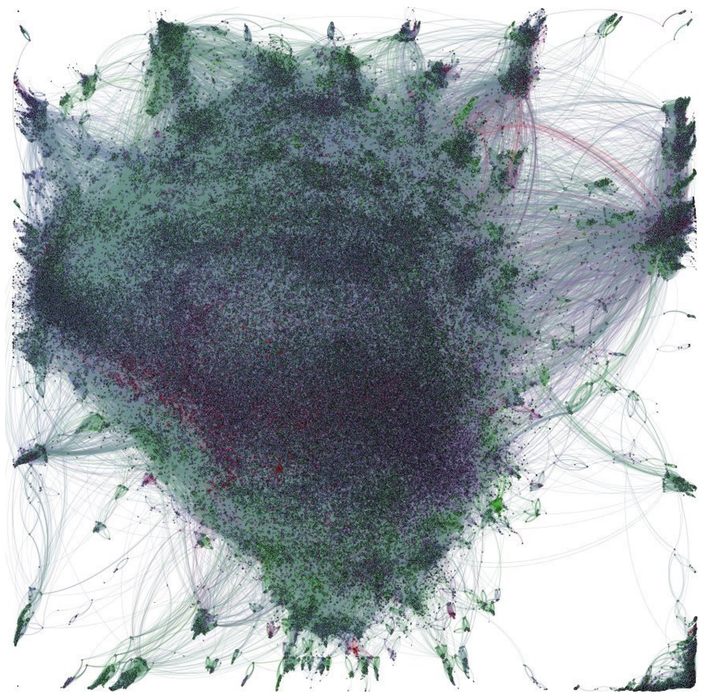
A First Principles Approach to Trust-Based Recommendation Systems

Paras Stefanopoulos (u7300546), Supervised by Dr Ahad Noori Zehmakan

Trust Based Social Networks

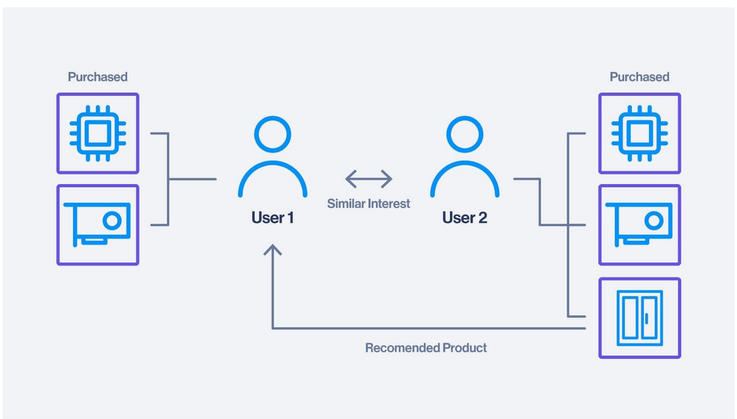
Social networks are large graph networks, where nodes represent users and edges represent “trust” or some form of relationship.



A large-scale social network visualized (Iguana S, 2020)

Recommendation Systems

A recommendation system tries to predict how much a given user will like a chosen item. It can use any information supplied available by the network, such as network structure, other’s ratings and the given user’s ratings of other products (Burke, Felfernig, & Göker, 2011).

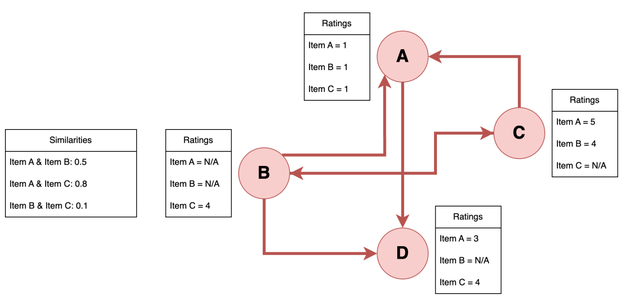


A depiction of a collaborative filtering approach to recommendation systems (Pham K, 2022)

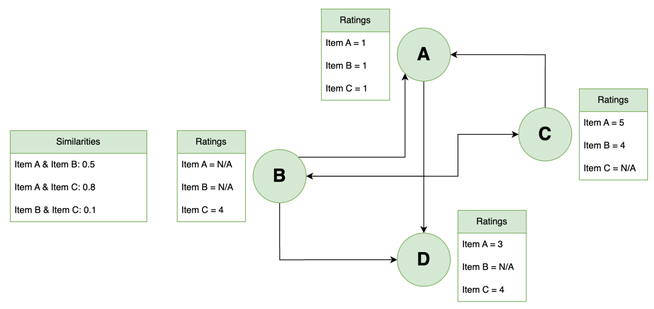
First Principles Approach

We determined there were three basic forms of information available to recommenders in all social networks which have the notion of items and opinion. We abstract users as ”nodes” and trust (following/friends) as edges to represent the network as a graph.

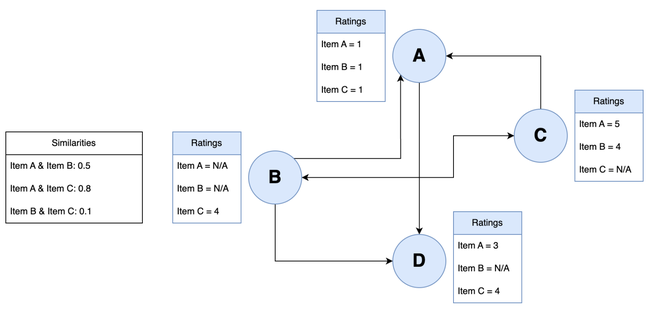
1. Trust Graph
   The trust graph is simply the nodes, and the trust connections between one another.



2. Intra-Item Information
   The intra-item graph is a sub-set of the data which contains how similar items are to each other. Along with each node’s neighbors.



3. Item-Rating Information
   The Item-Rating information is a sub-set of the data



With the data broken into these three components we can investigate how these very basic building blocks contribute to recommendation systems.

First Principles Approach (cont.)

Questions we can now address:

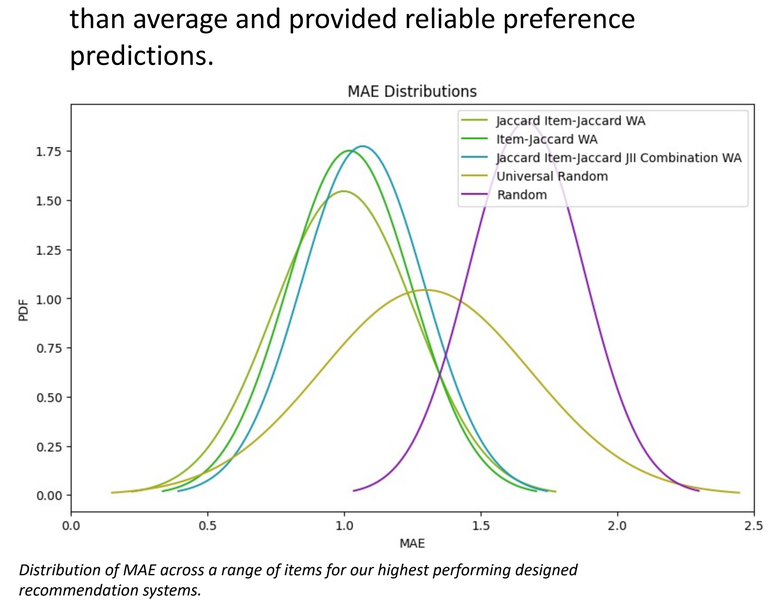
1. **How valuable are these forms of data to recommendation accuracy relative to one another?**
2. **What is the best recommender to address the “cold start” problem?**
   The cold start problem is where a node joins the network with little-to-no information provided. I.e. may add a few of their friends and have not rated any items (Lam et al., 2008).
   Recommenders which rely only on the trust graph or on the intra-item information are compatible and can be used for the cold start problem.
3. **Using ground-up knowledge/intuition gained from building recommenders for these sub-sets of the data - how can these forms of information be combined to create more performant recommendation systems?**
4. **How do these sub-sets of the information impact how robust our recommendation systems are to adversarial actors?**
5. **How can we develop robust and highly performant recommendation systems based on our newly gained first principles understanding?**

Evaluating Recommenders

To evaluate the recommenders on a given dataset, we take the top 5 most popular items, by number of ratings. We then follow the following procedure, for each of the top 5 items:

1. For 15% of the users, remove the rating they placed on the given item.
2. Predict the rating (star rating from 1-5) they’d provide for the item.
3. Compare with their actual rating.
4. We repeat this 10 times for each item to derive a distribution of Mean Absolute Errors associated with the recommender.

We then developed two control recommenders. Random and Universal Random. Universal Random provides a random rating with respect to the distribution of ratings for said item currently in the dataset.



Performance of control recommendation systems, the graph describes the distribution of mean absolute error (MAE) across a range of items and trials.

Designed, Implemented and Experimented with > 20 Recommenders

- Documented the strengths and weaknesses of all these designs and iterated to develop highly effective systems.
- Our best recommenders performed significantly better than average and provided reliable preference predictions.

Distribution of MAE across a range of items for our highest performing designed recommendation systems.

- We propose a novel framework for designing collaborative filtering recommenders called Weighted Average, which we show out-performs other traditional approaches like Random-Walk in non-adversarial environments.
- Based on this framework, we propose a novel recommender which offers high accuracy and consistent performance called the Jaccard Item-Jaccard WA.
  - The model combines trust-graph information with item-rating information through a combination of two similarity metrics based off the Jaccard Index.

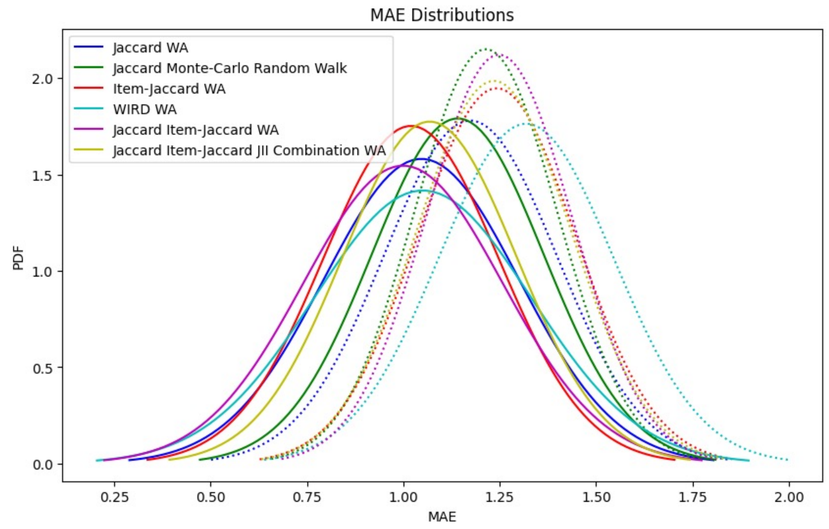
Validated With Popular Datasets

We validated the recommenders developed on datasets which are popular in the field of research, including Epinions, FilmTrust and CiaoDVD.

Algorithm	Datasets Epinions	FilmTrust	CiaoDVD	μ_{MAE}
Jaccard Item-Jaccard WA	**1.00**	**0.66**	**0.53**	**0.73**
Item-Jaccard WA	1.02	0.67	0.58	0.76
WIRD WA	1.05	0.67	0.72	0.81
Jaccard Item-Jaccard JII Combination WA	1.07	0.69	0.63	0.80
JWIRD WA	1.09	0.67	0.72	0.83
Item-Rating Difference WA	1.17	0.67	0.79	0.88
Universal Random	1.30	0.89	0.72	0.97
Jaccard WA	1.05	1.14	1.73	1.31
Jaccard Intra-Item WA	1.20	1.07	1.75	1.34
Mean of Neighbours	1.27	1.25	1.67	1.40
Jaccard Weighted Neighbours	1.31	1.22	1.66	1.40
Mode of Neighbours	1.32	1.23	1.67	1.41
Intra-Item WA	1.34	1.21	1.67	1.41
Monte-Carlo Random Walk	1.16	1.20	1.82	1.39
Jaccard Monte-Carlo Random Walk	1.14	1.20	1.81	1.38
Jaccard MoM	1.13	1.19	1.77	1.36
Median of Neighbours	1.27	1.26	1.76	1.43
Intra-Item WA (Pearson)	1.79	1.27	1.75	1.60
Random	1.67	1.34	1.82	1.61

Performance of most of our designed algorithms on an array of popular social-network datasets. Ordered by average performance across all datasets.

Investigated Robustness To Adversarial Attacks



Performance of a select group of our recommenders in both standard and adversarial environments. The dotted-lines depict the recommender’s performance when adversaries exist

The event of an adversarial actor in the system was simulated. I.e. a company creates fraudulent accounts and reviews to try manipulate ratings of a certain item.

Key Findings

- We propose two novel recommenders, Jaccard Item-Jaccard WA and a combination model. The former providing high mean accuracies, the latter offering slightly lower mean accuracy but better consistency in performance.
- Placing more emphasis on the trust graph (structure of the network) leads to better robustness against adversaries.
  - Random Walk recommendation frameworks are the most robust
  - Jaccard WA recommender was the best performing
- Item-rating information provides the best signal/noise for determining similarity between users for collaborative filtering.
  - Item-rating information suffers the most from adversaries.
- Intra-item information can be used to improve the consistency of recommendation systems at the cost of mean accuracy.
- We propose a new item-item similarity metric which in our experiments performs better than Pearson Correlation which is commonly used in research (Intra-Item Jaccard).
- We propose a new framework for quickly developing recommendation systems based on similarity metrics (collaborative filtering) we call Weighted Average.

Future Work

- Further experimenting with Intra-Item Jaccard relative to current intra-item similarity metrics. For example, replacing the Pearson Correlation with Intra-Item Jaccard in TrustWalker (Jamali and Ester, 2009), a widely renowned recommender from academia.
- Improving the computational complexity of the proposed algorithms to make them feasible for large-scale networks.
  - Also improving the efficiency of the Weighted Average framework, whether that is in time complexity or introducing concurrency and/or vectorization
- Extending the investigation into robustness against adversarial attacks. This could include experimenting with different forms of adversaries or designing recommenders specifically with this robustness in mind.

References

- Pham, K. (2022). *What are Recommendation Systems?* [online] Medium. Available at: https://medium.com/@khang.pham.exxact/what-are-recommendation-systems-6bb5036042db.
- Iguana, S. (2020). *Large Graph Visualization Tools and Approaches*. [online] Medium. Available at: https://towardsdatascience.com/large-graph-visualization-tools-and-approaches-2b8758a1cd59.
- Jamali, M. and Ester, M. (2009). TrustWalker. Proceedings of the 15th ACM SIGKDD international conference on Knowledge discovery and data mining - KDD ’09. doi:https://doi.org/10.1145/1557019.1557067.
- Lam, X. N., Vu, T., Le, T. D., & Duong, A. D. (2008). Addressing cold-start problem in recommendation systems. In Proceedings of the 2nd international conference on Ubiquitous information management and communication (ICUIMC ’08). DOI: 10.1145/1352793.1352837.
- Burke, R., Felfernig, A. and Göker, M.H., 2011. Recommender systems: An overview. Ai Magazine, 32(3), pp.13-18.