Posudek vedoucího diplomové práce

Jméno a příjmení autora posudku: Pavel Parízek

Jméno a příjmení autora práce: Vlastimil Dort

Název práce: String Analysis for Code Contracts

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

Cílem této práce bylo rozšířit velmi populární verifikační systém Code Contracts o podporu vlastností a podmínek, které se týkají textových řetězců. Code Contracts umožňují anotovat jednotlivé procedury a metody ve zdrojovém kódu pomocí kontraktů (preconditions, postconditions, invariants), a dále použít běhový nebo statický nástroj pro ověření platnosti kontraktů vzhledem ke implementaci třeba v jazyce C#. Statický nástroj, který se nazývá Clousot, používá verifikační techniky založené na takzvané abstraktní interpretaci.

Autor práce se rozhodl implementovat několik abstraktních domén, které definuje existující publikace [1], protože na základě důkladné analýzy zjistil, že tyto domény splňují naše požadavky. Implementace zahrnovala také rozšíření definice abstraktních domén na všechny operace nad řetězci, které podporuje platforma .NET. Jedná se o domény založené na délce řetězce, předponách, příponách, množinách znaků, takzvaných kostkách (to jsou množiny řetězců, kde intervaly určují počty opakování), a také doména založená na grafech.
Kromě toho autor ještě rozšířil jazyk Code Contracts o možnost specifikace vlastností ve formě regulárních výrazů, a integroval svou implementaci abstraktních domén do nástroje Clousot tak aby je bylo možné kombinovat s jinými doménami (určenými třeba pro číselné datové typy). Provedl také experimentální vyhodnocení přesnosti jednotlivých domén a rychlosti ověřování na několika menších programech.

Text je napsán v anglickém jazyce. Obsahuje úvod do abstraktní interpretace, popis systému Code Contracts a reprezentace textových řetězců na platformě .NET (včetně technických detailů), a také popis zajímavých vlastností, které se týkají řetězců a lze je zapsat pomocí regulárních výrazů. Největší část textu je věnována formální matematické definici abstraktních domén, jejich vlastností, a sémantice operací nad řetězci. Zbytek obsahuje popis architektury implementace a výsledky experimentálního vyhodnocení s krátkou diskuzí.

Kvalita zpracování implementace a textu je velmi vysoká. Nemám žádné výhrady ani k jednomu. Autor prokázal hluboký vhled do problematiky, a schopnost precizního uvažování a řešení složitých problémů výzkumného charakteru. Dokonce našel chybu v originální definici jedné z abstraktních domén a navrhl opravu.

Celkově tedy hodnotím práci jako výjimečně zdařilou.

[1] G. Costantini, P. Ferrara, and A. Cortesi. A Suite of Abstract Domains for Static Analysis of String Values. Software: Practice and Experience, 45(2), 2015.

Doporučení k obhajobě:

Z výše uvedených důvodů práci doporučuji 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: 19.8.2016

Podpis: