小口研究室　研究紹介　(2024年度)
(お茶の水女子大学理学部情報科学科)

イベント推薦精度向上のための生成AIのプロンプト分割最適化の検証
（研究担当:大本　詩織）

研究背景

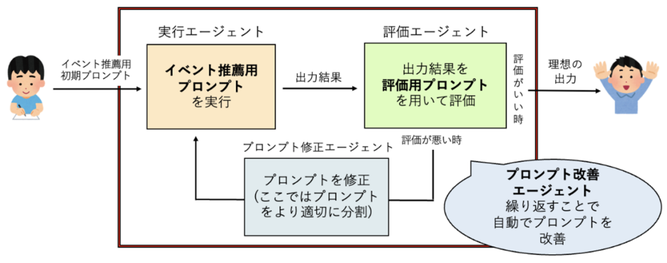
- 観光需要の増加・インバウンド市場の拡大に伴う，異なる背景や嗜好を持つユーザに適応したイベント推薦システムの必要性の高まり
- ユーザについての情報をSNSの投稿から取得可能
- LLMの急速な発展

LLMを利用した，SNS上のデータを用いた推薦システムの構築
ユーザのパーソナリティを利用した推薦精度の向上

課題

- システム構築に多くの労力・学習コストを必要とし，様々な要因を柔軟に組み合わせたイベント推薦が困難
  → 一連の流れをLLMによって行うことで，拡張性の高い柔軟なイベント推薦システムの構築を目指す
- 一連の包括的なプロンプトを用いると，回答の一括取得・回答時間の短縮などの利点があるが，精度が低下する
  → プロンプトの適切な分割が有効
- ChatGPTのバージョンによって精度が低下するプロンプトの長さに違いがある
  → 動的にプロンプトを修正することでChatGPTのバージョンの更新に対応

提案モデル



AIエージェントを用いて
自動でプロンプトを最適化
することで精度と利便性を
両立

本モデルの実現可能性を
ChatGPT-4oを用いて検証

実験

LLMによる評価

LLMに，評価項目を自動で生成させ，それらに基づいて評価するよう指示を与えたところ，問題がある場合でも常に評価が良くなってしまうことを確認
→ 評価用プロンプトを工夫することで評価の精度を改善できるか検証

- LLMに役割を与えるなどのプロンプトエンジニアリング手法を用いたが，精度の改善は見られなかった
- 評価項目を一度に与えるのではなく，各項目を一つずつ与えると評価精度の改善が見られた

LLMによる分割

LLMに，イベント推薦用プロンプトを与えて内容を基にn個に分割するよう指示
→ 指定した分割数通りに意味のまとまりで内容を分割できることを確認

分割の有効性の評価

プロンプトの分割が，回答精度の向上に寄与しているか検証

- イベント推薦用プロンプトを 0回, 2回, 4回, 6回 に分割した場合の4つの条件下で検証
- イベント推薦用プロンプトの分割から実行，評価までをそれぞれ20回実施し，期待値を算出(1項目につき100点 × 4項目　の400点満点)

評価スコアの結果

分割回数	期待値 $E[X]$	標準偏差 (SD)
なし (0 回)	357.45	17.39
2 回	375.85	15.64
4 回	387.80	10.17
6 回	389.40	8.03

t検定を実施した結果

比較	p 値
0 回 vs 2 回分割	0.0047
2 回 vs 4 回分割	0.0167
4 回 vs 6 回分割	0.6070 (n.s.)

