

(19) 日本国特許庁(JP)

(12) 特 許 公 報(B2)

(11) 特許番号

特許第6566515号
(P6566515)

(45) 発行日 令和1年8月28日(2019.8.28)

(24) 登録日 令和1年8月9日(2019.8.9)

(51) Int.Cl. F I
G O 6 F 16/9536 (2019.01) G O 6 F 16/9536
G O 6 F 16/9535 (2019.01) G O 6 F 16/9535

請求項の数 10 (全 23 頁)

<p>(21) 出願番号 特願2015-147269 (P2015-147269) (22) 出願日 平成27年7月24日 (2015.7.24) (65) 公開番号 特開2017-27480 (P2017-27480A) (43) 公開日 平成29年2月2日 (2017.2.2) 審査請求日 平成30年7月17日 (2018.7.17)</p>	<p>(73) 特許権者 504202472 大学共同利用機関法人情報・システム研究 機構 東京都立川市緑町10番3号 (74) 代理人 100097320 弁理士 宮川 貞二 (74) 代理人 100100398 弁理士 柴田 茂夫 (74) 代理人 100131820 弁理士 金井 俊幸 (74) 代理人 100155192 弁理士 金子 美代子</p>
--	---

最終頁に続く

(54) 【発明の名称】 アイテム推薦システム及びアイテム推薦方法

(57) 【特許請求の範囲】

【請求項1】

ユーザのアイテムに係る評価値を記入する評価マトリックスを記憶する評価マトリックス記憶部と；

ハブの出現を抑制する類似度尺度を用いてユーザ間の類似度を演算する第1の類似度演算部と；

前記第1の類似度演算部にて演算された類似度を用いて、前記対象ユーザとの類似度の高い方からk人のユーザを抽出する第1の近傍データ抽出部と；

前記第1の近傍データ抽出部にて抽出されたk人のユーザのアイテムに係る評価値を用いて、前記対象ユーザに係る未記入のセルに記入すべき評価値を予測する第1の評価値予測部と；

前記第1の評価値予測部にて予測された評価値の高いアイテムから前記対象ユーザに推薦すべきアイテムを抽出する推薦アイテム抽出して、前記対象ユーザに推薦するアイテム推薦部とを備える；

アイテム推薦システム。

【請求項2】

ユーザのアイテムに係る評価値を記入する評価マトリックスを記憶する評価マトリックス記憶部と；

ハブの出現を抑制する類似度尺度を用いてアイテム間の類似度を演算する第2の類似度演算部と；

10

20

前記第2の類似度演算部にて演算された類似度を用いて、前記対象アイテムとの類似度の高い方からk個のアイテムを抽出する第2の近傍データ抽出部と；

前記第2の近傍データ抽出部にて抽出されたk個のアイテムに係るユーザの評価値を用いて、前記対象ユーザに係る未記入のセルに記入すべき評価値を予測する第2の評価値予測部と；

前記第2の評価値予測部にて予測された評価値の高いアイテムから前記対象ユーザに推薦すべきアイテムを抽出して、前記対象ユーザに推薦するアイテム推薦部とを備える；

アイテム推薦システム。

【請求項3】

前記ハブの出現を抑制する類似度尺度を記憶する類似度尺度記憶部を備える；

10

請求項1又は請求項2に記載のアイテム推薦システム。

【請求項4】

一般的な類似度尺度に基づく類似度を前記ハブの出現を抑制する類似度尺度に基づく類似度に変換する類似度尺度変換部を備える；

請求項1ないし請求項3のいずれか1項に記載のアイテム推薦システム。

【請求項5】

前記対象ユーザに係る未記入のセルに記入すべき評価値を予測するに際し、前記記入すべき評価値として、重み付けをした平均値を用いる；

請求項1ないし請求項4のいずれか1項に記載のアイテム推薦システム。

【請求項6】

20

ユーザのアイテムに係る評価値を記入する評価マトリックスを記憶する評価マトリックス記憶工程と；

ハブの出現を抑制する類似度尺度を用いてユーザ間の類似度を演算する第1の類似度演算工程と；

前記第1の類似度演算工程にて演算された類似度を用いて、前記対象ユーザとの類似度の高い方からk人のユーザを抽出する第1の近傍データ抽出工程と；

前記第1の近傍データ抽出工程にて抽出されたk人のユーザのアイテムに係る評価値を用いて、前記対象ユーザに係る未記入のセルに記入すべき評価値を予測する第1の評価値予測工程と；

前記第1の評価値予測工程にて予測された評価値の高いアイテムから前記対象ユーザに推薦すべきアイテムを抽出して、前記対象ユーザに推薦するアイテム推薦工程とを備える；

30

アイテム推薦方法。

【請求項7】

ユーザのアイテムに係る評価値を記入する評価マトリックスを記憶する評価マトリックス記憶工程と；

ハブの出現を抑制する類似度尺度を用いてアイテム間の類似度を演算する第2の類似度演算工程と；

前記第2の類似度演算工程にて演算された類似度を用いて、前記対象アイテムとの類似度の高い方からk個のアイテムを抽出する第2の近傍データ抽出工程と；

40

前記第2の近傍データ抽出工程にて抽出されたk個のアイテムに係るユーザの評価値を用いて、前記対象ユーザに係る未記入のセルに記入すべき評価値を予測する第2の評価値予測工程と；

前記第2の評価値予測工程にて予測された評価値の高いアイテムから前記対象ユーザに推薦すべきアイテムを抽出して、前記対象ユーザに推薦するアイテム推薦工程とを備える；

アイテム推薦方法。

【請求項8】

一般的な類似度尺度に基づく類似度を前記ハブの出現を抑制する類似度尺度に基づく類似度に変換する類似度尺度変換工程を備える；

50

請求項 6 又は請求項 7 に記載のアイテム推薦方法。

【請求項 9】

請求項 6 ないし請求項 8 のいずれか 1 項に記載のアイテム推薦方法をコンピュータに実行させるためのプログラム。

【請求項 10】

請求項 9 に記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【技術分野】

【0001】

本発明はアイテム推薦システム及びアイテム推薦方法に関する。詳しくは、ユーザベースあるいはアイテムベースに代表される協調フィルタリング (CF) において、シリングアタック、すなわち、システムがユーザに推薦するアイテムを決定する工程に介入するために偽ユーザを不正投入する攻撃に対して、頑健なアイテム推薦システム及びアイテム推薦方法に関する。

10

【背景技術】

【0002】

ユーザベースの CF は、類似度演算に例えば k 近傍法を用い、アイテムに対する嗜好が類似する他のユーザの過去の評価値を参照してアイテムをユーザに推薦するシステムである。すなわち、アイテムに対する評価値の与え方が類似する他のユーザ k 人を選んで、アイテムに係る評価値を予測し、高い評価値が得られたアイテムをユーザに推薦する。

20

しかしながら、例えばアイテムが商品で、評価値が嗜好度の場合、平均的な嗜好度を有するように設計された偽ユーザがユーザベースの CF システムに投入される (アベレジアタックと呼ばれるシリングアタック) と、偽ユーザはどのユーザとも高い類似度を示すハブユーザ、すなわち、インフルエンサとなるため、偽ユーザの嗜好する商品が何時も推薦されるようになるおそれがある。

アイテムベースの CF、すなわち、類似する他のアイテムに対するユーザの過去の評価を参照してユーザに推薦するアイテムを決める推薦システム及び推薦方法に対しては、セグメントアタックあるいはポピュラーアタックと呼ばれるシリングアタックが効果を持つ。

【0003】

30

他方、発明者達は、k 近傍法でハブを軽減する方法を提案した。すなわち、大規模高次元データセットに対して類似度尺度にラプラシアンベースのカーネルを適用する方法 (非特許文献 1 参照)、センタリングを適用する方法 (非特許文献 2 参照)、及び、局在的センタリングを適用する方法 (非特許文献 3 参照) を提案した。

これらのハブを軽減する方法をユーザベースの CF あるいはアイテムベースの CF に適用することにより、ターゲットアイテムの評価を不正に高めるために攻撃者により偽ユーザが投入されたとしても、ターゲットアイテムの評価が変動しないようにするアイテム推薦システム及びアイテム推薦方法を提供できると期待される。

【先行技術文献】

【非特許文献】

40

【0004】

【非特許文献 1】Ikumi Suzuki, Kazuo Hara, Masashi Shimbo, Yuji Matsumoto, Marco Saerens, 「Investigating the Effectiveness of Laplacian-based Kernels in Hub Reduction」、In Proc. 26th AAAI Conference on Artificial Intelligence, pp. 1112 - 1118、2012 年

【非特許文献 2】鈴木郁美、原一夫、新保仁「k 近傍法でハブを軽減する類似度尺度」、情報処理学会研究報告、自然言語処理研究会、2012 - NL - 209、No. 11、pp. 1 - 8、2012 年

50

【非特許文献3】 Kazuo Hara, Ikumi Suzuki, Masashi Shimbo, Kei Kobayashi, Kenji Fukumizu, Milos Radovanovic, 「Localized Centering: Reducing Hubness in Large-Sample Data」、In Proc. 29th AAAI Conference on Artificial Intelligence、pp. 2645 - 2651、2015年

【発明の概要】

【発明が解決しようとする課題】

【0005】

ユーザベースのCFは、アベレジアタックと呼ばれる攻撃、すなわち、どのユーザとも高い類似度を示す多数の偽ユーザを投入する攻撃を受けると、偽ユーザの嗜好する商品が何時も推薦されるようになるおそれがある。

