Statement of Goals and Objectives

Ferdinando Fioretto
November, 2022

Overview. This document is organized as follows. Section 1 describes my current research, its impact, and planned mid-term future work. Section 2 details my teaching impact and planned objectives. Finally, Section 3 describes my diversity and inclusions activities and planned avenues.

1 Research Activities and Objectives

My work makes advances in foundational Artificial Intelligence (AI) research at the juncture of Machine Learning (ML), optimization, privacy, and ethics. Most of my research to date has focuses on two key areas:

AI for decision-making. It develops the foundations to blend deep learning and combinatorial optimization to serve the resolution of complex decision tasks and creates novel ways to integrate knowledge, constraints, and physical principles into learning models (see Section 1.1).

AI and society (with focus on privacy and equity). It analyzes the equity of AI systems in support of decision-making and learning tasks, and it designs practical algorithms to make AI systems more aligned with societal values, focusing especially on privacy and fairness (see Section 1.2).

My most significant contribution to the integration of optimization and learning has been the development of primal-dual surrogates to enable ML models to handle constraints and physical principles. These models have been used to approximate complex, NP-hard, optimization problems at extremely fast timescales. They have found applications in power systems, scheduling, and simulation tools and have a potentially transformative impact for scientific ML applications. My most significant contribution to the intersection of privacy and equity has been to develop novel theory to analyze and quantify the disparate impacts of differential privacy in key decision-making problems. These include funding allocations and distribution of benefits which affect hundreds of millions of people in the US alone.

For these contributions, my research has been recognized with the 2022 *Caspar Bowden PET Award*, the *IJCAI-22 Early Career Spotlight*, the *AI*AI Best AI dissertation award*, and several best papers awards. I am also the recipient of the 2022 *NSF CAREER award*, the 2022 *Amazon Research Award*, the 2022 *Google Research Scholar Award*, the 2021 *ISSNAF Young Investigator Award*, and the 2021 *ACP Early Career Researcher Award* (see my CV for more details).

1.1 AI for Decision-Making: Integrating Machine Learning and Optimization

Constrained optimization has made a profound impact in industrial and societal applications in numerous fields, including transportation, supply chains, energy, scheduling, and the allocation of critical resources. Despite their complexity these problems are solved routinely and the AI and Operations Research communities have devised a wide spectrum of techniques and algorithms to effectively leverage the problem structure. While these developments have made possible the deployment of constrained optimization solutions in many real-world contexts, the complexity of these problems often prevents them to be adopted in contexts of repeated (e.g., involving expensive simulations, multi-year planning studies) or real-time nature, or when they depend in nontrivial ways on empirical data. Yet, in many practical cases, one is interested in solving problem instances sharing similar patterns. Therefore, machine learning methods appear to be a natural candidate to aid constrained optimization decisions and have recently gained traction in the nascent area at the intersection between constrained optimization and machine learning [BLP20, KFVW21, VSPRB20].

However, ML systems present a fundamental challenge: while deep learning has proven its power for unconstrained problem settings, it has struggled to perform as well in domains where it is necessary to satisfy hard constraints, domain knowledge, or physical principles (system dynamics, conservation laws). For example, in power systems, materials science, fluid dynamics, and many other areas, the data follows well-known physical laws, and violation of these laws can lead to unreliable and unusable approximations. *There is thus a need to provide deep learning architectures with capabilities that would allow them to capture constraints and physical principles directly*.

Overview of my contributions. My research addresses this limitation and develops constraint-aware ML models that predict solutions to constrained optimization problems end-to-end. Such models can also enforce structure in the outputs of learned embedding and can have a transformative impact in many engineering and scientific applications.

1.1.1 Key result: Learning surrogate constrained optimization

My research shows that it is possible to *integrate key constrained optimization principles within the training cycle of deep learning models to endow ML methods with the capability of handling constraints and physical principles*.

Knowledge aware constrained optimization learning. In particular, I have presented the theoretical foundations to integrate Lagrangian duality in deep learning models to obtain constraint- and knowledge-aware predictors [FHM$^+$20]. The proposed framework exploits a gradient-based primal-dual procedure for training neural networks and was used to obtain, among other applications, state-of-the-art surrogate solvers to predict AC optimal power flows in energy systems and optimal compressor selection in gas networks [FMV20b, CFMV20, MFV21], two notoriously hard nonlinear nonconvex optimization problems. These predictors were shown to produce, in just a few milliseconds, highly accurate approximations with negligible constraint violations.

In [CFMV20], I have also combined these techniques with projection operators that are trained end-to-end to ensure that the solutions found by a neural network are satisfiable at test time. These results have opened a new avenue to approximate hard optimization problems and have stimulated a number of follow-up work, including exploiting Lagrangian decompositions to scale up to massive problems [CMH22, MCTH22], Benders' decomposition to accommodate discrete decisions [VVH21], and are becoming an important tool, especially for energy applications with profound effects on climate impact [RDK$^+$22].

Besides the vastly reduced computational complexity, a byproduct of enforcing knowledge in ML-based predictors is to improve the accuracy and interpretability of the resulting models while simultaneously reducing the amount of data required for model training. For example, in [FHM$^+$20] I have shown how enforcing relations between subsets of inputs and outputs allows training accurate models for transprecision computing using vastly reduced training datasets. This is especially important for scientific ML applications, where data collection is often noisy, error-prone, and expensive. Finally, my work also shows how the integration of machine learning and optimization can be used to enforce fairness constraints on predictors and obtain state-of-the-art results when minimizing disparate treatments [FHM$^+$20]. This technique is now commonly adopted and can be used in combination with differential privacy (see Section 1.2) to achieve a privacy-preserving deep learning algorithm that also encourages the satisfaction of a variety of fairness constraints [TFH21], as well as network compression [TFKN22], or pruning [KFS22].

Handling discrete domains. While learning over discrete structures poses a set of additional challenges for differentiability,[1] when combined with specialized architectures, the techniques reviewed above can be used to guarantee the satisfaction of a class of constraints (such as orderings). I have used them to produce orders of magnitude speedups over job shop scheduling problems when compared to state-of-the-art commercial solvers [KFV22]. Motivated by these key results, I have also proposed a unique integration of constrained optimization programs within a deep

[1] This, itself is also a topic of my current research.

learning pipeline which is trained end-to-end to produce optimal solutions in the context of fair learning to rank tasks [KFVZ22]. The task consists in learning a mapping between a list of items and a permutation of such list, which defines the order in which the items should be ranked in response to a user query while enforcing some desired notion of group fairness over rankings. Crucially, this integration allows providing certificates on the fairness constraints required. In addition, this method enables the modeler to enforce knowledge that can be formulated as linear constraints over discrete structures and is shown to significantly improve current state-of-the-art fair learning-to-rank systems concerning established performance metrics. My ongoing work applies this idea to several other consequential domains where *guaranteeing* fairness is crucial, including in various natural language processing tasks.

Data generation in constrained deep learning. In all these studies, the ML optimization surrogates are assumed to have access to supervision labels that can guide the construction of the solutions to target problems. However, when these labels are themselves approximations, when the optimization problem has symmetric solutions, and/or when the optimization solver uses randomization, solutions to closely related instances may exhibit large differences and the learning task can become inherently more difficult. In [KFVH21], I have analyzed this critical challenge, connecting the volatility of the training data to the ability of a model with a given capacity to approximate it. In addition to the theoretical analysis, which sheds light on when and why precise approximations can be constructed, I have proposed a method for producing (exact or approximate) labels that are amenable to supervising learning tasks accurately. This method has enabled learning targeted constrained optimization problems with discrete decisions at unprecedented levels of accuracy [KFVH21, KFV22].

Integrating Digital Twins. Finally, some of my ongoing work focuses on integrating digital twins within learned optimization surrogates to capture the optimality of the decision within the prescribed system's dynamics. For example, in [MBF22], I have also shown how one can integrate the physical principles regulating energy generators' dynamics directly into a learned optimization surrogate. This unique solution allows to obtain surrogates that are not only computationally efficient but also ensure that decisions capture the stability within power systems operations. These techniques have the potential to improve both problems relying on optimization and those relying on traditional numerical simulators and can be truly transformative in many engineering and scientific ML domains.

Research Impact. My research on the integration of constrained optimization and learning holds the promise to provide a new and transformative generation of optimization tools that will directly address the computational burden due to the need of solving hard optimization problems under stringent time constraints. These contributions have been the backbone for some prestigious awards, including the *2022 NSF CAREER Award*, the *IJCAI 2022 Early Career Spotlight*, the *2021 ACP Early Career Research Award* assigned by the Association of Constraint Programing, and the *2021 Mario Gerla Young Investigator Award* assigned by ISSNAF. This line of work is also partially supported by an NSF RI grant (2020–2023).

1.1.2 Moving Forward

Despite the encouraging results I reviewed above a number of challenges remain that must be addressed to allow an integration of constrained optimization with end-to-end machine learning that lives up to its full potential. Below, I discuss some of these challenges and outline a research agenda making both theoretical and practical advances to address them.

Integrating optimization layers in ML pipelines. Despite the variety of approaches, the success of integrating an optimization solver within a ML model in the loop has been demonstrated on a relatively limited set of optimization problems and, focusing mostly on linear programming formulations. Challenges posed by the parametrization of constraints stand in the way of broader applications. In [KFVW21] I compiled the first comprehensive survey of the existing techniques for differentiation through various classes of optimization problems. Differentiation of constrained

optimization problems is most straightforward when the problem is convex. For example, in the case of quadratic programs, the KKT conditions for optimality are well-posed, differentiable, and yield a linear system which can be efficiently solved for derivatives [AK17]. However, these theories fall short when an ML pipeline is to be integrated with general non-convex problems. Our ongoing work utilizes techniques for differentiation of second-order programs, in order to derive efficient hybrid automatic-analytic differentiable solvers based on well-known algorithms that apply to both convex and non-convex problems. *This promising direction will allow us to integrate for the first time nonconvex optimizers in ML pipeline to enhance both ML expressivity and its ability to be used in constrained optimization and control with an impact in many engineering areas.*

Additionally, issues associated with the runtime of combinatorial solvers in-the-loop still make some potential applications impractical. I plan to tackle this challenge by combining dual decomposition techniques with the learning pipelines. In power systems, for instance, there is a regional organization in which components at the sub-region level are operated by different transmission system operators. In scheduling, different subproblems are created by grouping tasks based on their order in their jobs. Each subproblem can be solved independently with a learning pipeline managing the additional constraints to couple the connected subproblems. Results in power systems show how one can scale the learning to optimize to country-size systems [CMH22].

Knowledge transfer and training data. The problem of training a model on a problem data and then refining it based on specialized data and settings is central to scientific ML and is also an avenue of development for the end-to-end constrained optimization learning. A critical shortcoming arising in current methods when predicting solutions to constrained optimization problems, is their inability to robustly generalize. My future work will focus on targeting this challenge exploiting various forms of transfer learning. For example, learning a surrogate optimization model that uses Lagrangian duality has the effect of approximating the values of the associated dual variables. These provide some statistical quantification of the degree of constraint violations on the training data, and, in turn, can be used to warmstart the training of a different surrogate optimization model to learn solutions to a new problem. The procedure may be an effective method to transfer the acquired knowledge from a source problem to a target one that exhibits some similarity in constraint sub-structure.

In addition to the difficulty of handling knowledge transfer, another challenge for constrained deep learning is the need to generate large and high-fidelity datasets, which consist of solutions to hard optimization problems themselves. This challenge may be partially addressed by adapting self-supervised approaches. This direction also calls for the development of new theoretical understanding on the classes of optimization problems that can be approximated via a learning surrogate and their performance.

Scientific-ML and digital twins. Next, I believe that the next frontier in the integration of optimization principles within ML pipelines relies in understanding how one can integrate digital twins within an optimization surrogate to make decisions which are both quick and can satisfy the systems' dynamics. While I made initial advances toward this endeavor [MBF22], much needs to be done to address scalability challenges arising from the complexity of the problem, to provide robustness guarantees of the resulting solutions, and to render the systems explainable. My future work will focus on the development of theoretically grounded frameworks to address these challenges.

Additional future work. Finally, I am also interested in studying the applicability of my solutions to generate counterfactual explanations which require the resolution of sophisticated optimization problems. This need arises, for instance, in energy systems, supply chains, material science, and many scientific ML applications where there is a requirement to explore several scenarios to answer "what if" questions. As solving many NP-hard decision problems is computationally prohibitive, we often settle for suboptimialities (e.g., a small subset of possible scenarios) or approximations (computationally viable approximated versions of the decision problem) resulting in potential high societal and economic costs. The application of ML surrogates in these contexts may be transformative. I am currently collaborating both with academic and industrial

partners to tackle some challenging problems at the junction of optimization and ML in applications domains including smart agriculture, energy systems, and chemical engineering with an impact on climate crises and beyond. I strongly believe that the integration between combinatorial optimization and machine learning is a promising direction for the development of new, transformative, tools in decision-making and learning.

1.2 AI and Society: Privacy and Equity in ML and Decision-Making

Data-driven AI systems have become instrumental for decision-making and policy operations involving individuals: they include assistance in legal decisions, lending, hiring, as well as determinations of resources and benefits, all of which have profound social and economic impacts. However, the use of rich datasets, combined with the adoption of black-box algorithms, has sparked concerns about how these systems operate. *How much information these systems leak about the individuals whose data is used as input and how they handle biases and discrimination are two critical concerns.*

Since its conception, *differential privacy (DP)* [DMNS06] has become an important privacy-enhancing technology for private analysis tasks. Several private companies and federal agencies are rapidly developing their implementations of DP, including the notable adoption by the US Census Bureau for their 2020 release [Abo18]. DP is appealing as it bounds the risks of disclosing sensitive information for individuals participating in a computation. However, to ensure privacy, a DP algorithm introduces calibrated perturbations, which inevitably introduce errors to the outputs of the task at hand. More importantly, these errors may have disparate impacts on different groups of individuals. The resulting societal and economic impacts are significant: classification errors may penalize some groups over others in important determinations, including criminal assessment, landing, and hiring, or can result in disparities regarding the allocation of critical funds, benefits, and therapeutics [PMK+20]. While these observations have become apparent, a complete understanding of why they arise has been limited.

Overview of my contributions. My research addresses this critical knowledge gap at the interface of privacy, fairness, and decision processes and is articulated into two research categories:

1. *Understanding and characterizing the impact of privacy on the equity of downstream decision-making and learning tasks* (see Section 1.2.1), and
2. *Designing accurate and efficient privacy-preserving algorithms for foundational problems in decision-making and machine learning* (see Section 1.2.2).

1.2.1 Key Result: On the Equity of Privacy-Preserving Models

My research showed for the first time that there is an *inherent fairness cost in privacy-preserving downstream decision-making and learning tasks*. For context, Bagdasaryan et al. [BPS19] experimentally showed that a DP learning model disproportionatelly affects the accuracy of the minority group, and Pujol et al. [PMK+20] report similar observations in tasks that use census data. I have shown that these costs cannot be avoided in general and provided the first analysis on the bias and fairness issues arising when differentially private data is used as input to several resource allocation problems [TFVY21, ZVF21, ZFV22] and learning tasks [TDF21, TFVY21, TDBF21].

Fairness of DP data-release tasks. Typical DP data-release tasks consist of two steps: (1) Generating a noisy, private, counterpart of the original data and (2) post-processing it to satisfy the desired data-independent constraints. This two-step approach is ubiquitous and adopted, among others, by the US Census Bureau for their 2020 data release. Therein, the constraints restrict the outputs to non-negative integers as well as to satisfy some geographical and publicly known invariants. Once post-processed, the released data are often used to make important policy decisions. For example, US census data users rely on the decennial census data to apportion the 435 congressional seats, allocate the $1.5 trillion budget, and distribute critical resources to states and jurisdictions.

In this context, I have shown that the "shape" of the downstream decision problem is key to characterizing the disparity in errors induced by a data release DP mechanism on the final decisions. In particular, in [TFVY21] I have shown that it is the non-linear nature of the decision problem itself to exacerbate the disparity in errors among different sub-populations when private data is used as input to these decision problems. This is true even if the added noise is unbiased and post-processing is absent. Practically, I have shown how these errors translate into sizable misallocations in funds to school districts based on current Census data release and how they may negatively impact voting benefits. To counteract this negative result, I have also examined the conditions under which decision-making is fair when using differential privacy and devised techniques to bound unfairness. Finally, I have proposed a number of mitigation approaches to alleviate the biases introduced by differential privacy on key decision problems [FTVZ22], including using an integration of optimization and learning, as discussed in Section 1.1 [TFH21].

In addition to analyzing the decision problem shape, I have shown that post-processing can have strong consequences on the fairness of the downstream decision problems [TFVY21, ZFV22]. Motivated by census applications, which enforce linear constraints on the released data, I have studied the behavior of a common class of post-processing functions called projections. I have showed that non-negativity constraints, or, more generally, box constraints, are responsible for the creation of the observed bias and have presented a tight upper bound on such bias. Importantly, this analysis provides some insights on the type of problems for which the bias and unfairness will be significant [TFVY21] and instructs how to create possible mitigating strategies, as those I have recently explored in [ZFV22].

Fairness of DP learning tasks. The analysis reviewed above also motivated me to study when and why unfairness arises in differential privacy learning tasks, including in supervised [TDF21] and semi-supervised contexts [TDBF21]. These studies report the first analysis of the disproportionate effects of differential privacy in privacy-preserving deep learning algorithms and pinpoint the sources of these negative effects. In particular, I have shown that in DP-SGD—the de-facto standard DP algorithm used to train deep learning models—properties of the training data, including input norms and the trace of the loss Hessian computed on the protected groups, are key characteristics connected with exacerbating the disparate errors observed. The trace of the loss Hessian, in particular, is often adopted as a proxy metric for model flatness and when different groups are associated with different flat regions their test error differences are exacerbated due to privacy. In a further analysis I have shown that algorithms properties (e.g., the clipping and noise addition adopted in DP-SGD) are crucial to explain why unfairness arises [TDF21]. Clipping, for example, is an important component of DP-SGD and is used to bound the maximal gradient norm of a data sample in each training epoch. When different groups of individuals produce updates with large differences in magnitude or directions of gradients norms, and when such values exceed the clipping bound, gradient clipping induces dissimilar information losses in these groups, thus penalizing those groups with larger gradients [TDF21, TFKN22].

Research impact. An important conclusion of these results is that using private inputs to make ordinary policy determinations will necessarily introduce fairness issues, even when the noise introduced is unbiased. Understanding these biases is especially important given the high stakes of the resulting policy decisions. Currently, I am using these results to inform (and collaborate with) companies and NGOs whose customers are data users and policymakers who work intensively with census and public safety data. For these results, my work was awarded the prestigious *Caspar Bowden PET Award* (in 2022) and constitute the backbone for a *Google scholar research award* (in 2022) and an AWS Amazon Research Award (starting in 2023). This line of work is also partially supported by an NSF SaTC grant (2021–2024).

1.2.2 The Privacy-Fidelity Tradeoff

As hinted in the previous section, preserving invariants and/or task-specific constraints is an important property for the release of high-fidelity privacy-preserving data. Consider the release

of socio-demographic features of a population organized hierarchically by census blocks, counties, and states, as common for census data. Releasing differentially private hierarchical statistics can be achieved by perturbing counts with noise scaled by the number of levels of the hierarchy. This approach, however, does not guarantee hierarchical invariants. For example, with a high probability, the sum of noisy counts at the county level will not equal the noisy count at the corresponding state level. Additionally, the private noisy counts may not satisfy the integrality and non-negativity constraints satisfied by the ground truth data.

My work has focused on overcoming this well-documented limitation while providing accuracy guarantees and efficiency on the resulting DP releases. The central idea relies on casting the problem of privately releasing a dataset as a *constraint optimization problem* that redistributes the noise introduced by a DP algorithm while ensuring consistency of various constraints [FV19a, FMV20a]. The optimization problem that redistributes noise optimally is however intractable for datasets involving hundreds of millions of individuals. Even its convex relaxation is challenging computationally. Thus, in [FVZ21], I have proposed a mechanism that exploits both the problem's (hierarchical) nature and the objective function's structure, yielding a polynomial time solution. In addition to retaining data invariant properties exactly over integers, this solution brings orders of magnitude improvements over state-of-the-art methods and has been tested over massive datasets sizes.

Similarly, in the context of energy systems, releasing high-fidelity test cases is crucial to support the design of effective algorithms aimed at improving energy operations. However, releasing these test cases is a delicate task as they contain sensitive customer information. I have shown that when standard DP methods are used to protect these data, the associated energy optimization problems may produce results that are fundamentally different from those obtained on the original data and even reveal severe feasibility issues [FV18]. To address these issues, in [MFSV20], I have proposed a mechanism that casts the production of privacy-preserving test cases as a bilevel optimization problem. Its goal is to redistribute the noise introduced by a randomized mechanism to guarantee the existence of accurate and feasible solutions to key energy optimization problems that take as input private data. The computational challenges of the bilevel optimization were addressed by exploiting efficient decompositions. Besides the desirable privacy properties, these mechanisms can produce feasible solutions for the target energy problems and are a constant factor away from optimality. These mechanisms have been used to release privacy-preserving test cases on the largest collection of AC optimal power flow benchmarks available.

In addition to releasing privacy-preserving census and energy datasets, these constrained optimization-based DP approaches have also been used to train models on private demands for a city-level multi-modal transportation system [FLV18], to design federated data-sharing schemes [FV19c], to construct private and fair classifier [TFV21], to produce private solutions of Stackelberg games [FMV20c], and to release continuous streams of data [FV19b].

Research Impact. Computational results in energy, transportation, and census applications have shown that these methods improve the accuracy by at least one order of magnitude over existing DP mechanism while ensuring strong privacy protection. Some of these contributions have resulted in prestigious awards, including two Best Paper Awards in the IEEE Transaction of Power System journal ([MFSV20] and [DFVH$^+$21]), which were selected among all papers published in 2018–2020 and 2019–2021, respectively, an invited journal track IJCAI paper [FV19b], and the techniques based on this research resulted in an award at the 2020 NIST DP Temporal Map Challenge [NIS20]. These results have also produced substantial followup research showing that constrained-based mechanisms are an important tool to release sensitive datasets for statistical analysis, competitions, and benchmarking.

1.2.3 Moving Forward

My agenda on privacy and equity of AI systems is rich. In the near future, I am particularly interested in studying generalization and extensions of the fairness analysis discussed above when considering other impactful areas for AI systems and machine learning.

Characterizing the disparate impacts of constrained ML systems. While machine learning models are designed to learn an hypothesis that best approximates a mapping from the available data to their labels, the resulting models are rarely deployed as is. They are often required to satisfy context- or application-specific restrictions. Examples include: privacy, robustness, and model size. By restricting the space of possible hypotheses to learn, however, the resulting models may introduce unintended disparate impacts. While my previous research has shown this effect on private ML models, I have recently shown that model pruning—a technique used to render neural networks storage and computations more efficient by removing parameters carrying seemingly low information—may have disparate impacts on different subpopulations in classification learning tasks [TFKN22]. I have shown that both model parameters (Hessians loss and gradient flow) and data characteristics (input norms and distance to decision boundary) are key aspects related with the observed disparate impacts. Studying these effects is important as it allows us to devise effective mitigation strategies, but a complete understanding of why these fairness issues arise in constrained ML settings is missing. *Part of my future efforts will go in addressing this critical knowledge gap at the intersection of fairness and constrained learning systems.*

Notably, while most of my efforts in this scope have focused on the impact of data properties and model parameters to fairness, an ongoing study from my group suggests that ML model architectural choices may also create disparate impacts. In addition to the impact of the model complexity (e.g., the number of parameters and the type of layers) an interesting aspect is the effect of the activation functions on the privacy and fairness of the ML model. The reasons behind these effects are once again greatly understudied and these observations may shed light on the existence of another dimension, in addition to the model and data properties, that may needed to be optimized in fair and private/robust/compressed learning: the choice for a model architecture.

Privacy and equity of decision-making and policy effects. While my current work focuses on the unintended negative impact of privacy to the decision tasks' errors, I also plan to reverse the question and look at the positive effects of DP in relation to the equity of decision-making tasks. I believe this is important as, following the release of the 2010 demonstration products by the US Census Bureau, the reported analysis of errors and equity issues have created a veil of skepticism about the effectiveness of DP among data users. This skepticism can cause other federal agencies to restrict data access, impeding important studies with profound economic and societal effects. I will thus analyze the cost of *data suppression* and the impact on public policy decisions. *In other words, I seek to answer whether no data or partial data suppression would create more inequity than releasing noisy DP statistics.* I plan to study this question both theoretically, by introducing new tools for comparing deterministic suppression algorithms with differentially private ones, and practically, by measuring these effects on census-based applications, leveraging my current collaborations with NGOs and policymakers who work closely with census and public safety data.

Additional future work. I also plan to extend my study at the intersection of privacy and fairness in other classes of decision problems, including redistricting and decision tasks concerned with granting benefits. These are ordinarily adopted policy decision tools with profound societal impacts. The discontinuous nature of these problems will require new tools for the analysis of fairness. Furthermore, the analysis considered so far is also restricted at single data releases. In the same vein as DP allow us to bound the privacy loss resulting from the application of multiple mechanisms to the data, I plan to study compositional results for fairness in decision and learning tasks. I believe these results will open the doors to a new understanding of the interaction between privacy and fairness with potentially transformative broader impacts on decision-making and learning tasks used to inform consequential decisions.

2 Teaching Activities and Objectives

As a teacher and mentor, I know that I have the potential to influence a student's intellectual and career trajectory. I take my role seriously because I want to have a positive impact on my student's future by stimulating their interest while challenging societal stigmas.

2.1 Current Teaching and Mentoring

In my instructor capacity, I have had the opportunity to be exposed to a pool of courses ranging from introductory, to senior undergraduate and graduate-level courses. In particular, I had the opportunity to teach *Introduction to Artificial Intelligence*, a popular undergraduate course, whose assessment relies strongly on a series of projects that help students consolidate the techniques thought in class, an aspect my students consistently praise. I have also developed *Security and Privacy in Machine Learning*, a graduate-level course focusing on some important issues arising when deploying machine learning (ML) systems. These opportunities allowed me to practice my teaching philosophy (see below) both at the group level, during class lectures, and at the individual level, during office hours. *My course evaluations received scores ranging from 4.48 to 4.93 out of 5.0 and a median of 5.0*. Additionally, during my graduate studies, I was also recognized with an *Outstanding TA Award*.

Hands-on mentoring. If I take pride in teaching, mentoring gratifies me even more. Currently I mentor 5 PhD students (among them, two just started their PhD studies) and 2 MS students. My students come from different backgrounds, ethnicities, and genders, and I strive to provide a stimulating, productive, and friendly environment in my lab. I meet with my students daily, we have weekly meetings as a team, we organize outing activities, and reading groups. I feel lucky to be part of what I consider to be a curious and productive group. I have also worked with a large number (>12) of undergraduates who joined my group for summer internships or to work on various projects, including those supported by NSF REU funds. The results of these undergraduate research experiences have been published in top AI conferences, presented in workshops, and led to several prestigious awards, including the 2022 Caspar Bowden PET award, the IEEE best paper award in 2021, and the most visionary paper award in the workshop series at AAMAS. The students I supervised are now pursuing doctoral degrees, working at national laboratories, and working in tech companies. Aside from these remarkably gratifying experiences, I had the chance to learn how to structure a project, break it down into small, achievable landmarks, and best cultivate students' specific attitudes and capabilities.

Outreach to K-12 students and teachers. Besides providing opportunities to engage and mentor undergraduate students in conducting research activities, I have been mentoring high schoolers from a local High school on a variety of data science projects. Additionally, I am designing a summer course on *AI and Optimization* for high school teachers through *Project Advance*[2], one of the largest concurrent enrollment programs in the country with over 200 partner schools. The course makes special emphasis on linking AI and optimization concepts that are relevant to the instructors' class syllabi. The goal is to increase awareness, about the concepts and applications of computing, as well as the societal issues they raise, in the areas of ethics, fairness, and privacy.

2.2 Teaching Philosophy

My teaching philosophy is based on two key concepts: **(1)** combining a deep conceptual understanding of learning by active *engagement and teaching through real-world problems*, and (2) fostering students to question and explore while providing a *psychologically safe environment*.

Active engagement and teaching through the lens of real-world problems. Students learn material best when they feel involved in the class and can actively participate. All classes I have thought so far start late in the afternoon. Often these are the last classes of the day for my students, who are thus tired, and I recognize how important is to have an engaging session while stimulating the students' curiosity. To this end, I often find some real-world examples I can discuss right at the start of the class: *"Welcome back to CS 476! Have you heard the latest in stable diffusion models and how you can do creative art with it?* I then try to connect the story with the daily class topic. *"Do you know what is the foundation of all these learning models? Back-propagation! Aren't you curious to learn how it works?"* I then proceed by walking students step-by-step, often alternating between slides presentation, media content, and short Q&A that tests the student understanding.