➢ イベント推薦用プロンプトの分割は精度向上に効果がある
➢ 分割回数の増加が一定の閾値を超えると効果が飽和する可能性
➢ 提案モデルにおいては，出力評価が一定の閾値を下回る場合に限り分割を行うことで，出力品質を最大化しつつ不要な分割を抑制できると考えられる

今後の課題

- マルチエージェントシステムとして実装し，実際のユーザー評価を通じて有効性を検証
- より効率的な手法の模索
- 提案アプローチの他領域への拡張

ダミートランザクションを利用したブロックチェーンのトランザクション処理手法に関する検討
（研究担当:坂本　明穂）

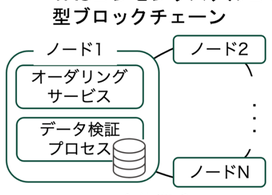
研究背景

背景
- DXの進展を受け企業間データ連携の需要の増加
- 安心安全なデータ共有プラットフォームとしてブロックチェーンが注目を集めている

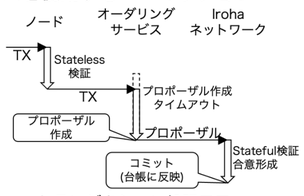
目的
- ブロックチェーンの性能評価
- 処理性能とサーバの負荷低減を両立する手法の提案

Hyperledger Iroha

- YACコンセンサスアルゴリズムを使用するパーミッション型ブロックチェーン



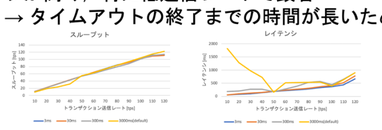
全体構成



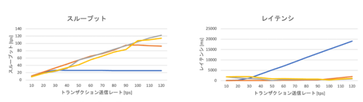
トランザクション処理フロー

Hyperledger Irohaの性能評価

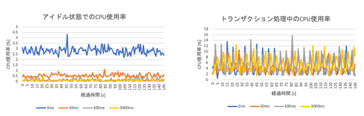
プロポーザル作成タイムアウト
(最大プロポーザルサイズ50)
- プロポーザル作成タイムアウトが長いほどレイテンシが高く，特に低送信レートで顕著
  → タイムアウトの終了までの時間が長いため



最大プロポーザルサイズ
(プロポーザル作成タイムアウト 3000ms)
- 最大プロポーザルサイズが大きいほど高いトランザクション送信レートに対応可能
- 特にトランザクションを1件ずつ処理する場合，非常に処理効率が悪い



サーバの負荷測定
(最大プロポーザルサイズ 10, トランザクション送信レート 90)
- アイドル状態ではプロポーザル作成タイムアウトが短いほどCPU使用率が高い
- トランザクション処理中のCPU使用率はプロポーザル作成タイムアウトの値に影響されない



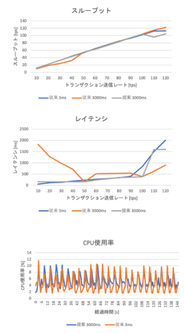
まとめ
プロポーザル作成タイムアウト
　トランザクション処理効率とサーバへの負荷はトレードオフの関係
最大プロポーザルサイズ
　大きいほど高い送信レートに対応可能
→ トランザクション処理性能とサーバ負荷の低減を両立する手法が必要

提案手法の評価

提案手法
- (通常TX数) + (ダミーTX数) = (最大プロポーザルサイズの整数倍)
  となるように通常トランザクションにダミートランザクションを付加してトランザクションを送信
  → プロポーザル作成タイムアウトの終了を待たずにプロポーザルを作成

実験条件
最大プロポーザルサイズ50，プロポーザル作成タイムアウト3000ms
- 本条件はアイドル状態でのCPU使用率は低いが他のタイムアウト値と比較して性能が低い場合が存在するため

実験結果
スループット，レイテンシ
- トランザクション送信レート100までは提案手法を用いることで性能の改善が見られ，従来手法プロポーザル作成タイムアウト3msのときと同程度の性能
- トランザクション送信レート110以降で提案手法は従来手法より性能が低下
  → 提案手法では150件のトランザクションを処理する必要があり，Hyperledger Irohaの性能限界を大きく超えたトランザクション数を処理したため



CPU使用率 (トランザクション送信レート 90)
- 提案手法のトランザクション処理実行中のCPU使用率は従来手法プロポーザル作成タイムアウト3msのときと同程度

→ 提案手法により，CPU使用率を低く抑えながら Hyperledger Irohaのトランザクション処理性能は高い状態を維持できた

まとめ

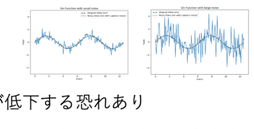
まとめ
- Hyperledger Irohaの処理性能とサーバの負荷について評価
- ダミートランザクションを使用し即座にプロポーザルを作成する手法を提案し，処理性能とサーバの負荷低減を両立

今後の課題
- ダミートランザクションの効率化
- 実ネットワークで接続されたHyperledger Irohaネットワークにおいて提案手法の性能を評価

GANを用いた時系列データの異常検知における適切なノイズ強度に関する考察
（研究担当:森　仁美）

研究背景

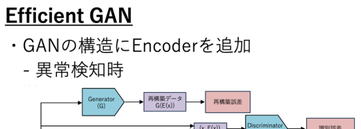
・プライバシ保護されたデータに対して、深層学習による異常検知を行う技術が必要
・時系列データについて、「個人の特定を許す一方で、元データの公開には抵抗がある」場合、
　データに対し確率的にノイズを加えて特徴を不明瞭に　→　元データの直接的な外部への公開防止
・**データにプライバシ保護を施した上で異常検知を行う**場合、ノイズが付加されたデータと
　異常データを区別するため検知の難易度が向上　→　一定量以上のノイズを付加すると異常検知精度が低下する恐れあり



▶ **ノイズを付加した時系列データ**に対して**GAN**を用いた異常検知を実施し、異常検知が可能となる適切な**ノイズの大きさ**について考察

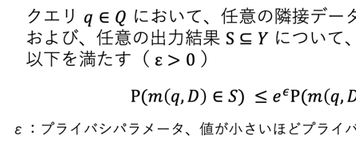
関連技術

GAN



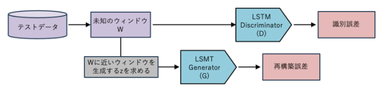
Efficient GAN

・GANの構造にEncoderを追加
　- 異常検知時

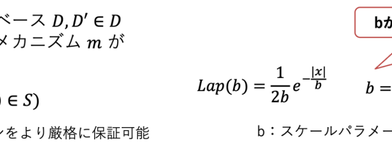


MAD-GAN

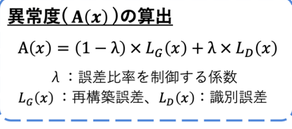
・**LSTM**を使用し、**多次元時系列データ**を検知対象に
　- 訓練時



　- 異常検知時



深層学習による教師なし異常検知
正常データで学習済みのモデルを対象データに適応



異常度($A(x)$)の算出

$$A(x) = (1-\lambda) \times L_G(x) + \lambda \times L_D(x)$$

λ ：誤差比率を制御する係数
$L_G(x)$ ：再構築誤差、$L_D(x)$ ：識別誤差

ε -差分プライバシ

クエリ $q \in Q$ において、任意の隣接データベース $D, D' \in D$ および、任意の出力結果 $S \subseteq Y$ について、メカニズム m が以下を満たす（$\varepsilon > 0$）

$$\mathrm{P}(m(q, D) \in S) \leq e^{\epsilon} \mathrm{P}(m(q, D') \in S)$$

ε ：プライバシパラメータ、値が小さいほどプライバシをより厳格に保証可能

ラプラスメカニズム

bが大 → ノイズが大、**bが小** → ノイズが小

$$Lap(b) = \frac{1}{2b} e^{-\frac{|x|}{b}} \qquad b = \frac{\Delta_{1,q}}{\varepsilon} \qquad \Delta_{1,q} = max_{D \sim D'} \| q(D) - q(D') \|_1$$

b：スケールパラメータ（ノイズ幅）、$\Delta_{1,q}$ ：sensitivity

実験と結果

・ε -差分プライバシにおけるラプラスメカニズムの考えを参考に、ラプラス分布に従ったノイズを付加
・**スケールパラメータb**を変化させ、異常検知が可能となる適切な**ノイズの大きさ**について2種類のデータで調査
・MAD-GAN＋Encoder（Efficient GANと同様）のモデルを用いて異常検知を実施