10

また、アイテムベースのCFは、セグメントアタックあるいはポピュラーアタックと呼ばれる攻撃、すなわち、ある特定のトピック（例えば、アクション映画、ホラー映画などのトピック）において、ポピュラーなアイテムと高い類似度をターゲットアイテムに持たせるために、ターゲットアイテムとポピュラーアイテムの両方に高い評価値を与える偽ユーザを多数投入する攻撃を受けると、当該トピックに属するアイテムを好むユーザに対して、ターゲットアイテムが推薦され易くなる。

上記のような推薦は不自然であり、推薦システムの本来の機能を阻害するという問題があった。

20

【0006】

本発明は、ハブの出現が抑制された類似度尺度を用いる、あるいは、与えられた類似度尺度をハブが出現しにくくなるように変換して用いることにより、インフルエンサとなるユーザ、あるいは、インフルエンサとなるアイテムの出現を抑制し、これらの影響力を低減することによって、結果的に攻撃者の意図通りにターゲットアイテムの評価値を変更されることがないようにする。

本発明は、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ない、アイテム推薦システム及びアイテム推薦方法を提供することを目的とする。

【課題を解決するための手段】

【0007】

上記課題を解決するために、本発明の第1の態様に係るアイテム推薦システム1は、例えば図5に示すように、ユーザuのアイテムiに係る評価値 $R(u, i)$ を記入する評価マトリックスRを記憶する評価マトリックス記憶部21と、ハブの出現を抑制する類似度尺度を用いてユーザ間の類似度を演算する第1の類似度演算部131と、第1の類似度演算部131にて演算された類似度を用いて、対象ユーザとの類似度の高い方からk人のユーザを抽出する第1の近傍データ抽出部141と、第1の近傍データ抽出部141にて抽出されたk人のユーザのアイテムに係る評価値を用いて、対象ユーザに係る未記入のセルに記入すべき評価値を予測する第1の評価値予測部151と、第1の評価値予測部151にて予測された評価値の高いアイテムから対象ユーザに推薦すべきアイテムを抽出して、対象ユーザに推薦するアイテム推薦部16とを備える。

30

40

【0008】

ここにおいて、アイテムは典型的には商品又はサービスである。さらに、商品又はサービスの種類、提供時期、提供地方、価格帯を限定する（夏季果物、X月公開映画等）等の条件を定めても良い。ただし、商品又はサービスに限定されず、評価可能であれば動植物、山河、都市、建築、絵画、音楽、演劇、武道、学問、生産性、効果でも良い。

また、マトリックスRは典型的にはユーザ数×アイテム数の評価マトリックスである。評価値 $R(u, i)$ として、典型的にはユーザuのアイテムiに係る嗜好度が使用される。ただし、嗜好度に限られず、定量的に評価可能であれば良い。例えば、健康への寄与度でも、不動産の価値でも、目的地への所要時間でも良い。また、定量的な評価はランク、レベルで表現するものでも良い。

50

【 0 0 0 9 】

また、類似度尺度とは、2つのデータの類似性を測る尺度として使用できるものすべてを含む。典型的には、内積、コサイン、ピアソン相関、距離が使用される。内積は2つのベクトルデータのスカラ積であり、コサインは長さ1に規格化されたベクトルデータの内積である。ピアソン相関は要素和がゼロになるように各要素値から要素和を差し引いた後に長さ1に規格化されたベクトルデータの内積である。さらに、内積の一般化とみなせる（機械学習分野で主に呼ばれるところの各種の）カーネルも含む。距離の典型は、2つのベクトルデータ間のユークリッド距離（L2ノルム）であるが、ユークリッド距離を一般化した距離（マンハッタン距離やLpノルムなど）も含む。さらに、ドメインの知識を持つ人間が各タスクの目的に応じて適宜定めた類似度スコア計算方法（BLASTなど）

10

【 0 0 1 0 】

また、ハブの出現を抑制する類似度尺度として、例えば全てのデータ対象がデータ中心に同等に類似になるように変換された類似度尺度、すなわちSpatial Centralityのない類似度尺度が該当する。例えば、上記一般的な類似度尺度に対して、原点をデータセットの平均（グローバルセントロイド）に移動する「（グローバル）セントリング」を適用して変換したもの、原点をローカルな部分集合の中心としてのローカルセントロイドに移動する「局在的セントリング」を適用して変換したものが挙げられる。さらに、ラプラシアンベースのカーネル、たとえば「コミュニティタイムカーネル」（Marco Saerens, Francois Fous, Luh Yen, and Pierre Dupont. 「The principal components analysis of graph, and its relationships to spectral clustering」, In Proc. 15th European Conference on Machine Learning (ECML), pp. 371 - 383, 2004年)を適用して変換したものが該当する。

20

また、ハブの出現を抑制する類似度尺度として、全てのデータ対象がデータ中心に同等に類似になるように変換された類似度尺度以外にも、ミューチュアルプロキシミティ、ローカルスケーリング等が挙げられる。

【 0 0 1 1 】

また、「ユーザとの類似度の高い方からk人のユーザを抽出する」とは、典型的にはk近傍法を使用して抽出することをいう。kとして任意の数値が可能であるが、たとえば、ムービーレンズデータセットでは、教師あり学習の結果、予測精度を高くするには、 $30 < k < 100$ が好ましく、 $40 < k < 70$ がより好ましく、 $k = 50$ が最も好ましい（図7参照）。

30

また、評価値を予測する際に、k人の平均値を使用できる。さらに、平均値を用いる際に、後述のように重み付けした平均値を用いると好ましい。重み付けには例えばユーザ間の類似度、季節による係数（果物の品質は季節に影響を受ける）等を使用できる。

【 0 0 1 2 】

ユーザベースのCFは、最近傍のk人（k近傍法（kNN）により抽出された最も近い方、及び類似度が高い方からk個のデータ）のユーザの過去の評価値を参照して未評価アイテムに対するユーザの評価値を予測する形態の推薦システムである。ユーザベースのCFの想定可能な欠点は、シリングアタックへの脆弱性である。シリングアタックは、システムに攻撃者によるバイアスのかかった（恣意的な）推薦を強制させるために、偽ユーザを推薦システムに投入する。ユーザベースのCFは、アイテムの特徴に基づく推薦を行わず、アイテムに対する他のユーザの過去の評価値に基づいて推薦を行う。このため、ユーザベースのCFは、どのユーザとも似るように偽ユーザを設計し、これを投入してシステムによる推薦アイテムの決定を変えさせようとする攻撃に対して、脆弱性を持つ。

40

【 0 0 1 3 】

他方、高次元データセットには、いわゆる「次元の呪い」の結果として、ハブデータが

50

出現し易いことが見出された (Milos Radovanovic, Alexandros Nanopoulos, Nirjana Ivanovic. 「Hubs in Space: Popular Nearest Neighbors in High-Dimensional Data」、Journal of Machine Learning Research, pp. 2487 - 2531, 2010年)。すなわち、高次元ではハブと呼ばれる少数のデータが他のデータのkNNに頻繁に現れる。ユーザベースのCFシステムにおいて、kNNが計算される時、各々のユーザはアイテム数の次元を持つベクトルとして表されるが、アイテムは一般に数多く存在するため、ベクトルは高次元ベクトルとなる。したがって、ハブとなるデータ(ハブデータ)が出現する。ハブユーザは推薦工程にインフルエンサとして寄与するので、推薦システムによる推薦アイテムの決定に大きな影響を与える。

10

シリングアタックは、ハブを利用する攻撃と見て取れる。ユーザベースのCFに対する攻撃では、システムによる推薦アイテムの決定を意図的にコントロールすることを目的とし、インフルエンサ、すなわち、ハブとなる偽ユーザを投入する。具体的には、偽ユーザをユーザに関するデータ中心に類似するように設計し、投入する。

【0014】

そこで、攻撃の影響を回避するために、kNNを求めるために使用される類似度尺度を全てのユーザがデータ中心に同等に類似するように変換することによって、ハブユーザ、すなわち、インフルエンサの出現自体を抑制し、偽ユーザをインフルエンサとしてシステムに送り込む攻撃者の企てを無効化することを提案する。ハブの出現を抑制する方法はいくつか提案されているが、たとえば、与えられた類似度マトリックスからコミュートタイムカーネルを計算することによって、又はより簡易に類似度マトリックスをセンタリングすることによって達成できる。ムービーレンズデータセットを用いて、かかる方法適用後に、偽ユーザがハブユーザと成りにくくなる傾向の存在を確認した(図8及び図9参照)。結果として、かかる類似度尺度の変換は、アイテム推薦の精度を劣化させることなく(図7参照)、攻撃に対して耐性の有るシステムを提供する。

20

【0015】

本態様のように構成すると、ハブの出現を抑制する類似度尺度を使用して類似度を演算するのでハブの出現を抑制でき、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ないアイテム推薦システムを提供することができる。

30

【0016】

上記課題を解決するために、本発明の第2の態様に係るアイテム推薦システム1は、例えば図5に示すように、ユーザuのアイテムiに係る評価値 $R(u, i)$ を記入する評価マトリックスRを記憶する評価マトリックス記憶部21と、ハブの出現を抑制する類似度尺度を用いてアイテム間の類似度を演算する第2の類似度演算部132と、第2の類似度演算部132にて演算された類似度を用いて、対象アイテムとの類似度の高い方からk個のアイテムを抽出する第2の近傍データ抽出部142と、第2の近傍データ抽出部142にて抽出されたk個のアイテムに係る対象ユーザの評価値を用いて、対象ユーザに係る未記入のセルに記入すべき評価値を予測する第2の評価値予測部152と、第2の評価値予測部152にて予測された評価値の高いアイテムから対象ユーザに推薦すべきアイテムを抽出して、対象ユーザに推薦するアイテム推薦部16を備える。

