Mechanical Engineering Thesis Defense

Adversarial Machine Learning for Recommendation Systems

School for Engineering of Matter, Transport and Energy

Aksheshkumar Ajaykumar Shah

Advisor(s): Dr. Hemanth Venkateswara, and Dr. Spring Berman

Abstract

Recently, Generative Adversarial Networks (GANs) have been applied to the problem of Cold-Start Recommendation, but the training performance of these models is hampered by the extreme sparsity in warm user purchase behavior. In this thesis we introduce a novel representation for user-vectors by combining user demographics and user preferences, making the model a hybrid system which uses Collaborative Filtering and Content Based Recommendation. Our system models user purchase behavior using weighted user-product preferences (explicit feedback) rather than binary user-product interactions (implicit feedback). Using this we develop a novel sparse adversarial model, SRLGAN, for Cold-Start Recommendation leveraging the sparse user-purchase behavior which ensures training stability and avoids over-fitting on warm users. We evaluate the SRLGAN on two popular datasets and demonstrate state-of-the-art results.

February 10, 2022; 1 PM;
Zoom Link: https://asu.zoom.us/j/83200492204