Posudek vedoucího bakalářské práce

Název: Robustní strojové učení a adversariální vzorky
Autor: Pavel Jakš

Shrnutí obsahu práce

Práce obsahuje dvě části rozdělených do sedmi kapitol. První část je zaměřena na vybudování teorie pro hledání adversiálních vzorků a pro trénování robustních klasifikátorů. Druhá část obsahuje implementaci teorie.

Celkové hodnocení práce

Téma bakalářské práce mi přijde jako nadprůměrně obtížné díky tomu, že student musel zkombinovat větší množství rozdílných teoretických konceptů a poté je naprogramovat.

Z mého pohledu student nezvolil pro psaní práce nejvhodnější strategii, kdy se snažil udělat spoustu věcí sám a na první konzultaci přišel až po několika měsících práce. Na druhou stranu tuto samostatnost oceňuji. Toto jsme si ale vyjasnili a konzultace se poté staly pravidelnějšími. Toto snad bylo též důvodem menšího časového presu v blízkosti termínu odevzdání, kdy jsem si přestavoval, že některé části budou lépe zpracovány (lépe natrénovaná síť či lépe zpracovaná metoda hledání parametru λ). Jako jedinou otázku bych položil:

- Jakým způsobem by vypadalo hledání λ pomocí metody bisekce? Je metoda bisekce konvergentní v klasickém a tomto případě? Proč?

Obecně jsem s prací a přístupem studenta spokojen a *doporučuji bakalářskou práci uznat jako splněnou*. Práci doporučuji k obhajobě a navrhuji hodnotit ji známkou B.

Mgr. Lukáš Adam, PhD
Fakulta elektrotechnická, České vysoké učení technické v Praze, Praha
12. 8. 2022