

Contrat doctoral – ED Galilée

Titre du sujet : Apprentissage fédéré et interprétable par analyse topologique : Méthodes et applications à la biologie computationnelle

- Unité de recherche : LAGA UMR 7539
- Discipline : Mathématiques
- Direction de thèse : Ian Morilla, Grégory Ginot (LAGA), Géraldine Falgarone (MASCOT)
- Contact : Université Sorbonne Paris Nord, 99, avenue Jean-Baptiste Clément,
Villetaneuse, 93430, ginot@math.univ-paris13.fr
- Domaine de recherche : Mathématiques appliquées à la biologie
- Mots clés : Analyse topologique de données, biologie computationnelle

Titre de la thèse

Apprentissage fédéré et interprétable par analyse topologique : Méthodes et applications à la biologie computationnelle

Contexte et problématique

Les modèles d'apprentissage automatique, en particulier les réseaux de neurones profonds, souffrent d'un manque d'interprétabilité, ce qui limite leur utilisation dans des domaines critiques comme la santé [1]. Parallèlement, l'apprentissage fédéré (FL), bien que prometteur pour le traitement distribué et confidentiel des données, présente des défis majeurs : hétérogénéité des données (non-IID), vulnérabilités aux attaques, et absence de transparence [2, 3, 4]. Ces limitations freinent son adoption pour des applications médicales où la confiance et la robustesse sont primordiales.

Opportunité scientifique

L'apprentissage topologique offre une approche innovante pour caractériser la structure complexe des modèles et des données [5]. Des outils tels que l'homologie persistante, les diagrammes de persistance, et la géométrie hyperbolique permettent d'extraire des signatures topologiques des représentations internes des réseaux de neurones [6, 7, 8]. Ces signatures ouvrent la voie à des méthodes d'agrégation et d'interprétation inédites en FL, combinant robustesse, confidentialité et transparence [9, 10].

Objectifs de la thèse

- Développer des métriques d'interprétabilité pour les modèles profonds en utilisant des outils de topologie algébrique (homologie persistante, entropie topologique) [5, 6].
- Intégrer des descripteurs topologiques dans les schémas d'apprentissage fédéré pour améliorer la personnalisation et la robustesse des agrégations aux données non-IID (e.g., pondération par distance de Wasserstein) [2, 9].
- Proposer des mécanismes de préservation de la vie privée basés sur des abstractions topologiques des données, plutôt que sur des gradients explicites [10, 11].

Méthodologie

Extraction de signatures topologiques depuis les couches internes des réseaux de neurones (diagrammes de persistance, courbes de Betti, Mapper) [5, 6, 7].

Développement de schémas d'agrégation "topologie-aware" en FL, adaptés à des données hétérogènes et non-IID [4, 9].

Validation sur des données cliniques et multi-omiques fournies par notre collaborateur du site Bobigny (UMR_S942 MASCOT, Hôpital Avicenne), en lien avec les thématiques de l'équipe MBI [4]. Ces données incluent des arbres généalogiques et des profils génétiques uniques, permettant d'étudier la polygénie des maladies chroniques [12, 13].

Résultats attendus

- Métriques et visualisations novatrices pour l'interprétabilité des modèles, fondées sur la topologie [1, 4].
- Méthodes de FL robustes aux biais structurels et aux attaques adversariales, avec des applications en biologie computationnelle et santé [2, 6, 3].
- Outils pour un apprentissage éthique, explicable et respectueux de la vie privée, directement applicables aux données sensibles des partenaires cliniques [6].

Encadrement et collaborations

Cette thèse sera co-dirigée par Ian Morilla (LAGA, équipe MBI, UMR 7539) et Grégory Ginot (LAGA, MBI et TA), en collaboration étroite avec l'équipe MASCOT (UMR_S942) pour l'accès aux données cliniques et l'expertise en biologie computationnelle ainsi comme pour développer des possibles approches multicentriques (Hôpitals de Avicenne, Bichat, ...).

Perspectives

Les résultats de cette thèse pourront être appliqués à la détection précoce de maladies chroniques et à l'identification de profils génétiques à risque [3, 12], contribuant ainsi à une médecine plus personnalisée et préventive. Les avancées méthodologiques en FL interprétable auront également un impact transversal en IA responsable [1, 3, 10].

Références

- [1] Molnar, C. *Interpretable Machine Learning: A Guide for Making Black Box Models Explainable*. 2nd ed., 2022.
- [2] Li, T., Sahu, A.K., Zaheer, M., Sanjabi, M., Talwalkar, A., Smith, V. "Federated Optimization in Heterogeneous Networks". *Proceedings of Machine Learning and Systems (MLSys)*, 2020.
- [3] Truex, S., Baracaldo, N., Anwar, A., Steinke, T., Ludwig, H., Zhang, R., Zhou, Y. "A Hybrid Approach to Privacy-Preserving Federated Learning". *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2021.
- [4] Lundberg, S.M., Lee, S.-I. "A Unified Approach to Interpreting Model Predictions". *Advances in Neural Information Processing Systems (NeurIPS)*, 2017.
- [5] Carlsson, G. "Topology and Data". *Bulletin of the American Mathematical Society*, 46(2):255-308, 2009.
- [6] Rieck, B., Togninalli, M., Bock, C., Moor, M., Horn, M., Gumbsch, T., Borgwardt, K. "Neural Persistence: A Complexity Measure for Deep Neural Networks Using Algebraic Topology". *International Conference on Machine Learning (ICML)*, 2019.
- [7] Moor, M., Horn, M., Rieck, B., Borgwardt, K. "Topological Autoencoders". *International Conference on Machine Learning (ICML)*, 2020.
- [8] Cohen, T., Geiger, M., Koehler, J., Welling, M. "Spherical CNNs". *International Conference on Machine Learning (ICML)*, 2019.
- [9] Hofer, C., Graf, F., Rieck, B., Niethammer, M., Kwitt, R. "Graph Filtration Learning". *International Conference on Artificial Intelligence and Statistics (AISTATS)*, 2021.
- [10] Wainrib, G., Clozel, L. "Local Differential Privacy for Federated Learning: Towards Robust and Interpretable Models". *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2020.
- [11] Kairouz, P., McMahan, H.B., Avent, B., Bellet, A., Bennis, M., Bhagoji, A.N., et al. "Advances and Open Problems in Federated Learning". *Foundations and Trends in Machine Learning*, 14(1-2):1-210, 2021.
- [12] Morilla, I., Chan, P., Caffin, F., et al. "Deep Models of Integrated Multiscale Molecular Data Decipher the Endothelial Cell Response to Ionizing Radiation". *iScience*, 25(1):103685, 2022.
- [13] Gouiaa, F., Tran-Dinh, A., Morilla, I. "Dimensionality Reduction with Topological Data Analysis Enhances Lung Transplantation Risk Prediction". *Computers in Biology and Medicine*, 2023