

HỆ THỐNG GỢI Ý SẢN PHẨM DỰA TRÊN MÔ HÌNH HỌC NHÂN QUẢ

(Causal learning models for building recommendation system)

Giáo viên hướng dẫn

Ths. Trần Trung Kiên
TS. Nguyễn Ngọc Thảo

Sinh viên thực hiện

Nguyễn Duy Vũ
Nguyễn Chiêu Bản

Nội dung báo cáo

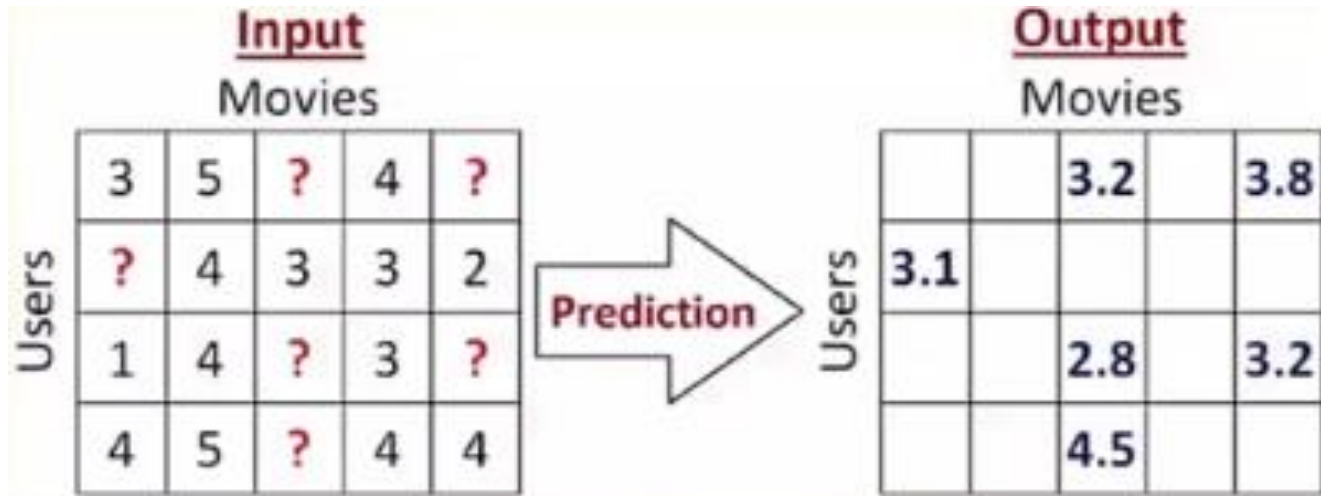
1. Giới thiệu
2. Kiến thức nền tảng
3. Phương pháp tìm hiểu
4. Các kết quả thí nghiệm
5. Tổng kết và hướng phát triển

1. Giới thiệu

- Phát biểu bài toán
- Ý nghĩa của bài toán
- Thách thức
- Phương pháp giải quyết tìm hiểu

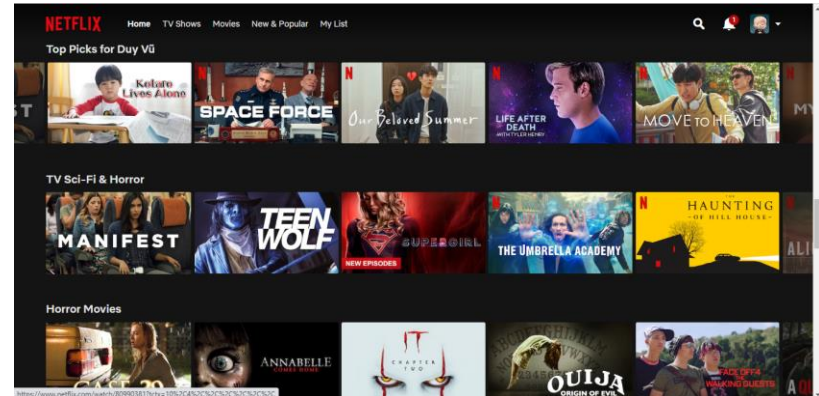
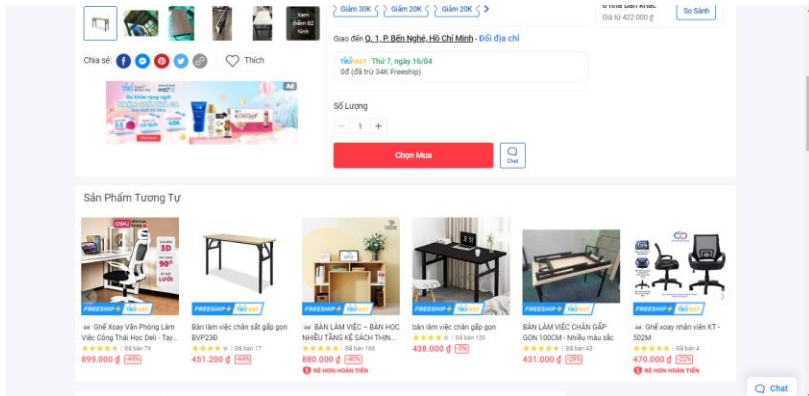
Phát biểu bài toán