40

【0017】

第1の態様では、ユーザ間の類似度に基づいて評価値を求めたが、本態様ではアイテム間の類似度に基づいて評価値を求める。第1の態様では、k人の平均値を使用した。本態様ではk個のアイテムの平均値を用いる。しかし、その他のシステム構成は第1の態様と同様であり、第1の態様と同様に、ハブの出現を低減できるので、偽ユーザが投入されても、結果として推薦アイテムの決定が偽ユーザの投入に影響されにくい、すなわち、攻撃に対して頑健なアイテム推薦システムを提供することができる。

このように構成すると、ハブの出現を抑制する類似度尺度を使用するので、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ないアイテム推薦シ

50

テムを提供することができる。

【0018】

また、本発明の第3の態様に係るアイテム推薦システム1は、第1又は第2の態様において、ハブの出現を抑制する類似度尺度を記憶する類似度尺度記憶部22を備える。

このように構成すると、システムに記憶されたハブの出現を抑制する類似度尺度を使用して類似度を演算するのでハブの出現を抑制でき、アイテム推薦時に偽ユーザによる影響を少なくすることができる。

【0019】

また、本発明の第4の態様に係るアイテム推薦システムは、第3の態様において、一般的な類似度尺度に基づく類似度を前記ハブの出現を抑制する類似度尺度に基づく類似度に変換する類似度尺度変換部135を備える。

ここにおいて、類似度の変換には、例えば一般的な類似度尺度の式をハブの出現を抑制する類似度尺度の式に変換して類似度を求める方法、一般的な類似度尺度で求めた類似度を行列によりハブの出現を抑制する類似度尺度に基づく類似度に変換する方法等が使用される。

このように構成すると、一般的な類似度尺度をハブの出現を抑制する類似度尺度に変換して使用することによりハブの出現を抑制でき、アイテム推薦時に偽ユーザによる影響を少なくすることができる。

【0020】

また、本発明の第5の態様に係るアイテム推薦システムは、第1ないし第4のいずれかの態様において、対象ユーザに係る未記入のセルに記入すべき評価値を予測するに際し、記入すべき評価値として、重み付けをした平均値を用いる。

ここにおいて、重み付けには例えばユーザ間あるいはアイテム間の類似度、季節による係数（果物の品質は季節に影響を受ける）等を使用できる。本態様のように構成すると予測精度を向上できる。

【0021】

上記課題を解決するために、本発明の第6の態様に係るアイテム推薦方法は、例えば図6(a)に示すように、ユーザ u のアイテム i に係る評価値 $R(u, i)$ を記入する評価マトリックス R を記憶する評価マトリックス記憶工程(S104)と、ハブの出現を抑制する類似度尺度を用いてユーザ間の類似度を演算する第1の類似度演算工程(S107)と、第1の類似度演算工程(S107)にて演算された類似度を用いて、対象ユーザとの類似度の高い方から k 人のユーザを抽出する第1の近傍データ抽出工程(S108)と、第1の近傍データ抽出工程(S108)にて抽出された k 人のユーザのアイテムに係る評価値を用いて、対象ユーザに係る未記入のセルに記入すべき評価値を予測する第1の評価値予測工程(S109)と、第1の評価値予測工程(S109)にて予測された評価値の高いアイテムから対象ユーザに推薦すべきアイテムを抽出して、対象ユーザに推薦するアイテム推薦工程(S110)とを備える。

【0022】

本態様は第1の態様に係るアイテム推薦システムに対応するアイテム推薦方法である。

本態様のように構成すると、ハブユーザの出現を低減できるので、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ないアイテム推薦方法を提供することができる。

【0023】

上記課題を解決するために、本発明の第7の態様に係るアイテム推薦方法は、例えば図6(b)に示すように、ユーザ u のアイテム i に係る評価値 $R(u, i)$ を記入する評価マトリックス R を記憶する評価マトリックス記憶工程(S104)と、ハブの出現を抑制する類似度尺度を用いてアイテム間の類似度を演算する第2の類似度演算工程(S207)と、第2の類似度演算工程(S207)にて演算された類似度を用いて、対象アイテムとの類似度の高い方から k 個のアイテムを抽出する第2の近傍データ抽出工程(S208)と、第2の近傍データ抽出工程(S208)にて抽出された k 個のアイテムに係る対象

10

20

30

40

50

ユーザの評価値を用いて、対象ユーザに係る未記入のセルに記入すべき評価値を予測する第2の評価値予測工程(S209)と、第2の評価値予測工程(S209)にて予測された評価値の高いアイテムから対象ユーザに推薦すべきアイテムを抽出して、対象ユーザに推薦するアイテム推薦工程(S110)とを備える。

【0024】

本態様は第2の態様に係るアイテム推薦システムに対応するアイテム推薦方法である。

本態様のように構成すると、ハブアイテムの出現を低減できるので、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ないアイテム推薦方法を提供することができる。

【0025】

また、本発明の第8の態様に係るアイテム推薦システムは、第6又は第7の態様において、一般的な類似度尺度に基づく類似度をハブの出現を抑制する類似度尺度に基づく類似度に変換する類似度尺度変換工程(S106)を備える。

このように構成すると、一般的な類似度尺度に基づく類似度をハブの出現を抑制する類似度尺度に基づく類似度に変換して使用することによりハブの出現を抑制でき、アイテム推薦時に偽ユーザによる影響を少なくすることができる。

【0026】

また、本発明の第9の態様に係るプログラムは、第6ないし第8のいずれかの態様のアイテム推薦方法をコンピュータに実行させるためのプログラムである。

【0027】

また、本発明の第10の態様に係る記録媒体は、第9の態様に係るプログラムを記録したコンピュータ読み取り可能な記録媒体である。

【発明の効果】

【0028】

本発明によれば、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ないアイテム推薦システム及びアイテム推薦方法を提供できる。

【図面の簡単な説明】

【0029】

【図1】評価マトリックスRの例を示す図である。

【図2】ユーザ間の相関を示す図である。図2(a)はユーザuとユーザvとの相関を説明するための図、図2(b)は相関が強い場合の散布図、図2(c)は相関が弱い場合の散布図である。

【図3】低次元と高次元における N_{10} 分布を示す図である。図3(a)は低次元、図3(b)は高次元における N_{10} のヒストグラムである。

【図4】 N_{10} 値とデータ中心への類似度の関係を示す散布図である。図4(a)は低次元、図4(b)は高次元における図である。

【図5】実施例1及び実施例2におけるアイテム推薦システム1の構成例を示す図である。

【図6】実施例1及び実施例2におけるアイテム推薦方法の処理フロー例を示す図である。図6(a)は実施例1における処理フロー例を示す図、図6(b)は実施例2における処理フロー例を示す図である。

【図7】最近傍パラメータkを横軸、平均絶対誤差(MAE)を縦軸とし、異なる類似度尺度を用いたアイテム推薦システムを比較する図である。

【図8】ユーザ間類似度尺度として一般的なピアソン相関を用いた場合、投入された偽ユーザがハブになっていることを示す図(その1)で、誠実なユーザ(偽ユーザ以外のユーザ)を含む全ユーザに関する N_{50} とデータ中心への類似度に係る散布図である。

【図9】ユーザ間類似度尺度として一般的なピアソン相関を用いた場合、投入された偽ユーザが(a)ハブとなること、(b)、(c)類似度尺度の変換によってハブとなりにくくなることを示す図(その2)である。図9(a)はユーザ間類似度尺度として一般的なピアソン相関を用いた場合の N_{50} に関するヒストグラムである。図9(b,c)はセンタ

10

20

30

40

50

リングによる変換後の N_{50} に関するヒストグラム、図 9 (c) は通勤タイムカーネルによる変換後の N_{50} に関するヒストグラムである。

【発明を実施するための形態】

【0030】

図面を参照して以下に本発明の実施の形態について説明する。なお、各図において、互いに同一又は相当する部分には同一符号を付し、重複した説明は省略する。

【0031】

〔ユーザベースのCF〕

ユーザ数 N_{user} × アイテム数 N_{item} のマトリックス R を、アイテムに対するユーザの過去の反応（評価値）からなるデータセットとする。 $R(u, i)$ は u 番目のユーザの i 番目のアイテムへの評価値を示す。マトリックス R は nil と称する値の無い空欄を含んでいる。この nil の値は、ユーザのアイテムに対する評価がまだ与えられていないことを意味する。一般に、マトリックス R は空欄が多く、大部分が nil である。ユーザベースの CF は（後述するアイテムベースの CF も）、 k 近傍法を利用してこれらの値を予測するものである。

【0032】

【数1】

$$Pred(u, i) = \frac{\sum_{n \in U} Sim(u, n) \{R(n, i) - \bar{R}(n)\}}{\sum_{n \in U} Sim(u, n)} + \bar{R}(u) \quad (1)$$

式 (1) は u 番目のユーザの i 番目のアイテムへの評価値 $R(u, i)$ を予測する予測関数 $Pred(u, i)$ を示す。ユーザ u とユーザ v 間の類似度を $Sim(u, v)$ 、類似度 Sim のもとでユーザ u と最近傍となる k 人のユーザの集合を U とし、 U に属するユーザ n について使用する評価値は、 $R(n, i) \neq nil$ を満たす。

【0033】

さらに

【数2】

$$\bar{R}(u) = \frac{\sum_{i=1}^{N_{item}} R(u, i) \delta[R(u, i) \neq nil]}{\sum_{i=1}^{N_{item}} \delta[R(u, i) \neq nil]}$$

である。

【数3】

$$\bar{R}(u)$$

はユーザ u が評価したアイテムに対する平均の評価値である。 $\delta[\dots]$ は $[\dots]$ 内の条件が満たされれば 1、それ以外は 0 となる指示関数である。

【0034】

図 1 にマトリックス R の例を示す。図 1 (a) は偽ユーザ投入前、図 1 (b) は偽ユーザ投入後の例を示す。列方向にアイテム i を、行方向にユーザ u を配置し、その交点となるセル（欄）に評価値 $R(u, i)$ が記入されている。ここでは評価値 $R(u, i)$ は 1 から 5 の 5 段階の整数で評価されている。ターゲットアイテムの評価値の引き上げを目的とするアベレジアタックでは、図 1 (b) の下側のように、ターゲットアイテムであるアイテム 1 に高い評価を、その他のアイテムには過去にそのアイテムに対して評価を与えたユーザが付与した評価の平均に近い値を与える偽ユーザが投入される。

【 0 0 3 5 】

図 2 を用いて、ユーザ間の類似度を、アイテムに与える評価値のピアソン相関により測る方法について説明する。図 2 (a) はユーザ u とユーザ v の相関を説明するための図である。図 1 (a) に示したアイテム 2 ($R(u, 2) = 1, R(v, 2) = 1$)、および、アイテム 3 ($R(u, 3) = 5, R(v, 3) = 4$) が図 2 (a) にプロットされている。図 2 (b)、(c) は全アイテム i ($R(u, i), R(v, i)$) をプロットした散布図であり、図 2 (b) はユーザ u とユーザ v の (正の) 相関が強い場合、図 2 (c) はユーザ u とユーザ v の相関が弱い場合の例である。相関が強い場合は、全アイテムのプロットは直線に乗り、相関が弱い場合はアトランダムとなる。

10

【 0 0 3 6 】

〔ユーザベースのCFに一般的に使用されるユーザ間類似度尺度〕

ユーザベースのCFにおいて、ユーザ間類似度を与える関数 $Sim(\cdot, \cdot)$ を適切に選定することは重要である。なぜなら、類似度関数はkNNに入るユーザ、及び式(1)に係るkNNに入るユーザの重みを決定するからである。

一般的な類似度尺度関数として、マトリックスRのnilを0に置換した後に、行ベクトル(各ユーザが与えた評価値のベクトル)がなす角度のコサイン(coss)を計算するコサイン類似度がある。式(2)にこれを示す。

【 0 0 3 7 】

【数4】

$$Sim(u, v) = Cos(u, v) = \frac{\langle x_u, x_v \rangle}{\sqrt{\langle x_u, x_u \rangle} \sqrt{\langle x_v, x_v \rangle}} \quad (2)$$

20

ここに、 x_u は N_{item} 次元ベクトルで、その成分は $R(u, i)$ nilならば $x_u(i) = R(u, i)$ 、それ以外は $x_u(i) = 0$ となる。上記関数使用の1つの欠点は、各々のユーザuがアイテムに与える平均的評価

【数5】

$$\bar{R}(u)$$

30

の違いに基づくバイアスが無視されるという点である。それ故、上記欠点の修正方法として、各ベクトル成分から

【数6】

$$\bar{R}(u)$$

を差し引く方法が一般的に使用される。

40

【 0 0 3 8 】

ユーザのバイアス

【数7】

$$\bar{R}(u)$$

を差し引いたベクトルを用いた類似度は、式(3)のように計算され、これはユーザ間のピアソン(Pearson)相関と呼ばれる。

【数 8】

$$Sim(u, v) = Pearson(u, v) = \frac{\langle x'_u, x'_v \rangle}{\sqrt{\langle x'_u, x'_u \rangle} \sqrt{\langle x'_v, x'_v \rangle}} \quad (3)$$

ここに、もし、 $R(u, i) = nil$ かつ $R(v, i) = nil$ ならば、

【数 9】

$$x'_u(i) = R(u, i) - \bar{R}(u), x'_v(i) = R(v, i) - \bar{R}(v) \quad 10$$

であり、そうでなければ $x'_u(i) = 0$ 、 $x'_v(i) = 0$ となる。

【0039】

〔CFへのアタック〕

ユーザベースのCF、すなわち、ユーザと類似する他のユーザの過去の評価を参照してユーザに推薦するアイテムを決める推薦システム及び推薦方法に対しては、アベレジアタックと呼ばれるシリングアタックが効果を持つ。システムが持つ評価値マトリックスRを、不正な評価値を加えることによって改ざんすれば、推薦されるアイテムは変更される。この目的で偽ユーザを投入する攻撃をシリングアタックと呼び、アベレジアタックはその一つである。この攻撃を受けると、どのユーザも偽ユーザとの類似度が高くなる。つまり、偽ユーザは、推薦アイテムの決定に影響力を持つインフルエンサ、すなわち、ハブユーザとなる。 20

アベレジアタックにおいて投入される偽ユーザは、ターゲットアイテム（攻撃対象アイテム）を好む振る舞いをし、他のアイテムに対しては誠実なユーザ（偽ユーザ以外のユーザ）の平均的な振る舞いをする。すなわち、偽ユーザはターゲットアイテムには高い評価値点を与え、残りのアイテムには平均的な評価値を与える。結果として、偽ユーザはターゲットアイテムを好み、かつ、任意の誠実なユーザとの類似が高くなる。それ故に、ユーザベースのCFは、アベレジアタックを受けると、偽ユーザが高い評価を与えるターゲットアイテムを全ての誠実なユーザに推薦しやすくなる。

【0040】

アイテムベースのCF、すなわち、類似する他のアイテムに対するユーザの過去の評価を参照してユーザに推薦するアイテムを決める推薦システム及び推薦方法に対しては、セグメントアタックあるいはポピュラーアタックと呼ばれるシリングアタックが効果を持つ。この攻撃を受けると、攻撃対象となるターゲットアイテムは、どのユーザも高い評価を与えるポピュラーアイテムとの類似度が高くなる。攻撃者は、ポピュラーアイテムが推薦アイテムの決定に影響力を持つインフルエンサ、すなわち、ハブアイテムであることを悪用し、システムによるターゲットアイテムの評価値を不当に高く変更しようとする。 30

【0041】

〔ハブ現象〕

ハブ現象は、「次元の呪い」の結果として起こる現象の一つである。Dをd次元データの集合とし、 $N_k(x)$ は、D内のデータxがD内の他のデータのkNN内に入る回数を示す。次元dが増加すると、 N_k の分布形状は右に長い尾を引くように変わる（図3参照）。又は、少数のデータが大きな N_k 値をとるようになる。かかる大きな N_k 値を示すデータをハブといい、かかる現象をハブネス（ハブ現象）という。 40

【0042】

ここでは、人工データセットを用いてハブ現象について説明する。推薦システムでは一般に各ユーザは数個のアイテムに対してのみ評価値を与えるため、評価マトリックスRは空欄の多いスパースなマトリックスとなるが、この状況を模してスパースなデータセットを人工的に生成した。データセットは2000個のデータからなり、それぞれd次元ベクトルである。各データの生成方法は次の通りである：まず、各次元 $i = 1, \dots, d$ に 50

対して、 $\text{Lognormal}(5; 1)$ 分布にしたがって発生させた正の実数を丸め、整数 n_i を得る。そして、2000個のデータからランダムに n_i 個を選択し、その各々に対して、範囲 $[0, 1]$ から一様に乱数を発生させ、それを各々のベクトルの i 番目の要素 (i 次元成分) とする。

【0043】

図3は、データ間の類似度をベクトル間の角度、すなわち、 \cos (コサイン類似度) を用いて測ったときの、 N_{10} 分布を示すヒストグラムである。図3(a)は低次元、図3(b)は高次元の場合のヒストグラムである。ハブ現象の出現を説明するために、次元が低い場合 ($d = 50$) と高い場合 ($d = 1000$) の2ケースにおいて N_{10} 分布を比較した。図3は、高次元では大きな N_{10} 値を持つデータが出現し、結果として N_{10} の分布が歪む (対称でなくなる) ことを示す。最大となる N_{10} は図3(a)で38、図3(b)で133である。

10

【0044】

図4は N_{10} 値とデータ中心への類似度の関係を示す散布図である。図4(a)は低次元、図4(b)は高次元における図である。 N_{10} 値とデータ中心への類似度との間には、高次元で強い相関がみられることから、ハブ現象の起源は、高次元で発生するデータ中心へのバイアス、すなわち、Spatial Centrality であることが分かる。

【0045】

[攻撃シリングアタックとハブ現象との関係]

20

ナノポウラス達 (A. Nanopoulos, and M. Radovanovic, M. Ivanovic. How does high dimensionality affect collaborative filtering? In Proc. 3rd ACM Conf. on Recommender Systems (RecSys), pages 293 - 296, 2009.) 及びニース達 (P. Knees, D. Schnitzer, and A. Flexer. "Improving neighborhood-based collaborative filtering by reducing hubness", In Proc. ICMR '14, pages 161 - 168, 2014年) は、ユーザベースあるいはアイテムベースのCFにおいては、kNNは高次元で計算されるので、ハブ現象が出現すると報告した。通常、ユーザ数及びアイテム数は大きいので、コサイン類似度やピアソン相関のような類似度の計算に使用されるベクトルは高次元となり、ハブ現象が生じる。そして、他のデータのkNN内に頻繁に現れるハブデータは、多くの推薦を決定するのに影響する。しかし、ハブデータは多くのデータにとってあまり意味を持たないデータである。なぜなら、ハブデータは高次元でデータ中心に類似するという理由によってのみkNNの中に頻繁に生じるのであり、個々のデータを特徴付けるための役には立たないからである。事実、ニース達の文献によれば、推薦システムのパフォーマンスはハブデータの存在により悪化する。さらに、ハブデータはシステムによる推薦アイテムの決定に強い影響を持つデータなので、もしもシステム外からハブデータを操ることができれば、システムを効果的に攻撃することが可能となる。

