Luiz F. O. Chamon
http://www.seas.upenn.edu/~luizf

Research Statement

# Learning under Requirements

The transformative power of learning lies in automating the engineering of complex systems. The traditional design cycle of these systems has engineers specifying requirements, acquiring data, building models, and optimizing operational settings. But as modern systems grow in scale and complexity, this process becomes increasingly challenging and costly. Learning can bypass parts of this cycle and take us from data directly to operation with little to no human intervention. The goal of my research program is to realize this **autonomous system engineering** vision by developing the theory and practice of **learning under requirements**.

Despite their central role in engineering, learning today does not incorporate requirements organically. This has led to many instances of data-driven solutions that are biased, prejudiced, and prone to tampering and unsafe actions. Ultimately, this is due to our inability to specify fairness, robustness, and safety requirements. I contend that we can no longer expect learning to have a positive impact on critical systems by improving existing methods. Instead, we must advance past the current learning paradigm of minimizing costs and *learn to satisfy requirements*. As in classical learning, this problem can be formulated as an optimization program, albeit one with constraints. This modification may appear innocuous, but we know from optimization theory that constraints are in fact a major source of complexity. Even linear regression, the most benign of problems, can be made NP-hard with a single sparsity constraint, forcing us to exploit additional structure to obtain approximate solutions [1–5]. These issues are only amplified by the lack of convexity of modern learning problems.

If constrained learning is necessary but seemingly intractable, we are left with somewhat of a Gordian knot. Nevertheless, my research suggests that constraints are the appropriate tool to learn under requirements as opposed to *ad hoc* modifications of the training objective. To cut across this intractability, my work relies on a key technical ingredient: (uncountable) *infinite dimensional nonconvex optimization* manifests the duality properties of convex optimization. For instance, *the infinite dimensional counterpart of that feature selection problem turns out to be tractable* and can be used to fit multiresolution kernels, learn Bayesian priors, and derive risk-aware estimators and controllers [6–10]. Leveraging this technical discovery, I have shown that despite appearances, *constrained learning is actually as hard as unconstrained learning*, i.e., they have essentially the same sample complexity. What is more, it is often possible to use duality to *tackle constrained learning tasks by solving only unconstrained learning problems* despite their non-convexity [11,12]. These advances have enabled (reinforcement) learning for resource allocation, safety, fairness, and robustness [11–15].

Building upon this foundation, I will bridge the gap between learning and the engineering of critical systems by *developing the theoretical underpinnings of constrained learning* (Figure 1). I envision this theory enabling a shift from the current, objective-centric paradigm to a *constraint-driven learning* one, giving rise to systems that can learn both *under* requirements and *from* their requirements. This


**Direction A** Constrained (reinforcement) learning

**Direction B** Learning from constraints

**Direction C** Resilient learning

**Direction D** Overparametrized learning

Figure 1: A plan to bridge the gap between learning and critical systems.

synergistic exploitation of constraints is the basis for systems that can *learn to learn under requirements* and showcases the potential of constrained learning to be the driving force behind *autonomy*.

The concrete directions of my research program are guided by four fundamental questions that current learning theory cannot answer:

**A.** *When* is it possible to learn *under* requirements?
**B.** *When* is it possible to learn *from* requirements?
**C.** *Which* requirements should be used to learn and how to specify them?
**D.** *How* can we learn under requirements in practice?

In the sequel, I provide a detailed description of each of these research directions.

**A. Constrained (reinforcement) learning.** The goal of this direction is to study *when learning under requirements is possible*. More specifically, I am interested in characterizing the effect of sample size on feasibility. This requires pushing constrained learning theory [11, 12] to new learning models—e.g., structured complexity and PAC-Bayes—and tasks—e.g., reinforcement learning [14, 15] and non-convex losses. The latter is especially important to tackle rate-constrained problems that arise, e.g., in fairness.

These advances provide a unique perspective for studying *when* requirements such as fairness or invariance are achievable without unnecessary performance harm by leveraging the duality between constrained optimization and Pareto optimality. I will exploit these results to develop a statistical analysis of the Pareto frontier to study how compromises between, e.g., performance, fairness, and robustness, arise when models are trained from data. This duality also relates constrained and minimax problems, allowing the theory developed in this direction to shed light on *when* minimax learning is viable. This has implications on the learning complexity of robustness, model auditing, and adversarial training—e.g., generative adversarial networks (GANs). Nevertheless, there are fundamental roadblocks to using duality in non-convex settings that I will address using non-convex variational results [6] rather than resorting to randomized solutions (mixed Nash equilibria). Additionally, it is not immediate that feasible, *deterministic* models/policies (primal solutions) can be recovered from minimax (dual) solutions even in the convex case. Preliminary results suggest that feasible policies can be obtained in sequential decision settings—e.g., reinforcement learning—by leveraging the implicit memory of primal-dual methods to build systems capable of compensating for their mistakes.

**B. Learning from constraints.** Direction A investigates how learning complexity affects feasibility. In contrast, this direction explores *how constraints in return affect learning complexity*. Indeed, whereas constraints should improve sample complexity by reducing the feasible hypotheses class, current results show that constrained and unconstrained learning have essentially the *same* sample complexity [11, 12]. Any gains from restricting the hypotheses set thus appears to be offset by the fact we use data to determine whether a hypothesis is feasible. Understanding this trade-off will allow us to separate the underlying learning complexity of the task from that of its requirements and provide conditions under which learning can occur through the constraints, i.e., by using constraints to describe not only requirements, but also the learning problem itself. I am particularly interested in the impact of generalization constraints and the use of cross-validated versions of stochastic gradient descent (SGD) to impose them, given their promising results for Bayesian prior learning [8].

Ultimately, the goal of this research direction is to enable *constraint-driven learning*, a paradigm in which learning occurs not *under* constraints, but *from* constraints. In other words, where learning tasks are feasibility problems as opposed to cost minimization ones. This formulation is attractive since practical problems are often expressed as requirements rather than costs—e.g., "accuracy above 80% and fairness parity within 5%" rather than "minimize a combination of performance and fairness

losses." Additionally, it decouples conflicting requirements such as fit and model complexity, facilitating their specification, both manually or systematically using resilient techniques (Direction C). This approach has been beneficial in optimal control problems [16, 17], but remains unexplored in the context of learning. Naturally, it poses new algorithmic challenges as it leads to optimization problems with a large—on the order of the number of samples—or even an infinite number of constraints. I will address this issue by studying large-scale programs as samples from infinite ones (see Direction D for details).

**C. Resilient learning.** Directions A and B deal with the issue of learning under requirements once they are specified. Here, I am concerned with *which requirements to specify* in the first place. This is particularly important in the presence of conflicting objectives, such as fit vs. model complexity and nominal vs. adversarial performance, or ill-posed requirements, such as the protected groups in fairness—women; women and person of color; or women, person of color, and women $\times$ person of color. The goal is to enable tasks to *adapt* to their learning conditions (sample size, distributions, requirement difficulty) by automatically trading off their requirements. In ecology, this property is known as *resilience*. I propose to advance a mathematical formulation of resilient learning based on *counterfactuals* of the form "what would have been the performance if the requirement were relaxed/tightened?" Evaluating these counterfactuals, however, can be challenging, particularly in the non-convex setting of machine learning. Leveraging duality results from previous directions, I will establish conditions under which this is possible, determining when learning requirements can be balanced and how it can be done efficiently. I will then leverage other forms of duality to study compromise in different domains, such as discrete and semi-infinite optimization, and develop new statistical notions of duality to study the effect of uncertainty on compromises (statistical Pareto, Direction A).

This approach to resilience has been fruitful in control [16, 17] and preliminary results show that it can be used to address learning issues such as outlier detection, classification confidence, and adversarial training. Indeed, modern parametrizations can—and possibly even should—interpolate training samples, making fit a poor measure of sample anomaly and leading to overconfident classifiers. Nevertheless, the credibility of a sample or prediction can still be assessed by balancing fit and model complexity [18] or classification and perturbation magnitude. In the case of adversarial training, the compromise between nominal and adversarial performance can be used to determine the strength, type, and number of adversaries. In this context, resilience enables what are essentially self-learning adversaries. For GANs, these multiple, diverse discriminators may be used to address issues such as mode collapse.

**D. Overparametrized learning.** Directions A–C primarily investigate *when* it is possible to learn under requirements and *which* requirements. This direction focuses on *how*. More specifically, how overparametrization affects the behavior of the primal-dual algorithms used to solve the dual learning problems from Directions A–C. This is motivated by the growing empirical and theoretical evidence that SGD finds good local minima for high-dimensional unconstrained learning problems despite their non-convexity. While there is strong empirical evidence that the same happens with stochastic gradient descent-ascent dynamics, the theory in this case remains scarce. What is more, it is not immediate that these methods can yield feasible models, especially due to fundamental roadblocks from duality to retrieving deterministic primal solutions.

To achieve these results, I will combine classical tools, such as concentration of measure, with new techniques based on approaching *high-dimensionality from above*. Inspired by the fact that certain non-convex functional problems are tractable [6], this perspective proposes to tackle high dimensional phenomena not asymptotically from low dimensional structures, but as approximations or samples of infinite dimensional ones. This technique was used to quantify the parametrization gap in dual learn-

ing [11–15] and study transferability in graph neural networks (GNNs) by introducing their continuous counterparts, graphon NNs [19]. I will use this approach to study both overparametrized problems—i.e., high dimensional primal problems—and the large-scale constrained optimization problems—i.e., high dimensional dual problems—from Directions B and C. I foresee this method will also provide a new functional outlook on the generalization properties of interpolating NNs beyond neural tangent kernels (NTK).