- Đầu vào là đánh giá của các người dùng đối với các sản phẩm trước đó trong hệ thống.
- Yêu cầu: đề xuất các sản phẩm trong hệ thống mà phù hợp với sở thích của mỗi người dùng (hoặc là: dự đoán đánh giá của người dùng đối với các sản phẩm mà người dùng chưa xem trong hệ thống, qua đó đưa ra các chiến lược đề xuất phù hợp)



Ý nghĩa của bài toán

- Giúp trải nghiệm của người dùng được cá nhân hóa, do các đề xuất được đưa ra thông qua các đánh giá trước đó của người dùng. Tiết kiệm thời gian cho người dùng trong việc lựa chọn sản phẩm, giúp cho người dùng tập trung hơn vào việc trải nghiệm dịch vụ.
- Đối với các công ty thì sẽ tăng lợi thế cạnh tranh bằng cách nâng cao sự hài lòng của khách hàng. Tăng doanh thu thông qua việc kích thích nhu cầu mua sắm của người dùng bằng các gợi ý sản phẩm.

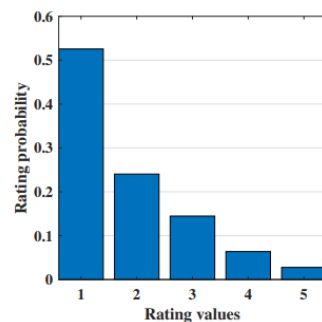
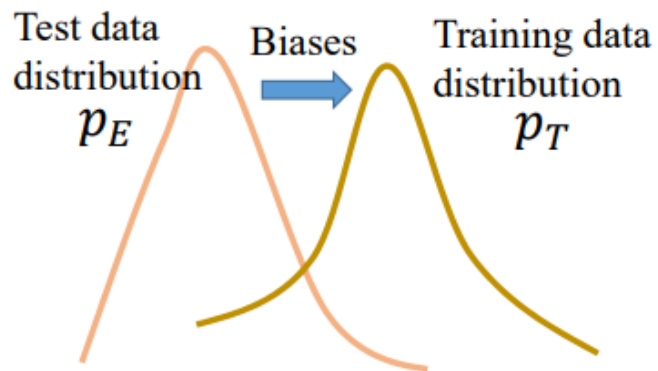


Thách thức

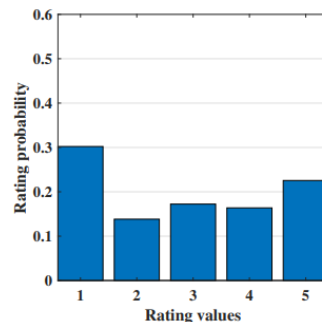
Dữ liệu quan sát được trong bài toán đề xuất sản phẩm thường bị gặp vấn đề lớn về thiên lệch dữ liệu.

Thiên lệch dữ liệu: phân phối của dữ liệu huấn luyện được thu thập khác với phân phối của dữ liệu kiểm tra lý tưởng (dữ liệu thực tế tuân theo phân phối uniform). Bắt nguồn từ 2 nguyên nhân sau:

- Do quá trình thu thập dữ liệu dựa trên việc người dùng tự đánh giá các bộ phim
- Do ảnh hưởng của hệ thống đề xuất sản phẩm đã triển khai từ trước chỉ đề xuất một vài loại sản phẩm nào đó.

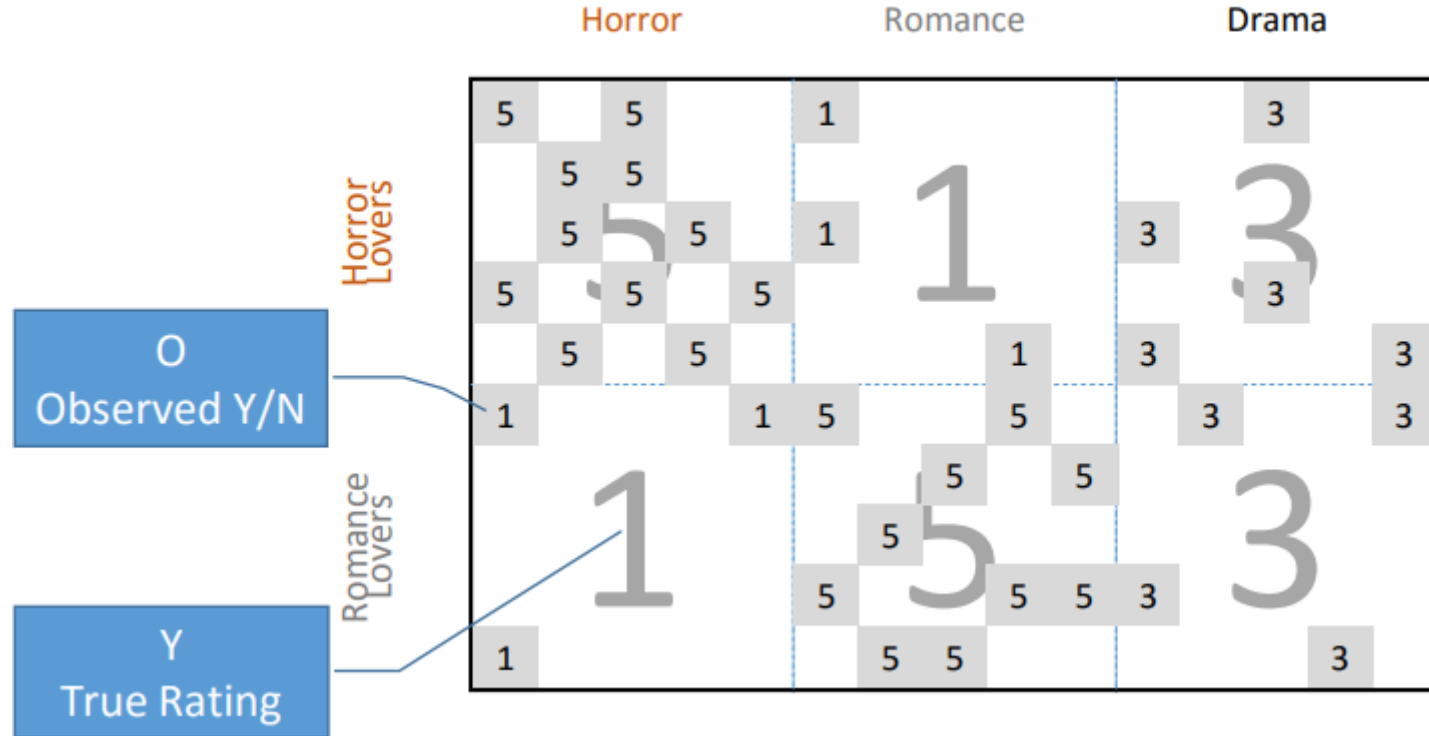


(a) Randomly-selected items

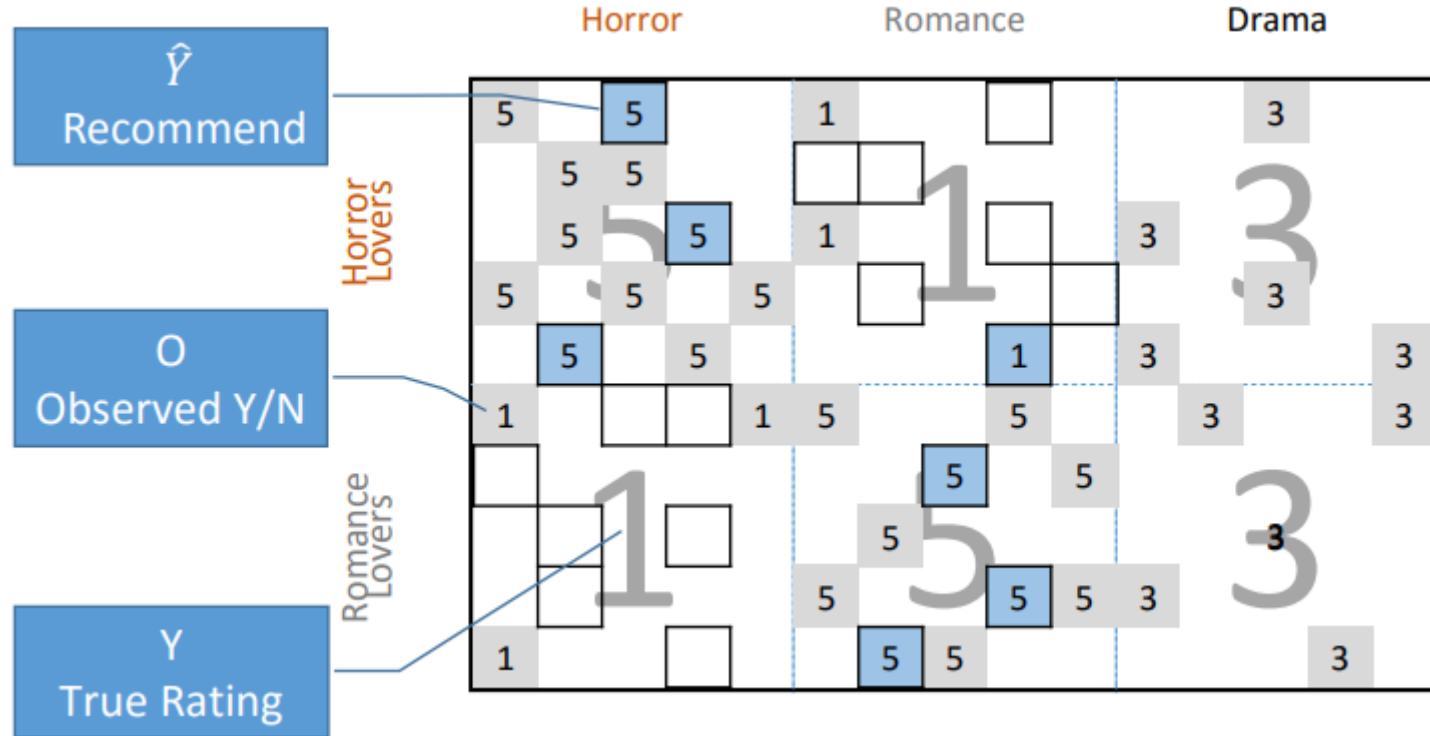


(b) User-selected items

Ví dụ về thiên lệch



Ví dụ về thiên lệch



Ví dụ về thiên lệch

\hat{Y}_1
Pred Ratings (worse)

