Review of Bachelor's Thesis

Student: Marek Daniel
Title: Static Analysis Using Facebook Infer Focused on Errors in RCU-Based Synchronisation (id 25138)
Reviewer: Malík Viktor, Ing., DITS FIT BUT

1. Assignment complexity — **more demanding assignment**

Zadanie radím k náročnejším, hlavne kvôli tomu, že vyžadovalo detailné naštudovanie a pochopenie technológie Read-copy-update (RCU). RCU je súčasťou jadra Linuxu, ktorého zdrojové kódy sú často problémom aj pre skúsených softvérových inžinierov. Ďalej musel študent navrhnúť nový prístup ku statickej analýze práce s RCU, čo je podľa mojich znalostí prvá práca tohoto druhu. K náročnosti zadania prispieva aj fakt, že pochopenie teórie statickej analýzy a nástroja Facebook Infer, ktorý bol v práci použitý, je netriviálnou úlohou prekračujúcou bežné znalosti bakalárskeho štúdia na FIT.

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

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

Práca obsahuje 50 strán vysádzaného textu, čo zodpovedá očakávanému rozsahu. Text je hutný a neobsahuje zbytočné časti.

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

Prvá časť práce popisujúca koncepty, na ktorých práca stavia je dobre štukturovaná. To však neplatí pre druhú časť práce, ktorá predstavuje samotné študentove riešenie. Táto časť je rozdelená do dvoch kapitol pomenovaných "Original design" a "Implementation", ktoré popisujú dve verzie riešenia, pričom v práci je použité len to uvedené v kapitole "Implementation". Kapitola "Original design" je teda venovaná prvej verzií návrhu, ktorá bola neskôr zahodená a nahradená inou. Nemám problém s predstavením viacerých verzií riešenia ilustrujúcich dôležité rozhodnutia, ktoré bolo nutné v priebehu riešenia spraviť, ale nechať čitateľa prečítať celú kapitolu o 11 stranách a následne mu oznámiť, že daný návrh bol do značnej miery prerobený, mi príde nešťastné. Navyše obidve zmienené kapitoly miešajú návrhové rozhodnutia a implementačné detaily, čo tiež neprospieva pochopiteľnosti textu.

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

Práca je písaná pomerne dobrou, no nie výbornou angličtinou. Text je bez problémov pochopiteľný, avšak obsahuje množstvo menších jazykových chýb (napr. používanie čiarok často pôsobí náhodne). Z typografického hľadiska je situácia podobná, na niektorých miestach by pomohlo lepšie formátovanie textu, ale tento problém nenarušuje celkovú pochopiteľnosť textu.

6. Literature usage — **98 p. (A)**

Práca s literatúrou je na výbornej úrovni. Študent bol schopný dohľadať a spracovať veľké množstvo textov súvisiacich s danou oblasťou, vďaka čomu je jasné, že uvedené riešenie je skutočne prvým svojho druhu v oblasti statickej analýzy paralelných programov. Mojou jedinou výhradou je formátovanie zoznamu literatúry, kde sa nachádza väčšie množstvo záznamov s autorom v tvare "Community, T. kernel development".

7. Implementation results — **90 p. (A)**

Riešenie je implementované ako plugin do nástroja Infer a obsahuje cca 1000 riadkov kódu v jazyku OCaml. Riešenie nie je extra zložité, no je plne funkčné a umožňuje automatické vyhľadávanie chýb v programoch používajúcich RCU, čo demonštrujú aj testovacie prípady vytvorené ako súčasť práce. Taktiež oceňujem pokus o spustenie analýzy nad jadrom Linuxu, ktorého komplilácia je pomerne zložitá a nástroj Infer ju nepodporuje. Napriek tomu, že tento pokus nebol úspešný, študent predstavil niekoľko originálnych nápadov, na ktorých je možné v budúcnosti stavať.

8. Utilizability of results

Podľa môjho názoru má práca veľký potenciál využitia ako v praxi, tak aj ako základ pre širší výzkum. RCU je synchronizačný mechanizmus používaný na mnohých miestach (hlavne v jadre Linuxu), ktorého správne použitie nie je úplne triviálne. Preto automatická analýza práce s RCU môže pomôcť včas odstrániť veľké množstvo programátorských chýb. Zároveň, keďže sa jedná o prvú prácu svojho druhu, považujem za pravedepodobnú možnosť publikovania výsledkov na medzinárodnom fóre, hoci v súčasnosti je navrhnutý prístup vcelku jednoduchý.

9. Questions for defence

1. V práci popisujete niekoľko rôznych typov chýb pri práci s RCU, ktoré ste odhalili pri analýze danej

technológie. Existujú podľa Vás ďalšie typy chýb, ktoré Váš zoznam nepokrýva?

2. Z popisu "less-or-equal" operátoru vyplýva, že na porovnanie dvoch abstraktných kontextov stačí, že obsahujú rovnaké zložky. Akým spôsobom sa zohľadňujú jednotlivé vlastnosti týchto zložiek (napr. skóre u post-conditions)?

10. Total assessment

88 p. very good (B)

Celkovo sa jedná o dobré spracovanie nadpriemerne náročného zadania, ktorého kvalitu však znižuje horší text. S ohľadom na vyššie uvedené skutočnosti navrhujem hodnotiť známkou **B (veľmi dobre)**, avšak v prípade kvalitnej obhajoby som ochotný podporiť zlepšenie známky na A.

In Brno 2 June 2022

Malík Viktor, Ing.
reviewer