POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Min-max optimization methods inadversarial learning**
Jméno autora:	**Tomáš Kasl**
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 **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Zadání se jeví jako náročnější, protože je vyžadována jednak implementace netriviálních state-of-the-art, jednak jejich analýza z pohledu teorie her a optimalizace (bod 2 v zadání).

Splnění zadání **splněno**

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.

Domnívám se, že zadání bylo splněno. Vlastnosti nalezených řešení byly analyzovány především empiricky, ale to se domnívám není na škodu. Splněna je i volitelná část zadání (bod 3).

Zvolený postup řešení **vynikající**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Z implementačního hlediska se postup jeví jako velmi dobře zvolený – v práci je dobře zdůvodněna volba JAX frameworku. Experimenty jsou navržené dobře. Celkově postup, zdá se, odpovídá zadání. Vzhledem k tomu, že úkolem bylo implementovat state-of-the-art metody a analyzovat je (tady znovu předpokládám, že se jednalo o analýzu empirickou – je možné, že tím vedoucí práce měl na mysli něco jiného, ale to ze zadání a z práce nedokážu posoudit), tak se jednalo o postup na jednu stranu přímočarý, ale dozajista na triviální. Z práce je vidět, že jí student věnoval velmi mnoho času.

Odborná úroveň **A - výborně**

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

Odborná úroveň, především z hlubokého učení, je na vysoké úrovni.

Formální a jazyková úroveň, rozsah práce **B - velmi dobře**

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

Práce obsahuje možná trochu příliš mnoho malých gramatických chyb a překlepů, které by bylo možné snadno odstranit (například s využitím automatických nástrojů). Způsob psaní citací i s názvem článku v hlavním textu je v tomto oboru poměrně nezvyklý (za to ale hodnocení nesnižuji). Co mi vadilo při čtení práce asi nejvíc, je její struktura. Autor řadí jednotlivé myšlenky a postřehy za sebe bez zjevné struktury, což má za následek, že se v práci čtenář velmi rychle ztratí (a je zahlcen detaily).

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.

Citace se zdají být vybrané správně (k jejich neobvyklému použití v textu jsem se vyjádřil v předchozím bodu).

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

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.*

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.

Na práci oceňuji především dvě věci – rozsah a střízlivé zhodnocení dosažených výsledků na konci práce. Domnívám se, že autor práce odvedl opravdu velký kus experimentální práce spočívající ve vyhodnocení zkoumaných metod na různých datasetech a různých architekturách neuronových sítí. Autor rovněž navrhl vlastní heuristické vylepšení původního algoritmu (které v práci označuje jako Algoritmus 2). Ačkoliv tento algoritmus, jak sám autor píše „[…] possibly break[s] the math behind making the inner optimization concave“, tak je založen na rozumném pozorování. Na konci pak autor shrnuje výsledkym jichž dosáhl, velmi střízlivě, když uvádí případy, kde zkoumané přístupy fungují a kde selhávají (a nejen, že nezajišťují robustnost vůči adversariálním datům, ale navíc i zhoršují kvalitu modelů na obyčejných datech). Myslím si, že takové realistické zhodnocení je velmi přínosné pro komunitu. Škoda jen, že práce není lépe strukturována a že obsahuje zbytečně mnoho chyb v angličtině, které trochu kazí dojem z ní. I tak se ale domnívám, že jde o práci zdařilou, především tedy experimentální, a pozitiva výrazně převažují nad negativy.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **A - výborně.**

Datum: 13.6.2024 Podpis: