AI Systems: A new frontier

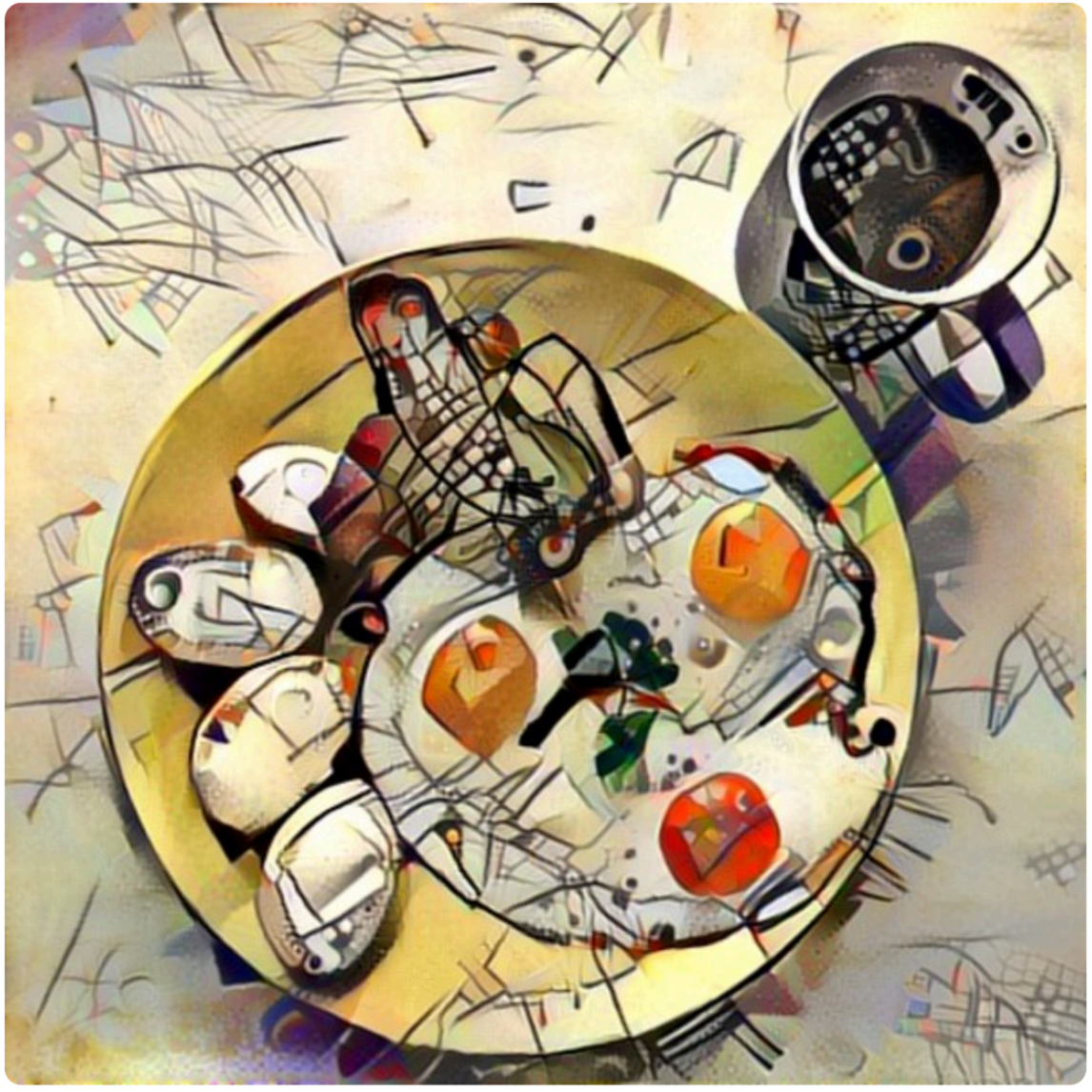
Siyuan Zhuang
USTC1411, UC Berkeley

（欢迎讨论任何 AI 相关或者 System 相关的问题）

Fun facts

- 如今大部分人在说**A**rtificial **I**ntelligence的时候，其实是在说 **M**achine **L**earning，而当代的 **M**achine **L**earning，大部分是在指 **D**eep **L**earning；**D**eep **L**earning 做的主要内容是训练 **N**eural **N**etworks，训练 **N**erual **N**etworks 其实就是在拟合函数。

- 然而确实相当多的 AI 任务可以表示为函数拟合。



Modern pipelines of AI applications

- **Data**
  - Collecting, cleaning, labeling
  - Data storage
- **Serving**
  - Online serving
  - Offline serving
  - Third-party platform
- **Training**
  - Model selection, hyper-parameter tuning
  - Distributed training
  - Preprocessing
  - Monitoring
  - Debugging
  - Visualization

The Rise of Full Stack Bottlenecks in AI applications

- **Deployment concerns**
  - robustness to adversarial influences
  - privacy and security, especially sensitive data
  - interpretability
  - fairness
- **Cost**
  - Training cost
  - Labeling cost
  - Serving cost
- **Accessibility**
  - usable by developers and organizations without PhD-level machine learning and systems expertise

Systems for AI

- **Software systems**
  - Interface, programming language
  - Metrics for models, architectures and systems
  - Tools for monitoring, interpretation, debugging, adaptation, tuning and maintenance of production AI application.

- **Hardware Systems**
  - Specialized hardware for certain tasks
  - Hardware using trade-offs with respect to precision, stability, fidelity, and more
  - Hardware supports distributed training/ serving

- **Intersection of hardware/software**
  - power, latency, memory limits
  - full-stack security & privacy
  - accessibility

Detailed examples

Data

- 数据采集硬件
- 数据采集质量
- 机器协助数据标注
- 数据标注系统（如何管理标注员和标注质量，如何自动分配标注任务）
- 数据质量的判断
- 数据清洗的分布式系统（动态调度）
- 数据存储（数据接口，压缩，备份，数据更新，某些特殊数据（比如明星的图片））

Training

- 大规模分布式训练
- 各种自动调参
- 训练过程的监控和调试
- 数据增强框架（特殊的噪声，特定的场景（车牌等））
- 可视化和解释结果

- 如何在第三方平台（比如云计算）中进行计算而不泄漏敏感数据
- 如何充分利用专用硬件
- 如何降低能耗

Serving

- 线上平台如何和现有web框架结合
- 如何部署在线下设备，特别是算力不足的情况，比如手机等
- 如何保证公开的模型不泄露训练数据等敏感内容
- 如何处理对抗样本
- 模型可解释吗？能够充分信任吗？

AI for system?

Thanks