30

40

実際、ハブ現象は推薦システムを攻撃に対して危うくする。例えば、アベレジアタックによりシステムに投入された偽ユーザは、ハブデータとなることで、システムに大きな影響を与える。よって、ハブ現象の発生を抑えることは攻撃回避につながると考えられる。

【0046】

[データ中心へのバイアス削減によるハブの抑制]

データ中心との類似度が高い少数のデータがハブになるというのであれば、類似度尺度を全てのデータ対象がデータ中心に同等に類似になる類似度尺度に変換することにより、ハブ現象を抑制できると考えられる。かかる類似度 (尺度) の変換は、与えられた類似度からコミュニティタイムカーネルを計算することによって得られ、より簡易には、与えられた類似度をセンタリングすることによって得られる。

50

Nをデータ数とし、KをサイズNの類似度行列とする。Kに対するコミュートタイムカネル $K^{C T}$ は、式(4)で与えられる。

$$K^{C T} = L + (L \text{ の一般化逆行列}) \cdots (4)$$

ここに、 $L = D - K$ はグラフラプラシアンと呼ばれる。Dは $D_{i i} = \sum_j K_{i j}$ となる対角行列である。

【0047】

次に、Iを単位行列、

【数10】

10

$\bar{1}$

を全要素が1であるN次元ベクトルとする。Kをセンタリングした類似度行列 $K^{C E N}$ は式(5)のように計算される。

【数11】

$$K^{CENT} = (I - \frac{1}{N} \bar{1}\bar{1}^T)K(I - \frac{1}{N} \bar{1}\bar{1}^T) \quad (5)$$

20

【実施例1】

【0048】

図5に実施例1におけるアイテム推薦システム1の構成例を示す。

本実施例では、アイテム推薦システム1としてユーザベースのCFを説明する。すなわち、類似度演算に例えばk近傍法を用い、対象ユーザと評価が似ている他のユーザの過去の評価値を参照してアイテムを推薦するシステムである。アイテムが商品で、評価値が嗜好度の場合は、対象ユーザと嗜好が似ている他のユーザの過去の嗜好度を参照して商品を推薦するシステムである。

30

なお、図5の構成は実施例1(ユーザベースのCF)及び実施例2(アイテムベースのCF)の両者に適用可能な構成である。このため、ユーザベースのCF及びアイテムベースのCFに共通する説明は本実施例で行うこととし、実施例2では差異を説明する程度とする。

【0049】

アイテム推薦システム1は、データ及びコマンドを処理するパーソナルコンピュータ(PC)10、各部で処理された又は入出力されたデータ・コマンド等を表示する表示部18、データ及びコマンドを入出力するための入出力部19、及び各部で処理された又は入出力されたデータ・コマンド等を記憶する記憶部20を含んで構成される。

パーソナルコンピュータ(PC)10は、ユーザ及びアイテムを登録する登録部11、ユーザのアイテムに係る評価の程度を表す評価値を評価マトリックスに記入する評価部12、類似度尺度を用いてユーザ間の類似度及び/又はアイテム間の類似度を演算する類似度演算部13、類似度の高い方から例えばk個の対象データ(ユーザ及び/又はアイテム)を抽出する近傍データ抽出部14、評価マトリックスRのセルに評価値が記入されていない時に、近傍データ抽出部14で抽出された評価値に基づいて、セルに記入されるであろうと予測される評価値を予測する評価値予測部15、評価値予測部15にて高い評価値を予測されたアイテムを推薦するアイテム推薦部16、アイテム推薦システム1の各部を制御して、アイテム推薦システムとして機能させる制御部17を備える。

40

【0050】

ここにおいて、登録部11はユーザを登録するユーザ登録部111とアイテムを登録す

50

るアイテム登録部 1 1 2 を有する。本実施例では、類似度演算部 1 3 は、類似度尺度として、ハブを抑制する類似度尺度を用いて、ユーザ間の類似度及び / 又はアイテム間の類似度を演算する。詳しくは、類似度演算部 1 3 はハブを抑制する類似度尺度を用いて、評価マトリックス R の各行のユーザの評価値に着目してユーザ間の類似度を演算する第 1 の類似度演算部 1 3 1 と、各列のアイテムの評価値に着目してアイテム間の類似度を演算する第 2 の類似度演算部 1 3 2 を有する。また、一般的な類似度尺度に基づく類似度からハブを抑制する類似度尺度に基づく類似度への変換を行う類似度尺度変換部 1 3 5 を有する。近傍データ抽出部 1 4 は、類似度の高い方から例えば k 個のユーザを抽出する第 1 の近傍データ抽出部 1 4 1 と、類似度の高い方から例えば k 個のアイテムを抽出する第 2 の近傍データ抽出部 1 4 2 を有する。評価値予測部 1 5 は、第 1 の近傍データ抽出部 1 4 1 で抽出された評価値に基づいて、対象ユーザの評価値を予測する第 1 の評価値予測部 1 5 1 と、第 2 の近傍データ抽出部 1 4 2 で抽出された評価値に基づいて、対象ユーザの評価値を予測する第 2 の評価値予測部 1 5 2 を有する。第 1 の評価値予測部 1 5 1 及び第 2 の評価値予測部は、対象ユーザに係る未記入のセルに記入すべき評価値を予測するに際し、記入すべき評価値として例えば平均値を用いることができる。また、重み付けをした平均値を用いるのが、推薦精度を高くできるので好ましい。

【 0 0 5 1 】

また、記憶部 2 0 は評価マトリックス R を記憶する評価マトリックス記憶部 2 1、類似度尺度及び第 1 の類似度演算部 1 3 1 で演算されたユーザに関する類似度データ、及び / 又は、第 2 の類似度演算部 1 3 2 で演算されたアイテムに関する類似度データを記憶する類似度尺度記憶部 2 2 を有する。第 1 の類似度演算部 1 3 1 及び第 2 の類似度演算部 1 3 2 の演算データはハブデータが出現しにくい類似度尺度を用いて演算したものである。類似度尺度記憶部 2 2 は、一般的な類似度尺度を記憶してもよい。また、記憶部 2 0 は近傍データ抽出部 1 4 にて抽出されたデータ（ユーザ及び / 又はアイテム）を記憶する近傍データ記憶部 2 3、評価値推定部 1 5 で推定されたアイテムを記憶する推薦アイテム記憶部 2 4 を有する。類似度尺度記憶部 2 2 は、類似度データの他に一般的な類似度尺度及び / 又はハブの出現を抑制する類似度尺度を記憶する。ハブの出現を抑制する類似度尺度を記憶せず、一般的な類似度尺度を記憶している場合には、類似度尺度変換部 1 3 5 にて一般的な類似度尺度をハブの出現を抑制する類似度尺度へ変換し、類似度尺度記憶部 2 2 には得られたハブの出現を抑制する類似度尺度が記憶し直される。類似度の変換には、例えば一般的な類似度尺度の式をハブの出現を抑制する類似度尺度の式に変換して類似度を求める方法、一般的な類似度尺度で求めた類似度を行列によりハブの出現を抑制する類似度尺度に基づく類似度に変換する方法等が使用される。この場合、変換前の一般的な類似度尺度を消去せずに残しておいても良い。一般的な類似度尺度とハブの出現を抑制する類似度尺度を共に記憶しておく、類似度演算結果及びアイテム推薦に係る評価値予測結果を組み合わせて用いたり、比較したりすることができる。近傍データ記憶部 2 3 は、第 1 の近傍データ抽出部 1 4 1 にて抽出されたユーザを記憶する第 1 の近傍データ記憶部 2 3 1 と、第 2 の近傍データ抽出部 1 4 2 にて抽出されたアイテムを記憶する第 2 の近傍データ記憶部 2 3 2 を有する。推薦アイテム記憶部 2 4 には、ユーザに対してアイテム推薦時に表示したい内容が記憶される。例えば、アイテム名の他に、アイテムについての説明、アイテムを使用するための説明、アイテムの画像等を記憶する。これらの内容は推薦時に表示部 1 8 に表示される。

【 0 0 5 2 】

なお、本実施例では、ユーザと類似度の高い方から k 人を抽出し、k 人の評価値の平均としてユーザの評価値を予測するので、類似度演算部 1 3 として第 1 の類似度演算部 1 3 1、近傍データ抽出部 1 4 として第 1 の近傍データ抽出部 1 4 1、評価値予測部 1 5 として第 1 の評価値予測部 1 5 1、近傍データ記憶部 2 3 としての近傍ユーザ記憶部 2 3 1 を使用できれば良く、第 2 の類似度演算部 1 3 2、第 2 の近傍データ抽出部 1 4 2、第 2 の評価値予測部 1 5 2、近傍アイテム記憶部 2 3 2 は無くても良い。これらは実施例 2 で使用される。

10

20

30

40

50

【 0 0 5 3 】

図 6 に実施例 1 におけるアイテム推薦方法の処理フロー例を示す。図 6 (a) は実施例 1 における処理フロー例を示す図、図 6 (b) は後述する実施例 2 における処理フロー例を示す図である。

まず、評価マトリックス R にアイテム i (S 1 0 1 : アイテム登録工程)、及びユーザ u を登録する (S 1 0 2 : ユーザ登録工程)。アイテム i の登録とユーザ u の登録はどちらが先でも良く、並行して行っても良い。次に、評価マトリックス R にユーザ u のアイテム i に係る評価の程度を表す評価値 $R (u , i)$ を登録する (S 1 0 3 : 評価値登録工程)。本実施例ではアイテムを商品とし、評価値を嗜好度とし、評価マトリックス R を嗜好度マトリックスとする。評価は例えば 5 段階評価 (1 ~ 5 の整数) で行う。ユーザ自身が登録しても良く、システム側で過去のユーザの当該アイテムに係る振る舞いを参照して登録しても良い。必ずしもマトリックス R 全体を記入する必要はなく、空欄のセルがあっても良く、通常は大部分が空欄になっている。評価マトリックス R は評価マトリックス記憶部 2 1 に記憶される (S 1 0 4 : 評価マトリックス記憶工程)。

