Posudek vedoucího na diplomovou práci
Petra Mandyse

Combining Temporal Logic and Behavior Protocols

Cílem práce bylo rozšířit temporální logiku CTL o operátory tzv. behavior protocols za účelem zvýšení čitelnosti temporálních formulí (přílišná složitost formulí popisujících komplexní vlastnosti systémů velice ztěžuje praktické používání temporálních logik). Nová temporální logika, která takto vznikla, byla označena jako BP-CTL. Součástí práce byla také implementace nástroje pro model checking BP-CTL a srovnání čitelnosti formulí v CTL a BP-CTL.

Text práce je koncipován následujícím způsobem: Kapitola 1 – úvod do problematiky model checkingu a temporálních logik a základní popis behavior protocols. V kapitole 2 autor podrobně popisuje integraci operátorů behavior protocols do CTL, nastiňuje více možných variant řešení a předkládá argumenty pro výběr jím zvoleného řešení. Kapitola 3 obsahuje formální definici BP-CTL pomocí Kripkeho struktur (obvyklý způsob definice sémantiky temporálních logik) a dále sadu pravidel pro transformaci libovolné BP-CTL formule do CTL. Tyto transformace mají dvojí význam: jednak jsou použity v implementaci nástroje pro model checking BP-CTL, jednak jsou důkazem, že sémantická síla BP-CTL je stejná jako u CTL. V kapitole 4 autor demonstruje použitelnost BP-CTL jednak na malém ukázkovém příkladu, a dále shrnuje výsledky své studie, v rámci které přepsal do BP-CTL databázi temporálních formulí vytvořenou v rámci Specification Patterns Project na Kansas State University. V kapitole 4 je dále stručně popsán nástroj bpctl – preprocesor, který ve spojení s model checkerem NuSMV slouží jako model checker BP-CTL. V kapitole 5 jsou vyhodnoceny výsledky práce a jsou prezentovány projekty, které řeší podobné problémy, v kapitole 6 najdeme závěr a výčet otevřených problémů. Práce má tři přílohy: popis použitých formalismů (behavior protocols, CTL), výčet formulí z databáze vytvořené v rámci Specification Patterns Project včetně jejich překladu do BP-CTL, a uživatelský manuál k nástroji bpctl.

Samotný nástroj bpctl je plně funkční a je koncipován jako preprocesor pro model checker NuSMV – je zde využita transformace BP-CTL na CTL. Jazyk pro specifikaci modelů zůstává stejný jako u NuSMV. Toto řešení je výhodné zejména proto, že není třeba znovu implementovat pokročilé optimalizační techniky, které moderní model checkery používají.

Nejzajímavějším výsledkem práce je porovnání délky ekvivalentních formulí v CTL a BP-CTL, které bylo provedeno na formulích ze Specification Patterns Project. Výsledky ukazují, že po přepsání z CTL do BP-CTL jsou formule v průměru o třetinu kratší, ovšem u velmi složitých CTL formulí s několika vnořenými operátory „until“ bývá zkrácení až několikanásobné. O dobré čitelnosti BP-CTL také hovoří fakt, že po přepsání formulí do BP-CTL byla v databázi Specification Patterns Project objevena chyba, která v původním CTL zápisu nebyla dlouhou dobu odhalena.

Celkově práci hodnotím velmi pozitivně a doporučuji ji uznat jako diplomovou.

V Praze dne 17. 5. 2006

Jiří Adámek