筑波大学
University of Tsukuba

2024 年 1 月 18 日

報道関係者各位

国立大学法人筑波大学

機械学習システムの信頼性を評価する理論モデルを構築

複数の機械学習モデルや入力データの組み合わせで構成される機械学習システムについて、これに用いる機械学習モデルと入力データの多様性が、どのように出力の信頼性に影響するかを評価し、適切なシステムの構成案を探索するための理論モデルを構築しました。

自動運転や医療画像診断などに用いられる機械学習システムでは、信頼性や安全性の高い出力が求められます。そのようなシステムの設計の一つに、N バージョン機械学習システムがあります。このシステムでは、複数の機械学習モデルや入力データを組み合わせることにより、機械学習モデルの推論エラーがシステムの最終出力に直結することを抑止します。しかしながら、これまで、機械学習モデルや入力データの多様性が出力の信頼性と関係していることは経験的に分かっていましたが、それを説明できる理論的なモデルはありませんでした。

本研究では、機械学習モデルの推論エラーに関して、機械学習モデルの多様性と入力データの多様性を指標化し、これに基づいて機械学習システムの出力の信頼性を評価する理論的モデルを構築しました。これにより、一般的に想定される状況においては、機械学習モデルの多様性と入力データの多様性の双方を生かす構成方法が最も安定的に信頼性を向上できることが示されました。

実際のシステム設計においては、複数の推論処理を実行する際の付随作業（オーバーヘッド）やコストも問題になります。今後さらに、N バージョン機械学習システムの高信頼化を、より低コスト・省電力・小オーバーヘッドで実現する方式について、理論および実装の両面から研究開発を進める予定です。

研究代表者
筑波大学システム情報系
町田 文雄　准教授

研究の背景

機械学習モデルを活用したソフトウェアシステムが広く開発されるようになり、その品質管理が新たな課題となっています。自動運転や医療画像診断など、高い信頼性や安全性の求められる機械学習システムでは、機械学習モデルの精度を高めるだけでなく、システム設計の段階での高信頼化対策が必要です。N バージョン機械学習システムはその一つとして知られており、複数の機械学習モデルや入力データを組み合わせることで、画像分類システムなどの出力の信頼性を高めることができます。これまで、N バージョン機械学習システムに関しては、複数の機械学習モデルを用いると推論エラーが低減され、より正確な推論結果が得られることや、複数の入力データを用いると出力の高信頼化が見込めることが、経験的に分かっていましたが、それらを組み合わせた場合の信頼性向上効果を説明できる理論的なモデルは、存在していませんでした。

研究内容と成果

本研究では、二つの異なる機械学習モデルと二つの異なる入力データ集合を用いる二重モデル二重入力（2 バージョン）機械学習システムに着目し、6 つの実現可能なシステムの設計方式による信頼性の違いを統一的に説明できる信頼性モデルを構築しました（図 1）。2 バージョン機械学習システムは、N バージョン機械学習システムの基本的な構成単位であり、その信頼性をモデル化することが、N バージョン機械学習システムの高信頼化の鍵となります。6 つの異なる設計方式の信頼性を評価するため、二つの多様性尺度を導入しました。一つは機械学習モデルの多様性です。これにより、二つの異なる機械学習モデルを用いた場合の出力の信頼性を比較評価できます。もう一つが機械学習モデルに与える入力データ集合の多様性です。これにより、二つの異なる入力データを用いた場合の出力の信頼性を比較評価できます。これらの多様性指標を組み合わせることで、異なる機械学習モデルと異なる入力データを組み合わせた場合の出力の信頼性も比較評価できるようになります。

このモデルを用いて 6 つの設計方式を比較したところ、与えられた条件下において、システムが取るべき望ましい構成を推定できることが明らかになりました。一方の機械学習モデルや入力データが他方に対して常により正確な出力を与えるような特殊な状況を除き、異なる機械学習モデルと異なる入力データを組み合わせた設計方式は、安定的に信頼性向上効果が見込めることが確かめられました（図 2）。つまり、自動運転などで利用されるような画像分類タスクでは、複数の異なる入力画像と複数の異なる機械学習モデルを組み合わせるシステム構成が、信頼性向上の観点で望ましいと言えます。

今後の展開

N バージョン機械学習システムでは複数の機械学習モデルや複数の入力データを用いるため、単一の機械学習モデルを用いた場合と比較してコストや付随作業（オーバーヘッド）が生じることから、実際のシステムではこれらを考慮した設計が必要になります。本研究グループでは、今後さらに、N バージョン機械学習システムの高信頼化を、より低コスト・省電力・小オーバーヘッドで実現する方式について、理論および実装の両面で研究を進める予定です。

参考図

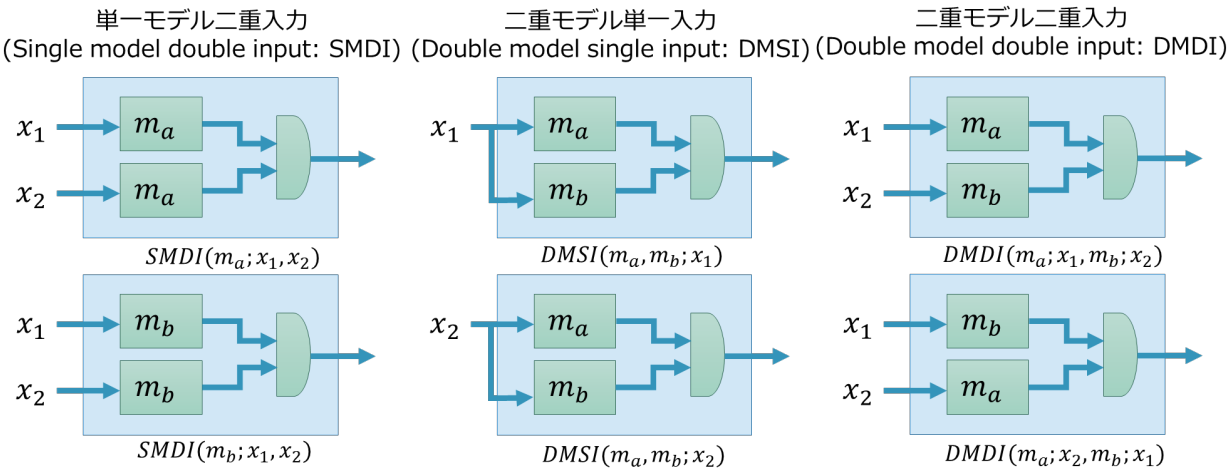

図 1　二重モデル二重入力（2 バージョン）機械学習システムの 6 つの異なる設計方式

このシステムでは、2 つの異なる入力x_1, x_2と 2 つの異なる機械学習モデルm_a, m_bの組み合わせ方により、6 つの異なる設計方式を取り得る。一つのモデルのみを使う設計を単一モデル二重入力（Single model double input, SMDI）、一つの入力のみを使う設計を二重モデル単一入力（Double model single input, DMSI）、二つの入力と二つのモデルを使う設計を二重モデル二重入力（Double model double input, DMDI）と呼ぶ。

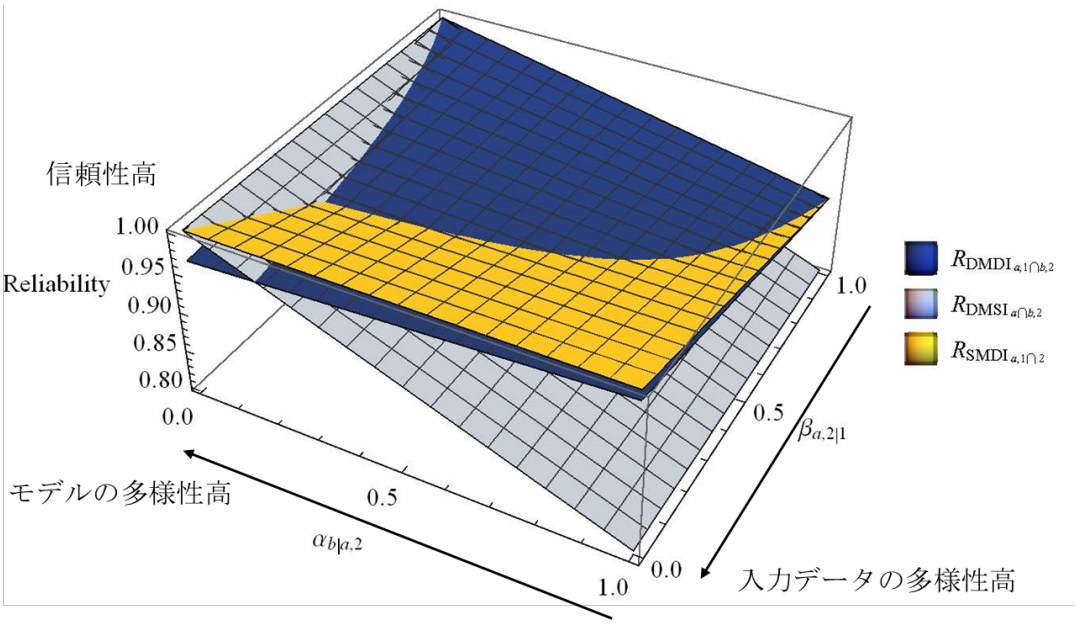

図 2　モデルの多様性と入力の多様性による異なる設計の信頼性比較の例

提案した理論モデルを用いて、異なるシステム設計による信頼性を比較評価した結果の一例。縦横軸がモデルの多様性と入力データの多様性の指標値をそれぞれ表しており、DMDI（青色）、DMSI（灰色）、および SMDI（黄色）による出力の信頼性の推定値をプロットしている。2 つの機械学習モデルと 2 つの入力データを組み合わせる DMDI は、他の設計よりも安定的に信頼性向上効果が見込める。

研究資金

本研究は科研費による研究プロジェクト（22K17871 、19K24337）の一環として実施されました。

掲載論文

【題　名】 Using Diversities to Model the Reliability of Two-version Machine Learning Systems
（多様性を用いた 2 バージョン機械学習システムの信頼性のモデル化）

【著者名】 F. Machida

【掲載誌】 *IEEE Transactions on Emerging Topics in Computing*

【掲載日】 2023 年 10 月 12 日

【DOI】 10.1109/TETC.2023.3322563

問合わせ先

【研究に関すること】
町田 文雄（まちだ　ふみお）
筑波大学システム情報系　准教授
URL: https://www.sd.cs.tsukuba.ac.jp/

【取材・報道に関すること】
筑波大学広報局
TEL: 029-853-2040
E-mail: kohositu@un.tsukuba.ac.jp