Oponentský posudek dizertační práce

Verification of Programs with Complex Data Structures

kterou na Fakultě informačních technologií VUT v Brně předložil

Mgr. Adam Rogalewicz

Autor posudku: **Doc. RNDr Petr Jančar, CSc.**
Fakulta elektrotechniky a informatiky VŠB-TU Ostrava

Předkládaná anglicky psaná práce Mgr. Rogalewicze podává v jednotném rámci výsledky z několika předchozích let, které autor dosáhl a publikoval společně se svým školitelem T. Vojnarem a zahraničními spolupracovníky (A. Bouajjani, P. Habermehl, R.Iosif). Tyto výsledky spadají do oblasti tzv. symbolické verifikace; zavádějí a rozvíjejí metodu, kterou bychom česky mohli nazvat „ověření vlastností modelu využitím regulárních stromových automatů a principu abstrakce“; anglický název je “abstract regular tree model checking” (ARTMC). Tento přístup zobecňuje metody verifikace založené na konečných automatech pracujících nad slovy i nad stromy, které byly zmíněnými spoluautory a dalšími výzkumníky zavedeny a zkoumány již dříve. Stručný výklad těchto výchozích metod je v dizertační práci podán v kapitole 2 a části kapitoly 3 (následujících po úvodní kapitole 1).

Jádro práce je obsaženo v části kapitoly 3 a v kapitolách 4 a 5. Kapitola 3 popisuje základní verifikační metodu používanou dále, tedy metodu ARTMC, která dřívější metodu pracující s konečnými automaty nad slovy zobecňuje pro případ konečných automatů nad stromy. Na tomto zobecnění se již autor dizertace přímo podílel.

Kapitola 4 se věnuje použití metody ARTMC při ověřování vlastností programů pracujících s dynamickými datovými strukturami. Autor ukazuje způsob reprezentace těchto dat pomocí stromů a standardní příkazy s ukazateli (pointers) reprezentuje jako stromové převodníky (tree transducers). Definuje speciální logiku umožňující formulovat základní vlastnosti konzistence u uvažovaných programů a pak popisuje plně automatizovatelnou metodu ověření těchto vlastností. Metoda byla implementována a experimentální výsledky potvrdily její aplikovatelnost na reálné procedury pracující s ukazateli. Autor podává stručný přehled jiných metod, použitých k podobným účelům; kvalitu nové metody prokazuje zprávou o experimentech na konkrétních příkladech. Ukazuje také několik směrů, ve kterých se metoda a její implementace mohou dále rozvíjet.

Poslední část jádra práce (kapitola 5) popisuje metodu automatického dokazovaní ukončení jisté třídy programů manipulujících se stromy. Opět se využívá přístup ARTMC, ve spojení se speciálními čítačovými automaty. Experimenty s implementací ukázaly použitelnost na konkrétních příkladech.

Celkově podává předkládaná práce zprávu o poměrně velkém výzkumném díle, které dále posunuje hranice v oblasti problémů, u nichž můžeme doufat v úspěšné použití automatizované verifikace. Jedná se o návrh, implementaci a experimentální aplikace nové netriviální metody; to vše bylo zpracováno solidně a srozumitelně, byť s drobnými chybami či nejasnostmi (např. v definici $L(M)$ na str. 8 chybí existenční kvantifikace q_f, na obr. 2.1. je v grafu převodníku dvakrát n/t, přičemž má být jednou t/n) a také s prohřešky proti anglické gramatice (např. “leave” místo “leaf” [str. 19], “than” místo “then” [str. 5], “two another abstraction methods” [2.3.2.]). Jistý nedostatek ovšem vidím v nepříliš průhledném srovnání kvality nové metody s jinými existujícími metodami. To asi není specifický problém této práce, ale je to možná obec-

nější problém v dané oblasti. Autor např. v tabulce 3.1. na str. 28 uvádí konkrétní doby běhu z experimentů a v textu zmiňuje, že jsou povzbudivé při srovnání s publikovanými výsledky jiné metody. Pokud ovšem jako čtenář nemám k dispozici autorem zmiňovaný prototypový nástroj, nemohu uvedené experimenty snadno zreprodukovat a výsledky takto ověřit; toto se týká všech částí práce. Přitom srovnávání takových metod se většinou nedá opřít o výsledky teoretického rázu; experimenty mají tedy významnou úlohu a jejich snadná reprodukovatelnost mi v této souvislosti připadá jako velmi důležitá. Prosím o vyjádření autora k tomuto bodu při obhajobě.

Nyní uvedu své vyjádření k explicitně žádaným bodům a poté přidám ještě další otázky k obhajobě.

1/ Námět práce jistě spadá do oboru Informační technologie a je celosvětově vysoce aktuální, neboť problém zdokonalování verifikačních metod a jejich zavádění do praxe návrhu a analýzy složitých (hardwarových a softwarových) systémů je v komunitě výzkumných a vývojových pracovníků obecně pociťován jako velmi naléhavý. To se mj. projevuje i pořádáním specializovaných konferencí, na nichž byly výsledky dizertační práce publikovány.

2/ Výše zmíněné jádro práce, tj. zavedení metody ARTMC a její aplikace při verifikaci programů s dynamickými datovými strukturami, je jistě netriviálním originálním přínosem, navazujícím na nejaktuálnější dění v oblasti symbolické verifikace.

3/ Jádro práce bylo publikováno na solidní mezinárodní úrovni, konkrétně na renomovaných sympoziích "Static Analysis (SAS 2006)" a "Automated Technology for Verification and Analysis (ATVA 2007)" a v elektronickém časopise "Electronic Notes in Theoretical Computer Science" (ENTCS 149, 2006). Tyto publikace se také již dočkaly mezinárodních ohlasů.

4/ Po přečtení dizertační práce a seznámení se s materiály o dalších činnostech uchazeče soudím, že se jedná o pracovníka se slibnou vědeckou erudicí, který již prokázal své schopnosti na solidní mezinárodní úrovni.

K hodnocení je ovšem potřeba poznamenat, že v uvedených mezinárodních publikacích, na nichž je práce založena, byl A. Rogalewicz vždy jedním ze čtveřice autorů. Chápu, že může být těžké přesně specifikovat vlastní autorův přínos k této práci více autorů, ale myslím si, že o tom autor měl v práci alespoň nějak pojednat. Takto ho žádám, aby se k této otázce vyjádřil u obhajoby, byť předpokládám, že o tom podá své vyjádření také jeho školitel. Hned ale dodávám, že sám nemám pochybnosti o tom, že vlastní přínos uchazeče byl dostatečně významný.

Také navrhuji, aby se uchazeč u obhajoby vyjádřil k následující věci. Práce se soustřeďuje na prezentování nových metod verifikace, jejich implementaci a experimenty při aplikaci na konkrétních příkladech. V této souvislosti může vyvstat řada zajímavých otázek. Např. jak co nejlépe charakterizovat třídu problémů, pro něž jsou uvedené metody úspěšné? Získal autor ze svých experimentů např. představu o nějaké „programátorské disciplíně", která by zaručila úspěšné použití zkoumaných verifikačních metod? Vycházejí z práce i impulsy ke zkoumání nějakých zajímavých otázek teoretického rázu?

Závěr: Podle mého názoru je dizertační práce Mgr. Rogalewicze velmi kvalitní a splňuje obecně uznávané požadavky kladené na tento podklad k udělení vědecko-akademického titulu doktor v oboru Informační technologie.

V Ostravě, 12. 11. 2007