FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Hodnocení vedoucího závěrečné práce

Vedoucí práce:	Mgr. Martin Jureček, Ph.D.
Student:	Bc. Matouš Kozák
Název práce:	Aplikace zpětnovazebního učení na vytváření adversariálních vzorků škodlivého softwaru
Obor / specializace:	Teoretická informatika
Vytvořeno dne:	23. ledna 2023

Hodnotící kritéria

1. Splnění zadání

- ▸ [1] **zadání splněno**
  [2] zadání splněno s menšími výhradami
  [3] zadání splněno s většími výhradami
  [4] zadání nesplněno

Všechny body popsané v pokynech pro vypracování práce považuji za splněné.

2. Písemná část práce 97 /100 (A)

Práce je dobře členěná a v textu se vyskytuje minimální počet překlepů. Uvedené zdroje jsou relevantní a práce má odpovídající rozsah. Je jasně vymezen přínos studenta a navíc poměrně široce zpracovaná část o souvisejících pracích.

3. Nepísemná část, přílohy 98 /100 (A)

Student upravil a doplnil stávající skripty pro generování adversariálních vzorků, přičemž kladl velký důraz na zachování původní funkčnosti programů, která často ve stávajících pracích byla porušena. Všechny nástroje použité v práci jsou relevantní a experimenty lze zopakovat a ověřit výsledky.

4. Hodnocení výsledků, jejich využitelnost 100 /100 (A)

Práce má potenciál být využita v praxi, konkrétně v antivirovém průmyslu, kde by se podobné generátory adversariálních vzorků mohly využít při vytváření obranných technik. Práce vylepšila stávající generátory adversariálních vzorků a má potenciál k publikování.

5. Aktivita studenta

▸ [1] **výborná aktivita**
[2] velmi dobrá aktivita
[3] průměrná aktivita
[4] slabší, ale ještě dostatečná aktivita
[5] nedostatečná aktivita

Student pravidelně konzultoval s vedoucím práce nejnovější výsledky a další kroky po celou dobu práce bez větších časových oken.

6. Samostatnost studenta

▸ [1] **výborná samostatnost**
[2] velmi dobrá samostatnost
[3] průměrná samostatnost
[4] slabší, ale ještě dostatečná samostatnost
[5] nedostatečná samostatnost

Protože se student v dané problematice pohybuje zhruba dva roky, tak v rámci své diplomové práce zvládl pracovat zcela samostatně.

Celkové hodnocení 98 /100 (A)

Práci hodnotím po teoretické i praktické části jako nadprůměrnou. Student si samostatně nastudoval potřebnou teorii z oblasti reinforcement learningu a dokázal ji aplikovat na generování adversariálních vzorků, přičemž musel překonat poměrně složité technické problémy související se zachováním funkčnosti škodlivých programů. Celkově práci hodnotím známkou A.

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Aktivita studenta

V souvislosti s průběhem a výsledkem práce posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven.

Samostatnost studenta

V souvislosti s průběhem a výsledkem práce posuďte schopnost studenta samostatné tvůrčí práce.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.