# Dr. Han Liang Wee, Eric

+6592982927 mail@eric-han.com eric-han.com eric_vader eric-vader

## Research Statement

My primary research interest lies in scaling Machine Learning (ML) models to accommodate higher dimensions and large datasets, with a particular focus on scaling Bayesian Optimization (BO). Many optimization problems of interest are high-dimensional, and scaling BO to such settings remains an critical challenge. In addition, I am also interested in addressing robustness in ML systems, exploring how these models can remain effective and reliable under various operational conditions and adversarial scenarios.

### Introduction

At the core of my PhD research interest is BO, which is an effective method of optimizing black-box functions that are expensive to evaluate. This optimization framework is important and effective for applications such as hyperparameter tuning, for example:

1. (Yang, 2024)[1] found that BO can effectively hyperparameter tune feature selection method and has the potential to considerably benefit downstream tasks.
2. (Chen, 2018)[2] used BO to automatically tune AlphaGo's hyperparameter, resulting in an improved win-rate from $50\%$ to $66.5\%$ in self-play games.

High-profile applications like AlphaGo highlight the growing significance of BO as ML models become more complex and require larger datasets.

### PhD Work

I studied and addressed scalability and robustness issues surrounding BO:

1. **(AAAI 2021)** Scaled BO to higher-dimensionality via decomposition and learning of its tree-structured dependency graphs, presenting a hybrid graph learning algorithm and a novel zooming-based method allowing optimization on continuous spaces. Model complexity is traded-off to enhance model efficiency and retain sample efficiency. It has birthed follow-up work that instead uses random tree decompositions.
2. **(ICML 2022)** Investigates adversarial attacks on BO by proposing various attack methods based on the attacker's knowledge and strength, and demonstrates that these attacks can effectively manipulate the algorithm's output with a limited budget.
3. **(Ongoing Work)** Used BO for adversarial attacks on Convolutional Neural Networks (CNNs) in a black-box hard-label setting, utilizing domain knowledge for dimensionality reduction and introducing query-efficient hyperparameter selection.

### Future Directions

(Xu, 2024)[3] challenges the prevailing belief that BO is ineffective in high-dimensionality, showcasing the cost (performance) of introducing strong additional assumptions. I would like to examine and explore applying alternate scaling techniques such as borrowing the idea of dropout[4], having different stages of BO on sampled data. With different trade-off characteristic, it can encourage wider applicability of BO.

Warm regards,
Eric Han

1. https://www.nature.com/articles/s41598-024-54515-w
2. https://arxiv.org/abs/1812.06855
3. https://arxiv.org/abs/2402.02746
4. https://www.ijcai.org/proceedings/2017/0291.pdf