使用データセット

	種類	次元数	訓練データ数	テストデータ数	異常データの割合
SWaT	水処理	51	495,000	449,919	約12%
PSM	産業システム	25	132,481	87,841	約28%

SWaT_test				
次元番号	5	17	23	38
最大値	0.82	0.66	-0.06	0.41
最小値	-20.00	-2.24	-0.06	-18.11
平均	-11.17	-0.15	-0.06	-1.18
分散	**53.94**	1.22	4.3E-34	22.05

PSM_test				
次元番号	3	4	15	23
最大値	8.55	4.98	12.59	-0.12
最小値	-4.91	-5.10	-5.87	-0.85
平均	1.55	-0.28	0.85	-0.74
分散	**11.89**	0.72	1.12	2.3E-03

実験１　ノイズなしでの異常検知（通常の異常検知）
・訓練と異常検知を200回実施し、異常検知精度の統計量を算出

	平均（μ）	分散（σ^2）	標準偏差（σ）
SWaT	**0.671**	0.00013	**0.01140**
PSM	**0.426**	0.00033	**0.01828**

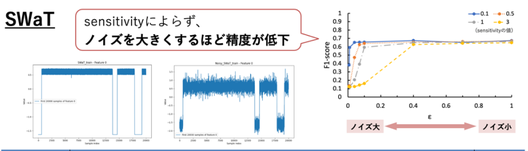
・SWaTの方が分散及び標準偏差が小さい
→全データ同じ数値の次元が複数存在することが要因と推察

以降の実験では、
「異常検知精度が $\mu - 2\sigma$ を下回る場合」＝ **異常検知が困難**と判断

実験２　ε を変化（付加するノイズの大きさを変化）

SWaT

sensitivityによらず、
ノイズを大きくするほど精度が低下

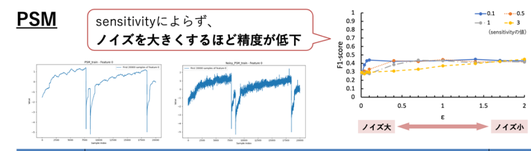


	ε 0.007	0.01	0.04	0.07	0.1	0.4	0.7	1	ノイズなし(200回平均)
sensitivity 0.1	0.381	0.592	0.652	0.654	0.656	0.675	0.652	0.674	0.671
0.5	0.130	0.135	0.472	0.625	**0.639**	0.656	0.662	0.669	
1	0.121	0.117	0.204	0.392	0.593	0.648	0.658	0.662	
3	0.122	0.121	0.124	0.143	0.162	0.626	**0.641**	0.648	

およそ**スケールパラメータb=4**以上のノイズを加えると異常検知が困難

PSM

sensitivityによらず、
ノイズを大きくするほど精度が低下



	ε 0.007	0.01	0.04	0.07	0.1	0.4	0.7	1	1.4	1.7	2	ノイズなし(200回平均)
sensitivity 0.1	0.288	0.291	**0.382**	0.432	0.440	0.425	0.429	0.433	0.449	0.435	0.431	0.426
0.5	0.291	0.284	0.309	0.299	0.330	0.432	0.422	0.446	0.420	0.422	0.417	
1	0.276	0.291	0.289	0.289	0.279	**0.385**	0.438	0.433	0.407	0.423	0.417	
3	0.293	0.293	0.276	0.296	0.295	0.310	0.331	0.371	0.398	0.424	0.450	

およそ**スケールパラメータb=2.5**以上のノイズを加えると異常検知が困難

まとめと今後の課題

まとめ
・付加ノイズが大きくなるほど、異常検知精度は低下
・SWaTはおよそb=4、PSMはおよそb=2.5を超えるノイズを加えると異常検知困難
→いずれのデータでも異常検知が可能となるノイズの大きさには限度あり

今後の課題
・ノイズの付加方法について比較検討を実施
・他の時系列データでも同様の実験を行い傾向を比較
→プライバシ保護を施した状態でも精度を落とさず異常検知可能なモデルの提案を目指す

https://www.is.ocha.ac.jp/~oguchi_lab/　　oguchi@is.ocha.ac.jp