



Πολυτεχνική σχολή Τμήμα Μηχανικών Η/Υ & Πληροφορικής

Διπλωματική εργασία

Έρευνα και ανάπτυξη συστήματος για την ανίχνευση μεροληψίας σε συστήματα μηχανικής μάθησης

Ρωμανός Καψάλης,

A.M.: 1056289

Επιβλέπων Συνεπιβλέπων

Χρήστος Μακρής, Ιωάννης Κανελλόπουλος,

Αναπληρωτής καθηγητής Ιδρυτής και CEO της εταιρείας Code4Thought

Μέλη εξεταστικής επιτροπής

Σπυρίδων Σιούτας, καθηγητής Δημήτριος Τσώλης, επίκουρος καθηγητής

Πάτρα, Φεβρουάριος 2022





02

Ανάπτυξη

εφαρμογής

05 Συμπεράσματα

1. Θεωρητικό υπόβαθρο

Ορισμός προβλήματος (γενικότερα)

Η ραγδαία ανάπτυξη της τεχνητής νοημοσύνης έχει φέρει στο προσκήνιο την ανάγκη για έλεγχο των συστημάτων που έχουν προκύψει από χρήση των αλγορίθμων της. Οι αλγόριθμοι αυτοί:

- Λαμβάνουν σημαντικές αποφάσεις που αφορούν διάφορες πτυχές της καθημερινότητας των ανθρώπων
- Υπάρχει ανάγκη να λαμβάνουν δίκαιες αποφάσεις

Μια σειρά από ηθικά ζητήματα εξετάζονται εκτενώς τα τελευταία χρόνια από την επιστημονική κοινότητα.

Κύριος στόχος — αναγνώριση και μετριασμός της μεροληψίας (bias) που εισάγεται από κάθε πιθανή πηγή, ώστε να λαμβάνονται δίκαιες αποφάσεις για όλα τα άτομα ή τις ομάδες ατόμων

Δικαιοσύνη (fairness): απουσία οποιασδήποτε προκατάληψης ή ευνοιοκρατίας προς ένα άτομο ή μια ομάδα που βασίζεται στα εγγενή ή επίκτητα χαρακτηριστικά¹

Ορισμός προβλήματος (ειδικότερα)

Στην ανάλυση των ηθικών ζητημάτων στην τεχνητή νοημοσύνη και ειδικότερα στην μηχανική μάθηση, η έρευνα που έχει γίνει στα συστήματα συστάσεων (recommender ή recommendation systems) δεν είναι ανάλογη της χρήσης τους στο χώρο του διαδικτύου. Επίσης, δεν έχουν διερευνηθεί επαρκώς τα πολύ σοβαρά ερωτήματα για ζητήματα ηθικής, που εγείρονται από την χρήση τους.

Τα κυριότερα είδη μεροληψίας που συναντάμε εδώ είναι:

- Μεροληψία δημοφιλίας (popularity bias)
- Μεροληψία θέσης (position bias)
- Μεροληψία κομφορμισμού (conformity bias)
- Μεροληψία συναισθήματος (sentiment bias)

Έναυσμα για την ενασχόληση με τη συγκεκριμένη διπλωματική: "How Facebook got addicted to spreading misinformation", της Karen Hao

Περιγράφει πως οι αλγόριθμοι συστημάτων συστάσεων προκειμένου να αυξήσουν την αφοσίωση (engagement) του χρήστη έχουν καταλήξει να επηρεάζουν ολόκληρες κοινωνίες οδηγώντας τα άτομα σε ακραίες απόψεις, επηρεάζοντας εκλογικές αναμετρήσεις και συμβάλλοντας μέχρι και στην έναρξη εμφυλίων πολέμων.



Συστήματα συστάσεων

Ως σύστημα συστάσεων (recommendation ή recommender system ή RecSys εν συντομία) ορίζεται το σύστημα όπου οι άνθρωποι παρέχουν προτάσεις ως εισόδους οι οποίες έπειτα συγκεντρώνονται και κατευθύνονται σε συγκεκριμένους παραλήπτες.

Τα συστήματα συστάσεων χρησιμοποιούνται πλέον στα περισσότερα συστήματα που υπάρχουν στο διαδίκτυο:

- Μέσα κοινωνικής δικτύωσης
- Ηλεκτρονικό εμπόριο
- Συστήματα παροχής υπηρεσιών ψυχαγωγίας
- Μηχανές αναζήτησης
- Χρηματοοικονομικές υπηρεσίες

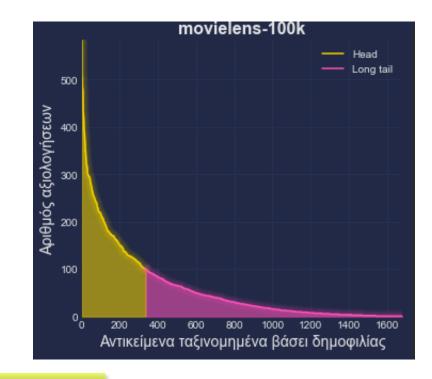
Popularity bias

Η τάση των συστημάτων συστάσεων να προτείνουν τα πιο δημοφιλή αντικείμενα πολύ πιο συχνά από τα λιγότερο δημοφιλή αντικείμενα, τα λεγόμενα long tail αντικείμενα, που στην μεγάλη πλειονότητα των περιπτώσεων είναι πολύ περισσότερα.

- > Head: 20% πιο δημοφιλών προϊόντων
- > Long-tail: το υπόλοιπο 80% των προϊόντων

Βασίζεται στην αρχή του Pareto: το 80% των επιπτώσεων προέρχεται από το 20% των αιτιών

Το φαινόμενο του popularity bias συνδέεται με:



Ζητήματα στο ηλεκτρονικό εμπόριο

Σημαντική μείωση των πωλήσεων και δυσαρέσκεια των πελατών/χρηστών.

Παραπληροφόρηση

Popularity bias



Μείωση ποιότητας και ποικιλίας του περιεχόμενου



Παραπληροφόρηση

Echo chambers

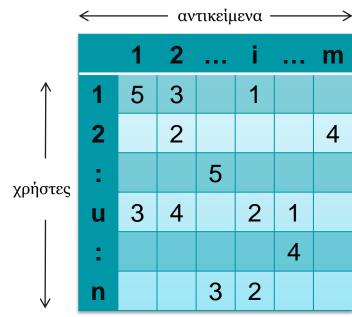
Ένα άτομο ή μια ομάδα ατόμων δημιουργούν ένα περιβάλλον μέσα στο οποίο συναντούν μόνο πληροφορίες ή απόψεις που αντανακλούν ή ενισχύουν τις δικές τους, χωρίς να συναντούν αντίθετες απόψεις.

Χαρακτηριστικά δεδομένων και αραιότητα

• Ένα από τα πιο γνωστά προβλήματα στα συστήματα συστάσεων είναι η πολύ μεγάλη αραιότητα (sparsity) του μητρώου χρηστών-αντικειμένων, η οποία μπορεί να οδηγήσει σε πολύ κακή απόδοση των συστημάτων συστάσεων.

$$Sparsity = 1 - \frac{\#ratings}{\#users \times \#items}$$

- Επίσης, έχει αποδειχθεί ότι η ακρίβεια των δεδομένων επηρεάζεται από χαρακτηριστικά των δεδομένων όπως:
 - Rating space $(RS) = |Users| \times |Items|$
 - User Item Ratio (UIR) = $\frac{|Users|}{|Items|}$
 - Rating Per User $(RP_u) = \frac{|Ratings|}{|Users|}$
 - Rating Per Item $(RP_i) = \frac{|Ratings|}{|Items|}$
- Στην παρούσα εργασία εξετάστηκε η επίδραση τόσο της αραιότητας των δεδομένων, όσο και των χαρακτηριστικών στην εισαγωγή της μεροληψίας



2. Ανάπτυξη εφαρμογής

Βασική ιδέα

Στα συστήματα συστάσεων λίγες είναι οι προσπάθειες για τη δημιουργία μιας εφαρμογής που θα επιτρέπει σε όλους τους χρήστες να υλοποιούν συστήματα συστάσεων και στη συνέχεια να τα ελέγχουν.

