Diplomová práce – posudek oponenta

Jan Calta: Analyzer of Windows Kernel Models

Cílem práce je analýza, návrh a prototypová implementace překladače z jazyka DeSpec do vstupního jazyka model checkeru Zing. Motivovaný snahou o verifikaci ovladačů Windows specifikační jazyk DeSpec byl navržen pro popis zjednodušeného modelu Windows kernel a popisu pravidel pro správné chování ovladačů. Jazyk DeSpec byl navržen v rámci předchozí diplomové práce na KSI MFF, na kterou autor předkládané práce navazuje.

Jelikož jazyk DeSpec obsahuje řadu netriviálních vlastností, zařazených spíše s ohledem na pohodlnost specifikace v tomto jazyce než snadnost případné implemenatce překladače či checkeru (originální návrh implementaci nezahrnoval), autor práce byl při vlastní implementaci přinucen k řadě kompromisů. Výsledkem je překladač podporující pouze podčást jazyka DeSpec bez analýzy kódu samotného ovladače, bez nástroje pro zjednodušení modelu a bez podpory volby úrovně abstrakce. Nutno říci, že i tak byla implementace této podmnožiny obtížným úkolem zcela na úrovni diplomové práce. Autor navíc navrhl překladač s ohledem na případnou budoucí implementaci chybějících nástrojů. Podmnožina jazyka a funkcionality je zvolena tak, aby byl výsledek samostatně fungující a použitelný alespoň na některá pravidla chování ovladačů. Tedy spíše než kompletní implementaci několika vlastností jazyka, nalezneme mnohdy částečnou implementaci všech důležitých vlastností (včetně dědičnosti a pravidel chování, které Zing přímo nepodporuje). Tím je ukázána schůdnost použití jazyka DeSpec, tedy motivace této práce.

Velice kladně hodnotím strukturu práce a nadprůměrnou úroveň psaného projevu v anglickém jazyce. Drobné nedostatky vídím zejména v následujících bodech. V úvodních kapitolách jsou pouze mlhavě zmíněny některé problémy překladu a jejich řešení, která jsou pro čtenáře v této fázi příliš detailní a tedy hůře pochopitelné, nicméně v dalších kapitolách se těmto dostane patřičného prostoru a vysvětlení. Za nevhodné ovšem považuji označení "finite Büchi automaton", neboť takový automat je pouze "standardní" konečný automat. Díky tomuto drobnému zmatení pojmů se pak zdá, že autor navrhuje Büchiho automaty převést na deterministickou variantu, což obecně nelze (deterministická varianta má menší vyjadřovací sílu). Ocenil bych také alespoň neformální analýzu vlivu použitých řešení jak na velikost stavu viditelného pro Zing, tak na velikost výsledného stavového prostoru.

I přes zmíněné nedostatky autor jednoznačně prokázal, že je schopen uchopit a komplexně zanalyzovat netriviální úkol, identifikovat podstatné části ambiciózního zadání a implementovat je v dostatečně stabilním nástroji. Předloženou práci tedy považuji po všech stránkách za práci splňující kritéria pro diplomové práce na MFF UK a doporučuji jí k obhajobě.

Praha, 21. 1. 2008

Mgr. Ondřej Šerý, KSI MFF UK