

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Student: Pavel Jakš
Studijní program: Aplikace přírodních věd
Studijní obor: Matematická informatika
Název práce (česky): Robustní strojové učení a adversariální vzorky
Název práce (anglicky): Robust machine learning and adversarial examples

Pokyny pro vypracování:

- 1) Nastudovat základy strojového učení.
- 2) Nastudovat základy neuronových sítí a konvolučních vrstev.
- 3) Nastudovat adversariální vzorky a vybrané typy útoků, například FGSM a CW útoky.
- 4) Nastudovat robustně trénované neuronové sítě.
- 5) Naimplementovat vybrané typy útoků.
- 6) Analyzovat rozdíly v útocích na standardní a robustně trénované neuronové sítě.

Doporučená literatura:

- 1) I. Goodfellow, Y. Bengio, A. Courville, Deep Learning. MIT Press, 2016.
- 2) I. Goodfellow, J. Shlens, C. Szegedy, Explaining and Harnessing Adversarial Examples. In 'International Conference on Learning Representations', ICLR 2015.
- 3) J. Nocedal, S. Wright, Numerical optimization. Springer Science & Business Media, 2006.

Jméno a pracoviště vedoucího bakalářské práce:

Mgr. Lukáš Adam, Ph.D.

Katedra počítačů, Fakulta elektrotechnická, České vysoké učení technické v Praze, Karlovo náměstí 13, 121 35, Praha 2

Jméno a pracoviště konzultanta:

Datum zadání bakalářské práce: 31.10.2021

Datum odevzdání bakalářské práce: 7.7.2022

Doba platnosti zadání je dva roky od data zadání.

V Praze dne 12. října 2021

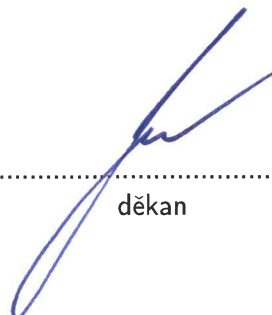


garant oboru



vedoucí katedry





děkan