Βασικός στόχος της διπλωματικής εργασίας → δημιουργία ενός εργαλείου ανάλυσης και μετριασμού μεροληψίας στα συστήματα συστάσεων.

Αυτό επετεύχθη μέσα από την υλοποίηση μιας διαδικτυακής εφαρμογής (web-app) με τίτλο "Bias and Fairness in RecSys".

Κύρια χαρακτηριστικά και πλεονεκτήματα της εφαρμογής

- ο χρήστης έχει άμεση πρόσβαση σε όλα τα πιθανά σημεία εισαγωγής της μεροληψίας: δεδομένα και αλγόριθμος
- η εφαρμογή υλοποιήθηκε με τέτοιο τρόπο, ώστε να μπορεί να χρησιμοποιηθεί από όλους τους χρήστες ακόμη και εάν οι γνώσεις τους γύρω από το ζήτημα είναι περιορισμένες.
- οι χρήστες δεν είναι απαραίτητο να ακολουθήσουν τα βήματα με την σειρά που αναφέρονται στο πείραμά μας.

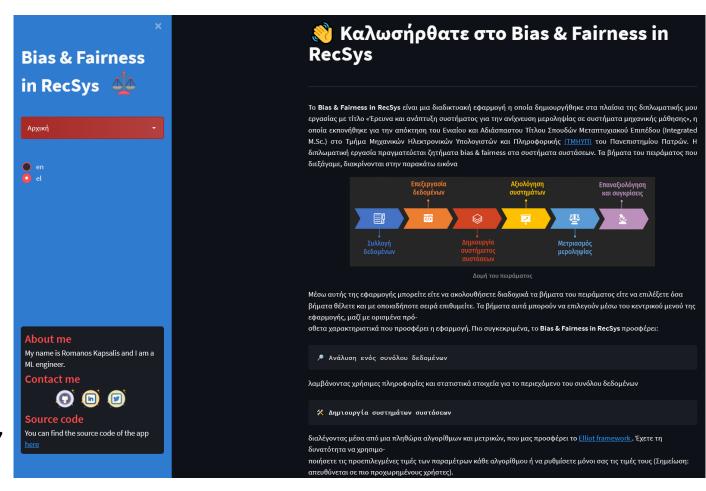
Το σύστημα αυτό ευελπιστούμε να αποτελέσει ένα χρήσιμο εργαλείο για τους ερευνητές, οι οποίοι μπορούν να υλοποιήσουν μια πληθώρα πειραμάτων με θέμα την μεροληψία στα συστήματα συστάσεων (και όχι μόνο).

Αρχιτεκτονική εφαρμογής

Η διαδικτυακή εφαρμογή αναπτύχθηκε σε γλώσσα Python μέσω του framework **Streamlit**. Για τη δημιουργία των συστημάτων συστάσεων χρησιμοποιήθηκε το **Elliot** framework και για τον μετριασμό της μεροληψίας το **Librec-auto**.