	Horror	Romance	Drama
Horror Lovers	5 5	5 5 5 5 5 5 5 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	3 3
Romance Lovers	5 5 5 5 5 5 5 1 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5 5	5 5	3 3

\hat{Y}_2
Pred Ratings (better)

	Horror	Romance	Drama
Horror Lovers	5 5	1 1	5 5
Romance Lovers	1 1	5 5	5 5

Ví dụ về thiên lệch

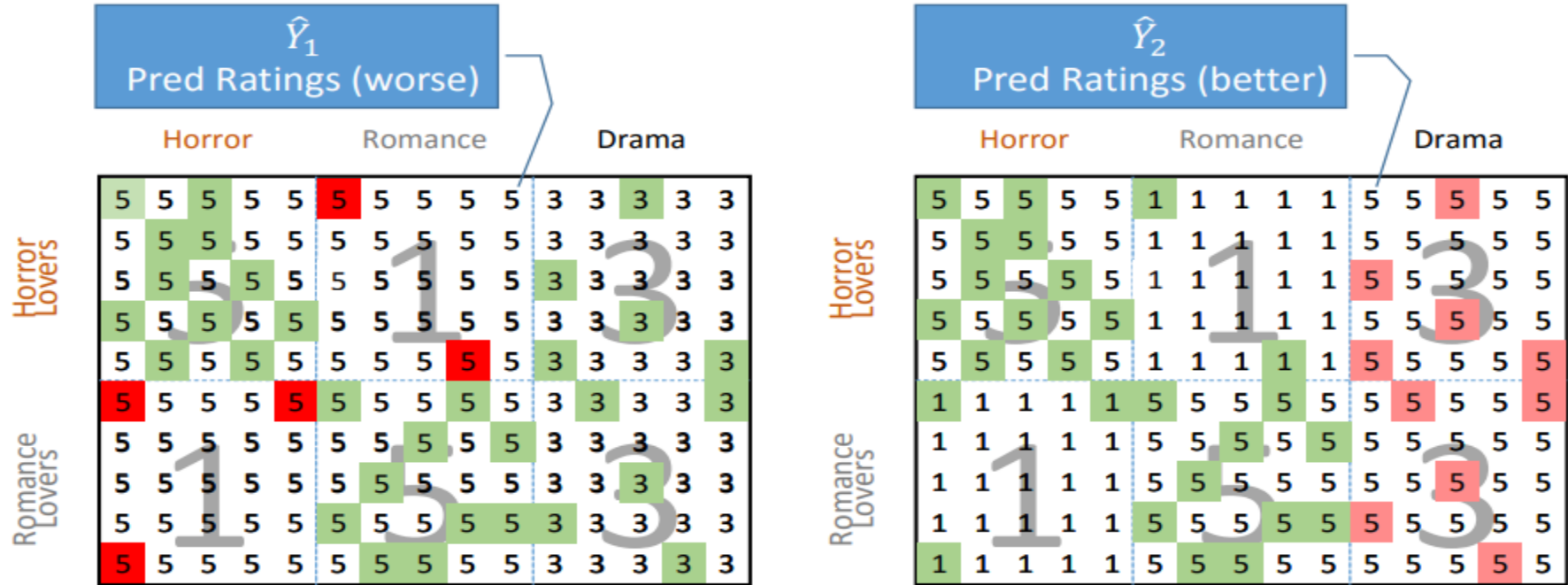
\hat{Y}_1
Pred Ratings (worse)

	Horror	Romance	Drama
Horror Lovers	5 5 5 5 5	5 5 5 5 5	3 3 3 3 3
Romance Lovers	5 5 5 5 5	5 5 5 5 5	3 3 3 3 3

\hat{Y}_2
Pred Ratings (better)

	Horror	Romance	Drama
Horror Lovers	5 5 5 5 5	1 1 1 1 1	5 5 5 5 5
Romance Lovers	1 1 1 1 1	5 5 5 5 5	5 5 5 5 5

