BACHELOR'S THESIS ASSIGNMENT

I. Personal and study details

Student's name: **Kasl Tomáš** Personal ID number: **474747**

Faculty / Institute: **Faculty of Electrical Engineering**

Department / Institute: **Department of Cybernetics**

Study program: **Open Informatics**

Branch of study: **Computer and Information Science**

II. Bachelor's thesis details

Bachelor's thesis title in English:

Strategic Games in Adversarial Classification Problems

Bachelor's thesis title in Czech:

Strategické hry v problémech strojové klasifikace s protivníkem

Guidelines:

1. The student will study the elements of game theory [4] with particular attention to the computation of Nash equilibria in two-person games over possibly infinite strategic spaces.
2. The main goal of the thesis is to investigate selected game-theoretic approaches to adversarial machine learning problems; see [1] and [3] for a recent survey. The main emphasis will be on adversarial hypothesis testing games developed in [2]. The student will investigate this model and evaluate its performance using simulations. Specifically, he will:
a) Compare the game-theoretic model of adversarial attacks with the usual Neyman-Pearson or Bayesian framework for hypothesis testing.
b) Run a series of experiments showing the convergence to equilibria for large sample sizes.
c) Evaluate the behavior of error exponents.

Bibliography / sources:

[1] P. Dasgupta and J. Collins. A survey of game theoretic approaches for adversarial machine learning in cybersecurity tasks. AI Magazine, 40(2):31–43, 2019.
[2] S. Yasodharan and P. Loiseau. Nonzero-sum adversarial hypothesis testing games. In Advances in Neural Information Processing Systems, pages 7310–7320, 2019.
[3] L. Dritsoula, P. Loiseau, and J. Musacchio. A game-theoretic analysis of adversarial classification. IEEE Transactions on Information Forensics and Security, 12(12):3094–3109, 2017.
[4] Y. Shoham and K. Leyton-Brown. Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations. Cambridge University Press, New York, NY, USA, 2008.

Name and workplace of bachelor's thesis supervisor:

doc. Ing. Tomáš Kroupa, Ph.D., Artificial Intelligence Center, FEE

Name and workplace of second bachelor's thesis supervisor or consultant:

Date of bachelor's thesis assignment: **08.01.2020** Deadline for bachelor thesis submission: _____

Assignment valid until: **30.09.2021**

doc. Ing. Tomáš Kroupa, Ph.D. Supervisor's signature	doc. Ing. Tomáš Svoboda, Ph.D. Head of department's signature	prof. Mgr. Petr Páta, Ph.D. Dean's signature

© ČVUT v Praze, Design: ČVUT v Praze, VIC

III. Assignment receipt

The student acknowledges that the bachelor's thesis is an individual work. The student must produce his thesis without the assistance of others, with the exception of provided consultations. Within the bachelor's thesis, the author must state the names of consultants and include a list of references.

Date of assignment receipt

Student's signature

© ČVUT v Praze, Design: ČVUT v Praze, VIC