Supervisor assessment of Bachelor's Thesis

Student: Gaňo Martin
Title: Improving Robustness of Neural Networks against Adversarial Examples (id 22999)
Supervisor: Češka Milan, RNDr., Ph.D., DITS FIT BUT

1. **Assignment comments**
   Jedná se o poměrně obtížné zadání, které vyžadovalo pochopení existujících metod pro útoky (typu "adversarial examples") na neuronové sítě (NS) a související metody obrany. Tyto metody byly implementovány a unifikovány v rámci jednoho frameworku a vyhodnoceny na klasických architekturách NS. Zadání bylo splněno: framework umožnuje reprodukovat state-of-the-art výsledky v této oblasti a rovněž dále experimentovat s těmito metodami.
2. **Literature usage**
   Student byl velice aktivní ve studiu existující literatury. Samostatně dohledával existující metody útoku a obrany a snažil se zorientovat v této velice aktivní vědecké oblasti.
3. **Assignment activity, consultation, communication**
   Student byl velice aktivní po celou dobu řešení BP. Student dodržoval stanovené termíny a na konzultace chodil připraven. Bohužel se však do psaní textu BP pustil velice pozdě a postupoval dost pomalu, což mělo negativní dopad na dokončení práce (viz další bod).
4. **Assignment finalisation**
   Práce nebyla dokončena v dostatečném předstihu, a tudíž její finální obsah nebyl dostatečně konzultován, což vedlo k tomu, že některé textové části práce mají horší kvalitu.
5. **Publications, awards**
   Práce byla publikována na studentské konferenci EXCEL 2020, kde získala cenu odborné veřejnosti. Vytvořený framework by měl být v budoucnu dostupný formou open-source, a tak umožnit dále experimentovat s metodami pro návrh robustních NS.
6. **Total assessment** **very good (B)**

Toto hodnocení reflektuje větší obtížnost zadání, samostatný přístup studenta ale i horší kvalitu textové části BP. Pozitivně hodnotím experimentální vyhodnocení jednotlivých metod - bohužel prezentace výsledků v BP byla dělána na poslední chvíli, a tudíž působí trochu chaoticky.

In Brno 18 June 2020

Češka Milan, RNDr., Ph.D.
supervisor