Η εφαρμογή περιέχει τις σελίδες:

- Αρχική σελίδα
- Οπτικοποίηση συνόλων δεδομένων
- Δημιουργία συστημάτων συστάσεων
- Αξιολόγηση αποτελεσμάτων
 - > Αξιολόγηση ενός συνόλου δεδομένων
 - ✓ Ανάλυση υπερπαραμέτρων
 - ✓ Ανάλυση cutoff
 - ✓ Προβολή καλύτερων αποτελεσμάτων
 - > Σύγκριση συνόλων δεδομένων
- Μετριασμός μεροληψίας
- Επεξήγηση μετρικών
- Μεταφόρτωση συνόλου δεδομένων

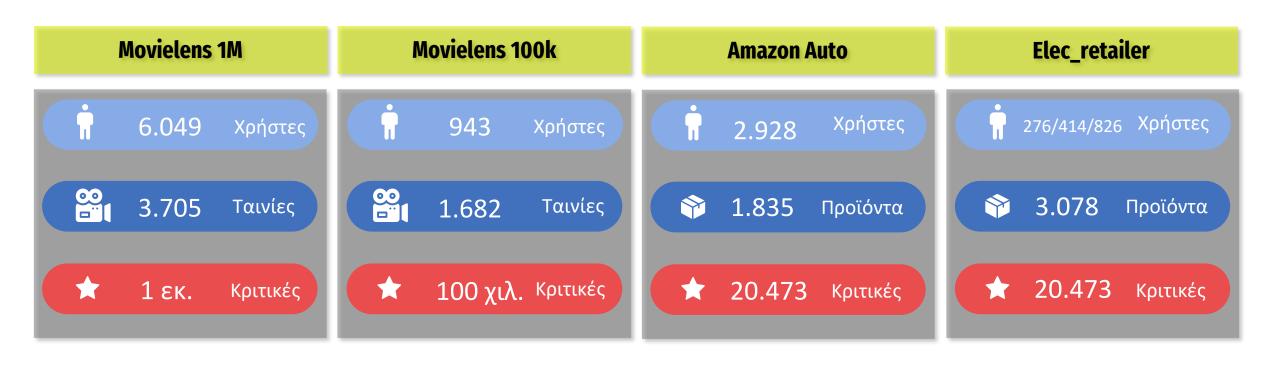


3. Μεθοδολογία

Δεδομένα

Για την υλοποίηση των πειραμάτων χρησιμοποιήθηκαν συνολικά 4 σύνολα δεδομένων:

- 1 πραγματικό σύνολο δεδομένων (Elec_retailer)
 - μας παραχωρήθηκε από μεγάλη εταιρία λιανικών πωλήσεων ηλεκτρικών και ηλεκτρονικών ειδών
- 3 σύνολα δεδομένων από το διαδίκτυο



Αλγόριθμοι συστημάτων συστάσεων

Αλγόριθμοι Περιγραφή Οικογένεια itemKNN βρίσκουν παρόμοια αντικείμενα ή παρόμοιους ΚΟΝΤΙΝΟΤΕΡΟΙ ΓΕΙΤΟΝΕΣ χρήστες (τους κοντινότερους γείτονες) μέσω κάποιων userKNN απλών μετρικών ομοιότητας. **Matrix factorization** αναλύουν τα δεδομένα προκειμένου να βρουν κάποια ΛΑΝΘΑΝΟΝΤΩΝ χαρακτηριστικά και συσχετίσεις σε αυτά, που δεν είναι **BPRMF** άμεσα ορατά, και θα δίνουν στους αλγορίθμους τις ΠΑΡΑΓΟΝΤΩΝ προτιμήσεις των χρηστών. SVD++ **WRMF** οι αλληλεπιδράσεις των χρηστών με τα αντικείμενα ΒΑΘΙΑΣ ΜΑΘΗΣΗΣ **SLIM** αναπαρίστανται με νευρωνικά δίκτυα **DeepFM** όπου οι αλληλεπιδράσεις των χρηστών με τα ΒΑΣΙΣΜΕΝΑ ΣΕ ΓΡΑΦΗΜΑΤΑ αντικείμενα αναπαρίστανται με γραφήματα **NGCF** + 2 μη-εξατομικευμένοι αλγόριθμοι ως baseline (αλγόριθμοι που δίνουν τις ίδιες λίστες συστάσεων σε όλους τους χρήστες χωρίς να λαμβάνουν υπόψη τους τα δεδομένα που έχουν δοθεί ως είσοδος)

MostPop: δίνει σε όλους τους χρήστες τα top-k πιο δημοφιλή αντικείμενα

• **Random:** προτείνει τυχαία αντικείμενα ακολουθώντας την κανονική κατανομή.

4. Αποτελέσματα

Πραγματικό σύνολο δεδομένων (popularity bias) Average Recommendation Popularity δημοφιλία των αντικειμένων που προτείνοντο

ARP

Algorithm	Users=276	Users=414	Users=826		
ItemKNN	1,32	1,36	1,41		
UserKNN	25,98	23,02	15,42		
WRMF	12,18	20,8	31,07		
BPRMF	33,55	34,63	39,34		
SVD++	25,25	19,92	20,46		
MF	13,49	11,01	7,60		
DeepFM	14,95	14,46	9,76		
NGCF	2,7	2,71	2,61		
Random	2,39	2,45	2,36		
MostPop	34,08	36,44	39,70		

Average Recommendation Popularity (ARP): υπολογίζει τη μέση δημοφιλία των αντικειμένων που προτείνονται σε κάθε λίστα, δηλαδή τον μέσο αριθμό των αξιολογήσεων των αντικειμένων σε κάθε λίστα συστάσεων.

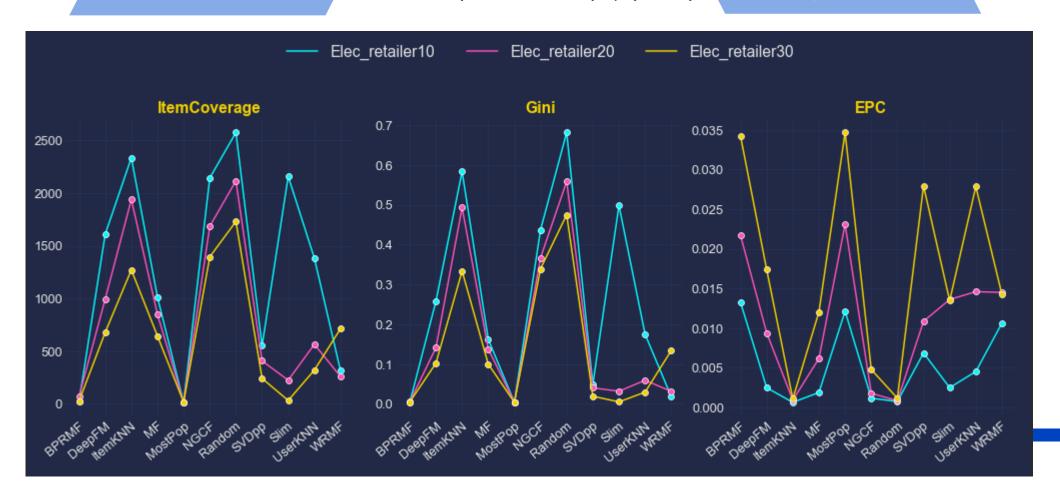
- Παρόλο που σχεδόν το 90% των προϊόντων έχει λάβει 1-2 αξιολογήσεις, ο μέσος αριθμός των αξιολογήσεων των προϊόντων στις λίστες συστάσεων που έχουν παράξει οι αλγόριθμοι για κάθε χρήστη, είναι αρκετά μεγαλύτερος από όσο θα περιμέναμε και θα θέλαμε.
- Για όλους τους αλγόριθμους εκτός από τον ItemKNN και τον NGCF έχουμε μέτρια ή κακή επίδοση.
- Ο μέσος αριθμός αξιολογήσεων αναφέρεται στις αξιολογήσεις στο σύνολο εκπαίδευσης (training set) και αποτελεί σοβαρή ένδειξη για την ύπαρξη του popularity bias.

