ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK VEDOUCÍHO ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Min-max optimization methods in adversarial learning**
Jméno autora:	**Bc. Tomáš Kasl**
Typ práce:	diplomová
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra počítačů
Vedoucí práce:	Doc. Ing. Tomáš Kroupa, Ph.D.
Pracoviště vedoucího práce:	Katedra počítačů

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **průměrně náročné**

Hodnocení náročnosti zadání závěrečné práce.

Práce vyžadovala znalost základních technologií pro deep learning a dále novější poznatky z oblasti tzv. adversariálního učení, které se týkají elementárních iteračních metod (projektovanýc gradient a jeho varianty). Cílem práce nebyl rozvoj těchto metod ani nástrojů hlubokého učení jako takových, ale spíše jejich dovedné využití a skloubení v jedné implementaci pomocí známých nástrojů.

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.

Zadání DP bylo zcela splněno.

Zvolený postup řešení **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Autor využil známé útoky na neuronové sítě i poměrně jednoduché modifikace dat pomocí eps-perturbace. Implementoval i nové metody pro robustifikaci neuronových sítí, jejich srovnání na datech bylo jedním z hlavních cílů práce.

Odborná úroveň **A - výborně**

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

Student dokázal plně využít znalosti z kurzu Deep Learning a ze studia článku [M. Nouiehed, M. Sanjabi, T. Huang, J. D. Lee, and M. Razaviyayn, "Solving a class of non-convex min-max games using iterative first order methods," in Advances in Neural Information Processing Systems 32, 2019]. Dokázal tak implementovat několik modelů na základě pestré sbírky dat a použít při tom nejmodernější herně-teoretické metody pro adversarialní ML. Kladně lze hodnotit jeho pokus o modifikaci jedné z nich, I když není teroreticky podložen.

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

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

Zmíním několik drobných formálních nedostatků, které bohužel nebyl student schopen odstranit. Jedná se zejména o strukturu některých kapitol a mnoho odstavců, které by si zasloužily spojit do jednoho. Citace jsou místy nestandardní a citovaná práce jen tak „visí" v textu bez zakončení věty.

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.

Student byl značně aktivní při shánění zdrojů a nových dat. DP obsahuje všechny důležité reference.

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.

Tomáš Kasl provedl mnoho experimentů s různými daty a to i nad rámec mého očekávání a požadavků v zadání DP. Díky konzultaci s D. Myshkinem se dokázal rychle zorientovat i v oblasti klasifikace obrázků a adversariálních útoků na ně. Kladně hodnotím vlastní invenci při přípravě a zpracování zvukových dat. I přes výše zmíněné drobné formální nedostatky tak práci hodnotím nejvyšším stupněm.

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

Datum: 16.6.2024 Podpis: