Artificial Intelligence Laboratory

Boi Faltings
Artificial Intelligence
Artificial Intelligence

- People are good in the natural world:
  - irregular shapes
  - reactive
- Modern world is artificial:
  - precision machinery
  - schedules and interdependencies
- AI: helps people work in the artificial world
NexThink

- Starting point: social engineering attacks.
- Idea: illicit use shows up in behavior.
- Student project: machine learning for behavior profiling, with very successful results (2002).
- => commercial prototype.
Product Evolution

- Initial idea: security is the killer application.
- However, cannot put $$$ value on avoiding security problems!
- Main selling point: detect performance problems and network activity.
- Security difficult to market.
NexThink Story

• 2004: founded by Pedro Bados (student), Patrick Herzog, Jean-Luc Gianduzzo, and myself.
• 2005: first customer: Rolex.
• 2006: first venture round.
• 2007-2019: raised over 100 Mio CHF
• over 500 employees, offices world-wide
LIA: Laboratoire d'intelligence Artificielle

- Director: Boi Faltings
- 6 Ph.D. students + 2 co-supervised.
- 4 will finish next year: several openings.
Range of LIA Work

- Creative design of mechanism shapes (1985-1996)
- Recommender systems (1997-now): conversational, ontology-based, sequential
- Truthful mechanisms for information elicitation (2003-now)
Examples of current work at LIA

- Recommender systems
- Truthful information elicitation
- Multi-agent coordination
Recommendation: where AI impacts everyday life

- What advertisements you see (Google)
- What movie you watch (Netflix)
- What products you buy (Amazon)
- What news you read (Google, Facebook, ...)
- What friends you make (Facebook, Linkedin, ...)
- Who will be your spouse (Match.com, ...)
- The most profitable of all AI applications.
Recommendation systems

- Infer preferences from past behavior.
- Collaborative filtering:
  - use preferences of like-minded users.
- Problems:
  - requires too much information (30-40 rated items per user)
  - slow to incorporate new items.
Ontology Filtering

- Structure user preferences into an ontology.
- => better accuracy with less information (5 items)
- => new items can be placed in ontology and are immediately accessible.
- Chorafas award/patent.
• Startup company Prediggo commercializes technology.

• Currently used at about 60 e-commerce sites, including Moevenpick, MediaMarkt, Conforama, etc.
News recommendation

• Challenges:
  • short traces
  • items change all the time
  • avoid redundant recommendations
• new technique: context trees.
Practical Performance

- Online at Swissinfo (1 year) and Le Point (15 months).
- Big difference in online/offline optimisation.
- CTR more than 3x higher than state of the art.
E-Commerce Application

- Version for e-commerce = BVMM, sold by Prediggo (published in IAAI 2019)
TPCF: Topic Profile
Collaborative Filtering

- Hotel ratings are too sparse for CF
- Instead, base similarity on review texts.
**Improvements over Default Ranking**

\[
\tau = \frac{\sum_{i \in U} sp(i) - np(i)}{\sum_{i \in U} sp(i) + np(i)}
\]
Some open issues

- Reliable profile building from review texts.
- Beyond accuracy.
Issues with Crowd data: music ratings

ratings on Amazon

ratings in controlled experiment

Figure 3: Distribution of the Ratings on Amazon.com (fitted with a U-shaped curve) for a Music CD (Mr. A-Z)

[Hu, Pavlou & Zhang, 2006]
Quality Control

- Quality of data gathered from other sources can be questionable.
- Machine learning => poor data quality is hidden.
- Can lead to terrible results...
Great Leap Forward (China, 1958-60)

- Progress measured by grain/steel production figures.
- Village chiefs pressured to report inflated grain production (up to 10 times).
- Result: grain was exported in spite of shortage, at least 30 million people died.
Subprime Mortgages (USA, 2008)

• Risk of financial products assessed by statistical models.

• Debt bundled into large packages cut into slices with different priorities and ratings.

• Banks reverse-engineered models and made risky debt look unrisky.

• We know the rest...
Truthfulness

• Reporting data is a lot of work.
• Agents only do it for ulterior motives:
  • promote themselves or their friends
  • punish their rivals
  • take revenge
Better Results

• Reward contributors for their efforts!
• Challenge: scale rewards so that only accurate data is paid.
  • payoff is a function of report and outcome.
  • truthful report maximizes expected reward.
Incentives for Prediction

• Truth $t$ eventually becomes known:
  • reward if prediction $x = t$
  • reward probability distribution $p(x)$ using scoring rules
    (e.g. Brier score: $r = 2p(t) - \Sigma p^2(x)$; $E[r]$ maximal for true $p$)
• Truth-telling is a dominant strategy
What if truth is never known?

