Collaborative Filtering under Model Uncertainty

Robin M. Schmidt
Department of Computer Science
University of Tübingen
Tübingen, Germany
rob.schmidt@student.uni-tuebingen.de

Moritz Hahn
Department of Computer Science
University of Tübingen
Tübingen, Germany
moritz.hahn@student.uni-tuebingen.de

Abstract—In their work, Dean, Rich, and Recht [1] create a model to research recourse and availability of items in a recommender system. We used the definition of predictive multiplicity by Marx, Pin Calmon, and Ustun [2] to examine different variations of this model, using different values for two model parameters. Pairwise comparison of their models show, that most of these models produce very similar results in terms of discrepancy and ambiguity for the availability and only in some cases the availability sets differ significantly.

All analysis code for our experiments and models can be found on GitHub: 
https://github.com/SirRob1997/collaborative_filtering

Index Terms—reachability, collaborative filtering, recommender system, multiplicity, ambiguity, discrepancy

I. INTRODUCTION

In toady’s society, recommendation systems have a huge influence on how individuals explore and experience information [1]. Generally, they are applied in a broad variety of domains including media (e.g. videos or music), product recommendations or travel and real estate. This raises some interesting questions like: “How easy can a user be pigeon-holed by their viewing history?” or “How does a recommender system encode bias that limits the availability of content?” These are some of the main question which inspired the work by Dean, Rich, and Recht [1] which form the basis of our contributions by providing the respective models and definition frameworks.

II. MODEL BY DEAN, RICH, AND RECHT [1]

A. Problem Setting

For their model Dean, Rich, and Recht [1] define a recommender system as a collection of $n$ users $u$ and $m$ items $i$. A rating for a user-item combination is then denoted as $r_{ui} \in R \subseteq \mathbb{R}$. The observed ratings $\Omega_u$ for a user are stored inside a rating history sparse vector $r_u \in \mathbb{R}^m$ with defined values at $\Omega_u$ and 0 at every other position. This allows the recommender system to make decisions following a policy based on this sparse vector denoted as $\pi(r_u)$ which yields a subset of items.

Based on these constraints, Dean, Rich, and Recht [1] define an item $i$ to be reachable from user $u$ if there is a modification to the rating history $r_u$ that results in item $i$ being recommended to user $u$. With that, they define the whole reachability problem as

$$\min_{r \in \mathcal{M}(r_u)} \text{cost} (r; r_u)$$

subject to $i \in \pi(r)$

utilizing a modification set $\mathcal{M}(r_u) \subseteq R$ which describes the possibilities of modifications to their respective rating history and the difficulty of making these changes in cost $(r; r_u)$. Intuitively, the cost function can correlate to the number of needed changes or how far these changes are away from the current preferences of the user [1].

Moreover, Dean, Rich, and Recht [1] focus on linear preference models which use a user vector $p_u$ and an item vector $q_i$ in combination with item bias $b_i$, user bias $c_u$ and over all bias $\mu$ to yield a predicted user rating $\hat{r}_{ui}$ as

$$\hat{r}_{ui} = q_i^\top p_u + b_i + c_u + \mu .$$

When incorporating matrix factorization with user and item representations as factors lying in a latent space of size $d$ we can represent the factors as $P \in \mathbb{R}^{n \times d}$ and $Q \in \mathbb{R}^{m \times d}$. Together with the regularizer $\Gamma$, this yields

$$\min_{P,Q} \sum_{u \in \Omega_u} \sum_{i \in \pi(r_u)} (r_{ui} - p_u^\top q_i)^2 + \Gamma(P,Q)$$

for fitting the model where Dean, Rich, and Recht [1] use the $\ell_2$ regularization on user and item factors.

When defining the cost function, instead of modeling it as the penalty on change from existing ratings, Dean, Rich, and Recht [1] penalize the change from predicted ratings. For edits on observed items (history edits) it is defined as

$$\text{cost}_{\text{hist}} (r; r_u) = ||r - r_u||$$

while edits on the recommended items (reactions) are defined as

$$\text{cost}_{\text{react}} (r; r_u) = ||r_{\pi(r_u)} - \hat{r}_{\pi(r_u)}|| .$$

B. Recourse and Availability

Further, Dean, Rich, and Recht [1] define recourse and availability as they are respectively important for understanding how a user’s preferences limited the reachable content and how available a certain item is inside the recommender system. Hence, they are defined as:
**Definition 1 (recourse):** The amount of recourse available to a user \( u \) is defined as the percentage of unseen items that are reachable, i.e. for which Equation (1) is feasible. The difficulty of recourse is defined by the average value of the recourse problem over all reachable items \( i \).

**Definition 2 (availability):** The availability of items in a recommender system is defined as the percentage of items that are reachable by some user.

### C. User Cold-Start

When a new user enters the recommender system, he has no prior rating history from which to predict preferences from. This process is known as the User Cold-Start problem and common strategies for recommender systems include presenting items which are most likely to be rated highly or be most informative about the respective users’ preferences [1]. With the definition of recourse, Dean, Rich, and Recht [1] define the onboarding set not only for its contribution to the model accuracy but also its provided amount of recourse.

### D. Sufficient Conditions for Top-\( N \)

The recommender system described by Dean, Rich, and Recht [1], a Top-1 recommender system, only ever recommends one item at a time. Since most real world applications involve serving several items at once, to model reality more closely, Dean, Rich, and Recht [1] expand this system to recommend \( N \) items at the same time instead, creating a Top-\( N \) recommender system with \( N > 1 \).

Dean, Rich, and Recht [1] define an item-region for the Top-\( N \) case, when \( i \in \pi(p, \Omega) \) as follows:

\[
\mathcal{P}_i = \{ p : (q_i - q_j)^\top p > 0 \}
\]  

with all but at most \( N \) items \( j \in \Omega \).

Although, according to Dean, Rich, and Recht [1], this region is contained in the latent space, generally of relatively small dimensions, the description depends on the number of items which in general will be quite large. While linear for \( N = 1 \), for \( N > 1 \), the description for each region requires \( \mathcal{O}(m^N) \) linear inequalities, becoming expensive very quick, even for small values of \( N \).

1) **Sufficient Condition for Availability:** To bypass those computational concerns, Dean, Rich, and Recht [1] show that the full description of the Region \( \mathcal{P}_i \) is not necessary, but instead finding any point in the latent space \( v \in \mathbb{R}^d \) that satisfies \( v \in \mathcal{P}_i \) is sufficient. They propose a sampling approach to determine the availability of an item with a complexity of only \( \mathcal{O}(m^d \log(m)) \).

Dean, Rich, and Recht [1] call items \( i \) that are inside an item-region defined via sampling aligned-reachable, which is a lower bound on the availability of items, yielding an underestimate of the availability of items in a system.

Using the aligned-reachable condition as a generic model audit, Dean, Rich, and Recht [1] propose an item-based audit algorithm with \( \Omega = \emptyset \) and an increased value for \( N \). The model audit counts the number of aligned-unreachable items, returning a lower bound on the overall availability of items. The model audit can also be used to propose constraints or penalties on the model during training.

2) **Sufficient Condition for Recourse:** As user recourse inherits the same computational problems as described for availability, Dean, Rich, and Recht [1] continue with the sampling perspective to test feasibility. This yields a lower bound on the amount of recourse available to a user, based on their specific rating history and the allowable actions. They show, that items who are aligned-reachable are also reachable by users, implying that item availability implies recourse for any user with control over at least \( d \) ratings whose corresponding item factors are linearly independent.

Dean, Rich, and Recht [1] conclude, that user recourse follows from the ability to modify ratings for a set of diverse items, and immutable ratings ensure the reachability of some items, potentially at the expense of others.

### E. Experimental Demonstration

Dean, Rich, and Recht [1] demonstrate how the proposed analyses can be used for auditing and interpreting characteristics of a matrix factorization model. They use the MovieLens 10M dataset [3], a common benchmark for evaluating rating predictions and the method described by *On the Difficulty of Evaluating Baselines* [4] in their recent work on baselines for...
recommender systems. The methods did match those presented by On the Difficulty of Evaluating Baselines [1] and reproduced their reported accuracies. Models of a variety of latent dimension ranging from $d = 16$ to $d = 512$ were examined. Additionally, they conducted a similar set of experiments on the LastFM dataset [5], which yielded similar results. Those results were included in Appendix B of the original paper.

After performing the item-based audit previously described, Dean, Rich, and Recht [1] found, that for larger values of $d$ as well as $N$, the number of items that are aligned-reachable is significantly higher. Baseline reachability is especially low for small values of $d$. At the same time, they found that unavailable items do have systematically lower popularity, while popularity alone does not determine reachability.

1) System Recourse for Users: For this, Dean, Rich, and Recht [1] used continuous ratings instead of rounded to the nearest 0.5 step, since it was easier for the model to work with, also only the 1000 most rated items were chosen to significantly reduce the computation time needed. This does produce a small overestimation because of popularity bias but was still considered a good approximation.

