AI and Systems

Monica Lam and Qun Li

Problems

- **How can AI improve systems?**

  - System Algorithms

  - Natural language programming

- **How can systems improve AI?**

  - Performance

  - Data privacy

Classical → AI Algorithms

- Motivation:
  - Complex problems: we can't observe the behavior. congestion control, traffic optimization, fixing software bugs
  - Errors/problems are often caused by human (87%)
- Challenges
  - What are the best problems amenable to this approach?
  - AI solutions are mostly statistical and can have errors
    - Use systems to back it up to provide a guarantee
  - Engineering artifacts, all of a kind, and many of them
    - What kind of algorithms?   Can we map this to images?

Natural Language Programming

- Highest level programming: Natural language

  - A neural semantic parser maps NL to a formal language

  - All consumers can "program", mainly to automate their digital tasks

  - Doctors and knowledge workers can become more productive

- Need to be done by systems, and not AI people

  - Formal target language design, with formal syntax and semantics

  - Tools to engineer training data since there is no natural real data

  - Preliminary results suggest solving the problem in 5 years.

AI Needs High Performance

- Active hardware explorations

  - High-performance computing for training

  - On-chip inference supports scaling and privacy,

    - Energy consumption is a major concern

  - Real-time training

- Bottleneck is still: compiler technology to use the HW

  - Dense computations, sparse computations

Big Data with Privacy

- Virtual Assistants access more data than FB

- Full potential of ML needs privacy protection
  e.g. HiPPA protects privacy, but prevents research progress

- A private data architecture for consumers

  - Federated systems: e.g. Almond federated virtual assistants

  - Access control

    - Policies in natural language

    - Flow control; 3rd party sharing control e.g. with blockchain technology

  - Edge-cloud co-operation to reduce disclosure of personal details to the cloud

  - An economically viable infrastructure with brokerage of select personal info