• Reward for coherence with others:
  • Agreement (OA, CA mechanisms)
  • Mutual information (log PTS)
  • Model improvement (Peer Truth Serum)
• => Truhttelling is a game-theoretic equilibrium
Properties

• Truth-telling is focal: equilibrium with the highest payoff for data providers.
• Heuristic/random data provides no payoff, and does not eliminate truth-telling incentives.
• Schemes learn by themselves, no information about agent beliefs needed.
Peer Truth Serum

- Model = distribution of data.
- Quality measured on prediction of a randomly chosen data point, using scoring rules.
- Reward proportional to improvement of model quality.
- Easier if restricted to specific ML model.
Community Sensing

- Goal: Maintain a map of pollution in a city.
- Need to distribute sensors in many places.
- Community sensing: citizens operate sensors and get paid for the data.
Peer Truth Serum: Sensor Incentives

• Simulation of city of Strasbourg:

• Accuracy is rewarded for every sensor.
Opinion Polls

Predict the future!

Ask
Start by asking any forecasting questions you might want to know. The crowd's wisdom will help you predict the outcome of your event.

Predict
You make a prediction on the outcome of future events by buying or selling shares on a market.

Win!
If your prediction is correct, the market rewards you for every share you hold.

Sign up for free!

The contest is running!
The player with the highest profit of the week wins! You can get up to USD100 in prizes! Interested? sign up! More info about the rules of the contest here.

What's hot?
[int] Will the NATO conduct a military intervention in Syria?
The crowd predicts:

- yes (97.9%)
- no (2.1%)

[TV] Which character(s) will die by the end of the final episode of Breaking Bad?
The crowd predicts:

- Walter (79.3%)
- Jesse (3.6%)
- Hank (3.4%)
- others (12.8%)

Latest tweets

swissnoise [swissnoise] [TV] Will Walter White end up in jail at the end of the final episode of Breaking Bad? 29 Aug

swissnoise [swissnoise] [TV] Which character(s) will die by the end of the final episode of Breaking Bad? 29 Aug

umanytics
Monitoring Smart Contracts

• Smart contracts require oracles that decide when they are triggered.

• Oracles without central authority require incentive/reputation schemes to be truthful.

• Example: crop insurance - verify through crowdsourcing (Koinearth)
Privacy vs. Truthfulness

- Privacy is an important concern.
- Easiest way to achieve: report non-truthful or noisy data.
- Privacy schemes without concern for truthfulness are useless...
- Challenge when using personal data.
Federated Learning

- Establish data markets where contributions are paid.
- Peer truth serum as mathematical basis.
- Can implement on blockchains.
- Cost of on-chain storage is the major issue.
Some open issues

• Privacy in incentive computations (e.g. using secret sharing).
• Influence functions for different machine learning algorithms.
• Privacy bounds in federated learning for random forests/SVMs/etc.
Use AI to organize our environment efficiently and seamlessly.

Examples:
- airport slot allocation
- sharing truck capacity
- project planning
Airport Slot Allocation

• Planes need to take off and land.

• => intended schedule only works if all slots are granted.

• otherwise airlines find another use...

• => huge inefficiencies.
Sharing Truck Capacity

- Most trucks drive home empty.
- Sharing capacity among operators could eliminate a lot of truck traffic and cost.
- So can sharing orders among competing companies.
Construction project involves 50-100 contractors.

All need to be scheduled.

All plan independently and are self-interested.
Issues in Multi-Agent Coordination

- Efficient multi-agent optimization:
  - information exchange.
  - computation time.
  - memory.
- Rationality: incentives to cooperate?
- Privacy: not revealing competitive information.
Multi-Agent Optimization

- Information about constraints and preferences distributed among agents.
- Centralize all information
  - insufficiently formalized.
  - lack of control.
  - privacy concerns.
- => distributed algorithms.
Progress on Distributed Constraint Optimization

Meeting Scheduling: problem size solvable within an hour

<table>
<thead>
<tr>
<th>Year</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>1992</td>
<td>ABT</td>
</tr>
<tr>
<td>2000</td>
<td>AAS</td>
</tr>
<tr>
<td>2003</td>
<td>ADOPT</td>
</tr>
<tr>
<td>2005</td>
<td>DPOP</td>
</tr>
<tr>
<td>2013</td>
<td>DUCT</td>
</tr>
<tr>
<td>2019</td>
<td>ALMA</td>
</tr>
</tbody>
</table>
Some open issues

• Differential privacy in randomized algorithms?
• Solve rationality issues through randomized decisions?
Current AI Challenges

- Modern AI depends on data, for learning and decision-making.
- Data often is gathered from independent sources.
- Thus, data quality and privacy are the main issues going forward.