

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Combining verification methods and adversarial sample generation with game-theoretic frameworks
Jméno autora:	Bc. Ondřej Skoumal
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Vedoucí práce:	doc. Mgr. Branislav Bošanský, Ph.D.
Pracoviště vedoucího práce:	Katedra počítačů

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání	náročnější
<i>Hodnocení náročnosti zadání závěrečné práce.</i>	
Zadáním, ktoré bohužiaľ nie je uvedené v samotnej práci, bola analýza existujúcich metód verifikácie neurónových sietí a metód pre hľadanie adversariálnych príkladov a preskúmanie možnosti ich využitia pre riešenie situácie, kedy je klasifikátor strojového učenia použitý pre rozhodovanie jedného hráča nad vstupom, ktorý generuje jeho oponent. Zásadným rozdielom oproti štandardnej formulácii problému verifikácie prípadne hľadania adversariálnych príkladov je prítomnosť ohodnocujúcej funkcie – oponent nielen že hľadá adversariálny príklad, ale zo všetkých možných adversariálnych príkladov hľadá taký, ktorý maximalizuje jeho očakávaný zisk. Vzhľadom k tomu, že úlohou študenta bolo preskúmať adaptáciu rôznych metód novým smerom, ktorý nie je bežný a zároveň zásadne komplikuje úlohu hľadania adversariálnych príkladov, hodnotím zadanie ako náročnejšie.	

Splnění zadání	splněno
<i>Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a příčiny jednotlivých nedostatků.</i>	
Študent v podstate splnil zadanie – naštudoval danú problematiku, popísal a zakategorizoval možné prístupy a vybrané metódy z nich implementoval. Bohužiaľ vlastné zhrnutie nadobudnutého poznania a porovnanie rôznych metód je v práci popísané veľmi nejasne.	

Aktivita a samostatnost při zpracování práce	D - uspokojivě
<i>Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven. Posuďte schopnost studenta samostatně tvůrčí práce.</i>	
Študentova aktivita v priebehu vypracovávaní diplomovej práce zásadne kolísala – miestami bolo vidieť veľký záujem a postup v prácach, študent prichádzal samostatne s nápadmi ako riešiť technické problémy a spolupráca bola príkladná. Inokedy sa študent dlhé obdobie vôbec neozval a práca nepokračovala. Termín odovzdania bol na študentovu žiadosť posunutý, pričom hlavne v roku 2021 pred odovzdaním študent vykonal najviac práce. Zlé časové rozvrhnutie postupu však spôsobilo, že text práce je veľmi slabý keďže nebolo možné spraviť viacero iterácií nad hotovým textom a viaceré kapitoly som ako vedúci čítal prvýkrát až po odovzdaní.	

Odborná úroveň	C - dobře
<i>Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.</i>	
Po technickej stránke (nehľadiac na popis v texte práce) je výsledok študentovej práce zaujímavý – hlavne návrh a technická realizácia novej neurónovej siete (nazvanej Utility Estimation Net), pomocou ktorej je možné vôbec uvažovať o využití existujúcich metód verifikácie a hľadania adversariálnych príkladov pre danú úlohu. Špeciálne pozitívne hodnotím ako študent identifikoval a riešil problémy týkajúce sa hľadania optimálnych adversariálnych príkladov proti zmiešanej stratégii obrancu.	

Formální a jazyková úroveň, rozsah práce

D - uspokojivě

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Ako už bolo spomenuté, vlastný text práce je jej najslabšou časťou a je vidieť, že študent ho dokončoval na poslednú chvíľu – v texte je veľa gramatických chýb, miestami chýbajú správne číselné odkazy na kapitoly / obrázky, používanie termínov predchádza ich definície (napr. popis double-oracle frameworku pre spojité hry využíva terminológiu predstavenú v ďalších kapitolách), popis experimentov je nejasný, v texte nie je jasné porovnanie jednotlivých metód, aby boli zrejme diskutované výhody a nevýhody jednotlivých prístupov.

Výběr zdrojů, korektnost citací

A - výborně

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

K výběru zdrojov a ich spracovaniu nemám výhrady.

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

Vložte komentář (nepovinné hodnocení).

III. CELKOVÉ HODNOCENÍ A NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení.

Študent spracovával náročnejšie zadanie, ktorého rozsah a technické riešenie dostatočne napĺňa predpoklady kladené na diplomovú prácu. Text však pôsobí nedokončeným dojmom, zásadne komplikuje pochopiteľnosť navrhnutých riešení a znižuje kvality práce.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **D - uspokojivě**.

Datum: 18.1.2022

Podpis: