POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Využití algoritmů verifikace a generování adversariálních vstupů v herně-teoretických algoritmech**
Jméno autora:	**Ondřej Skoumal**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Oponent práce:	Ing. Ondřej Kuželka, Ph.D.
Pracoviště oponenta práce:	Katedra počítačů

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **průměrně náročné**

Hodnocení náročnosti zadání závěrečné práce.

V práci vložené zadání neobsahuje pokyny pro vypracování. Z toho důvodu mohu jen odhadovat, co bylo skutečným zadáním. Nejsem si jistý, jestli je vůbec možné práci s chybějícími pokyny uznat, ale nechám to na komisi a vedoucím práce.

Předpokládané zadání se mi jevilo jako průměrně náročné. Na druhou stranu je ale možné, že v důsledku byla práce mnohem náročnější, než jak se zdá, a to z nějakých praktických problémů vzniklých při implementaci.

Splnění zadání **splněno s většími výhradami**

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 případně i příčiny jednotlivých nedostatků.

Stejně jako u předchozího bodu, toto nemohu ohodnotit, protože v práci chybí pokyny pro vypracování. Nechávám tedy na komisi a vedoucím práce (který práci akceptoval, takže předpokládám, že zadání splněno bylo), aby toto zhodnotili – já to teď nemohu zhodnotit bez znalosti pokynů řešení.

Zvolený postup řešení **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Postup řešení se zdá vhodný. Student zkombinoval double-oracle algoritmus s několika metodami pro generování adversariálních příkladů (z nichž jako nejlepší se ukázala metoda založená na optimalizačním algoritmu známém jako projected gradient descent).

Odborná úroveň **A - výborně**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Práce využívá netriviálních poznatků z teorie her. Dále využívá poznatků z neuronových sítí a především metod pro hledání adversariálních příkladů apod.

Formální a jazyková úroveň, rozsah práce **E - dostatečně**

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

Jazyková stránka práce je velmi špatná. Začátek práce mi sice přišel čtivý a byl bych ochotný i přimhouřit oči nad mnohými gramatickými chybami, jenže jak jsem postupoval se čtením, jazyková stránka byla horší a horší a text často i díky tomu (ale nejen kvůli tomu) méně srozumitelný. Přitom jsou dnes k dispozici nástroje (zdarma), které by většinu gramatických chyb pomohly odstranit. Kromě velmi špatné angličtiny je dalším problémem struktura práce, která není nejvhodnější pro práci tohoto typu.

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.

Rozsah i volba citací je podle mne v pořádku.

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, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Téma práce je zajímavé, stejně tak se mi líbí i základní myšlenka zkombinování double-oracle algoritmu s existujícími metodami pro generování adversariálních příkladů. Oceňuji, že student nezůstal u jedné metody, ale popsal a vyzkoušel jich v práci hned několik. Taky oceňuji, že se v práci snažil rozebírat a zdůvodňovat jednotlivá rozhodnutí ohledně zvoleného postupu řešení, vážit jejich pozitiva a negative. Některá rozhodnutí mi nebyla úplně jasná - například proč bylo nutné modelovat útočníkovu nejlepší odpověď pomocí neuronové sítě (koneckonců utilita se, alespoň pokud jsem to pochopil, neučí z dat, ale je známa), a ne nějak přímočařeji. Věřím, že v tomto případě šlo jen o to, že jsem něco z práce nepochopil. Tím se dostávám k samotnému textu práce, který ji poměrně dost sráží. Nejde jen o gramatické chyby, které jsem popisoval výše, ale celkově je úroveň textu nevalná. Z toho důvodu práci hodnotím stupněm C (na druhou stranu, vzhledem k tomu, že jsem ne vše pochopil, což dávám za vinu jednak textu samotnému, ale částečně také tomu, že nejsem úplným expertem v oboru, je možné, že mi unikly některé jiné nedostatky práce).

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **C - dobře.**

Datum: 20.6.2021 Podpis: