Universidade de Pernambuco
Programa de Pós-Graduação em Engenharia da Computação (PPGEC)

Proposta de Dissertação de Mestrado

Área: Computação Inteligente

Título: Towards Robust Out-of-Distribution Generalization for Deep Neural Networks with Tailored Data Regularization

Orientador(a): Diego Marconi Pinheiro Ferreira Silva (dmpfs@ecomp.poli.br)
Coorientador: Carmelo José Albanez Bastos Filho (carmelofilho@ecomp.poli.br)

Descrição:

Robust generalization refers to the ability of models to maintain reliable performance under distribution shifts — when test data deviate from the training distribution. This remains a significant challenge for Deep Neural Networks (DNNs), which are highly susceptible to overfitting in such scenarios [1,2]. Although regularization techniques are widely employed to mitigate this issue, they often fall short or even lead to over-regularization, ultimately degrading performance [3]. These limitations suggest the need for carefully tailored regularizers [4,5], whose effectiveness may depend on both the task (e.g., classification) and the data domain (e.g., vision, language). **This motivates the development of domain-aware and task-sensitive regularization approaches.** This proposal adopts the categories defined in previous work [6] for Out-of-Distribution (OOD) data, focusing specifically on the transformed-OOD setting, where label-preserving corruptions are applied to in-distribution inputs. To characterize the impact of such shifts, the project will compute statistical distances — such as KL divergence — between clean and corrupted latent representations, enabling a quantification of distributional deviation and its interaction with regularization. Building on this perspective, the proposed research will investigate whether stochastic data regularization — through random transformations [7,8] and input noise [9,10,11] — can function as an implicit regularizer when applied dynamically. The study will explore the hypothesis that organizing these perturbations as a curriculum [12,13], gradually increasing their intensity, constitutes a promising yet underexplored strategy in computer vision [4], particularly for compact models aiming at robust generalization. To systematically examine this idea, the project will employ a modular framework composed of three components: a *Selection Policy* (e.g., choosing between noise types or augmentation pipelines), a *Combination Policy* (e.g., composing augmentations and noise), and a *Scheduling Policy* (Curriculum Learning-based approach). This structure will support controlled experimentation and facilitate understanding of how each component influences model robustness. Accordingly, the central research question guiding this proposal is: **How can data regularization be dynamically adapted to a model's capacity to improve robustness while mitigating overfitting and underfitting, thereby enhancing out-of-distribution performance?** The working hypothesis is that *stochastic data regularization* — whether applied uniformly or progressively — can yield consistent gains in robustness across domains, with curriculum-based organization further stabilizing learning by aligning perturbation strength with model maturity. Additionally, the project will examine whether unstructured randomness in augmentations and noise can still provide meaningful benefits when appropriately tuned. Model evaluation will consider both average performance and the reliability of performance estimates. A miscoverage-based analysis across cross-validation folds, consistent with recent analyses of cross-validation behavior [14], will be incorporated to quantify how well confidence intervals reflect true variability. This perspective is

expected to provide a more nuanced understanding of robustness, particularly regarding the bias–variance trade-off and the stability of out-of-distribution generalization.

Referências Bibliográficas:

[1] LI, B.; JIN, J.; ZHONG, H.; HOPCROFT, J.; WANG, L. Why robust generalization in deep learning is difficult: Perspective of expressive power. Advances in Neural Information Processing Systems, v. 35, p. 4370–4384, 2022.

[2] HENDRYCKS, D.; CARLINI, N.; SCHULMAN, J.; STEINHARDT, J. Unsolved problems in ml safety. arXiv preprint arXiv:2109.13916, 2021.

[3] LIN, C.-H.; KAUSHIK, C.; DYER, E. L.; MUTHUKUMAR, V. The good, the bad and theugly sides of data augmentation: An implicit spectral regularization perspective. Journal of Machine Learning Research, v. 25, n. 91, p. 1–85, 2024.

[4] CHOI, J.; KIM, Y. Colorful cutout: Enhancing image data augmentation with curriculum learning. arXiv preprint arXiv:2403.20012, 2024.

[5] SRIVASTAVA, N.; HINTON, G.; KRIZHEVSKY, A.; SUTSKEVER, I.; SALAKHUT-DINOV, R. Dropout: A simple way to prevent neural networks from overfitting. Journal of Machine Learning Research, v. 15, n. 56, p. 1929–1958, 2014.

[6] FARQUHAR, S.; GAL, Y. What'out-of-distribution'is and is not. In: NeurIPS ML Safety Workshop. [S.l.: s.n.], 2022.

[7] CUBUK, E. D.; ZOPH, B.; SHLENS, J.; LE, Q. V. Randaugment: Practical automated data augmentation with a reduced search space. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, p. 702–703, 2020.

[8] Dan Hendrycks, Norman Mu, Ekin D Cubuk, Barret Zoph, Justin Gilmer, and Balaji Lakshmi- narayanan. Augmix: A simple data processing method to improve robustness and uncertainty. arXiv preprint arXiv:1912.02781, 2019.

[9] BISHOP, C. M. Training with noise is equivalent to Tikhonov regularization. *Neural Computation*, v. 7, n. 1, p. 108–116, 1995.

[10] YUAN, X.; LI, J.; KURUOGLU, E. E. Robustness enhancement in neural networks with alpha-stable training noise. *Digital Signal Processing*, v. 156, p. 104778, 2025.

[11] BARROS FILHO, U. T.; ROCHA, P.; OLIVEIRA, M.; CAVALCANTI RIBEIRO, A. M. N.; MONTEIRO, R. de P.; PINHEIRO, D. Regularizing neural networks with noise injection for classification of brain tumor in magnetic resonance imaging. In: 2023 IEEE Latin American Conference on Computational Intelligence (LA-CCI), p. 1–6, 2023.

[12] BENGIO, Y.; LOURADOUR, J.; COLLOBERT, R.; WESTON, J. Curriculum learning. In: Proceedings of the 26th Annual International Conference on Machine Learning (ICML '09), New York, NY, USA, p. 41–48, 2009. Association for Computing Machinery.

[13] LU, H.; LAM, W. PCC: Paraphrasing with bottom-k sampling and cyclic learning for curriculum data augmentation. In: **Proceedings of the 17th Conference of the European Chapter of the Association for Computational Linguistics**, Dubrovnik, Croatia, p. 68–82, May 2023. Association for Computational Linguistics.

[14] BATES, S.; HASTIE, T.; TIBSHIRANI, R. Cross-validation: what does it estimate and how well does it do it? *Journal of the American Statistical Association*, p. 1–12, 2023.