \dots, n\}$  of  $n$  players, and a utility function  $v : 2^C \rightarrow \mathbb{R}^+$  representing the value of sub-coalitions
- The Shapley value of  $i$  is computed as

$$\varphi_i = \sum_{S \subseteq C \setminus \{i\}} w(|S|) \cdot (v(S \cup \{i\}) - v(S))$$

with

$$w(k) = \frac{k!(n-k-1)!}{n!}$$

- The weight  $w(|S|)$  is to compensate for having  $1/w(|S|)$  possible coalitions of size  $|S|$

- Consider a ML problem where you have either many features or heterogeneous data sources
- Choose a suitable utility function (e.g., accuracy for classification problems)
- Select top  $k$  features or data sources out of  $n$  according to their Shapley value
- Bonus: Shapley value is hard to compute for large values of  $n$  (Complexity is  $O(2^n)$ ); use approximators such as Monte Carlo estimation or gradient-based methods
- *Main reference*: Ghorbani and Zou, 2019, May. Data shapley: Equitable valuation of data for machine learning. In International conference on machine learning (pp. 2242-2251). PMLR.

More topics



- Autonomous vehicles = self-driving cars
- Traffic-related scenarios can be modeled as games: reacting to moving obstacles, multi-story parking
- *Main reference*: Crosara et al., 2023, June. Game Theoretic Analysis of Overtaking Maneuvers for Autonomous Vehicles with Moving Obstacles. In 2023 International Balkan Conference on Communications and Networking (BalkanCom) (pp. 1-6). IEEE.

- Jamming = an attacker aims to disrupt communications at the physical layer using noise
- Simplest jamming game: multiple available channels, attacker needs to decide which channel to disrupt, transmitter should try to avoid that channel (zero-sum game)
- *Main reference*: Scalabrin et al. A zero-sum jamming game with incomplete position information in wireless scenarios. In Proceedings of European Wireless 2015; 21th European Wireless Conference 2015 May 20 (pp. 1-6). VDE.

Questions?