****
********** HORA INFORMATICAE **********
****
**********(založeno v r. 1994)**********
****

V pondělí 19. 2. 2018 ve 14:00 se bude
ve velké zasedačce (č. 318, 2. poschodí)
Ústavu informatiky AV ČR, v. v. i.,
Pod Vodárenskou věží 2, Praha 8 - Libeň
konat přednáška

Evolving Deep Neural Networks Architectures

Petra Vidnerova, UI AV CR

Abstract:
Deep neural networks have become the state-of-art methods in many fields of machine learning recently. Still, there is no easy way how to choose a network architecture which can significantly influence the network performance.

This work is a step towards an automatic architecture design. We propose an algorithm for an optimization of a network architecture based on genetic algorithms and evolution strategies. The algorithm is inspired by and designed directly for the Keras library which is one of the most common implementations of deep neural networks. The proposed algorithm is tested on MNIST data set and the prediction of air pollution based on sensor measurements, and it is compared to several fixed architectures and support vector regression. Both fully connected feed-forward networks and convolutional networks are evolved.

In the second part of the talk, we mention a simple way how to increase the robustness of deep neural network models to adversarial examples.
We propose a new architecture obtained by stacking deep neural network and RBF network. It is shown on experiments that such architecture is much more robust to adversarial examples than the original one while its accuracy on legitimate data stays more or less the same.