Ví dụ về thiên lệch

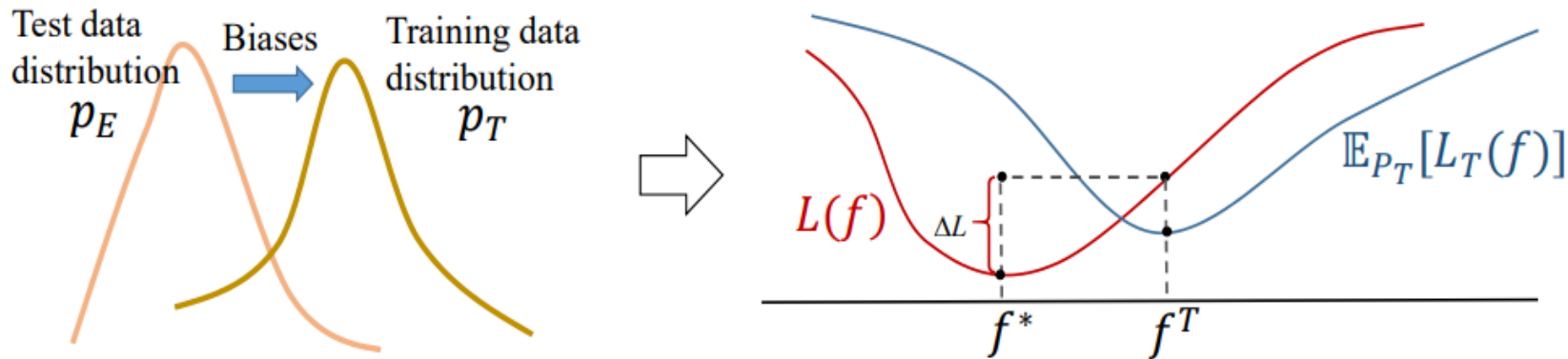


Ta có thể thấy thì \hat{Y}_1 là mô hình dự đoán tệ hơn tuy nhiên khi đánh giá mô hình do số lượng mẫu dữ liệu dự đoán sai lệch nghiêm trọng này (dự đoán 5, giá trị thực là 1) ít dẫn đến độ lỗi của nó nhỏ và không tác động nhiều đến mô hình

Tác hại của thiên lệch dữ liệu

Khi đánh giá mô hình thông thường ta cần chia tập dữ liệu thành 2 tập là: tập train và tập test, việc chia tập dữ liệu như vậy nhằm giúp cho mô hình huấn luyện được sẽ không bị thiên lệch.

Tuy nhiên đối với bài toán recommendation thì cách chia tập dữ liệu như vậy không giải quyết được vấn đề bias. Do tập train và tập test tương tự nhau, nên khi dữ liệu bị bias sẽ làm cho tập test cũng bị bias theo. Dẫn đến kết quả của mô hình không phản ánh chính xác hiệu năng của mô hình trong thực tế.



Phương pháp giải quyết tìm hiểu

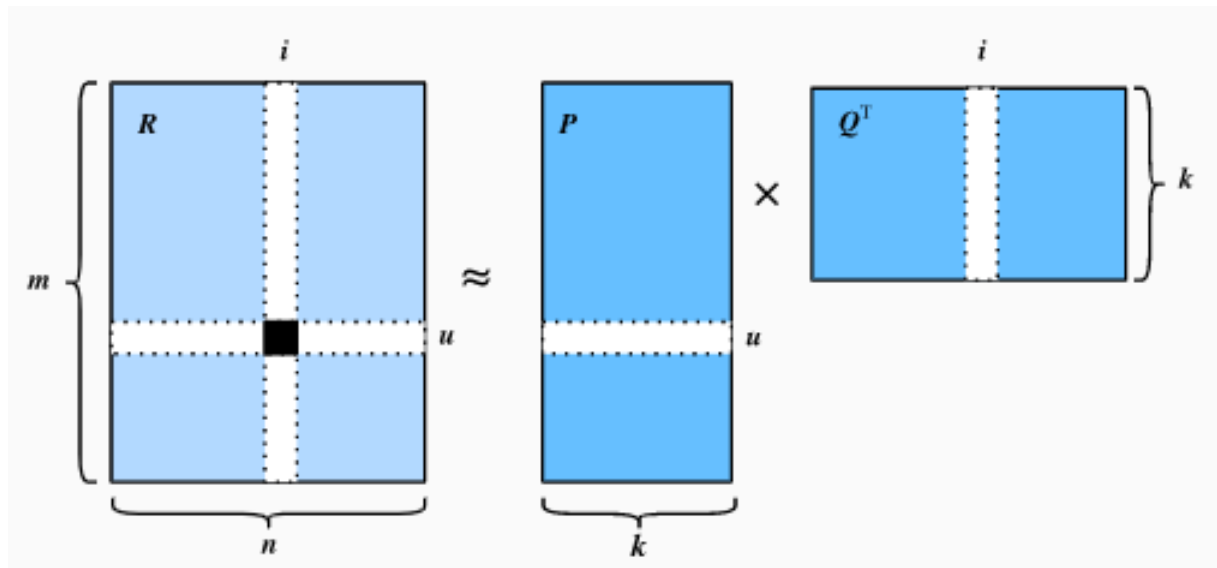
Để khắc phục vấn đề thiên lệch dữ liệu tác giả Tobias Schnabel và các cộng sự [?] trong bài báo “Recommendations as Treatments: Debiasing Learning and Evaluation” tại hội nghị “ICML 2016”, đã đề xuất việc áp dụng phương pháp **Chấm điểm theo nghịch đảo điểm xu hướng** (Inverse Propensity Scoring – IPS) vào quá trình huấn luyện và đánh giá mô hình. IPS hoạt động bằng cách đánh lại trọng số của các mẫu dựa trên điểm số xu hướng, theo cách giảm trọng số của các mẫu thường quan sát được, trong khi tăng trọng số của các mẫu hiếm gặp. Điều này sẽ giúp kiểm soát được vấn đề thiên lệch của dữ liệu

2. Kiến thức nền tảng

- Matrix Factorization
- Naive Bayes
- Logistic Regression

Matrix Factorization

Phân rã ma trận là một phương pháp thuộc nhóm lọc cộng tác. Mô hình này sẽ phân tích ma trận tương tác của user – item thành tích hai ma trận có hạng thấp hơn, nhằm nắm bắt cấu trúc bậc thấp trong tương tác giữa user – item.