Πραγματικό σύνολο δεδομένων

Ορισμένα αντικείμενα δεν θα προταθούν ποτέ

- Μείωση των πωλήσεων
- Δυσαρέσκεια του πελάτη
- Δυσαρέσκεια του προμηθευτή

Έλλειψη ποικιλίας στα αντικείμενα που προτείνονται



Ανάλυση υπερπαραμέτρων

Υπερπαράμετροι

Batch size Learning **Factors** rate dataset lr EPC bs nDCG IC Gini ARP APLT PREO PRSP 0.7829 0.3100 2245 0.1287 0.2015 829.8737 0.0665 0.9396 256 20 256 0.3151 2290 0.1283 0.1940 828.3989 0.0634 0.7826 50 0.9425 818.4174 256 0.2036 0.0727 70 0.3147 2433 0.1278 0.7557 0.9338 0.001 0.3186 2162 0.1832 856.2911 0.0519 0.8290 512 20 0.1295 0.9533 0.3285 0.1986 832.1122 512 50 2316 0.1336 0.0644 0.7787 0.9416 0.3265 2232 0.1305 0.1809 855.8623 0.0557 0.8093 0.9498 512ml1m 0.1608 256 2636 0.2477 0.8679 20 0.1393 0.0705 686.4904 0.6872256 0.0904 3535 0.0438 0.3994 510.4456 0.2902 0.6969 0.5724 3668 256 70 0.0602 0.0306 0.5123 406.4007 0.4100 0.4621 0.5342 0.01 0.2322 512 2539 0.1167 0.6928 0.8909 0.2122 0.0894 731.0409 512 3151 0.8101 0.3676 5120.1239 0.0562 0.7498

Παράδειγμα από τον αλγόριθμο MF στο σύνολο δεδομένων Movielens1M

Η ανάλυση έγινε για:

- 9 αλγορίθμους
- Με χρήση
- 12 μετρικών αξιολόγησης
- Διαφορετικών συνδυασμών υπερπαραμέτρων

Υψηλή ακρίβεια => μεγάλη εισαγωγή μεροληψίας

Χαμηλή ακρίβεια => πιο δίκαια αποτελέσματα

Ζητούμενο: η ισορροπία

Σύγκριση συνόλων δεδομένων



 Σε ορισμένους αλγορίθμους το πρόβλημα εισαγωγής μεροληψίας είναι αρκετά πιο έντονο

Μετριασμός μεροληψίας

- ✓ Ίδιο μοτίβο στους περισσότερους αλγορίθμους που εξετάστηκαν
- ✓ Εμφανής η βελτίωση της μεροληψίας, με σχετικά μικρή μείωση της ακρίβειας
- ✓ Όταν όμως το πρόβλημα είναι μεγάλο, δεν φαίνεται να βοηθάει η τεχνική του post-processing

Παρόμοια συμπεράσματα και στους αλγορίθμους:

