Model-based machine learning

Contact: Gergő Bognár, bognargergo@staff.elte.hu, bogqaai@inf.elte.hu (Teams)

Goals: Development and application of model-based machine learning methods: fusion of model-based and artificial intelligence approaches in order to efficiently solve signal and image processing problems. The main focus is on adaptive transformation methods (see variable projections [1, 2]), and related model-based neural networks (see VPNet [3] and WaveletKernelNet [4]). Development environment: Matlab and Python (numpy/pytorch).

Topics:

1. **VarPro and VPNet implementations**
   Implementation of variable projection and VPNet using state-of-the-art frameworks (like Matlab, R, PyTorch, TensorFlow, Keras, Scikit-learn, MXNet, etc.). Expectations: CPU and GPU support, numerical stability, efficiency, scalability.

2. **Generalized VPNet**
   Development of model-based machine learning methods based on the idea of VPNet: combination of variable projection with neural networks and other learning methods. The tasks include mathematical modelling, architecture design, learning and optimization, application and validation with simulated and real-world data. Possible examples:

   - ~~VP-SVM~~ (in progress)
   - ~~Deep unfolding VP~~ (in progress)
   - VP-k-means, VP-C-means, VP-k-NN
   - VP-RNN, like transformer, attention
   - VP-U-Net

3. **Adversarial machine learning**
   Adversarial machine learning investigates attacks and defenses on machine learning methods (see [5]). The basic observation is that deep neural network are significantly discontinuous and sensitive to their input: well-crafted, but hardly perceptible perturbations of the input data may cause serious misclassifications (see [6]). The task is to apply and develop adversarial attacks for VPNet and for 1D convolutional networks, and then develop defense methods against these attacks, which possibly leads to more reliable and robust methodology.

4. **Compartmental modeling**
   Compartmental modeling is a widely used technique, for instance to model material flow in physiological processes, and disease spread in epidemiology. In a mathematical point of view, a system identification problem need to be solved, where the parameters of a dynamic model needs to be identified based on the output of the system. These models are related to variable projections and wavelets as well, which motivates the application of VPNet and WaveletKernelNet. The task is the simulation of compartmental models, and parameter estimation with model-based neural networks. The long term goal is the validation of the method on real dynamic PET measurements. Further reading: [7]

5. **~~Blind deconvolution~~ (in progress)**
Deconvolution is a widely used approach to enhance images that are blurred due to environmental effects or motion. The parameter estimation of deconvolution is a numerical optimization problem that can be addressed using transformation methods (like wavelets, VarPro, see [8]), and using neural networks as well (see [9]). The task is to apply and develop model-based machine learning: VPNet and/or WaveletKernelNet for image deconvolution.

References:

[1] G. H. Golub and V. Pereyra. **"The differentiation of pseudo-inverses and nonlinear least squares problems whose variables separate."** In: *SIAM J. Num. Anal. (SINUM)* 10(2) (1973), 413–432. DOI: 10.1137/0710036

[2] D. P. O'Leary and B. W. Rust. **"Variable projection for nonlinear least squares problems."** In: *Comput. Opt. Appl.* 54(3) (2013), 579–593. DOI: 10.1007/s10589-012-9492-9

[3] P. Kovács, G. Bognár, C. Huber, and M. Huemer. **"VPNet: Variable Projection Networks."** In: *Int. J. Neural Syst.* (2021), 2150054. DOI: 10.1142/S0129065721500544

[4] T. Li et al. **"WaveletKernelNet: An Interpretable Deep Neural Network for Industrial Intelligent Diagnosis."** In *IEEE Trans. Syst. Man Cybern.* 52(4) (2022), 2302–2312. DOI: 10.1109/TSMC.2020.3048950

[5] L. Huber. **"A friendly intro to adversarial attacks."** Online: https://towardsdatascience.com/fooling-neural-networks-with-adversarial-examples-8afd36258a03 (accessed 16 September 2023)

[6] C. Szegedy et al. **"Intriguing properties of neural networks."** (2014), arXiv: 1312.6199

[7] D. Y. Riabkov and E. V. R. Di Bella. **"Blind identification of the kinetic parameters in three-compartment models."** In *Phys. Med. Biol.* 49(5) (2004), 639. DOI: 10.1088/0031-9155/49/5/001

[8] Q-Y. Chen et al. **"BFGS method based variable projection approach for image restoration."** In: *IET Image Process.* 15 (2021), 2854–2865. DOI: 10.1049/ipr2.12270

[9] D. Ren et al. **"Neural Blind Deconvolution Using Deep Priors."** (2020), arXiv: 1908.02197