[2]Syracuse Project Advance: https://supa.syr.edu/

As a student wrote in my teaching review, *"I really enjoyed this course. You can definitely see the passion that Professor Fioretto has for the subject, and it makes the course very engaging."*

Psychological safe, student-centered learning experience. Toward encouraging active participation, I strive to foster an environment where students feel "safe" to ask questions and share opinions. As a student wrote in my teaching review: *"[the course] was initially very difficult for me, but professor Fioretto made me very comfortable in class and I could soon start asking [questions] in class and outside."* To cultivate judgment-free dialog, I believe it is imperative to listen to students' needs, be present, and be emphatic. I try to encourage discussion and collaboration both during my classes (e.g., through small group discussions) and outside classes. I do so by using tools like Teams or Discord to create safe spaces where students can share their experiences and doubts about the class content and ask for suggestions and feedback regarding homework and projects. This is how one of my students describes such an aspect in their evaluations: *"I like that the Professor and the TA are readily available for help through Discord outside class time. Professor Fioretto was accommodating and would adjust deadlines when we were in need, which was a big help. It's nice to have a professor who is understanding, passionate, and actually a good teacher."*

2.3 Future Goals

My goal is to actively contribute to the strategic plan of the department and to the growth of the next generation of computer science students.

Beside my current teaching commitments, I am excited to develop a new seminar course on *AI and Optimization for societal benefits* for first- and second-year undergraduate students. The idea, as formulated in my CAREER proposal, is to involve speakers from various institutions, with emphasis on under-represented minorities, and assign small group projects to students. Based on their performance, students will be encouraged to further pursue their interests offering targeted course selections and helping them navigate available research internship opportunities. I would be also excited to design a course on the *foundations of privacy and fairness in machine learning systems* for undergraduate students. The learning goal would to be able to implement a variety of privacy-preserving algorithms and fairness auditing and mitigation approaches for ML systems.

I am also eager to design a graduate course on *decision focused learning*, which focuses on the integration of optimization and machine learning to create new hybrid models. The proposed course would start with a review of concepts from convex optimization and duality, combinatorial optimization, and supervised and unsupervised (deep) learning and examines how to use supervised learning and reinforcement learning to solve combinatorial problems. I would also advertise the course to research groups beyond CS and across the campus, including in the Mechanical, Chemical, and Aerospace Engineering departments where the need for ML and optimization often arises.

3 Diversity, Equity, and Inclusion: Current Efforts

As an instructor and mentor, I firmly believe I have a core responsibility to improve my community and society at large. Within this philosophy, I take diversity, equity, and inclusion (DEI) very seriously. Diversity allows us to expose students to knowledge presented from different angles, creates strong bonds, and teaches them not to take things for granted. More importantly, being a member of a diverse group triggers a sense of respect for other cultures. This is especially pertinent to today's polarized society. Being an immigrant myself and in an interracial marriage to someone who grew up in a Hispanic country, I have witnessed an increase in polarization in this country. Therefore, the need to encourage a more inclusive society resonates strongly with me.

Research and teaching agenda. The goal of building a more inclusive and fair community emerges in different aspects of my research and teaching agenda. My research has a strong connection with equity and inclusion. One of my research areas focuses on how to contrast discriminatory behaviors observed in data-driven decision-making and learning processes. To this end,

I collaborate with non-profits, governmental agencies, and educators to create algorithms that guarantee fairness and protect privacy at the service of broader societal goals. Additionally, my current courses (Security and Privacy in Machine Learning and Introduction to Artificial Intelligence) include modules pertaining to fairness and inclusion in Artificial Intelligence, including a discussion around diversity, inclusion, and challenges to participating in research activities.

Efforts in scientific and local communities. I believe that broadening participation at the local level is critical to building a more diverse, inclusive, and equitable global community. In my capacity of scholarship chair of AAMAS-23[3], and general co-chair of CP-22[4], I had the opportunity to interact with different non-profit organizations (e.g., AIJ, IFAAMAS, NSF, ACM, etc.) and companies (e.g., Google, Amazon, etc.) to request and distribute funds for students to attend the conference and related events (including the Doctoral Consortium Programs). These selection processes carry great responsibility and come with important DEI considerations, which I have learned to profoundly appreciate. I am also the principal organizer of the Privacy-Preserving Artificial Intelligence workshop series, which originated at AAAI-20, and is now in its fourth edition[5], of the AAMAS Workshop on Optimization and Learning[6] since 2018, and co-chair of the Algorithmic Fairness through the lens of Causality and Privacy[7], at NeurIPS. In all these events, I have been a firm advocate for broadening participation (e.g., by offering access via *free* hybrid platforms) and facilitating access to students from underrepresented countries or communities. These efforts have costs, thus I have and will continue to allocate funds to help me achieve these goals. Finally, in my current tenure, I serve as an *academic integrity panelist* and on the selection committee for the *remembrance scholars*, a highly selective award that puts particular emphasis on shaping students' efforts to improve the DEI climate of the campus. Throughout these experiences, I've learned to guide students to educate themselves and help them create plans for improving diversity and inclusion programs.

Broadening participation in computing (BPC). I am currently involved in a number of educational initiatives. Some of these are partially sponsored by my recent NSF CAREER award. I am a faculty mentor for students at NEXIS, an organization at Syracuse supporting undergraduates to explore emerging technologies through innovative and collaborative research projects. I am designing lectures in AI, Optimization, and Fairness for K-12 teachers, as part of Project Advance at Syracuse, one of the largest concurrent enrollment programs in the country with over 200 partner schools in seven states and four other countries[8]. I also interact with students at a local high-school to expose them to research in AI and ML.

