

Review of Bachelor's Thesis

Student: Hudák David
Title: Formal Analysis of Neural Networks (id 24620)
Reviewer: Lengál Ondřej, Ing., Ph.D., DITS FIT BUT

1. Assignment complexity **more demanding assignment**

Zadání je obtížnější, bylo potřeba seznámit se s principy práce neuronových sítí a s principy verifikace jejich robustnosti, což jsou témata na fakultě nevyučovaná, a dále bylo nutné proniknout do frameworku VeriNET a upravit ho za pomoci nových strategií pro větvení.

2. Completeness of assignment requirements **assignment fulfilled**

Zadání bylo splněno.

3. Length of technical report **in usual extent**

Technická zpráva je v obvyklém rozmezí.

4. Presentation level of technical report **75 p. (C)**

Prezentační stránka technické zprávy je vcelku dobrá, struktura je v pořádku, kapitoly na sebe navazují a mají vhodný rozsah. Práce však bohužel není příliš vhodná pro širší publikum, např. předpokládá znalost neuronových sítí a úvod do toho, jak probíhá verifikace těchto sítí, je také velmi zrychlený a obtížný na pochopení. Určitě by pomohlo více jednoduchých a názorných příkladů.

První dvě kapitoly obsahují různá subjektivní tvrzení autora, např. odstavce "A little technical reflection" u podsekcí v sekci 2.5 působí dojmem "co autora zrovna napadlo."

V kapitole s experimenty občas výsledné časy překračují timeout a v některých tabulkách se místo čísla vyskytuje hodnota not-a-number (nan), což nevím, jaký má význam. Dále se v této kapitole objevují neodkazované tabulky.

Některé odstavce se v práci vyskytují dvakrát, např. poslední dva odstavce kapitoly 2 jsou téměř stejné a podobně poslední dva odstavce sekce 4.2.

5. Formal aspects of technical report **85 p. (B)**

Technická zpráva je formálně na solidní úrovni. Má jediná výtka k typografii je, že popis tabulky se běžně dává nad tabulku, zatímco v práci je vždy pod tabulkou. Tabulky a obrázky v sekci 6 mohly být lépe rozmístěné.

Práce je psána angličtinou, kde se střídají velmi hezky čitelné pasáže s ne tak hezky čitelnými pasážemi obsahujícími zvláštní neanglické obraty. Určitě by pomohlo, kdyby si práci přečetl ještě někdo znalý angličtinu a tyto artefakty odstranil.

6. Literature usage **85 p. (B)**

Práce s literaturou je relativně v pořádku, až na to, že autor často cituje technickou zprávu na arXivu, i když by bylo lepší citovat článek ve sborníku konference či časopise (např. reference [21,24] by měli citovat článek na konferenci NeurIPS). Reference [16] je uvedena špatně.

Dále by bylo některé poznámky pod čarou, které obsahují jen odkaz, raději uvést jako normální referenci.

7. Implementation results **85 p. (B)**

Realizační výstup je ve formě

1. doplnění několika strategií pro výběr uzlu ve verifikační smyčce nástroje VeriNET a
2. vytvoření několika podpůrných skriptů.

Student demonstroval běh nástroje na svém počítači. Odevzdané zdrojové kódy, jejichž autorem je student, jsou vhodně komentované, avšak rozsah je velmi malý (cca 300 řádků Python kódu bez komentářů). Vzhledem k tomu, že původní nástroj VeriNET je distribuován ve verzovacím systému git, bych doporučoval, kdyby student pokračoval v používání nástroje pro správu verzí, což se bohužel nestalo.

Experimentální vyhodnocení je, na druhou stranu, extenzivní: porovnává vliv různých strategií na rychlost hledání nerobustního chování v neuronových sítích. Očekával bych však lepší shrnutí výsledků: místo 17 tabulek udělat vhodnou agregaci a prezentovat jen to nejzajímavější, a vhodně to zdůraznit. Zbytek výsledků by mohl být v příloze. Takto jsou možná zajímavé výsledky zředěny množstvím nezajímavých informací.

8. Utilizability of results

Dokáží si představit, že nově navržené metody by šlo použít pro urychlení některého z nástrojů pro verifikaci neuronových sítí a dotáhnout metody k publikaci či účasti v soutěži VNN-COMP pro verifikaci neuronových sítí.

9. Questions for defence

1. Plánujete se zúčastnit konference VNN-COMP, případně dotáhnout práci do podoby publikace?

10. Total assessment

83 p. very good (B)

Bakalářská práce Davida Hudáka přichází s novými strategiemi výběru uzlů pro větvení v přístupech pro formální verifikaci robustnosti neuronových sítí. Výsledky jsou zajímavé a mohou sloužit jako základ další práce. Práci navrhuji hodnotit známkou **velmi dobře (B)**.

In Brno 30 May 2022

Lengál Ondřej, Ing., Ph.D.
reviewer