10

【 0 0 5 4 】

次に、評価マトリックス R に基づいて各ユーザに対して推薦すべきアイテムを定める。まず、ユーザ本人に似た他のユーザを求めるための類似度演算を行う。類似度演算を行うに際し、類似度尺度記憶部 2 2 には類似度尺度として予め一般的な類似度尺度又はハブの出現を抑制する類似度尺度が記憶されているものとする。まず、類似度尺度記憶部 2 2 にハブの出現を抑制する類似度尺度が有るか無いかを判定する (S 1 0 5 : ハブ抑制類似度尺度の有無判定工程)。類似度尺度記憶部 2 2 に、ハブの出現を抑制する類似度尺度が記憶されておらず、一般的な類似度尺度が記憶されている場合には (S 1 0 5 で No の場合)、一般的な類似度尺度に基づく類似度をハブの出現を抑制する類似度尺度に基づく類似度に変換する (S 1 0 6 : 類似度尺度変換工程)。ハブの出現を抑制する類似度尺度として、例えば全てのデータ対象がデータ中心に同等に類似になる類似度尺度、すなわち *Spatial Centrality* のない類似度尺度を使用できる。具体的には、例えば、センタリングを行う又はコミュートタイムカーネルへの変換を行う。変換されたハブを抑制する類似度尺度は類似度尺度記憶部 2 2 に記憶される。次に、ハブの出現を抑制する類似度尺度を用いてユーザ間の類似度を演算する (S 1 0 7 : 第 1 の類似度演算工程)。なお、類似度の変換を行列で行う場合には類似度尺度変換工程 (S 1 0 6) と第 1 の類似度演算工程 (S 1 0 7) とが一括して行われる。この場合類似度尺度は必ずしも式として残るとは限らないが、演算結果においてハブを抑制する類似度尺度に基づく類似度データに内在して残ることになる。類似度尺度記憶部 2 2 に、ハブの出現を抑制する類似度尺度がすでに記憶されている場合には (S 1 0 5 で Yes の場合)、類似度尺度変換工程 (S 1 0 6) を省略し、ハブの出現を抑制する類似度尺度を用いてユーザ間の類似度を演算する (S 1 0 7 : 第 1 の類似度演算工程)。ハブの出現を抑制する類似度尺度を用いて演算された結果は、類似度尺度記憶部 2 2 に記憶される。

20

30

【 0 0 5 5 】

次に、類似度尺度記憶部 2 2 に記憶された類似度が高い方から例えば k 人のユーザを抽出する (S 1 0 8 : 第 1 の近傍データ抽出工程)。そして、抽出された k 人のユーザの平均評価値等に基づき、対象ユーザの空欄になっている評価値を予測する (S 1 0 9 : 第 1 の評価値予測工程)。第 1 の評価値予測工程 (S 1 0 9) では、対象ユーザに係る未記入のセルに記入すべき評価値を予測するに際し、例えば平均値を用いて予測することができる。また、重み付けをした平均値を用いるのが好ましい。最後に、予測値の高いアイテムを推薦する (S 1 1 0 : アイテム推薦工程)。例えば、アイテムを提供するインターネットのサイトにユーザが訪れた時に、当該ユーザに関して予測値の高い順にアイテムを提示する。また、電子メールで当該ユーザ宛に配信しても良い。

40

【 0 0 5 6 】

〔実験〕

ハブデータの出現を抑制することが、ユーザベースの CF を、アベレジアタックに対し

50

て頑健にすることを確かめる実験を行った。実験には、推薦タスクのベンチマークデータとして使用されるムービーレンズ1Mデータセット(m1-1m)を用いた。このデータセットは、6,040ユーザ、3,706アイテムに対する1,000,209個の評価値(整数1~5の5段階評価)から成る。どのユーザも少なくとも20アイテムを評価している。ベースラインとなるユーザ間の類似度尺度として、一般的に使われるコサイン類似度(Cos)、及び、ピアソン相関とshrunkピアソン相関(Pearson)を用い、式(1)を用いて評価値を予測した。shrunkピアソン相関がピアソン相関より良い精度が出ることが知られているので、今回はピアソン相関として、shrunkピアソン相関を使用する。今後は、shrunkピアソン相関をピアソン相関(Pearson)と表記する。ピアソン相関(Pearson)のパラメータは、過去の研究報告に倣い、 $\alpha = 100$ に設定した。ハブデータの出現を抑制するための方法として、ベースラインとなる類似度を式(4)によりコミュートタイムカーネルに変換する方法(CT)、又は、式(5)によりセンタリング変換する方法(CENT)を用いた。この実験の主な目的は変換の前後における攻撃に対するシステムのロバスト性(耐性)を比較することである。

【0057】

〔攻撃が無いときの予測精度〕

攻撃に対するロバスト性を調べる前に、攻撃が無いときに、CT変換及びCENT変換が評価値の予測精度を劣化させることがないかを検証した。推薦業務をシミュレートするために、データセット中の1,000,209個の評価値を、939,809個の訓練データ(テストデータの予測に使用するデータ)と60,400個のテストデータ(予測の対象となるデータ)に分割した。CFアルゴリズムの評価に一般的に使用される平均絶対誤差(MAE)を用いて、変換前後の類似度尺度の良し悪しを比較した。

$$MAE = 1 / |T| \sum_{(u, i) \in T} |Pred(u, i) - R(u, i)|$$

として計算した。ここにTはテストデータ(|T|=60400)として与えられたユーザ-アイテムのペアの組である。

【0058】

図7に最近傍パラメータkを10から100の間で変動させ、ベースラインとなる類似度尺度であるコサイン類似度(Cos)及びピアソン相関(Pearson)を、コミュートタイムカーネル変換(CT)あるいはセンタリング変換(CENT)した場合の、平均絶対誤差(MAE)を比較して示す。図7より、CENTは殆どの場合にMAEを減少(予測精度を増加)させ、CTはピアソン相関の場合はMAEを減少する。このことから、CENT変換及びピアソン相関に対するCT変換は、攻撃が無い時の予測精度を悪化させるどころか、改良することが分かる。

以下でアベレジアタックに対するロバスト性を評価するに際し、上記実験で概ねベストとなるMAEを達成するk=50と設定する。

【0059】

〔攻撃に対するロバスト性〕

アベレジアタックのターゲットアイテムとして21個の映画アイテムを選択した。これらのアイテムは、アベレジアタックに関する最初の研究を行ったラム達(S.K.Lam and J.Riedl.Shilling.Recommender Systems for Fun and Profit.In Proc.WWW'04,pages 393-402,2004年)が実験で用いたアイテムにできるだけ近いもの(評価ユーザ数、平均評価値の観点から)になるように選んだ。アベレジアタックとして、100の偽ユーザを投入し、偽ユーザはターゲットアイテムには高い評価(すなわち5)を付与し、残り他のアイテムにはノイズを加えた平均的評価を付与するよう作成した。すなわち、残りの各アイテムの各々に対して、 μ =平均評価値、 $\sigma=1.0$ となる、正規分布($\mu; \sigma$)に従う乱数を生成し、もっとも近い整数値1~5に変換して付与した

。予測シフトと呼ばれる値、すなわち、攻撃前後の予測評価値の差となる値を用い、変換前後の類似度尺度のよし悪しを比較した。より正確には、訓練用データを除き、誠実なユーザ（偽ユーザを除く全ユーザ）とターゲットアイテムの各ペアに対する予測シフトを計算し、その平均値を比較に用いた。

【0060】

【表1】

アベレジアタックにより生じた予測シフトと N_k 分布の歪度 ($k=50$)

類似度尺度	変換	歪度	予測シフト
コサイン類似度	(オリジナル)	3.422	0.902
	CENT	1.629	0.319
	CT	1.526	0.205
ピアソン相関	(オリジナル)	6.389	1.542
	CENT	2.648	1.084
	CT	1.173	0.981

10

表1はアベレジアタックにより生じた予測シフトと、 N_k 分布の歪度を示す。大きい N_k を持つデータ、すなわちハブデータが存在するほど、 N_k 分布の歪度は大きい値となる。 N_k 分布の歪度は、 $S_{N_k} = E \left[\frac{(N_k - \mu_{N_k})^3}{N_k^3} \right]$ ($E[\]$ は期待オペレータ、 μ_{N_k} と N_k はそれぞれ N_k 分布の平均と標準分散である) で表される。 N_k 分布の歪度、予測シフトのどちらも、CENT 又は CT 変換後に減少した。このことは、変換された類似度尺度の使用は、ハブデータの出現を抑制し、その結果、推薦システムを攻撃に対してロバストにすることを示している。

【0061】

図8及び図9は、ユーザ間類似度尺度として一般的なピアソン相関を用いた場合、投入された偽ユーザがハブとなること、及び、類似度尺度の変換によって偽ユーザがハブとなりにくくなることを示す図(その1及びその2)である。図8は、ユーザに関する N_{50} 値とデータ中心への類似度との関係を見るために、各々のユーザをプロットした散布図である。横軸は N_{50} 、縦軸はデータ中心への類似性を示す。図8より、投入された偽ユーザはデータ中心と高い類似度を持ち、ゆえにハブとなっていることが見て取れる。図9(a), (b), (c) は、 N_{50} 値に係るユーザのヒストグラムである。図9(a) はピアソン相関(オリジナル)を、図9(b) はセンタリング変換後のピアソン相関を、図9(c) はコミュートタイムカーネル変換後のピアソン相関を、それぞれ類似度尺度として使用した場合のヒストグラムである。

20

30

次に、ハブ現象において、何故、CENT 又は CT がロバスト性を提供するかを解析する。

40

【0062】

図8の散布図において、最大961の N_{50} 値を持つハブユーザが存在すること、及び、 N_{50} 値とデータ中心への類似度との間に強い相関が生じていることが見て取れる。誠実なユーザは○、投入された偽ユーザは×で示されるが、投入された偽ユーザは平均的な誠実なユーザを模倣して作られているため、ユーザに関するデータ中心と高い類似度を持つ。それ故、図9(a)の N_{50} 分布から分かるように、多くの誠実なユーザと比較して、投入された偽ユーザは大きい N_{50} 値(最小465、最大961)を有するハブユーザ(インフルエンサ)となる。これに対して、CENT 又は CT 変換は、ハブ現象の発生を抑制する。結果的に、図9(b)に示すように、CENT では、偽ユーザの N_{50} 値は最小101、最大156に減少した。また、図9(c)に示すように、CTを用いた場合は

50

、最小 0、最大 4 に減少した。このことは、オリジナルのピアソン相関をユーザ間類似度尺度として使用する場合と比較して、 $C_{E N T}$ 又は $C T$ 変換後の類似度尺度を使用することにより、投入された偽ユーザは、他のユーザの $k N N$ にさほど頻繁に表れなくなったことを明確に示している。つまり、偽ユーザは推薦アイテムの決定にさほど影響しないようになった（もはや投入された偽ユーザはインフルエンサではない）。

【 0 0 6 3 】

以上から、ハブ現象の発生を抑制するように類似度尺度を変換することにより、攻撃に対してロバスト、かつ、オリジナルな類似度尺度と同等又は良い予測精度を示す推薦システムを得られることが分かった。

【 0 0 6 4 】

〔 結論 〕

外部から偽ユーザを投入することによって推薦されるアイテムの変更を狙う攻撃に対し、ハブ現象を抑制することによって協調フィルタリング ($C F$) をロバストにする方法を提案した。

我々のアプローチは、ハブ現象はシリングアタックにより利用される主要因子の 1 つであるという基盤に立つものである。我々は、ハブデータの出現を抑制する 2 つの変換（センタリング及びコミュータムカーネルへの変換）を、一般的に使用される類似度尺度（コサイン類似度及びピアソン相関）に適用した。ムービーレンズデータセットを用いて、これらの変換が推薦システムを、推薦精度を劣化させることなく、シリングアタックに対してロバストにすることを示した。

【 0 0 6 5 】

以上により、本実施例によれば、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ない、アイテム推薦システム及びアイテム推薦方法を提供できる。

【 実施例 2 】

【 0 0 6 6 】

実施例 1（ユーザベース $C F$ ）では、ユーザ間の類似度に基づいて評価値を予測したが、本態様ではアイテム間の類似度に基づいて評価値を予測する例について説明する。すなわち、実施例 2（アイテムベース $C F$ ）では、対象アイテムと類似度の高い方から k 個のアイテムを抽出し、その k 個のアイテムに対して対象ユーザが過去に与えた評価値の平均として、対象ユーザの対象アイテムに対する評価値を予測する例について説明する。

【 0 0 6 7 】

実施例 1 に比して、類似度演算部 1 3 では、ユーザ間の類似度を演算する第 1 の類似度演算部 1 3 1 に代えて、アイテム間の類似度を演算する第 2 の類似度演算部 1 3 2 を使用する。アイテム間の類似度尺度として例えば全てのアイテムがアイテムに関するデータ中心に同等に類似になるものを使用する。近傍データ抽出部 1 4 では、第 1 の近傍データ抽出部 1 4 1 に代えて、第 2 の類似度演算部 1 3 2 にて演算されたアイテム間の類似度を用いて、ターゲットアイテムとの類似度の高い方から k 個のアイテムを抽出する第 2 の近傍データ抽出部 1 4 2 を使用する。評価値予測部 1 5 では、第 1 の評価値予測部 1 5 1 に代えて、第 2 の近傍データ抽出部 1 4 2 にて抽出された k 個のアイテムに係る評価値を用いて、対象ユーザのターゲットアイテムに対する未記入のセルに記入すべき評価値を予測する第 2 の評価値予測部 1 5 2 を使用する。その他の構成は実施例 1 と同様である。

【 0 0 6 8 】

実施例 1 に比して、類似度演算工程では、ユーザ間の類似度を演算する第 1 の類似度演算工程（ $S 1 0 7$ ）に代えて、アイテム間の類似度を演算する第 2 の類似度演算工程（ $S 2 0 7$ ）を行う。アイテム間の類似度尺度として例えば全てのアイテムがアイテムに関するデータ中心に同等に類似になるものを使用する。近傍データ抽出工程では、第 1 の近傍データ抽出工程（ $S 1 0 8$ ）に代えて、第 2 の類似度演算工程（ $S 2 0 7$ ）にて演算されたアイテム間の類似度を用いて、ターゲットアイテムとの類似度の高い方から k 個のアイテムを抽出する第 2 の近傍データ抽出工程（ $S 2 0 8$ ）を行う。評価値予測工程では、第

10

20

30

40

50

1の評価値予測工程(S109)に代えて、第2の近傍データ抽出工程(S207)にて抽出されたk個のアイテムに係る評価値を用いて、対象ユーザのターゲットアイテムに対する未記入のセルに記入すべき評価値を予測する第2の評価値予測工程(S209)を行う。その他の処理フローは実施例1と同様である。

このように、対象アイテムと類似度の高い方からk個のアイテムを抽出し、k個のアイテムの評価値の(重み付き)平均としてユーザの評価値を予測する。

【0069】

本実施例によれば、実施例1と同様に、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ない、アイテム推薦システム及びアイテム推薦方法を提供できる。

10

【実施例3】

【0070】

以上の実施例では、偽ユーザを投入する攻撃について説明したが、攻撃が無いときでも、高次元又は大規模データセットには元来ハブデータが存在し易い。この場合でも、ハブの出現を抑制するように類似度尺度を変換すれば、インフルエンサとなるデータの出現を抑制できる。これにより、本来推薦したいアイテムを推薦することが可能になる(ニース達による研究報告、前述の「攻撃シリリングアタックとハブ現象との関係」に記載、を参照)。

本実施例においては、偽ユーザ投入による攻撃が無いときでも、インフルエンサによる推薦のバイアスを受けない、アイテム推薦システム及びアイテム推薦方法を提供できる。

20

【実施例4】

【0071】

以上の実施例では、ユーザ毎に嗜好に合うアイテムを推薦する例について説明したが、大勢の人、大衆に広告を出す場合を想定してみる。もし、平均的なユーザ向けに広告するのが良いと仮定する。この場合、各ユーザ間の類似度を演算する代わりに、平均的な評価値を有する仮のユーザを生成し、当該仮のユーザについて、他のユーザとの類似度を演算して、k人のユーザを抽出し、評価値を予測すれば、大衆を対象としてアイテムを推薦すると好適である。

本実施例においても、偽ユーザを投入する攻撃を受けても、結果として攻撃の影響を受けることが少ない、アイテム推薦システム及びアイテム推薦方法を提供できる。

30

【0072】

また、本発明は、以上の実施例のフローチャート等に記載のアイテム推薦方法をコンピュータに実行させるためのプログラムとしても実現可能である。プログラムはアイテム推薦システムの記憶部に蓄積して使用してもよく、外付けの記憶装置に蓄積して使用してもよく、インターネットからダウンロードして使用しても良い。また、当該プログラムを記録した記録媒体としても実現可能である。

【0073】

以上、本発明の実施の形態について説明したが、実施の形態は以上の例に限られるものではなく、本発明の趣旨を逸脱しない範囲で、種々の変更を加え得ることは明白である。

【0074】

例えば、アイテム及び評価値については、本明細書中に列挙しなかったアイテム及び評価値についても定量的に評価可能であれば本発明を適用できる。また、類似度尺度については、パラメータを用いて調整可能としても良い。アイテム推薦については、アイテム名に添えて画像、説明文を追記可能である。また、推薦は、各ユーザがウェブページにアクセスした時のほか、各ユーザへのメールからアクセス可能にしても良く、メールで配信することも可能である。また、評価マトリックスの寸法、k近傍法のパラメータkは目的、状況に応じて適宜定めることができる。

40

【産業上の利用可能性】

【0075】

本発明はユーザベースあるいはアイテムベースに代表される協調フィルタリングに基づ

50

く推薦システムに利用される。

【符号の説明】

【 0 0 7 6 】

1	アイテム推薦システム	
1 0	パーソナルコンピュータ (P C)	
1 1	登録部	
1 2	評価部	
1 3	類似度演算部	
1 4	近傍データ抽出部	
1 5	評価値予測部	10
1 6	アイテム推薦部	
1 7	制御部	
1 8	表示部	
1 9	入出力部	
2 0	記憶部	
2 1	評価マトリクス記憶部	
2 2	ハブデータを抑制した類似度尺度記憶部	
2 3	近傍データ記憶部	
2 4	推薦アイテム記憶部	
1 1 1	ユーザ登録部	20
1 1 2	アイテム登録部	
1 3 1	第 1 の類似度演算部	
1 3 2	第 2 の類似度演算部	
1 3 5	類似度尺度変換部	
1 4 1	第 1 の近傍データ記憶部	
1 4 2	第 2 の近傍データ記憶部	
1 5 1	第 1 の評価値予測部	
1 5 2	第 2 の評価値予測部	
2 3 1	近傍ユーザ記憶部	
2 3 2	近傍アイテム記憶部	30
i	アイテム	
R	評価マトリクス	
$R(u, i)$	評価値	
u	ユーザ	

