A-027

悪質データに対して頑強なデータコラボレーション解析

矢中 祥吾 †　　高野 祐一 ‡
筑波大学 †　　筑波大学 ‡

1 はじめに

近年，データ収集コストの低下によって，各機関がそれぞれデータの収集・蓄積を行い，それらを用いたデータ解析が注目されている．

データが複数の機関に分散した状況の解析手法には，各機関が保有する元データのみを用いて個々に解析を行う個別解析と，各機関の保有する元データを一つにまとめて解析を行う集中解析が存在する．データの共有によって十分な量のデータが確保されるため，集中解析の方が個別解析よりも高い解析精度を達成することが可能である．しかし，元データをそのまま共有，集約することは機密情報保護の観点から困難である．

上記の課題を克服する解析手法として，データコラボレーション（DC：Data Collaboration）解析 [1] が提案された．DC 解析では，各機関が保有する元データに対して次元削減を行い，データを抽象化した中間表現を共有する．共有された中間表現は，そのままでは一つにまとめて解析をすることができない．そのため，統合関数と呼ばれる関数を用いて中間表現を一つにまとめて解析可能な状態である統合表現に変換する．その後，各機関の統合表現を一つに結合したデータセットを用いて解析を行う．

DC 解析では各機関からデータを集約するため精度の高い解析が可能となる．しかし，DC 解析の精度を低下させようとする悪意を持った機関や外部からの攻撃者によって悪質なデータが共有された場合，DC 解析の解析精度が低下することが考えられる．

本研究では，悪質データに対して頑強な DC 解析を提案する．提案手法では，各機関のデータに対する予測精度から，正常データを共有する機関と悪質データを共有する機関を分割し，正常と判定された機関のデータのみを解析する．これにより，悪質データの共有による DC 解析の解析精度低下を防止することができる．

2 提案手法

本節では，DC 解析において悪質データを共有する機関を検出し，解析から除外する手法を説明する．ここで DC 解析の参加機関数を m，各機関の統合表現を $\hat{\boldsymbol{X}}^{(k)}$ $(k \in [m])$ とする．

はじめに，各機関から共有された中間表現を統合表現 $\hat{\boldsymbol{X}}^{(k)}$ に変換し，一つにまとめたデータセットを訓練データとして暫定モデル h を構築する．その後，機関ごとの統合表現 $\hat{\boldsymbol{X}}^{(k)}$ に対する暫定モデル h の予測精度 a_k $(k \in [m])$ を計算する．DC 解析の参加機関において悪意のある機関は全機関の一部分で，正常な機関が多数を占めていると仮定すると，悪意のある機関の統合表現に対する暫定モデル h の予測精度は正常な機関の統合表現に対する暫定モデル h の予測精度よりも低くなることが考えられる．機関ごとに計算される a_k に対して K 平均法 [2] によるクラスタリングを行い，正常な機関と悪意のある機関を異なるクラスタに分割する．

最適なクラスタ数を求めるための評価指標としてシルエット係数 [3] を用いる．シルエット

Robustification of the data collaboration analysis against malicious data
† Shogo Yanaka, University of Tsukuba
‡ Yuichi Takano, University of Tsukuba

係数はクラスタ内のデータ点がどの程度密にグループ化されていて，クラスタ間がどれだけ離れているかを示す尺度である．シルエット係数は各データ点ごとに計算され，-1 から 1 の範囲の値をとる．シルエット係数の値が高いほどクラスタリングが良好であると考えられる．

機関ごとの統合表現 $\hat{\boldsymbol{X}}^{(k)}$ に対する暫定モデル h の予測精度 a_k をデータ点としてクラスタ数を変更しながらクラスタリングを行い，各データ点に対するシルエット係数を計算する．指定したクラスタ数の範囲でシルエット係数の平均の最大値が α 未満 $(-1 \leq \alpha \leq 1)$ のとき，クラスタリングの結果が良好ではなく，正常な機関と悪意のある機関を十分に分割できていないと考えられる．したがって，暫定モデル h を出力し，アルゴリズムを終了する．指定したクラスタ数の範囲でシルエット係数の平均の最大値が α 以上のとき，対応するクラスタ数を最適なクラスタ数とする．改善モデルの学習のために十分なデータ数を確保するために，データ数が共有された全データ数の β 倍以上 $(0 < \beta < 1)$ になるまで予測精度の平均が高い順番にクラスタを選択する．選択されたクラスタに含まれる機関の統合表現 $\hat{\boldsymbol{X}}^{(k)}$ を結合したデータセットを用いて改善モデル h' を構築する．その後，改善モデル h' を出力してアルゴリズムを終了する．

提案手法のアルゴリズムは以下のようになる．

提案手法のアルゴリズム

Step 0（暫定モデルの構築） 統合表現 $\hat{\boldsymbol{X}}^{(k)}$ $(k \in [m])$ を結合したデータセットを用いて暫定モデル h を構築する．

Step 1（予測精度の計算） 機関ごとの統合表現 $\hat{\boldsymbol{X}}^{(k)}$ に対する暫定モデル h の予測精度 a_k $(k \in [m])$ を計算する．

Step 2（予測精度のクラスタリング） 予測精度 a_k $(k \in [m])$ をデータ点としてクラスタリングを行い，シルエット係数の平均が最大となるクラスタ数を選択する．シルエット係数の平均の最大値が α 未満の場合には暫定モデル h を出力して終了する．

Step 3（改善モデルの構築） 全データ数の β 倍以上になるまで，予測精度の平均が高い順番にクラスタを選択し，選択された機関の統合表現 $\hat{\boldsymbol{X}}^{(k)}$ を統合したデータセットを用いて改善モデル h' を構築し，これを出力して終了する．

3 数値実験

公開データセットを用いて提案手法の有効性を確認する．参加機関が正常な機関のみの場合と，悪意のある機関が含まれる場合に，個別解析，集中解析，DC 解析，提案手法の解析精度の比較を行う. 実験に使用したデータおよび結果の詳細は当日報告する．

参考文献

[1] Imakura, A., Sakurai, T. (2020). Data collaboration analysis framework using centralization of individual intermediate representations for distributed data sets. ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part A: Civil Engineering, 6(2), 04020018.

[2] MacQueen, J. (1967, June). Some methods for classification and analysis of multivariate observations. In Proceedings of the fifth Berkeley symposium on mathematical statistics and probability (Vol. 1, No. 14, pp. 281-297).

[3] Rousseeuw, P. J. (1987). Silhouettes: A graphical aid to the interpretation and validation of cluster analysis. Journal of Computational and Applied Mathematics, 20, 53–65.