When Deep Learning Meets Nontrivial Constraints

Introduction: The use of explicit constraints is a relatively new but increasingly important aspect of deep learning (DL), which has been stimulated by the need for trustworthy AI that can perform robust optimization over complex perturbation sets, as well as scientific and engineering applications that require adherence to physical laws and constraints. However, solving constrained DL problems reliably can be challenging for those without optimization expertise, and existing optimization software is not able to handle general constrained DL problems. In this poster, we highlight NCVX[1], a user-friendly optimization package specifically designed to solve constrained DL problems easily, and discuss practical techniques to accelerate its convergence in applications [1]. Additionally, we will integrate our description of the computational techniques into various applications of constrained DL in science and engineering, including 1) robustness evaluation, 2) topology optimization, 3) learning with label imbalance.

Adversarial Robustness of Vision Recognition: DL models for visual recognition are vulnerable to perturbations that are imperceptible to humans. Two popular ways of robustness evaluation (RE) are to solve adversarial loss and robustness radius formulations, which are nontrivial constrained DL problems. Although real-life perturbations can go way beyond the imperceptible level and are natural, the non-lp adversarial attacks (e.g., perceptual distance) are inaccessible to SOTA adversarial packages, as the PGD-based attack requires analytical projectors which are impossible to derive in general constraints case. In our recent work, we proposed a novel algorithmic framework based on NCVX that offers several advantages [2][3]: 1). Generality: Our method can handle general RE problems, which offers the robustness community the possibility to easily explore different attack metrics; 2). Reliability: Our algorithm obtains reliable solutions based on a gold-standard step-size rule and a principled stopping criterion.

Neural Topology Optimization (TO) with Principled Constrained Optimization: TO is a mathematical approach to designing mechanical and multiphysics systems that aims to maximize their structural performance while complying with physical and manufacturing constraints. However, when it comes to designing metamaterials using conventional TO, there are additional challenges due to implicit physical constraints, combinatorial constraints, and nonlinear physical constraints. To address these issues, we have developed a user-friendly TO computing framework based on NCVX for general nonlinear metamaterial design [4]. Our framework offers several advantages in addressing the following difficulties: 1). Implicit Physical Constraints: We use the deep image prior technique to bias the optimization process towards spatially smooth structures. 2). Combinatorial Constraints: We developed a generalized straight-through technique and its equivalent reformulation to enforce combinatorial constraints. 3). Nonlinear Physical Constraints: SOTA methods can not handle nonlinear physical constraints. However, our TO computing framework has successfully solved various design problems with SOTA compliance while guaranteeing feasibility.

Imbalance Classification: In statistical learning, it is ideal for the training objectives to align with the evaluation metrics. However, when there is a substantial class imbalance, metrics such as accuracy, balanced accuracy, and AUROC that do not take precision into account can be misleading. In such cases, precision-aware metrics are more relevant and practical. For example, in imbalanced binary classification scenarios, which are common in medical diagnosis and information retrieval, one might want to fix the recall and optimize precision, or vice versa, or directly optimize the AUPRC. In the recent work, these are all complex optimization problems that can be effectively addressed using NCVX [5].

[1] See our website https://ncvx.org/ for more detailed information about NCVX.

[1] Liang, B., Mitchell, T., & Sun, J. (2022). NCVX: A general-purpose optimization solver for constrained machine and deep learning. In OPT 2022: Optimization for Machine Learning (NeurIPS 2022 Workshop)

[2] Liang, H., Liang, B., Peng, L., Cui, Y., Mitchell, T., & Sun, J. (2023). Optimization and Optimizers for Adversarial Robustness. arXiv preprint arXiv:2303.13401.

[3] Liang, H., Liang, B., Cui, Y., Mitchell, T., & Sun, J. (2022). Optimization for robustness evaluation beyond ℓp metrics. In OPT 2022: Optimization for Machine Learning (NeurIPS 2022 Workshop)

[4] Liang, B., Vera, R., Liang, H., Cui, Y., Mitchell, T., He, Q., & Sun, J. (2023). Neural Topology Optimization with Principled Constrained Optimization. In preparation for Structural and Multidisciplinary Optimization.

[5] Peng, L., Travadi, Y., Cui, Y., & Sun, J. (2022). Direct Metric Optimization for Imbalanced Classification. In preparation for the Journal of Machine Learning Research.