



Seminar Hora Informaticae

Institute of Computer Science, Prague

Tuesday, November 18, 2025, 13.30 – 15.30 (1.30 – 3:30 PM) CET

Meeting Room 318, Address: Pod Vodárenskou věží 2, Prague 8

Meeting ID: 914 0834 4018, Passcode: 668534



<https://cesnet.zoom.us/j/91408344018?pwd=x2QlZ4F42BxlMSmWc1HOwHHA7Uw7PN.1>

Věra Kůrková (Institute of Computer Science, CAS, Prague).

Robustness of Deep ReLU Networks to Misclassification of High-Dimensional Data.

The reliability of AI computational models based on neural networks is crucial for their practical applicability. It is desirable that networks maintain their intended functionality even when exposed to changes or variations in their inputs, caused either by data corruption (due to errors or noise) or by intentionally crafted adversarial perturbations. In the lecture, we will examine the susceptibility of trained deep ReLU networks to misclassification. We will introduce a probabilistic approach to robustness characterized by a likelihood of misclassification of data corrupted by small additive random perturbations. We will describe inputs with low and high probabilities of misclassification and demonstrate that the robustness of deep ReLU networks improves rapidly with increasing dimensionality of the network inputs, while it decreases mildly with the number of network units, independently of their arrangement in layers. To prove the importance of influence of the input dimension on the robustness of ReLU networks, we combine properties of high-dimensional geometry with the plane-wave shape and piecewise linear character of their units.

References:

- [1] V. Kůrková, M. Sanguineti: Approximation of classifiers by deep perceptron networks, *Neural Networks* 165: 654–661, 2023. DOI 10.1016/j.neunet.2023.06.004
- [2] V. Kůrková, M. Sanguineti: Classification of large data sets by neural networks: A probabilistic viewpoint. In *ICANN 2025, LNCS 16068*, Eds. W. Senn et al. (pp. 480-486), Springer, 2026. DOI 10.1007/978-3-032-04558-4_38

Věra Kůrková (www.cs.cas.cz/~vera) is a senior scientist from the Department of Artificial Intelligence, Institute of Computer Science of the Czech Academy of Sciences. She received PhD. in mathematics from the Charles University, Prague, and DrSc. (Prof.) in theoretical computer science from the Czech Academy of Sciences. She has been affiliated with the Institute of Computer Science since 1990 (in 2002-2008 she was the Head of the Department of Theoretical Computer Science). In 2010, she received the Bolzano Medal for her contribution to mathematical sciences from the Czech Academy of Sciences.

Her main research interests are mathematical theory of neurocomputing and machine learning. Her work includes analysis of capabilities and limitations of shallow and deep networks, dependence of network complexity on increasing dimensionality of computational tasks, connections between theory of inverse problems and generalization in machine learning, and nonlinear approximation theory.

She has been a member of the Board of the European Neural Network Society since 2008 (in 2017-2019 she was its president) and of the editorial boards of the journals Neural Networks, Neural Processing Letters, and Applied and Computational Harmonic Analysis. She has been involved in organization of conferences ICANN and EANN in various roles (general chair, co-chair, or honorary chair).

HORA INFORMATICAЕ (meaning: TIME FOR INFORMATICS) is a broad-spectrum scientific seminar devoted to all core areas of computer science and its interdisciplinary interfaces with other sciences and applied domains. Original contributions addressing classical and emerging topics are welcome. Founded by Jiří Wiedermann, the seminar is running since 1994 at the Institute of Computer Science of the Czech Academy of Sciences in Prague.

<https://www.cs.cas.cz/horainf>