



ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
Fakulta jaderná a fyzikálně inženýrská



Robustní strojové učení a adversariální vzorky

Robust machine learning and adversarial examples

Bakalářská práce

Autor: **Pavel Jakš**
Vedoucí práce: **Mgr. Lukáš Adam, Ph.D.**
Akademický rok: 2021/2022

- Zadání práce -

- Zadání práce (zadní strana) -

Poděkování:

Chtěl bych zde poděkovat především svému školiteli - panu doktoru Adamovi - za pečlivost, ochotu, vstřícnost a odborné i lidské zázemí při vedení mé bakalářské práce.

Čestné prohlášení:

Prohlašuji, že jsem tuto práci vypracoval samostatně a uvedl jsem všechnu použitou literaturu.

V Praze dne 7. července 2022

Pavel Jakš

Robustní strojové učení a adversariální vzorky

Obor: Matematická informatika

Vedoucí práce: Mgr. Lukáš Adam, Ph.D., Katedra počítačů, Fakulta elektrotechnická, České vysoké učení technické v Praze, Karlovo náměstí 13, 121 35, Praha 2

[illegible]

Klíčová slova: klíčová slova (nebo výrazy) seřazená podle abecedy a oddělená čárkou

Robust machine learning and adversarial examples

[illegible]

Key words: keywords in alphabetical order separated by commas

Obsah

Úvod	11
1 Neuronové sítě	13
1.1 MLP	13
1.2 Konvoluční neuronové sítě	13
1.3 Učení neuronové sítě	13
2 Adversariální vzorky	15
2.1 Metody generování adversariálních vzorků	15
2.1.1 FGSM	15
2.1.2 Iterativní FGSM	15
3 Robustní učení neuronové sítě	17
Závěr	19

Úvod

Text úvodu....

Kapitola 1

Neuronové sítě

1.1 MLP

1.2 Konvoluční neuronové sítě

1.3 Učení neuronové sítě

Kapitola 2

Adversariální vzorky

2.1 Metody generování adversariálních vzorků

2.1.1 FGSM

2.1.2 Iterativní FGSM

Kapitola 3

Robustní učení neuronové sítě

Závěr

Text závěru....

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.