Huawei Interview

Self-introduction > Working Experiences > Research

Eric Han

Apr 30, 2024

Self-introduction

Educational Background

My educational journey to CS, R&D:

- **Secondary School** [2004-2008] Interest started with scripting / Java - games
  - Curious as to how computers work
- **Pioneer JC** [2009-2010] Nurture interest to a passion.
  - Studied H2 Computing - Basics of CS, C++.
  - A*STAR IHPC Quest 2009 (Bronze) - Implement distributed K-Means
- **B.Com. NUS** [2013-2018] Further develop CS, R&D skills.
  - A*STAR Scholarship - Internships working on R&D projects
- **PhD. NUS** [2018-2023] PhD in AI/ML
  - Research is in AI/Machine Learning regarding scaling and robustness.

Key skills

- **Programming Languages**: Python, C++, Java...
- **Numerical Computing**: NumPy, SciPy, PyTorch...
- **Databases**: Firebase, SQL...
- **Typesetting / Presentation Tools**: LaTex, Markdown (This slides!)...
- **Tools/Platforms**: Git, Mlflow, Plotly, Slurm, GCP...
- **Operating Systems**: Linux (also administration), Windows, macOS

Service

Contributed in voluntary capacity, service to:

- **Research Community**
  - Reviewer, Student Volunteer, Session Chair
- **National University of Singapore**
  - Admission reviewer (Masters), Program Committee
- **Agency for Science, Technology and Research**
  - Outreach volunteer, Invited speaker, Mentoring
- **Impact Life Church**
  - Head of IT - Manage a volunteer team
  - Software development of Church apps.
  - IT infrastructure/ops.

Keen to contribute above and beyond what is necessary, to improve others/org.

Working Experiences

Teaching Assistant / Graduate Tutor [2018 - 2024]

Teach ($>$ 500 contact hours), while persuing a PhD.

- AI/ML
  - CS2109s - Introduction to AI and Machine Learning
  - CS3243 - Introduction to Artificial Intelligence
- Software Engineering
  - CS3217 - Software Engineering on Modern Application Platforms
  - CS3203 - Software Engineering Project
  - CS2030/CS2030S - Programming Methodology II

Commitment to excellent teaching, effective communication:

- Full-Time Teaching Assistant Award [Apr 23]
- High teaching feedback scores / Nomination rates

A Cloud-based Collaborative Model Building Platform [Dec 15, May 15 - Jun 15]

Design, implement & deploy dockerized, distributed ML platform (before Azure ML)

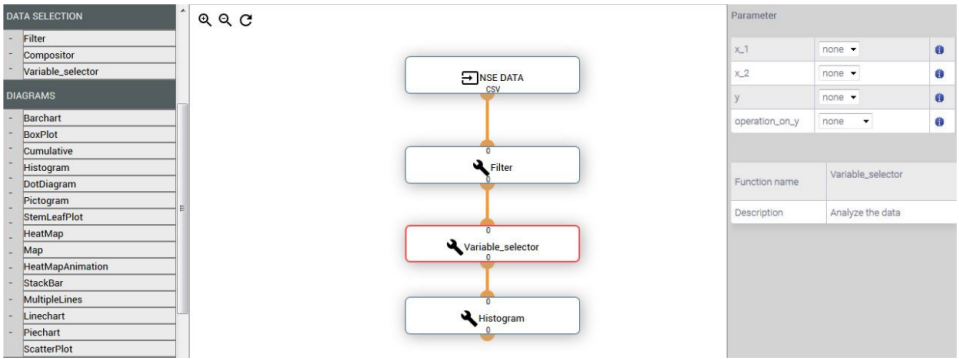


Figure 1: Interface @ National Science Experiment Big Data Challenge

Route My Day (Recommendation System) [Jan 13 - Jul 13]

Design, implement & deploy visualization, distributed web crawler & MongoDB.

Improve productivity, optimizing people's time:

1. Select items to do
2. Add locations to visit
3. Finds a route.

Second place for Apps4SG Competition 2013 [8 Jan 2014].

Research

Statement

I am interested in **scaling** machine learning towards higher dimensions in Bayesian Optimization, Gaussian Processes, Convex and non-convex optimization and Reinforcement Learning. I am also interested in **robustness concerns** in machine learning.

PhD Research

Bayesian Optimisation Techniques for **High-Dimensional** and **Adversarial** Settings

Advised by: *Asst. Prof. Scarlett Jonathan*

Optimization

We have a function $f : \mathcal{X} \to \mathbb{R}$ that we want to find $x_{\max}$ on $\mathcal{X} \subseteq \mathbb{R}^{N_{\dim}}$:

$$x^* = x_{\max} \in \arg\max_{x \in \mathcal{X}} f(x); \quad f^* = f(x^*) = \max_{x \in \mathcal{X}} f(x)$$

Situations such as tuning the hyper-parameters, ie. AlphaGo: **Unknown**, **High Cost**

Bayesian Optimization

Bayesian Optimization (BO) is a popular and important technique for sequential global optimization of black-box functions in a query efficient manner.

$$y_i = f(x_i) + \epsilon_i, \quad \epsilon_i \sim \mathcal{N}(0, \sigma^2)$$

After tuning, AlphaGo win-rate improved by *at least* 50% to 66.5% in self-play games.

High Dimensionality in Bayesian Optimization (Method)

Each lower-dimensional component $f^G : \mathcal{X}^G \to \mathbb{R}$ is either a 1 or 2-dimensional function defined on the variables in G, where $\mathcal{X}^G = \bigtimes_{v \in G} \mathcal{X}_v$.

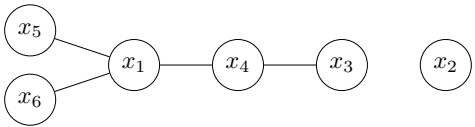


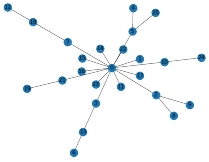
Figure 2: $h(x) = h^A(x_1, x_6) + h^B(x_1, x_5) + h^C(x_1, x_4) + h^D(x_3, x_4) + h^E(x_2)$

Our Goal

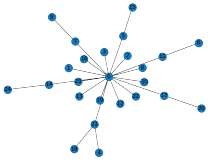
Exploit tree structures (Additive Structure) for efficacy, to mitigate curse of dimensionality.

High Dimensionality in Bayesian Optimization (Results)

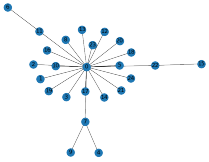
Tree is competitive on both synthetic and real datasets:



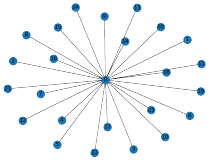
(a) Star-25, Iter 15



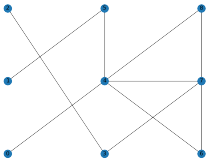
(b) Star-25, Iter 30



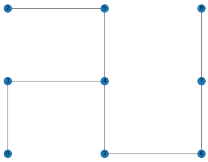
(c) Star-25, Iter 45



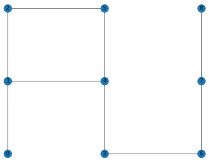
(d) Star-25, Iter 60



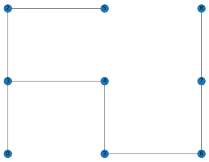
(e) Grid-3, Iter 15



(f) Grid-3, Iter 30



(g) Grid-3, Iter 45



(h) Grid-3, Iter 60

Adversarial Attacks on BO (Method)

At time t, with random Noise $z_t \sim \mathbb{N}(0, \sigma^2)$, adversarial noise c_t and budget C:

$$y_t = \underbrace{f(\mathbf{x}_t) + c_t}_{\tilde{f}(\mathbf{x}_t)} + z_t, \qquad \text{where } \sum_{t=1}^{n} |c_t| \leq C, \quad |c_t| \leq B_0.$$

