FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	prof. Ing. Pavel Tvrdík, CSc.
Student:	Tomáš Homola
Název práce:	Certifikované algoritmy pro hledání minimální kostry
Obor / specializace:	Bezpečnost a informační technologie
Vytvořeno dne:	20. srpna 2021

Hodnotící kritéria

1. Splnění zadání

[1] zadání splněno
▸ **[2] zadání splněno s menšími výhradami**
[3] zadání splněno s většími výhradami
[4] zadání nesplněno

BP se zabývá obecně obtížným problémem verifikace správnosti algoritmů. V zadání byl uveden požadavek vydat s využitím lemmatu o řezech certifikát o optimálnosti minimální kostry. Splnění tohoto požadavku jsem však v práci nenašel. V příkladech implementace Jarníkova algoritmu doplněné vstupní a výstupní podmínky pro kontrakty funkcí se týkají stanovení mezí správných hodnot, ale aserce verifikující, že funkce pro nelezení minima vrací skutečně minimum jsem v příloze BP_Homola_Tomas_2021_Attachments/src/impl/Jarnik/findMin.c také nenašel. Nemyslím si tedy, že plně platí poslední věta abstraktu říkající, že výsledkem práce je plně verifikovaný algoritmus pro hledání minimální kostry v grafu. Verifikace se týká pouze kontrol rozsahu hodnot proměnných v rámci uvažovaných datových struktur. Dále bylo v zadání požadováno vyzkoušet verifikaci na verze Jarníkova algoritmu s různými datovými strukturami pro udržování hran budované komponenty, v BP se uvažuje pouze implementace s nejjednoššími datovými strukturami (poli) a nejjednodušší metodou hledání minima (lineární průchod neseřazeným polem). Autor měl zřejmě situaci ztíženou zjištěním, že původně zamýšlený framework VerifyableC, který byl v zadání předpokládán, se ukázal jako nepoužitelný a bylo nutné najít jiný, což se podařilo, v závěrech je toto vysvětleno.

2. Písemná část práce 75 / 100 (C)

Po formální stránce je BP typograficky v pořádku. Strukturovaný text je čitelný. Po stránce gramatické jsou chyby v interpunkci. Po věcné stránce BP začíná popisem instalace určitých balíčků frameworku Frama-C pro vytvoření prostředí pro formální deduktivní verifikaci programu v C, čtenář ale nemá představu o cílové architektuře prostředí. Cenná

je rešeršní část popisující základy Hoareovy logiky a neobvyklý anotační jazyk ACSL, byť některé teoretické koncepty nebyly v BP použity (např. axiomy). Na druhou stranu ale příklady ilustrující teoretické koncepty jsou primitivní a moc toho neilustru1jí. Kapitola 5 je sice strukturovaná v souladu s kroky metodiky minimálního kontraktu, které jsou pro funkci Jarnik.c postupně popisovány, ale ten hlavní výsledek, certifikát bezpečnosti celého programu v sekci 5.4., je prezentován pouze jako posloupnost snímků obrazovek systému Frama-C, kde se objevují i kroky, které v předchozí části nebyly pro implementaci Jarníkova algoritmu vysvětleny, např. výsledek interního dokazovacího systému Qed a Alt-Ergo. Očekával jsem zde hlubší analýzu nebo podrobnější komentáře, co všechno je tímto vlastně verifikováno. V kroku 4 výpis 50 chybí klauzule assigns, výpis 50 je identický s výpisem 49. Štítek old je vysvětlen na str. 27, ale použit byl už na str. 24.

3. Nepísemná část, přílohy 77 /100 (C)

Protože verifikace klíčové funkce findMin.c byla z důvodu nedostatku místa přesunuta do přílohy, očekával jsem podobně komentované vysvětlení, jak tato verifikace byla postupně vybudována, v příloze jsem však našel pouze výsledek.

4. Hodnocení výsledků, jejich využitelnost 80 /100 (B)

BP byla pojata jako úvod do metod a technologií formálních verifikací netriviálních algoritmů a pravděpodobně je zamýšleno tímto směrem pokračovat, čili očekávám navazující práce.

Celkové hodnocení 78 /100 (C)

Celkově BP hodnotím jako dobrou (C), nicméně vzhledem k tomu, že obtížnosti tématu a teorie, která se na fakultě nevyučuje v bakalářském programu, přesahuje práce náročnost předpokládanou u BP, lze ji hodnotit i lépe.

Otázky k obhajobě

Jak byste v daném prostředí zvoleného frameworku pro danou implementaci Jarníkova algoritmu formálně verifikoval minimálnost vytvořené kostry? Jaké vidíte limity použitého postupu a použité technologie v případě, že použijete pokročilejší datové struktury a rychlejší implementace Jarníkova algoritmu, kdy důkazy korektnosti začnou být komplikovanější?

Instrukce

Splnění zadání

Posuďte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posuďte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti.

Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posuďte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.