【 図 1 】

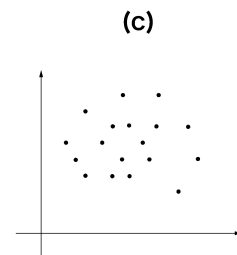
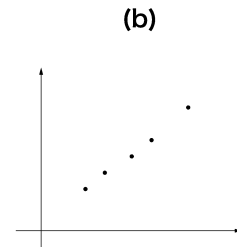
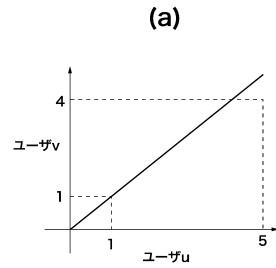
(a)

	アイテム1	アイテム2	アイテム3	アイテム4	……	アイテムm
ユーザ1	5	4		4		
ユーザ2	4			1	1	
ユーザ3						
ユーザ4						
ユーザu	5	1	5	4		
ユーザv	5	1	4	4	1	
ユーザn						

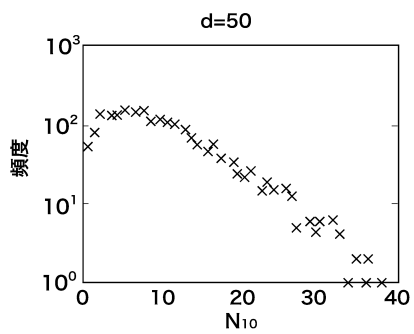
(b)

	アイテム1	アイテム2	アイテム3	アイテム4	……	アイテムm
ユーザ1	5	4		4		
ユーザ2	4			1	1	
ユーザ3						
ユーザ4						
ユーザu	5	1	5	4		
ユーザv	5	1	4	4	1	
ユーザn						
ニセ1	5	1	5	4		
ニセ2	5	1	4	4		
……	……					
ニセ100	5	1	4	4		

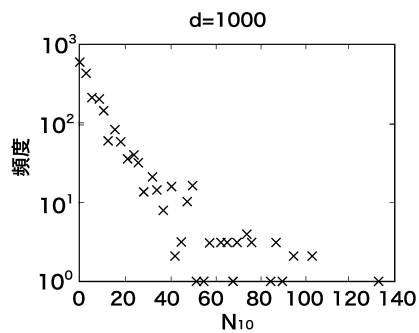
【 図 2 】



【 図 3 】

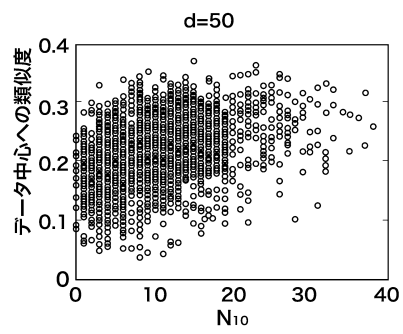


(a) 低次元

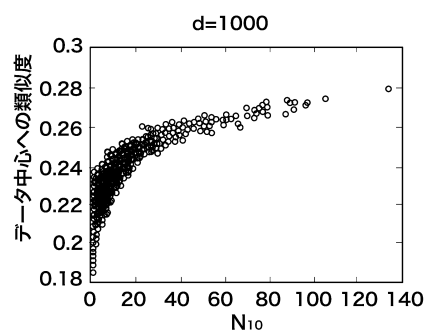


(b) 高次元

【 図 4 】

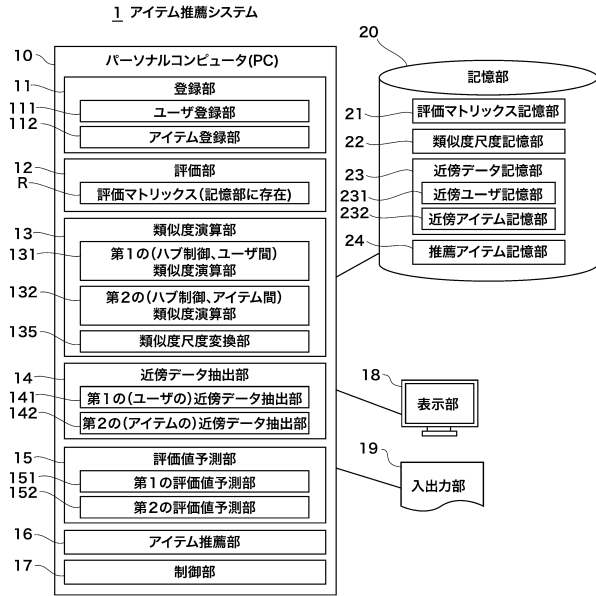


(a) 低次元

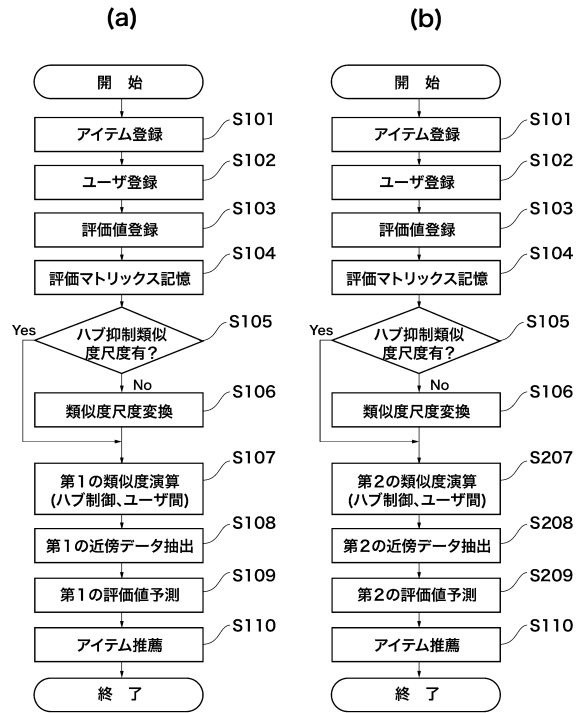


(b) 高次元

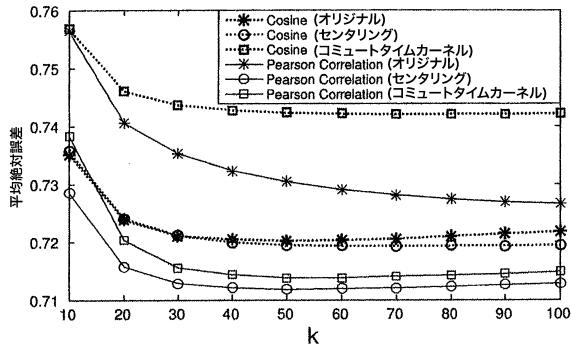
【図5】



【図6】

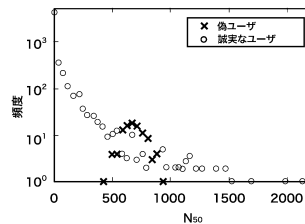


【図7】

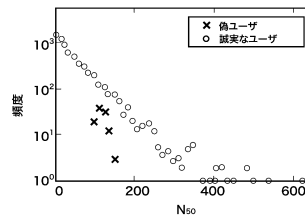


【図9】

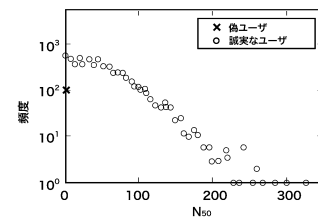
(a) オリジナル類似度



(b) センタリング変換後

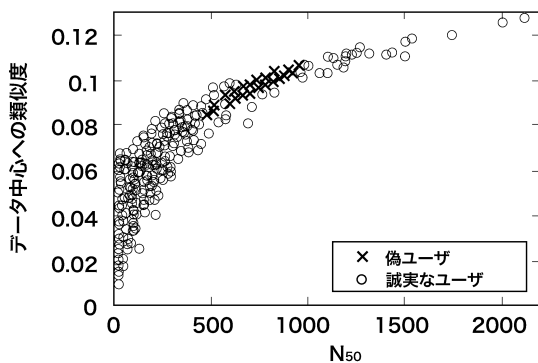


(c) コミュートタイムカーネル変換後



【図8】

オリジナル類似度



フロントページの続き

(72)発明者 原 一夫

静岡県三島市谷田 1 1 1 1 大学共同利用機関法人情報・システム研究機構 国立遺伝学研究所内

(72)発明者 鈴木 郁美

東京都立川市緑町 1 0 番 3 号 大学共同利用機関法人情報・システム研究機構 統計数理研究所内

審査官 後藤 彰

(56)参考文献 国際公開第 2 0 1 7 / 2 0 3 6 7 2 (W O , A 1)

特開 2 0 1 1 - 2 5 7 9 5 5 (J P , A)

土方 嘉徳, " 嗜好抽出と情報推薦技術", 情報処理, 日本, 社団法人情報処理学会, 2 0 0 7 年 9 月 1 5 日, 第 4 8 卷, 第 9 号, p.957-965

鈴木 郁美, " k 近傍法でハブを軽減する類似度尺度", 情報処理学会研究報告 自然言語処理 (N L), 日本, 一般社団法人情報処理学会, 2 0 1 2 年 1 2 月 1 5 日, 第 2 0 9 卷, 第 1 1 号, p.1-8

Peter Knees, " Improving Neighborhood-Based Collaborative Filtering by Reducing Hubness ", [online], 平成 2 6 年 4 月 1 日, ICMR 2014, 英国, ACM, [令和元年 6 月 2 0 日検索], インターネット <<https://dl.acm.org/citation.cfm?id=2578747>>

(58)調査した分野(Int.Cl., D B 名)

G 0 6 F 1 6 / 9 5 3 6

G 0 6 F 1 6 / 9 5 3 5