Posudek *vedoucího/oponenta** diplomové práce

Jméno a příjmení autora posudku: Jan Kofroň

Jméno a příjmení autora práce: David Škorvaga

Název práce: Analysis of a File System Using the Verifying C Compiler

---

Vlastní text (sem prosím napište text posudku, délka textu posudku není omezena):

Cílem diplomové práce bylo jednak demonstrovat použitelnost nástroje VCC pro verifikaci reálného kódu, konkrétně implementaci některého filesystému. Kromě případného nalezení chyb bylo úkolem i zdokumentovat postup a problémy při verifikaci a doplnit tak ne příliš kompletní dokumentaci nástroje VCC, který patří k nejlepším v oblasti verifikace vícevláknového kódu v jazyce C pomocí kontraktů. Je třeba zdůraznit, že se jednalo o výzkumnou práci, kde by selhání při pokusu o verifikaci, ke kterému nicméně nedošlo, neznamenalo selhání studenta ve smyslu diplomové práce, jak je explicitně uvedeno v zadání.

Práce není implementační, autor nicméně vytvořil velké množství specifikací jednotlivých funkcí v podobě kontraktů, které sumarizují sémantiku jednotlivých funkcí. Při modulární verifikaci jde o zejména o to, nenapsat preconditions příliš silné, aby bylo možné je splnit a místě volání těchto funkcí, a zároveň ani ne příliš slabé, aby bylo možné z nich dokázat odpovídající postcondition, To je obecně obtížný úkol, zejména proto, že v implementaci mohou být chyby a v tomto konkrétním případě i z důvodu absence formálního popisu jednotlivých typů anotací v dokumentaci.

Autor práce navzdory všem překážkám odvedl výbornou práci a vymezenou část implementace se mu povedlo dostatečně anotovat a na základě kontraktů ověřit i absenci odpovídajících typů chyb. Práci tedy plně doporučuji k obhajobě.

Doporučení k obhajobě:

Z výše uvedených důvodů práci *doporučuji* / ~~*nedoporučuji*~~* k obhajobě.

Vynikající práce vhodná pro soutěž studentských prací	ANO ☐

Seznam soutěží studentských prací, viz http://www.mff.cuni.cz/studium/bcmgr/prace/

Pokud jste výše zaškrtli ANO, zdůvodněte prosím svůj návrh, případně uveďte konkrétní soutěž, pro kterou je práce vhodná (rámeček lze nechat prázdný, pokud za dostatečné zdůvodnění považujete text posudku):

V Praze dne: 16.1.2015

Podpis:

** nehodící se škrtněte (vymažte)*

*** do SISu vkládejte formulář nepodepsaný (ve formátu PDF), podpis je potřeba doplnit až na vytištěný posudek.*