Matrix Factorization

Mô hình sẽ được huấn luyện bằng cách cực tiểu hóa trung bình bình phương sai số giữa đánh giá dự đoán và đánh giá thực. Hàm mục tiêu được định nghĩa như sau:

$$\operatorname{argmin}_{\mathbf{P}, \mathbf{Q}, b} \sum_{(u,i) \in \mathcal{K}} \|\mathbf{R}_{ui} - \hat{\mathbf{R}}_{ui}\|^2 + \lambda(\|\mathbf{P}\|_F^2 + \|\mathbf{Q}\|_F^2 + b_u^2 + b_i^2)$$

Naive Bayes

Mô hình Naive Bayes là một mô hình phân lớp và là một mô hình học có giám sát dựa vào định lý Bayes.

Mô hình sẽ hoạt động bằng cách kết hợp các xác suất của mỗi đầu vào X là $P(X|y)$, $P(X)$ để tính toán xác suất của từng lớp với đầu vào đó $P(y|X)$, sau đó chọn lớp có xác suất cao nhất. Hay nói cách khác với đầu vào X và các lớp y_1, y_2, \dots thì quá trình phân lớp sẽ được định nghĩa như sau:

$$\text{Giá trị dự đoán} = \max_i (P(y_i|X))$$

Với $P(y_i|X)$ được tính toán dựa trên công thức Bayes

Naive Bayes

Định lý Bayes được sử dụng để tính toán xác suất thu được đầu ra y khi biết đầu vào là đặc trưng X , được kí hiệu là $P(y|X)$. Xác suất này được tính toán theo công thức sau:

$$P(y|X) = \frac{P(X|y) * P(y)}{P(X)}$$

Trong đó:

- $P(X|y)$ là xác suất của đặc trưng X khi biết đầu ra là y
- $P(y)$ là xác suất đầu ra y
- $P(X)$ là xác suất đặc trưng X

Logistic Regression

Logistic Regression là một mô hình phân lớp nhị phân và là một mô hình học có giám sát. Thuật toán tính toán mối quan hệ giữa các đặc trưng trong input và output dựa trên hàm sigmoid. Đầu ra dự đoán của Logistic Regression thường được viết dưới dạng:

$$f(x) = \sigma(w^T x)$$

Trong đó:

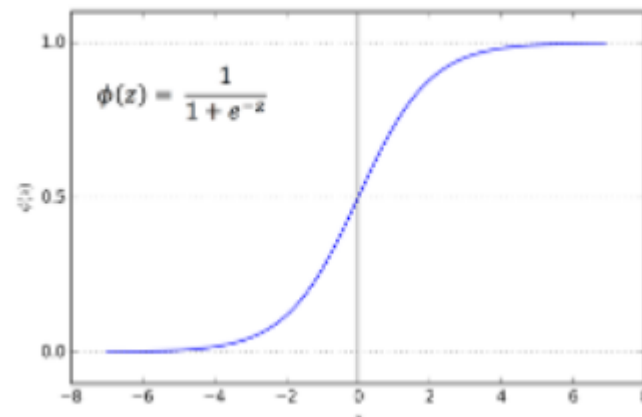
- w được gọi là trọng số của mô hình
- x là dữ liệu đầu vào
- $\sigma(.)$ là hàm sigmoid

Logistic Regression

Hàm sigmoid là hàm số toán học có công thức như sau:

$$\sigma(x) = \frac{1}{1 + e^{-x}}$$

Đây là một hàm số liên tục và nhận giá trị trong khoảng (0,1), đầu vào càng tiến đến ∞ thì giá trị khi đi qua hàm sigmoid càng tiến đến 1 và ngược lại khi đầu vào càng tiến đến $-\infty$ thì giá trị khi đi qua hàm sigmoid càng tiến gần về 0



Logistic Regression

Với toàn bộ tập huấn luyện X là tập hợp các đặc trưng, y là tập hợp các nhãn, mô hình Logistic Regression sẽ tìm bộ trọng số w để phương trình sau đạt cực đại:

$$w = \underset{w}{\operatorname{argmax}}(P(y|X; w))$$

3. Phương pháp tìm hiểu

- Inverse propensity scoring (IPS)
- Ước lượng ma trận xu hướng
- Matrix Factorization từ xu hướng

Xu hướng

- Theo giả định rằng người dùng có thể không đánh giá một bộ phim mà họ đã xem, do đó một đánh giá của người dùng u dành cho sản phẩm i có thể không xuất hiện trong tập dữ liệu
- Ta đặt $P_{u,i}$ là xác suất mà đánh giá $Y_{u,i}$ có thể quan sát được (hay $O_{u,i} = 1$)
- $P_{u,i} = P(O_{u,i} = 1)$
- $P_{u,i}$ được gọi là xu hướng của đánh giá $Y_{u,i}$

Ma trận quan sát O

	Horror				Romance				Drama				
1	0	1	0	1	0	0	0	0	0	0	1	0	0
0	1	1	0	0	0	0	0	0	0	0	0	0	0
0	1	0	1	0	1	0	0	0	0	1	0	0	0
1	0	0	0	0	0	0	0	0	0	0	1	0	0
0	1	0	1	0	0	0	0	1	0	1	0	0	1
1	0	0	0	1	1	0	0	1	0	1	0	0	1
0	0	0	0	0	0	0	1	0	0	1	0	0	0
0	0	0	0	0	0	1	0	0	0	0	1	0	0
0	0	0	0	0	1	0	0	0	1	1	0	0	0
1	0	0	0	0	0	1	1	0	0	0	0	0	1

Ma trận xu hướng P


	Horror	Romance	Drama
p	p/10	p/2	
p/10		p	p/2

Inverse propensity scoring (IPS)

Để tính độ chính xác của ma trận đánh giá dự đoán \hat{Y} đối với ma trận đánh giá Y :

$$\hat{R}_{naive}(\hat{Y}) = \frac{1}{|\{(u, i) : O_{u,i} = 1\}|} \sum_{(u,i): O_{u,i}=1} \delta_{u,i}(Y, \hat{Y})$$

Người ta muốn tăng trọng số của những đánh giá ít có xu hướng $P_{u,i}$ thấp để loại bỏ thiên lệch, do đó ta nhân độ lỗi của mỗi đánh giá mà ta quan sát được với nghịch đảo xu hướng của nó:

$$\hat{R}_{IPS}(\hat{Y}|P) = \frac{1}{U \cdot I} \sum_{(u,i): O_{u,i}=1} \frac{\delta_{u,i}(Y, \hat{Y})}{P_{u,i}}$$


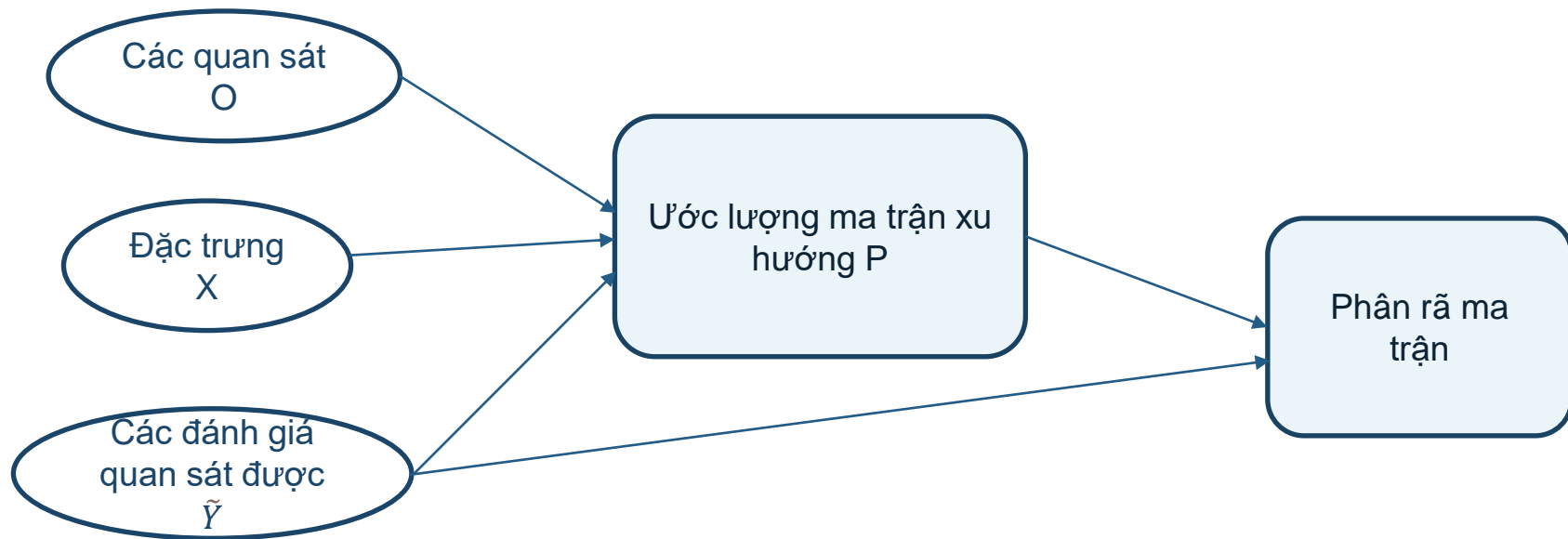
Self-Normalized IPS

- Một hàm lỗi có phương sai lớn như vậy sẽ khiến mô hình không ổn định, do đó tác giả đã sử dụng một nghiên cứu của Hesterberg gọi là tự chuẩn hóa (self-normalized) để giảm phương sai của hàm lỗi.
- Phương pháp này chia hàm lỗi IPS cho một biến ngẫu nhiên có tương quan với hàm lỗi này, rồi nhân với giá trị trung bình đã biết của biến ngẫu nhiên đó

Ta có
$$\mathbb{E}_O \left[\sum_{(u,i): O_{u,i}=1} \frac{1}{P_{u,i}} \right] = U \cdot I$$

→
$$\hat{R}_{SNIPS}(\hat{Y}|P) = \frac{\sum_{(u,i): O_{u,i}=1} \frac{\delta_{u,i}(Y, \hat{Y})}{P_{u,i}}}{\sum_{(u,i): O_{u,i}=1} \frac{1}{P_{u,i}}}$$

Quá trình huấn luyện



Ước lượng xu hướng

Dựa vào những đặc trưng quan sát được như đặc trưng của người dùng, đặc trưng của sản phẩm, ma trận đánh giá,... ta có thể ước lượng được xu hướng của từng sản phẩm bằng các mô hình đơn giản như Naive bayes, hồi quy Logistic

Phân rã ma trận

Ta xem việc phân rã ma trận như tìm ma trận V, W sao cho

$$\hat{Y}^{ERM} = V^T W + A$$

Do đó mục tiêu của quá trình huấn luyện dựa trên tập dữ liệu quan sát được là:

$$\operatorname{argmin}_{V, W, A} \left[\sum_{O_{u,i}=1} \frac{\delta_{u,i}(Y, V^T W + A)}{P_{u,i}} + \lambda (\|V\|_F^2 + \|W\|_F^2) \right]$$

4. Các kết quả thí nghiệm

- Đánh giá các phương pháp ước lượng điểm xu hướng
- Đánh giá các phương pháp phân rã ma trận
- Đánh giá hiệu suất trên dữ liệu thế giới thực

Thí nghiệm 1

- Dữ liệu: tập dữ liệu ML100k chứa đánh giá cho 1683 bộ phim bởi 944 người dùng
- Nội dung thí nghiệm: So sánh trung bình và độ lệch chuẩn của các độ đo Naive, IPS, SNIPS với các hàm tính độ lỗi là MAE và DCG@50 thông qua 5 cách dự đoán đánh giá từ dữ liệu được tổng hợp từ ML100K

Thí nghiệm 1

- REC_ONES: ma trận dự đoán \hat{Y} giống với ma trận Y , ngoại trừ n đánh giá 1 sao sẽ được chuyển thành 5 sao với n là tổng số đánh giá 5 sao
- REC_FOURS: giống phương pháp trên, sử dụng với các đánh giá bằng 4
- ROTATE: khi $Y_{u,i} \geq 2$, thì $\hat{Y}_{u,i} = Y_{u,i} - 1$, khi $Y_{u,i} = 1$ thì $\hat{Y} = 5$
- SKEWED: dự đoán $\hat{Y}_{u,i}$ tuân theo phân phối chuẩn với $\mu = Y_{u,i}$ và $\sigma = \frac{6 - Y_{u,i}}{2}$
- COARSENEDED: dự đoán $\hat{Y}_{u,i} = 3$ nếu $Y_{u,i} \leq 3$, $\hat{Y}_{u,i} = 3$ với các trường hợp còn lại

Kết quả thí nghiệm 1

	MAE			
	True	IPS	SNIPS	Naive
REC_ONES	0.102	0.102 ± 0.007	0.102 ± 0.007	0.011 ± 0.001
REC_FOURS	0.026	0.026 ± 0.000	0.026 ± 0.000	0.173 ± 0.001
ROTATE	2.579	2.581 ± 0.031	2.579 ± 0.012	1.168 ± 0.003
SKEWED	1.306	1.304 ± 0.012	1.304 ± 0.009	0.912 ± 0.002
COARSENEDED	1.320	1.314 ± 0.015	1.318 ± 0.005	0.387 ± 0.002

	DCG@50			
	True	IPS	SNIPS	Naive
REC_ONES	30.76	30.64 ± 0.75	30.66 ± 0.74	153.07 ± 2.13
REC_FOURS	52.00	51.98 ± 0.41	52.08 ± 0.58	313.48 ± 2.36
ROTATE	12.90	13.00 ± 0.85	12.99 ± 0.83	1.38 ± 0.09
SKEWED	24.59	24.55 ± 0.92	24.58 ± 0.93	54.87 ± 1.03
COARSENEDED	46.45	46.45 ± 0.53	46.44 ± 0.70	293.27 ± 1.99

Thí nghiệm 2

Dữ liệu

Tập dữ liệu Yahoo: đánh giá của các bài hát

- Tập dữ liệu huấn luyện chứa hơn 300k đánh giá của 15400 người dùng
- Tập dữ liệu đánh giá chứa đánh giá của 5400 người dùng cho 10 bài hát được chọn ngẫu nhiên

Tập dữ liệu Coat: đánh giá cho 300 chiếc áo khoác của 290 người dùng

- Tác giả tạo ra một giao diện web mua sắm đơn giản, sau đó chọn chiếc áo khoác họ muốn mua nhất rồi đánh giá 24 chiếc áo khoác do họ tự lựa chọn và 16 chiếc được chọn ngẫu nhiên trên thang điểm 5

Kết quả thí nghiệm 2

	YAHOO		COAT	
	MAE	MSE	MAE	MSE
<i>MF-IPS</i>	0.810	0.989	0.860	1.093
<i>MF-Naive</i>	1.154	1.891	0.920	1.202

5. Tổng kết và hướng phát triển

Tài liệu tham khảo

[1] Re