Research Project - PhD Graduate program - PPGCC - DCC - UFMG

1 Introduction

Recent resarch[13][1][8][10] indicates numerous tensions and synergies between many concepts that surround the Machine Learning literature, including Fairness, Privacy, Accuracy and Interpretability. For instance, there is an inherent tradeoff between Fairness and Accuracy such that, depending on the data distribution, it might be impossible to develop a model that achieves acceptable values for both fairness and accuracy, if we consider some reasonable fairness metrics[22]. Also, there has been some work on introducing Causality concepts into the discussion, for instance, to develop better fairness metrics[20]. It has also been suggested to use interpretable models (as explanations to more complex models) for auditing systems and checking if they are fair, although this might lead to difficulties in differentiating honest from dishonest explanations[28]. This area of research is especially relevant nowadays, given the importance that Machine Learning and Artificial Intelligence systems have: we now have computational systems that are part of processes of making decisions with big impacts on people's lives, for instance, recidivism prediction[6], loan approvals[25], hiring decisions[16], and others.

Our goal is to identify the theoretical relations between fairness, privacy and Quantitative Information Flow (QIF), which is a theoretical framework derived from Information Theory[26] that aims to quantify the flow of information in a way that encompasses more scenarios than classical Information Theory. More specifically, we aim to model Differential Privacy and Local Differential Privacy with the QIF framework, and prove new theoretical results that establish this relation. Afterwards, we aim to explore the relationships between privacy and fairness metrics, with focus on Equal Opportunity Difference, Statistical Disparity and Conditional Statistical Disparity. Finally, causalily concepts (based on Judea Pearl's work[21]) will be explored to provide better mathematical understanding of fairness and privacy in machine learning systems.

2 Theoretical Reference

Causality refers to the study of causal relationships between variables, and how to model and infer causal relationships from the combination of domain knowledge and data[21]. This area of research has matured a lot in the last 50 years, with many different approaches still being developed. Fairness in Machine Learning is concerned with measuring how unfair the results provided by Machine Learning models are to certain groups or individuals[19], and improving how fair the models are[15]. There are tensions between different fairness measures[14][2]. Privacy is concerned with quantifying how much sensitive information leaks

about individuals and methods to avoid this information leakage. In Machine Learning settings, the data collection might be hard for information that is considered very sensitive (for instance, whether or not a person regularly uses illegal drugs) and approaches such as Differential Privacy[9] might improve trust in the data collection. Also, the model itself might allow the identification of individuals and sensitive features, which is not desirable[17]. Accuracy is a metric of how many mistakes the Machine Learning model makes, and there are trade-offs between Accuracy and the other concepts presented[13][22][8]. The area of Interpretability focus on developing Machine Learning models that have human-comprehensible decisions (either directly or to explain the decisions of more complex models), which might be useful when developing these models[24] and also to help experts with domain knowledge decide when to trust the results presented by the models[23]. Quantitative Information Flow is a general theoretical framework for measuring amounts of information, with a focus on privacy applications but, in principle, a broader scope[5].

Previous work extensively explored the relationships between Fairness, Interpretability and Privacy[13]. Other works focus on: relationships between Privacy and Fairness[10], the relationship between Privacy, Fariness and Accuracy[8], the feasibility regions of Accuracy and Fairness metrics[22][1], and Causality-Aware fairness metrics[20]. There are also explorations of the relations between Quantitative Information Flow and Fairness[4].

More specifically to the relation between Differential Privacy and Quantitative Inforamtion Flow, there are important results in the literature. There are works discussing the relations between differential privacy and g-vulnerability, including bounds on g-leakage as a function of the ϵ parameter of differential privacy, and the fact that there is no bound on differential privacy as a function of the g-vulnerability [3]. Also, we have recent work [11] discussing how the ϵ parameter of Differential Privacy is related to max-case g-vulnerability: e^{ϵ} is exactly the multiplicative max-case channel capacity under a fixed prior. This work also discusses many other theoretical results relating g-vulnerability notions with differential privacy. Finally, recent contributions show that it is possible to model the ϵ parameter of local differential privacy with the Quantitative Information Flow framework [12], and thus show the viability of our pursuit of modeling (ϵ, δ)-LDP and Differential Privacy.

3 Methodology

This work aims to explore the intersection of Information Theory (by the lens of Quantitative Information Flow), Privacy, and Fairness in Machine Learning. The primary goal is to investigate how these concepts can be effectively integrated and applied to ensure that machine learning models are transparent, robust, and fair, while maintaining the privacy of sensitive data.

First, we will conduct a comprehensive literature review to identify what is currently known and unkown about the relationship between the concepts of privacy, fairness and information flow in machine learning systems. The review will aim to highlight gaps in existing theoretical frameworks, particularly in terms of guarantees provided by common fairness and privacy metrics and notions.

Next, we will explore novel theoretical relationships among these areas. We are particularly interested in modeling the concept of $(\epsilon, \delta)-$Local Differential Privacy from the perspec-

tive of Quantitative Information Flow, as both the Differential Privacy and the Quantitative Information Flow frameworks propose methods of quantifying privacy, and there are already methods of modeling $\epsilon - LDP$ in the literature[11].

Additionally, we will explore the fundamental theoretical relationships between fairness and privacy, obtaining, for instance, the exact trade-offs between privacy and fairness constraints. The focus will be theoretical: by rigorous mathematical reasoning we aim to prove theorems that establish these relationships. We will also experiment with machine learning models trained on real-world datasets, testing empirically various privacy and fairness trade-offs, and identifying patterns that could lead to more robust theoretical results.

Finally, through the exploration of causality notions[21], we aim to provide new insights into the meaning of different quantitative notions of information flow, privacy, fairness, and of their relations, ultimately contributing to the creation of more transparent, accountable, and ethical AI systems.

3.1 Tasks

The project can be organized into the following tasks:

1. **Task 1: Formalization of Local Differential Privacy using concepts from the QIF framework.**

   The first step is to formalize the Local Differential Privacy scenario and definitions, including ϵ and δ parameters, as limitations in information leakage on Information-Theoretical Channels according to specific g-vulnerabilities. Previous work in the literature[11] already modeled the ϵ parameter by using alternative axioms in QIF, which points to the possibility of modeling also the δ parameter.

2. **Task 2: Obtain theoretical and empirical trade-offs between privacy and fairness using causal notions.**

   Recent research in the literature indicates trade-offs between fairness and privacy in machine learning[7][18], but most work focus on the tension between classical fairness and privacy metrics, instead of utilising causal fairness[20] and privacy[27] notions, which we aim to do. Also, we will search for real-world examples and execute simulations of plausible examples to illustrate this tension and what it means in practice.

3. **Task 3: Model differentially-private data obfuscation when variables have different sensibility and utility values.**

   One approach to improve user privacy in Machine Learning is to obfuscate (add randomized noise) to the data, such as in Local differential Privacy mechanisms. But in many practical scenarios the data points are composed of many variables, and not all are sensitive or useful. So, we aim to verify the feasibility of applying noise in a way that reduces the privacy violation while preserving utility as much as possible. This is one of the main goals of the QIF framework, so the results of Task 1 might be useful at this point, and causal notions verified at Task 2 can be used to model the utility of variables.

4. **Task 4: Search for practical scenarios where the results obtained can be applied.**

   After the exploration of the concepts of the previous tasks, we will search for real-world scenarios in which the results obtained can be applied, and verify if they improve the analysis and results obtained, when compared to current solutions. This includes not only Machine Learning models currently in use in industry, but also general statistical research, which might be used for business or governamental decisions.

4 Course plan

In this section we describe the course plan to fulfill the requirements for obtaining the PhD degree, listing the courses to be taken. The publication of at least two papers on the project and participation in conferences are also expected.

1. Information Theory
2. Project and Analysis of Algorithms
3. Teaching Internship I
4. Teaching Internship II
5. Cyberscurity
6. Algebraic Combinatorics
7. Deep Learning
8. Statistical Foundations of Data Science
9. Measure Theory

5 Cronogram

1. 2025/1:
   (a) Literature review.
   (b) Formalization of Local Differential Privacy using concepts from the QIF framework (Task 1).
   (c) Coursework: Information Theory, Project and Analysis of Algorithms, Cyberscurity.
2. 2025/2:
   (a) Literature review.

(b) Formalization of Local Differential Privacy using concepts from the QIF framework (Task 1).

(c) Coursework: Deep Learning, Statistical Foundations of Data Science, Teaching Internship I.

3. 2026/1:

   (a) Literature review.

   (b) Finish Task 1.

   (c) Coursework: Algebraic Combinatorics, Measure Theory, Teaching Internship II.

4. 2026/2:

   (a) Start writing first paper on obtained results.

   (b) Obtain theoretical and empirical trade-offs between privacy and fairness using causal notions (Task 2)

   (c) Prepare and defend the dissertation proposal.

5. 2027/1:

   (a) Finish Task 2.

   (b) Submit first paper on obtained results.

   (c) Model differentially-private data obfuscation when variables have different sensibility and utility values (Task 3).

6. 2027/2:

   (a) Finish Task 3

   (b) Start writing second paper on obtained results.

7. 2028/1:

   (a) Search for practical scenarios where the results obtained can be applied (Task 4)

   (b) Start writing the final dissertation.

   (c) Submit the second paper on the obtained results

8. 2028/2:

   (a) Finish Task 4

   (b) Defend the dissertation.

Bibliography

[1] Agarwal, A., Beygelzimer, A., Dudik, M., Langford, J., Wallach, H.: A reductions approach to fair classification. In: Dy, J., Krause, A. (eds.) Proceedings of the 35th International Conference on Machine Learning. Proceedings of Machine Learning Research, vol. 80, pp. 60–69. PMLR (10–15 Jul 2018), https://proceedings.mlr.press/v80/agarwal18a.html

[2] Alves, G., Bernier, F., Couceiro, M., Makhlouf, K., Palamidessi, C., Zhioua, S.: Survey on fairness notions and related tensions. EURO Journal on Decision Processes **11**, 100033 (2023). https://doi.org/https://doi.org/10.1016/j.ejdp.2023.100033, https://www.sciencedirect.com/science/article/pii/S2193943823000067

[3] Alvim, M.S., Andrés, M.E., Chatzikokolakis, K., Degano, P., Palamidessi, C.: On the information leakage of differentially-private mechanisms. Journal of Computer Security **23**(4), 427–469 (2015)

[4] Alvim, M., Fernandes, N., Nogueira, B., Palamidessi, C., Silva, T.: On the duality of privacy and fairness (extended abstract). In: International Conference on AI and the Digital Economy (CADE 2023). Institution of Engineering and Technology, United Kingdom (2023). https://doi.org/10.1049/icp.2023.2563, 9th International Conference on AI and the Digital Economy, CADE 2023 ; Conference date: 26-06-2023 Through 28-06-2023

[5] Alvim, M., Chatzikokolakis, K., McIver, A., Morgan, C., Palamidessi, C., Smith, G.: The Science of Quantitative Information Flow. Information Security and Cryptography, Springer International Publishing (2020), https://books.google.com.br/books?id=jJH-DwAAQBAJ

[6] Angwin, J., Larson, J., Mattu, S., Kirchner, L.: Machine bias: There's software used across the country to predict future criminals. and it's biased against blacks. URL https://www. propublica. org/article/machine-bias-risk-assessments-in-criminal-sentencing (2019)

[7] Arcolezi, H.H., Makhlouf, K., Palamidessi, C.: (local) differential privacy has no disparate impact on fairness. In: IFIP Annual Conference on Data and Applications Security and Privacy. pp. 3–21. Springer (2023)

[8] Cummings, R., Gupta, V., Kimpara, D., Morgenstern, J.: On the compatibility of privacy and fairness. In: Adjunct Publication of the 27th Conference on User Modeling, Adaptation and Personalization. p. 309–315. UMAP'19 Adjunct, Association for Computing Machinery, New York, NY, USA (2019). https://doi.org/10.1145/3314183.3323847, https://doi.org/10.1145/3314183.3323847

[9] Dwork, C.: Differential privacy. In: International colloquium on automata, languages, and programming. pp. 1–12. Springer (2006)

[10] Dwork, C., Hardt, M., Pitassi, T., Reingold, O., Zemel, R.: Fairness through awareness. In: Proceedings of the 3rd Innovations in Theoretical Computer Science Conference. p. 214–226. ITCS '12, Association for Computing Machinery, New York, NY, USA (2012). https://doi.org/10.1145/2090236.2090255, https://doi.org/10.1145/2090236.2090255