- DeepFM
- WRMF

	Movielens100k			Movielens1M			Amazon					
	base	FAR	PFAR	cali	base	FAR	PFAR	cali	base	FAR	PFAR	cali
nDCG	0.305	0.298	0.300	0.268	0.241	0.231	0.236	0.222	0.043	0.037	0.038	0.032
Prec.	0.2090	0.2046	0.2060	0.1947	0.2076	0.2000	0.2029	0.1968	0.0054	0.0051	0.0051	0.0051
Recall	0.3610	0.3545	0.3567	0.3447	0.2425	0.2341	0.2375	0.2343	0.0906	0.0856	0.0858	0.0854
IC	495	510	504	597	1818	1833	1825	1926	1656	1707	1703	1713
EPC	0.1797	0.1757	0.1769	0.1633	0.1872	0.1807	0.1837	0.1748	0.0073	0.0063	0.0065	0.0054
Gini	0.118	0.121	0.121	0.143	0.154	0.175	0.169	0.185	0.346	0.398	0.392	0.404
HR	0.973	0.977	0.978	0.966	0.953	0.951	0.951	0.950	0.147	0.141	0.141	0.141
ACLT	0.524	0.584	0.573	1.047	1.16	1.45	1.34	1.74	4.12	5.06	4.95	5.28
ARP	194.47	191.15	192.06	177.87	940.00	883.24	901.49	862.31	19.42	17.63	17.85	17.41
APLT	0.017	0.019	0.019	0.035	0.039	0.048	0.045	0.058	0.137	0.169	0.165	0.176
PopREO	0.951	0.949	0.951	0.888	0.866	0.846	0.855	0.795	0.809	0.793	0.813	0.791
PopRSP	0.985	0.983	0.984	0.970	0.965	0.957	0.960	0.948	0.645	0.570	0.578	0.552

Συμπεράσματα

τεχνικών.

Σε αυτή τη διπλωματική εργασία αναπτύχθηκε μια εφαρμογή με στόχο την ευκολότερη ανάδειξη των προβλημάτων μεροληψίας και δυνατότητα ελέγχου της. Παράλληλα, με χρήση της εφαρμογής υλοποιήθηκαν ορισμένα πειράματα, τα κύρια συμπεράσματα των οποίων είναι:

- Χρειάζεται προσεκτική ρύθμιση των υπερπαραμέτρων, διότι όπως παρατηρήθηκε επηρεάζει πολύ το ποσοστό εισαγωγής της μεροληψίας. Δυστυχώς πολλοί χρήστες ρυθμίζουν τις υπερπαραμέτρους με μόνο γνώμονα την ακρίβεια.
- Η αραιότητα του μητρώου χρηστών αντικειμένων επηρεάζει όχι μόνο την ακρίβεια αλλά και το popularity bias. Παρόμοια συμπεράσματα προκύπτουν και για τα υπόλοιπα χαρακτηριστικά των δεδομένων.
- Στον τομέα του ηλεκτρονικού εμπορίου προέκυψε, ύστερα και από την εξέταση ενός πραγματικού συνόλου δεδομένων, πως το φαινόμενο της μεροληψίας δημοφιλίας είναι αρκετά έντονο, ενώ αρκετά αντικείμενα μπορεί να μην υπάρχουν σε καμία λίστα συστάσεων που δίνονται από τους αλγορίθμους στους χρήστες.
 - Συνέπειες: μείωση των πωλήσεων, μείωση της ποικιλίας, δυσαρέσκεια των πελατών
- Στις πιο κλασικές προσεγγίσεις φάνηκε να μην είναι τόσο έντονο το φαινόμενο. Ορισμένοι αλγόριθμοι της οικογένειας λανθανόντων παραγόντων εισάγουν πολύ μεγάλη μεροληψία. Προσεγγίσεις που βασίζονται στα νευρωνικά δίκτυα έχουν αρκετά μέτρια επίδοση.
- Μετριασμός της μεροληψίας: η κατηγορία post-processing αποδείχθηκε μέσω των πειραμάτων ότι δεν ενδείκνυται για σύνολα δεδομένων με πολύ μεγάλη αραιότητα, ενώ δεν είναι αρκετά αποτελεσματική σε περίπτωση όπου έχουμε πολύ μεγάλη εισαγωγή μεροληψίας. Η in-processing ενδείκνυται για περιπτώσεις όπου έχουμε πολύ μεγάλη εισαγωγή μεροληψίας και ευθύνεται το μοντέλο για αυτό. Όμως συνήθως απαιτείται συνδυασμός

Αναφορές (1/2)

- 1. W. Liu and R. Burke, "Personalizing Fairness-aware Re-ranking," arXiv:1809.02921 [cs], Sep.2018.
- 2. H. Steck, "Calibrated recommendations," in *Proceedings of the 12th ACM Conference on Recommender Systems*. Vancouver British Columbia Canada: ACM, Sep. 2018, pp. 154–162.
- 3. M. Zehlike, F. Bonchi, C. Castillo, S. Hajian, M. Megahed, and R. Baeza-Yates, "FA*IR: A Fair Top-k Ranking Algorithm," *Proceedings of the 2017 ACM on Conference on Information and Knowledge Management*, pp. 1569–1578, Nov. 2017.
- 4. V. W. Anelli, A. Bellogin, A. Ferrara, D. Malitesta, F. A. Merra, C. Pomo, F. M. Donini, and T. Di Noia, "Elliot: A Comprehensive and Rigorous Framework for Reproducible Recommender Systems Evaluation," in *Proceedings of the 44th International ACM SIGIR Conference on Research and Development in Information Retrieval*. Virtual Event Canada: ACM, Jul. 2021, pp. 2405–2414.
- 5. H. Guo, R. Tang, Y. Ye, Z. Li, and X. He, "DeepFM: A factorization-machine based neural network for CTR prediction," in *Proceedings of the 26th International Joint Conference on Artificial Intelligence*, ser. IJCAI'17. Melbourne, Australia: AAAI Press, Aug. 2017, pp. 1725–1731.
- 6. X. Wang, X. He, M. Wang, F. Feng, and T.-S. Chua, "Neural Graph Collaborative Filtering," in Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval. Paris France: ACM, Jul. 2019, pp. 165–174.
- 7. S. Rendle, C. Freudenthaler, Z. Gantner, and L. Schmidt-Thieme, "BPR: Bayesian personalized ranking from implicit feedback," in *Proceedings of the Twenty-Fifth Conference on Uncertainty in Artificial Intelligence*, ser. UAI '09. Arlington, Virginia, USA: AUAI Press, Jun. 2009, pp. 452–461.

Αναφορές (2/2)

- 8. Y. Hu, Y. Koren, and C. Volinsky, "Collaborative Filtering for Implicit Feedback Datasets," in *2008 Eighth IEEE International Conference on Data Mining*. Pisa, Italy: IEEE, Dec. 2008, pp. 263–272.
- 9. X. Ning and G. Karypis, "SLIM: Sparse Linear Methods for Top-N Recommender Systems," in *2011 IEEE 11th International Conference on Data Mining*. IEEE, Dec. 2011, pp. 497–506.
- 10. Y. Koren, "Factorization meets the neighborhood: A multifaceted collaborative filtering model," in *Proceedings of the* 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, ser. KDD '08. New York, NY, USA: Association for Computing Machinery, Aug. 2008, pp. 426–434.
- 11. C. Gini, "Measurement of Inequality of Incomes," *The Economic Journal*, vol. 31, no. 121, pp.124–126, 1921.
- 12. S. Vargas and P. Castells, "Rank and relevance in novelty and diversity metrics for recommender systems," in *Proceedings of the Fifth ACM Conference on Recommender Systems RecSys '11*. Chicago, Illinois, USA: ACM Press, 2011, p. 109.
- 13. H. Abdollahpouri, R. Burke, and B. Mobasher, "Controlling Popularity Bias in Learning-to-Rank Recommendation," in *Proceedings of the Eleventh ACM Conference on Recommender Systems*. Como Italy: ACM, Aug. 2017, pp. 42–46.
- 14. H. Abdollahpouri, R. Burke, and B. Mobasher, "Managing Popularity Bias in Recommender Systems with Personalized Re-Ranking," in *The Thirty-Second International Flairs Conference*, May 2019.
- 15. K. Hao, "How Facebook got addicted to spreading misinformation," https://www.technologyreview.com/2021/03/11/1020600/facebook-responsible-aimisinformation/.

Σας ευχαριστώ πολύ!