Research group. I currently mentor seven students, including three women and four men, three of them are Caucasian, two are Asians, and two are Middle Eastern. In the past, I have mentored students from several under-represented communities, including Hispanic and African-American. Teaching and mentoring such a diverse student population brings opportunities but also challenges. To promote a healthy and productive environment I have started a group activity to facilitate communication between students and professors. Without me being present, the students discuss possible concerns and give practical suggestions on how the research group should move forward. These include mentoring suggestions, lab habits, and expectations. From these activities, I have learned how important and straightforward is to implement a feedback channel that supports a healthy environment.

[3]AAMAS 2023: https://aamas2023.soton.ac.uk/
[4]CP 2022: https://cp2022.a4cp.org/
[5]PPAI Workshop: https://aaai-ppai23.github.io/
[6]OptLearnMAS Workshop: https://optlearnmas22.github.io/
[7]AFCP Workshop: https://www.afciworkshop.org/
[8]Project Advance: https://supa.syr.edu/

3.1 Moving Forward

I am firmly committed to continue to apply my philosophy of inclusiveness and diversity in my classes, mentoring activities, and service. In my capacity as an instructor, I will increase my efforts in designing DEI modules and will continue fostering psychological safety in my classes. In my capacity as a researcher, I will continue providing research opportunities to undergraduates, through REU programs, and outreaching to K-12 students and teachers in local communities to further broaden participation in computing. In my service activities to my department and scientific communities, I will continue to be focused on diversity and inclusion with pragmatic efforts, including allocating time and funds to broaden participation from underrepresented and marginalized communities.

References

[Abo18] John M Abowd. The us census bureau adopts differential privacy. In *Proceedings of the SIGKDD International Conference on Knowledge Discovery & Data Mining*, pages 2867–2867, 2018.

[AK17] Brandon Amos and J Zico Kolter. Optnet: Differentiable optimization as a layer in neural networks. In *Proceedings of the International Conference on Machine Learning (ICML)*, pages 136–145. JMLR. org, 2017.

[BLP20] Yoshua Bengio, Andrea Lodi, and Antoine Prouvost. Machine learning for combinatorial optimization: a methodological tour d'horizon. *European Journal of Operational Research*, 290(2):405–421, 2020.

[BPS19] Eugene Bagdasaryan, Omid Poursaeed, and Vitaly Shmatikov. Differential privacy has disparate impact on model accuracy. In *Proceedings of the Advances in Neural Information Processing Systems (NeurIPS)*, pages 15479–15488, 2019.

[CFMV20] Minas Chatzos, Ferdinando Fioretto, Terrence W. K. Mak, and Pascal Van Hentenryck. High-fidelity machine learning approximations of large-scale optimal power flow. *CoRR*, abs/2006.16356, 2020.

[CMH22] Minas Chatzos, Terrence W. K. Mak, and Pascal Van Hentenryck. Spatial network decomposition for fast and scalable ac-opf learning. *IEEE Transactions on Power Systems*, 37(4):2601–2612, 2022.

[DFVH+21] Vladimir Dvorkin, Ferdinando Fioretto, Pascal Van Hentenryck, Pierre Pinson, and Jalal Kazempour. Differentially private optimal power flow for distribution grids. *IEEE Transactions on Power Systems*, 36(3):2186–2196, 2021.

[DMNS06] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating noise to sensitivity in private data analysis. In *Theory of Cryptography Conference (TTC)*, volume 3876, pages 265–284. Springer, 2006.

[FHM+20] Ferdinando Fioretto, Pascal Van Hentenryck, Terrence W. K. Mak, Cuong Tran, Federico Baldo, and Michele Lombardi. Lagrangian duality for constrained deep learning. In *Machine Learning and Knowledge Discovery in Databases - European Conference, ECML PKDD*, volume 12461, pages 118–135. Springer, 2020.

[FLV18] Ferdinando Fioretto, Chansoo Lee, and Pascal Van Hentenryck. Constrained-based differential privacy for mobility services. In *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pages 1405–1413, 2018.

[FMV20a] Ferdinando Fioretto, Terrence W. K. Mak, and Pascal Van Hentenryck. Differential privacy for power grid obfuscation. *IEEE Transactions on Smart Grid*, 11(2):1356–1366, 2020.

[FMV20b] Ferdinando Fioretto, Terrence W.K. Mak, and Pascal Van Hentenryck. Predicting ac optimal power flows: Combining deep learning and lagrangian dual methods.

In *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, pages 630–637, 2020.

[FMV20c] Ferdinando Fioretto, Lesia Mitridati, and Pascal Van Hentenryck. Differential privacy for stackelberg games. In *Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI)*, pages 3480–3486, 2020.

[FTVZ22] Ferdinando Fioretto, Cuong Tran, Pascal Van Hentenryck, and Keyu Zhu. Differential privacy and fairness in decisions and learning tasks: A survey. In *In Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI)*, pages 5470–5477, 2022.

[FV18] Ferdinando Fioretto and Pascal Van Hentenryck. Constrained-based differential privacy: Releasing optimal power flow benchmarks privately - releasing optimal power flow benchmarks privately. In *International Conference on the Integration of Constraint Programming, Artificial Intelligence, and Operations Research (CPAIOR)*, volume 10848 of *Lecture Notes in Computer Science*, pages 215–231, 2018.

[FV19a] Ferdinando Fioretto and Pascal Van Hentenryck. Differential privacy of hierarchical census data: An optimization approach. In *Proceedings of the International Conference on Principles and Practice of Constraint Programming (CP)*, volume 11802 of *Lecture Notes in Computer Science*, pages 639–655, 2019.

[FV19b] Ferdinando Fioretto and Pascal Van Hentenryck. Optstream: Releasing time series privately. *Journal of Artificial Intelligence Research*, 65:423–456, 2019.

[FV19c] Ferdinando Fioretto and Pascal Van Hentenryck. Privacy-preserving federated data sharing. In *Proceedings of the International Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, pages 638–646, 2019.

[FVZ21] Ferdinando Fioretto, Pascal Van Hentenryck, and Keyu Zhu. Differential privacy of hierarchical census data: An optimization approach. *Artificial Intelligence*, 296:103475, 2021.

[KFS22] Sawinder Kaur, Ferdinando Fioretto, and Asif Salekin. Deadwooding: Robust global pruning for deep neural networks. *arXiv preprint arXiv: Arxiv-2202.05226*, 2022.

[KFV22] James Kotary, Ferdinando Fioretto, and Pascal Van Hentenryck. Fast approximations for job shop scheduling: A lagrangian dual deep learning method. In *In Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, pages 7239–7246, 2022.

[KFVH21] James Kotary, Ferdinando Fioretto, and Pascal Van Hentenryck. Learning hard optimization problems: A data generation perspective. In *Advances in Neural Information Processing Systems (NeurIPS)*, volume 34, pages 24981–24992. Curran Associates, Inc., 2021.

[KFVW21] James Kotary, Ferdinando Fioretto, Pascal Van Hentenryck, and Bryan Wilder. End-to-end constrained optimization learning: A survey. In *Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI)*, pages 4475–4482, 2021.

[KFVZ22] James Kotary, Ferdinando Fioretto, Pascal Van Hentenryck, and Ziwei Zhu. End-to-end learning for fair ranking systems. In *In Proceedings of the ACM Web Conference (WWW)*, pages 3520–3530, 2022.

[MBF22] Mostafa Mohammadian, Kyri Baker, and Ferdinando Fioretto. Gradient-enhanced physics-informed neural networks for power systems operational support. *CoRR/abs arXiv:2206.10579*, 2022.

[MCTH22] Terrence W. K. Mak, Minas Chatzos, Mathieu Tanneau, and Pascal Van Hentenryck. Learning regionally decentralized ac optimal power flows with admm. *CoRR/abs ArXiV:2205.03787*, 2022.

[MFSV20] T. W. K. Mak, F. Fioretto, L. Shi, and P. Van Hentenryck. Privacy-preserving power system obfuscation: A bilevel optimization approach. *IEEE Transactions on Power Systems*, 35(2):1627–1637, 2020.

[MFV21] Terrence W. K. Mak, Ferdinando Fioretto, and Pascal Van Hentenryck. Load embeddings for scalable AC-OPF learning. *CoRR*, abs/2101.03973, 2021.

[NIS20] NIST. Differential privacy temporal map challenge. online: `https://www.nist.gov/ctl/pscr/open-innovation-prize-challenges/current-and-upcoming-prize-challenges/2020-differential`, 2020.

[PMK+20] David Pujol, Ryan McKenna, Satya Kuppam, Michael Hay, Ashwin Machanavajjhala, and Gerome Miklau. Fair decision making using privacy-protected data. In *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FaTC)*, pages 189–199, 2020.

[RDK+22] David Rolnick, Priya L. Donti, Lynn H. Kaack, Kelly Kochanski, Alexandre Lacoste, Kris Sankaran, Andrew Slavin Ross, Nikola Milojevic-Dupont, Natasha Jaques, Anna Waldman-Brown, Alexandra Sasha Luccioni, Tegan Maharaj, Evan D. Sherwin, S. Karthik Mukkavilli, Konrad P. Kording, Carla P. Gomes, Andrew Y. Ng, Demis Hassabis, John C. Platt, Felix Creutzig, Jennifer Chayes, and Yoshua Bengio. Tackling climate change with machine learning. *ACM Comput. Surv.*, 55(2), feb 2022.

[TDBF21] Cuong Tran, My H. Dinh, Kyle Beiter, and Ferdinando Fioretto. A fairness analysis on private aggregation of teacher ensembles. *CoRR*, abs/2109.08630, 2021.

[TDF21] Cuong Tran, My H. Dinh, and Ferdinando Fioretto. Differentially private deep learning under the fairness lens. In *Advances in Neural Information Processing Systems (NeurIPS)*, 2021.

[TFH21] Cuong Tran, Ferdinando Fioretto, and Pascal Van Hentenryck. Differentially private and fair deep learning: A lagrangian dual approach. In *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, 2021.

[TFKN22] Cuong Tran, Ferdinando Fioretto, Jung-Eun Kim, and Rakshit Naidu. Pruning has a disparate impact on model accuracy. In *Advances in Neural Information Processing Systems (NeurIPS)*, volume 35, page TBA. Curran Associates, Inc., 2022.

[TFV21] Cuong Tran, Ferdinando Fioretto, and Pascal Van Hentenryck. Differentially private and fair deep learning: A lagrangian dual approach. In *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, pages 9932–9939, 2021.

[TFVY21] Cuong Tran, Ferdinando Fioretto, Pascal Van Hentenryck, and Zhiyan Yao. Decision making with differential privacy under a fairness lens. In *Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI)*, pages 560–566, 2021.

[VSPRB20] Natalia Vesselinova, Rebecca Steinert, Daniel F Perez-Ramirez, and Magnus Boman. Learning combinatorial optimization on graphs: A survey with applications to networking. *IEEE Access*, 8:120388–120416, 2020.

[VVH21] Alexandre Velloso and Pascal Van Hentenryck. Combining deep learning and optimization for preventive security-constrained dc optimal power flow. *IEEE Transactions on Power Systems*, 36(4):3618–3628, 2021.

[ZFV22] Keyu Zhu, Ferdinando Fioretto, and Pascal Van Hentenryck. Post-processing of differentially private data: A fairness perspective. In *In Proceedings of the International Joint Conference on Artificial Intelligence (IJCAI)*, pages 4029–4035, 2022.

[ZVF21] Keyu Zhu, Pascal Van Hentenryck, and Ferdinando Fioretto. Bias and variance of post-processing in differential privacy. In *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, pages 11177–11184, 2021.