[11] Fernandes, N., McIver, A., Sadeghi, P.: Explaining epsilon in local differential privacy through the lens of quantitative information flow. arXiv preprint arXiv:2210.12916 (2022)

[12] Fernandes, N., McIver, A., Sadeghi, P.: Explaining epsilon in local differential privacy through the lens of quantitative information flow. In: 2024 IEEE 37th Computer Security Foundations Symposium (CSF). pp. 419–432. IEEE (2024)

[13] Ferry, J., Aïvodji, U., Gambs, S., Huguet, M.J., Siala, M.: Sok: Taming the triangle - on the interplays between fairness, interpretability and privacy in machine learning. ArXiv **abs/2312.16191** (2023), https://api.semanticscholar.org/CorpusID:266573131

[14] Friedler, S.A., Scheidegger, C., Venkatasubramanian, S.: The (im)possibility of fairness: different value systems require different mechanisms for fair decision making. Commun. ACM **64**(4), 136–143 (mar 2021). https://doi.org/10.1145/3433949, https://doi.org/10.1145/3433949

[15] Holstein, K., Wortman Vaughan, J., Daumé III, H., Dudik, M., Wallach, H.: Improving fairness in machine learning systems: What do industry practitioners need? In: Proceedings of the 2019 CHI conference on human factors in computing systems. pp. 1–16 (2019)

[16] Li, L., Lassiter, T., Oh, J., Lee, M.K.: Algorithmic hiring in practice: Recruiter and hr professional's perspectives on ai use in hiring. In: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society. pp. 166–176 (2021)

[17] Liu, B., Ding, M., Shaham, S., Rahayu, W., Farokhi, F., Lin, Z.: When machine learning meets privacy: A survey and outlook. ACM Computing Surveys (CSUR) **54**(2), 1–36 (2021)

[18] Makhlouf, K., Arcolezi, H.H., Zhioua, S., Brahim, G.B., Palamidessi, C.: On the impact of multi-dimensional local differential privacy on fairness. Data Mining and Knowledge Discovery pp. 1–24 (2024)

[19] Makhlouf, K., Zhioua, S., Palamidessi, C.: On the applicability of machine learning fairness notions. SIGKDD Explor. Newsl. **23**(1), 14–23 (may 2021). https://doi.org/10.1145/3468507.3468511, https://doi.org/10.1145/3468507.3468511

[20] Makhlouf, K., Zhioua, S., Palamidessi, C.: Survey on causal-based machine learning fairness notions (2022)

[21] Pearl, J.: Causality: Models, Reasoning and Inference. Cambridge University Press, USA, 2nd edn. (2009)

[22] Pinzón, C., Palamidessi, C., Piantanida, P., Valencia, F.: On the incompatibility of accuracy and equal opportunity. Machine Learning (May 2023). https://doi.org/10.1007/s10994-023-06331-y, https://doi.org/10.1007/s10994-023-06331-y

[23] Roscher, R., Bohn, B., Duarte, M.F., Garcke, J.: Explainable machine learning for scientific insights and discoveries. Ieee Access **8**, 42200–42216 (2020)

[24] Santos, G., Figueiredo, E., Veloso, A., Viggiato, M., Ziviani, N.: Predicting software defects with explainable machine learning. In: Proceedings of the XIX Brazilian Symposium on Software Quality. pp. 1–10 (2020)

[25] Sheikh, M.A., Goel, A.K., Kumar, T.: An approach for prediction of loan approval using machine learning algorithm. In: 2020 international conference on electronics and sustainable communication systems (ICESC). pp. 490–494. IEEE (2020)

[26] Smith, G.: On the foundations of quantitative information flow. In: International Conference on Foundations of Software Science and Computational Structures. pp. 288–302. Springer (2009)

[27] Tschantz, M.C., Sen, S., Datta, A.: Sok: Differential privacy as a causal property. In: 2020 IEEE Symposium on Security and Privacy (SP). pp. 354–371. IEEE (2020)

[28] Zhou, J., Joachims, T.: How to explain and justify almost any decision: Potential pitfalls for accountability in ai decision-making. In: Proceedings of the 2023 ACM Conference on Fairness, Accountability, and Transparency. p. 12–21. FAccT '23, Association for Computing Machinery, New York, NY, USA (2023). https://doi.org/10.1145/3593013.3593972, https://doi.org/10.1145/3593013.3593972