When allowing history edits, for a growing number of items in the history, Dean, Rich, and Recht [1] recognised two distinct shapes in the recourse curve. For all values of $d$, there first was a sharp increase in the available recourse, which did level after a while for each value of $d$. This can be explained by two factors: The sharp increase is determined by the limiting effect of the projection, which rises continuously. The leveling of effect on the other hand is determined by the baseline item-reachability. Dean, Rich, and Recht [1] note at this point that while higher complexity and therefore a larger number of latent dimensions provides a larger amount of recourse, lower complexity lets the model reach the maximum faster.

When considering fixed ratings and allowing no history edits, Dean, Rich, and Recht [1] were able to come up with the following conclusions:

1) The amount of recourse is actually bigger for a lower number of latent dimensions
2) For a small history length, more recourse is available
3) When rating random items, the available recourse is bigger, compared to rating only the recommended items

This does not contradict the previous results, as using a fixed history does eliminate the availability of additional recourse and only concerns the anchor points. It is worth noting, that the advantages of additional recourse seem to outweigh the disadvantages of the anchor points for large histories and more
 latent dimensions.

2) Recourse difficulty: At last, Dean, Rich, and Recht [1] did examine the cost of recourse over all users for a single item. A Top-1 recommender system was used to once again reduce the computational burden of computing the exact set \( \mathcal{P} \). The cost was posed as the size of the difference between the user input and the predicted ratings. In two trial runs, the cost of recourse was determined for a set of 20 random items as well as for the set of the 20 highest rated items. Here, Dean, Rich, and Recht [1] was able to arrive at the following findings:

1) The cost does not increase, but the amount of recourse is lower for a larger number of latent dimensions.
2) The cost was actually lower for random, then for Top-20

The experimental demonstration ended with the conclusion, that future work should more carefully examine methods for constructing recommended sets that trade-off predicted ratings with measures like diversity under the lens of user recourse.

III. DRAWBACKS OF THE DEAN ET AL. MODEL

The method proposed by Dean, Rich, and Recht [1] has a number of drawbacks, which are described briefly and left for further research. These drawbacks include the user cold start problem, popularity biases, filter bubbles and human-model interactions.

1) User Cold Start: While proposing onboarding sets to provide additional recourse, rather than focusing on model accuracy, Dean, Rich, and Recht [1] do not provide any demonstration of how the onboarding set plays a potential role in availability and recourse.

2) Popularity bias: Dean, Rich, and Recht [1] find that, the differences in availability of items does, to some extend, relate to their general popularity or unpopularity in the training data. According to Steck [9], this seems to be a phenomenon in recommender systems in general which amongst other things reproduces undesirable demographic biases. Dean, Rich, and Recht [1] provide no further explanation on how to combat this problem.

3) Filter Bubbles: The model used by Dean, Rich, and Recht [1] solely provides a reachability criteria which is based on the possibility of a user reaching a specific item. However, it does not provide any predictions if a specific user in a real-world scenario will actually reach the specific item or not. The possibility of recourse, for example, does not fix the problem of filter bubbles, as it merely provides the means to do so, but the user also has to use these means. Therefore, further
research would be warranted to examine if the cost function proposed models actual user behaviour or if it needs to be fundamentally changed to not provide a false appearance of fairness.

4) Human-Model Interactions: Lastly, there are untapped possibilities of future work to examine the interactions between users and models as the models evolve over time and the user behaviour might be influenced by the model at the same time. Dean, Rich, and Recht [1] note, that this path likely would lead towards understanding phenomena like filter bubbles.

IV. MODEL BY MARX, PIN CALMON, AND USTUN [2]

Shifting our focus, the key concept in the work by Marx, Pin Calmon, and Ustun [2] is the concept of multiplicity. If there are at least two competing models within an error tolerance $\epsilon \geq 0$ the respective problem exhibits multiplicity [2]. Marx, Pin Calmon, and Ustun [2] refer to the set of competing models as the $\epsilon$-level set and extend that term to predictive multiplicity where two models within the $\epsilon$-level set assign different predictions to a instance $x_i$ in the training data.

Further, Marx, Pin Calmon, and Ustun [2] propose formal measures for the possibility of multiple competing models (predictive multiplicity) in the form of discrepancy and ambiguity and define them as:

Definition 3 (discrepancy): Maximum number of conflicting predictions between a baseline model and any good model. If the discrepancy is small, near-optimal models (in the $\epsilon$-level set) output similar predictions and vice versa.

Definition 4 (ambiguity): Number of individuals that can be assigned a different prediction by at least one model in the $\epsilon$-level set.

