Fakulta informatiky
Masarykova univerzita

Oponentský posudok disertačnej práce

Verification of Programs with Complex Data Structures

ktorú na FIT VUT predkladá **Mgr. Adam Rogalewicz**

Autor posudku: Doc. RNDr. Ivana Černá, CSc.
Fakulta informatiky, Masarykova Univerzita

Dizertačná práca Mgr. Adama Rogalewicza je venovaná otázkam verifikácie nekonečnestavových modelov. Autor sa podrobne venuje automatickej verifikácii vlastností dosiahnuteľnosti pre nekonečné systémy s regulárnou štruktúrou.

Téma práce považujem z hľadiska súčasného stavu výzkumu v oblasti formálnej verifikácie za veľmi zaujímavé, riešené otázky majú priamu aplikáciu pri vývoji a návrhu počítačových systémov. Dosiahnuté výsledky sú pôvodné. Prezentovaná práca vychádza zo známych techník pre modelovanie a overovanie sytémov s lineárnou regulárnou štruktúrou, ktoré inovatívne rozširuje na systémy s regulárnou stromovou štruktúrou. Navrhnuté postupy boli implementované a experimentálne overené. Výsledky boli publikované na troch medzinárodných konferenciách (INFINITY, SAS a ATVA) a na doktorských sympóziach a workshopoch (EEICT, MEMICS).

Hodnotenie dosiahnutých výsledkov

Jadrom dizertačnej práce je návrh techniky pre automatickú verifikáciu nekonečnestavových systémov s tzv. regulárnou stromovou štruktúrou. Technika vychádza z metódy overovania regulárnych systémov, tj. systémov, ktorých jednotlivé stavy je možné kódovať konečným slovom nad fixovanou abecedou a množina všetkých dosiahnuteľných stavov systému tvorí regulárny jazyk. Otázka verifikácie je formulovaná ako otázka dosiahnuteľnosti tzv. *zlých* stavov. V kombinácii s akceleračnými technikami a abstrakciou je tento prístup prakticky použiteľný a má svoje uplatnenie.

Dizertačná práca predkladá komplexné rozšírenie metódy overovania regulárnych systémov na systémy s regulárnou stromovou štruktúrou. K popisu stavov sa používaju konečné stromy a množina dosiahnuteľných stavov tvorí regulárny jazyk stromov. Pre účely abstrakcie sú definované dve ekvivalencie - predikátová ekvivalencia a ekvivalencia na počiatočných prefixoch stromov. Regulárne jazyky stromov sa dajú použiť

na modelovanie súbežných procesov, kde komunikujúce procesy majú stromovú topológiu. V práci je uvedených niekoľko príkladov takýchto systémov, na ktorých je následne experimentálne overená implementácia navrhnutého postupu verifikácie.

Druhú kľúčovú časť práce tvorí rozpracovanie metódy overovania systémov so stromovou šruktúrou pre programy, ktoré manipulujú s dynamickými dátovými štruktúrami. Základom je (automatický) postup kódovania dátových štruktúr pomocou stromových štruktúr, čo umožňuje aplikáciu techník navrhnutých v úvodnej časti práce. Navrhnuté techniky boli implementované a experimentálne overené. Vďaka svojej efektivite a plnej automatizovateľnosti umožnili overenie takých programov a systémov, ktoré nebolo možné vefirikovať pomocou predtým dostupných nástrojov. Technika overovania programov s dynamickými dátovými štruktúrami je logickým a veľmi elegantným rozšírením techniky pre systémy s regulárnou stromovou štruktúrou. Zároveň ju významne zhodnocuje, pretože rozširuje množinu systémov, na ktoré je aplikovateľná.

Za neoddeliteľnú súčasť práce považujem úvodnú kapitolu ako aj úvodné paragrafy jednotlivých kapitol, ktoré poskytujú širší vhľad do problematiky verifikácie, špeciálne verifikácie nekonečných systémov. Vzhľadom na rozsiahlosť skúmanej problematiky a existenciu veľkého počtu navzájom ťažko porovnateľných výsledkov v oblasti, prináša aj prehľadová časť práce novú kvalitu.

Prezentácia dosiahnutých výsledkov

Dosiahnuté výsledky sú v práci prezentované na veľmi vysokej úrovni, formulácie sú precízne, presné a zrozumiteľne. Práca má vysokú jazykovú úroveň (je napísaná v anglickom jazyku) a aj typografickú úpravu.

Otázky

Výsledky prezentované v práci vychádzajú z troch publikácií (16, 17, a 41 podľa zoznamu uvedeného v Rozšírenom abstrakte). Mohol by ste, prosím, bližšie špecifikovať svoj podiel na týchto prácach?

Aký je Váš pohľad na použiteľnosť navrhovaných techník? Konkrétne, technika je použiteľná na systémy so špecifickými vlastnosťami a vyžaduje nie celkom triviálne modelovanie systému. Je aj napriek tomu prístupná "laickým" užívateľom?

Súčasťou predkladanej práce sú implementácie navrhnutých algoritmov. Sú verejne dostupné? Predpokladáte, že budú základom pre komplexnejší verifikačný nástroj?

Celkové hodnotenie

Obsahový prínos dizertačnej práce hodnotím kladne, prezentované výsledky sú nové, prínosné a dobre motivované. Navrhnuté postupy a techniky boli implementované a sú pripravené pre priame použitie. Experimenty ukázali, že pre reálne systém môžu poskytnúť hľadanú odpoveď v akceptovateľnom čase.

Celkove predkladaná dizertačná práca zodpovedá obecne uznávaným požiadavkam k udeleniu akademického titulu a doporučujem ju k obhajobe.

V Brne, 25.10.2007 Ivana Černá