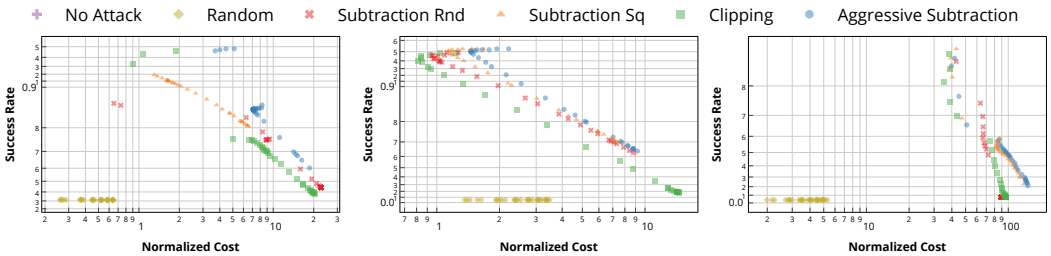
Types of attack:

1. Targeted Attack - make the player choose actions in a particular region $\mathcal{R}_{\text{target}}$.
2. Untargeted Attack - make the player's cumulative regret as high as possible.

Our Goal

Examine from an attacker's perspective, focusing on adversarial perturbations.

Adversarial Attacks on BO (Results)



- Clipping works consistently.
- Aggressive Subtraction works, but with higher cost.
- Subtraction Rnd and Subtraction Sq is 'in between'.
- Subtraction Rnd tends to narrowly beat Subtraction Sq (due to smooth $h(\mathbf{x})$).

Black-box Adversarial Attacks on CNNs (Method)

We pose the *untargeted* attack as a constrained optimization problem, to find the adversarial perturbation δ where $f(\mathbf{x}, y, \delta)$ is maximal.

$$\delta = \arg\max_{\delta} f(\mathbf{x}, y, \delta) \quad \text{subject to } ||\delta||_p < \epsilon \bigwedge \mathbf{x}' \in [0,1]^D$$

$$\text{where } f(\mathbf{x}, y, \delta) = \begin{cases} 0 & \text{if } F(\mathbf{x}') \neq c \\ -1 & \text{otherwise} \end{cases}$$

- ℓ_∞ Attack - CNNs are constructed with shift-invariant components.
- ℓ_2 Attack - Tradeoff in how the CNN is trained

Our Goal

Apply domain knowledge to dimensionality reduction to improve success rate.

Results

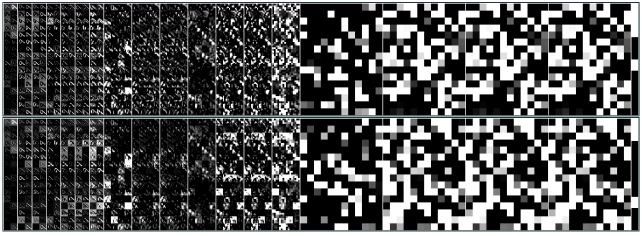


Figure 3: ℓ_∞ Attack

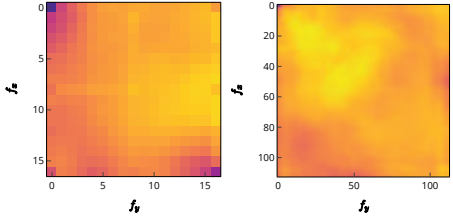


Figure 4: ℓ_2 Attack Heatmap.

Misc Projects

- Reinforcement Learning for Feature Subset Selection
  - Drawbacks does not outweigh benefits
- Scaling Gaussian Processes to large datasets (datapoints) via rearrangement
  - Difficult to obtain rearrangement
  - Few benefits
- Scaling Combinatorial Bayesian Optimization
  - Literature Review

Career Aspirations

Career Aspirations @ Huawei

After my PhD, I applied quite broadly to anywhere that I am interested in. For a career at Huawei, I am interested to:

- Perform R&D in AI/ML
- Applied Research to Business use case
- Management / Leadership

For the role **LLM R&D Researcher**, I am willing to pick up NLP skills.