While discrepancy is an upper bound for the number of predictions that can change, ambiguity determines that value for a particular model choice between a set of good models. Further, they provide integer programming tools to compute these measures for linear classification problems taking into account all possible models within a certain performance margin [2].

For their experiments, they construct binary classification problems based on the ProPublica COMPAS dataset [7], the Felony Defendants in Large Urban Counties dataset [8] and the Recidivism of Prisoners Released in 1994 dataset [9]. The results by Marx, Pin Calmon, and Ustun [2] show that for example on the COMPAS dataset a competing model with only 1% less accuracy can disagree on over 17% of the predictions (discrepancy) and 44% of predictions are vulnerable to model selection (ambiguity). Further, they try to raise awareness that discrepancy and ambiguity should not be overlooked when deploying classification systems in highly influential real-world scenarios and should be reported similarly to model statistics such as the test error [2].

V. EXPERIMENTAL SETUP

For our experiments, we want to apply the definition of predictive multiplicity and evaluate the proposed measures...
(discrepancy and ambiguity) from Marx, Pin Calmon, and Ustun [2] on the recommendation system of Dean, Rich, and Recht [1]. Therefore, we first need to determine a relevant \( \epsilon \)-level set. For our experiments, we used the trained models from [1], using the same settings as used in the paper for both, the MovieLens 10M dataset as well as the LastFM 1K dataset. Hence, we use the same values for the number of latent dimensions \( d = \{16, 32, 64, 128, 256, 512\} \) while setting the size of the recommender set to \( N = \{1, 2, 3, 5, 20, 100\} \).

As shown in Figure 1 when deploying an \( \epsilon = 0.02 \) on the Root-Mean-Squared-Error (RMSE), all our trained models with different latent dimensions lie within the \( \epsilon \)-level set. According to Marx, Pin Calmon, and Ustun [2], an \( \epsilon \)-value of 1% represents a conservative default for accuracy based measures and hence a RMSE with \( \epsilon = 0.02 \) is reasonable when applied in our application scenario. We also verified this by looking at the absolute changes in prediction on the testset in Figure 6. These are also marginally small which verifies our choice of \( \epsilon \)-level set.

Based on this set of competing models, we can evaluate the discrepancy in availability on the testset by choosing a baseline classifier from the \( \epsilon \)-level set and comparing it to all other models in this set. This way, we can construct \(|N|\) comparison matrices for the discrepancy of availability with varying \( d \) of size \(|d| \times |d|\) which for us are 6 matrices of size \(6 \times 6\) for each dataset. Additionally, by also considering \( N \) as a model parameter, we can construct comparison matrices of size \(|d| \cdot |N| \times |d| \cdot |N|\) for the discrepancy of availability with varying \( d \) and \( N \) which for us is 1 matrix for each dataset of size \(36 \times 36\). By taking the row-wise maximum value, we evaluate the final discrepancy for each baseline model choice. With this structure of our experiments, the constructed comparison matrices are symmetric and have diagonal entries with zero values since the set of conflicting elements between the same model is always an empty set.

Note, Dean, Rich, and Recht [1] also compare their definitions of recourse and availability for the different models in our \( \epsilon \)-level set (cf. Figures 3-7 and 10-13 in [1]), however, they do not include an analysis of the conflicting elements on this set. Hence, we base our analysis of the availability on the conflicting elements when comparing any baseline model and its available set \( \hat{Y} \) with any model of the \( \epsilon \)-level set and its available set \( X \) where we define the set of conflicting elements \( Z \) to be the negated intersection as \( Z = \neg (\hat{Y} \cap X) \). This set includes all items of \( \hat{Y} \) that are not included in \( X \) and vice versa. We want to stress that we consider the set difference \( Z = \hat{Y} \setminus X \) as especially relevant metric since these highlight available items in a smaller set which are not available in the broader set which has already progressed further. Therefore, we ensure that the baseline model for \( \hat{Y} \) has a smaller set size \(|\hat{Y}| \) than the model of the \( \epsilon \)-level set for \(|X|\) formalized as \( |\hat{Y}| < |X| \). This yields available items which are available in the smaller available set but not in the larger one.

Further, we analyse the ambiguity on the respective prediction items by comparing how often each item falls into a conflicting prediction set \( Z \) for each model of the \( \epsilon \)-level set. This allows us to compute an average percentage value of ambiguity items (items that at least fall into one conflicting prediction set) for each element of the recommender set \( N \). This yields \(|N|\) percentage values of average ambiguity values for the respective recommender system which, in our case, are 6 values for each dataset.

VI. RESULTS & DISCUSSION

We observe some high-level trends where for the same latent space size \( d \) for any two Top-\( N \) recommender systems with \( N_1 < N_2 \) the available items of the Top-\( N_1 \) recommender system are a proper subset of the Top-\( N_2 \) recommender system. This observation partly motivated our experiments for Figures 2 and 3 where we compare the availability for different latent space sizes \( d \) for consistent Top-\( N \) recommender systems. The results illustrate that, generally speaking, we observe contradicting availability sets when comparing two latent space sizes \( d \) that are rather small (e.g. 16, 32 or 64). However, for the majority of the Top-\( N \) recommender systems (mostly all but \( N = 1 \)), contradicting availability
values exclusively appear in the upper left quadrant for both the MovieLens and the LastFM dataset. Even if contradicting available items appear, they tend to be a comparably small amount with regard to the overall size of available items. This leaves us with the conclusion that when keeping the Top-N recommendation system constant, different models have very little discrepancy in availability.

Further, when looking at at the ambiguity of the conflicting available items illustrated by Figure 5, we observe a similar pattern. Overall, the number of ambiguous items for the models in our ϵ-level set with varying latent dimension size d tends to be very low. For the MovieLens dataset this value ranges from roughly 0.02 – 0.25% while for the LastFM dataset the range is from 0.005 – 0.115%. Since this value is so low, it is highly unlikely that it will have an overall meaningful impact and therefore can be neglected.

When we expand our ϵ-level set from only considering the latent space dimension d as a model parameter to considering the Top-N recommendation sets in addition to the latent space dimension, we can construct a similar heatmap as seen previously. Now, this new heatmap has shape 36 × 36 and is illustrated in Figure 6. Here, we observe larger values with a maximum for the MovieLens dataset of 659 and for the LastFM dataset of 2322. The maximum values respectively occur when comparing N = 2, d = 32 (baseline) to N = 20, d = 16 and N = 1, d = 256 (baseline) to N = 100, d = 64. For the MovieLens dataset, 8.73% of pairings produce a set difference above 1%, while 0.79% produce a set difference above 10% with a maximum discrepancy of 16.35%. For the LastFM dataset, 17.78% of pairings produce a set difference above 1%, while 4.29% produce a set difference above 10% with a maximum discrepancy of 29.19%. There seems to be no direct correlation between the discrepancy and the difference in set size.

VII. OUTLOOK

As one can see, there are a lot of possible aspects one can analyse when looking at a recommendation system. Obviously, it is impossible to cover all possible choices of such degrees of freedom and hence our analysis is mostly biased towards the availability (and therefore inherently the recourse) in recommendation systems, since we identify this as a key challenge and very critical point across different models. Further, additional analysis can be done in the future on comparing the discrepancy and ambiguity for recommendations for the user cold start, cost of recourse or recommendations based on a fixed history on models with different latent space size d.

REFERENCES

[1] S. Dean, S. Rich, and B. Recht, “Recommendations and User Agency: The Reachability of Collaboratively-Filtered Information,” in FAT* ’20: Conference on Fairness, Accountability, and Transparency, Barcelona, Spain, January 27-30, 2020, M. Hildebrandt, C. Castillo, E. Celis, S. Ruggieri, L. Taylor, and G. Zanfir-Fortuna, Eds., ACM, 2020, pp. 436–445.
[2] C. T. Marx, F. du Pin Calmon, and B. Ustun, Predictive multiplicity in classification, 2019.
[3] F. M. Harper and J. A. Konstan, “The MovieLens datasets,” ACM Transactions on Interactive Intelligent Systems, vol. 5, no. 4, pp. 1–19, 2016.
[4] On the Difficulty of Evaluating Baselines: A Study on Recommender Systems, 2019.
[5] T. Bertin-Mahieux, D. P. Ellis, B. Whitean, and P. Lamere, “The million song dataset,” in PROCEEDINGS OF THE 12TH INTERNATIONAL CONFERENCE ON MUSIC INFORMATION RETRIEVAL (ISMIR 2011), 2011.
[6] H. Steck, “Item popularity and recommendation accuracy,” en, in Proceedings of the fifth ACM conference on Recommender systems - RecSys ’11, Chicago, Illinois, USA: ACM Press, 2011, p. 125.
[7] J. Angwin, J. Larson, S. Mattu, and L. Kirchner, Machine bias, ProPublica, 2016.
[8] United States Department Of Justice. Office Of Justice Programs. Bureau Of Justice Statistics, State court processing statistics, 1990-2009: Felons defendants in large urban counties, eng, 1998.
[9] ——, Recidivism of prisoners released in 1994, eng, 2002.