

Oponentský posudek na diplomovou práci

Název: Checking Primitive Component Behavior

Autor: David Klika

Úkolem diplomové práce bylo navrhnout vlastní řešení problému chybějícího prostředí komponenty a na základě toho implementovat nástroj pro ověřování kódu softwarových komponent proti specifikaci jejich chování. Jako cílová platforma byl zvolen komponentový model Fractal a programovací jazyk Java, a chování komponent se specifikuje pomocí behavior protokolů.

Autor vytvořil verifikační nástroj JANE, který využívá existující model checkery Java PathFinder (JPF) a BPChecker. Součástí JANE jsou také moduly pro sledování pokrytí kódu a specifikace při ověřování. Řešení problému chybějícího prostředí je realizováno pomocí modulu, který na základě specifikace chování komponenty vygeneruje množinu Java tříd reprezentujících prostředí. Během ověřování komponenty se pak běh prostředí řídí informacemi od BPCheckeru.

Volbě tohoto řešení předchází důkladná analýza možných přístupů vzhledem ke dvěma kritériím: míře závislosti na verzi JPF (tj. nutnosti modifikace JPF) a co nejvyšší výkonnosti JANE. Autorovi musím vytknout jen nedostatečné zdůvodnění postupů zvolených pro vyřešení některých dílčích problémů. V sekci 3.1.3 postrádám širší diskuzi výhod a nevýhod generovaného prostředí oproti obecnému (generickému) – autor pouze tvrdí, že důsledkem použití generického prostředí by byl nižší výkon JANE, ale nijak svoje tvrzení nezduodňuje. Dále v sekci 4.2.1, kde je diskutováno časování notifikace BPCheckeru při zavolání nebo návratu z nesynchronizované metody, chybí důkaz, že libovolné proložení událostí a notifikací v různých vláknech nemůže mít za následek falešné hlášení o porušení specifikace kódem.

Na implementaci nástroje JANE nejvíce oceňuji to, že je dotažená do konce, a vyzkoušená na netriviálních komponentách. Velmi užitečné jsou tipy pro konfiguraci JANE, které jsou podloženy výsledky experimentů. Součástí práce je také srovnání JANE s dvěma jinými nástroji pro ověřování kódu komponent proti jejich behavior protokolům, ze kterého JANE vychází ve většině případů vítězně.

Práce je napsána v anglickém jazyce – text obsahuje gramatické i stylistické chyby, které ale až na výjimky nesnižují jeho čitelnost a srozumitelnost.

Doporučuji předkládanou diplomovou práci připustit k obhajobě.

7.5.2007

Pavel Parížek