**Funding opportunities.** My research fits within the Computing and Communication Foundations (CCF) core program of the National Science Foundation (NSF). In the last couple years, the NSF has started large scale programs such as TRIPODS, HDR, and MoDL where my research fits well. My ideas on constrained learning are featured in successful TRIPODS and MoDL proposals. This year, one of the AI institutes the NSF is aiming to seed on Dynamic Systems (Theme 5). Learning under requirements is a topic that fits well in this theme. I am not likely to benefit from these ongoing programs, but they show that the NSF is committed to invest in learning. I believe that my ideas align well with NSF priorities. I will also pursue funding opportunities within the DoD. Learning under requirements is a topic of interest to the Army, Navy, and Air Force research offices (ARO, ONR, and AFOSR). I am aware that there is also significant activity on constrained learning at the Army Research Lab (ARL). I have participated as a student and postdoc in ARL's Distributed Collaborative Intelligent Systems and Technology (DCIST) Alliance, where my research is central to two different tasks. I should add that I have contributed to the writing of successful proposals for the DCIST, TRIPODS, and MoDL programs. As a junior faculty, I also intend to apply within my first three years for the NSF CAREER Award and the DARPA Young Faculty Award (YFA).

## References


[1] **L.F.O. Chamon** and A. Ribeiro. Greedy sampling of graph signals. *IEEE Trans. on Signal Process.*, 66[1]:34–47, 2018. [**arXiv**].

[2] **L.F.O. Chamon** and A. Ribeiro. Approximate supermodularity bounds for experimental design. In: *NeurIPS*, p. 5403–5412, 2017. [**arXiv**].

[3] **L.F.O. Chamon**, G.J. Pappas, and A. Ribeiro. Approximate supermodularity of Kalman filter sensor selection. *IEEE Trans. on Autom. Control. (accepted)*, 2020. [**arXiv**].

[4] V.L. Silva, **L.F.O. Chamon**, and A. Ribeiro. Model predictive selection: A receding horizon scheme for actuator selection. In: *ACC*, p. 347–353, 2019. [**pdf**].

[5] **L. F. O. Chamon**, A. Amice, and A. Ribeiro. Approximately supermodular scheduling subject to matroid constraints. *IEEE Trans. on Autom. Control. (under review)*, 2020. [**ArXiv**].

[6] **L.F.O. Chamon**, Y.C. Eldar, and A. Ribeiro. Functional nonlinear sparse models. *IEEE Trans. on Signal Process.*, 68[1]:2449–2463, 2020. [**arXiv**].

[7] M. Peifer, **L.F.O. Chamon**, S. Paternain, and A. Ribeiro. Sparse multiresolution representations with adaptive kernels. *IEEE Trans. on Signal Process.*, 68[1]:2031–2044, 2020. [**arXiv**].

[8] **L.F.O. Chamon**, S. Paternain, and A. Ribeiro. Learning Gaussian processes with Bayesian posterior optimization. In: *Asilomar*, p. 482–486, 2019. [**pdf**].

[9] D.S. Kalogerias, **L.F.O. Chamon**, G.J. Pappas, and A. Ribeiro. Better safe than sorry: Risk-aware nonlinear Bayesian estimation. In: *IEEE ICASSP*, 2020. **[Best paper award]** [**ArXiv**].

[10] A. Tsiamis, D.S. Kalogerias, **L.F.O. Chamon**, A. Ribeiro, and G.J. Pappas. Risk-constrained linear-quadratic regulators. In: *IEEE CDC*, 2020. [**arXiv**].

[11] **L.F.O. Chamon**, S. Paternain, M. Calvo-Fullana, and A. Ribeiro. The empirical duality gap of constrained statistical learning. In: *IEEE ICASSP*, 2020. **[Best student paper award]** [**pdf**] [**video**].

[12] **L.F.O. Chamon** and A. Ribeiro. Probably approximately correct constrained learning. In: *NeurIPS*, 2020. [**arXiv**].

[13] M. Eisen, C. Zhang, **L.F.O. Chamon**, and D.D. Lee A. Ribeiro. Learning optimal resource allocations in wireless systems. *IEEE Trans. on Signal Process.*, 67[10]:2775–2790, 2019. **[Top 50 most accessed articles in IEEE TSP: May, July, Sept, Oct 2019]** [**arXiv**].

[14] S. Paternain, M. Calvo-Fullana, **L.F.O. Chamon**, and A. Ribeiro. Safe policies for reinforcement learning via primal-dual methods. *IEEE Trans. on Autom. Control. (under review)*, 2019. [**ArXiv**].

[15] S. Paternain, **L.F.O. Chamon**, M. Calvo-Fullana, and A. Ribeiro. Constrained reinforcement learning has zero duality gap. In: *NeurIPS*, p. 7555–7565, 2019. [**arXiv**].

[16] **L.F.O. Chamon**, S. Paternain, and A. Ribeiro. Counterfactual programming for optimal control. In: *L4DC*, 2020. [**pdf**].

[17] **L.F.O. Chamon**, A. Amice, S. Paternain, and A. Ribeiro. Resilient control: Compromising to adapt. In: *IEEE CDC*, 2020. [**arXiv**] [**video**].

[18] **L. F. O. Chamon**, S. Paternain, and A. Ribeiro. Trust but verify: Assigning prediction credibility by counterfactual constrained learning. 2020.

[19] L. Ruiz, **L.F.O. Chamon**, and A. Ribeiro. Graphon neural networks and the transferability of graph neural networks. In: *NeurIPS*, 2020. [**arXiv**].