ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK VEDOUCÍHO ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Adversarialní útoky na klasifikátory textu
Jméno autora:	David Herel
Typ práce:	diplomova
Fakulta/ústav:	FEL CVUT
Katedra/ústav:	13136 - katedra počítačů
Vedoucí práce:	Tomas Mikolov
Pracoviště vedoucího práce:	CIIRC CVUT

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání **A**

Hodnocení náročnosti zadání závěrečné práce.

Prace byla vyzkumneho charakteru. Bylo treba prostudovat soucasnou literaturu, nalezt slabiny soucasnych pristupu a navrhnout nove reseni problemu.

Splnění zadání **A**

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.

Prace splnuje zadani. To bylo v prubehu vypracovani rozsireno, protoze student nalezl necekanou slabinu soucasnych adversarialnich utoku na textove klasifikatory. Timto pribyla nutnost definovat lepsi metriku podobnosti textu, ktera zachova semantickou informaci vcetne sentimentu.

Zvolený postup řešení **A**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Postup byl zvolen spravne a pravidelne konzultovan s vedoucim.

Odborná úroveň **A**

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

Prace vyraznym zpusobem rozsiruje state-of-the-art v dane oblasti, vysledky jsou publikovatelne na mezinarodni NLP konferenci.

Formální a jazyková úroveň, rozsah práce **A**

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

Jazykova i formalni uroven prace je v poradku.

Výběr zdrojů, korektnost citací **A**

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 vyuzil vsechny relevantni zdroje a spravne je v praci cituje.

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.

Hlavni vysledky prace ukazuji, ze soucasne techniky pouzivane pro utoky na klasifikatory textu maji zasadni nedostatek - casto nezachovavaji puvodni vyznam textu. Dale je navrzen zpusob, jak lze tento nedostatek castecne odstranit pomoci nove

metody pro vypocet reprezentaci textu. Tyto nove poznatky jsou publikovatelne na mezinarodni vedecke konferenci v oblasti zpracovani jazyka a mohou mit potencialne velky impakt v oboru.

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.

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

Datum: 6/5/2022 Podpis: