MUNI
FAKULTA
INFORMATIKY

POSUDEK OPONENTA
DISERTAČNÍ PRÁCE

Název práce: *Automated Verification in HW/SW Co-design*

Autor práce: *Ing. Lukáš Charvát*

Oponent: *doc. RNDr. Vojtěch Řehák, Ph.D.*

Předložená práce se zaměřuje na techniky kontroly správnosti společného HW/SW návrhu komponent. Práce je psána v anglickém jazyce a je na dobré jazykové, typografické i stylistické úrovni. Prvních pět kapitol je úvodních a přehledových; detailně zavádějí relevantní pojmy a referují o dosaženém stupni poznání v daných oblastech. Vlastní přínos studenta je uveden v kapitolách 7 až 9, proto se zaměřím hlavně na ně.

Sedmá kapitola řeší problematiku kontroly paměťových registrů, které nelze kontrolovat hrubou silou (velmi se zde uplatňuje stavové exploze). Student si všímá toho, že paměťové bloky jsou pravidelnou strukturou a uplatňuje při vytváření modelu techniky abstrakce. Užitá verifikační metoda je BMC (bounded model checking), čili kontrola shody do omezeného počtu kroků. V tomto kontextu je to dobrá volba, protože v paměťových blocích lze očekávat, že případnou chybu lze demonstrovat při vhodné volbě kroků rychle (chybový stav není vzdálen o počáteční konfigurace). Model je vytvářen v nástroji Cadence SMV, který pro BMC techniku generuje vstup pro externí SAT solver. Jednotlivé kroky modelování byly implementovány a celý proces byl experimentálně otestován.

Kapitola 8 se zaměřuje na kontrolu shody (equivalence checking) mezi návrhovými modely v jednotlivých fázích v průběhu implementace. Konkrétně se věnuje shodě mezi specifikacemi na úrovni RTL (register-transfer level) a ISA (instruction-set architecture). Student navrhl algoritmus kontroly. Nově zavedenou metodu detailně popisuje a vysvětluje. Jádro spočívá v převodu RTL i ISA specifikace do modelu v jazyce symbolického model checkeru Cadence SMV. Verifikace se zaměřuje na separátní kontrolu jednotlivých instrukcí z instrukční sady. Pro tento převod je tedy možné znovu obhájit aplikování metody BMC. Celý postup byl implementován a experimentálně implementován.

V kapitole 9 se student věnuje potenciálním chybám vzniklým při souběhu paralelních akcí, tj. datové (read-after-write, write-after-read a write-after-write) a řídící hazardy. Při vlastní kontrole jsou využívány techniky analýzy datového toku, kontroly konzistence, statická analýza pro identifikaci potenciálních hazardů na datových cestách. Celý postup je v práci detailně popsán a vysvětlen. Student referuje i o implementaci a experimentálním vyhodnocení.

Námět práce odpovídá oboru disertace a prezentované výsledky jsou aktuální z hlediska současného stavu vědy. Při hodnocení jsem si kladl zásadní otázku, zda představená práce není jen souborem „diplomových prací“, tj. přímočarých řešení, která nemají dostatečný inovativní přínos klíčový pro disertaci. Po přečtení práce jsem dospěl k závěru, že prezentované výsledky dosahují požadované úrovně, ač fóra na kterých byly prezentovány nejsou nijak zvlášť excelentní. Originálním přínosem je aplikace technik v konkrétních studovaných oblastech včetně nutných modifikací a vylepšení.

Závěr: Vzhledem k výše uvedenému prohlašuji, že práce odpovídá obecně uznávaným požadavkům k udělení akademického titulu Ph.D. a *doporučuji tuto disertační práci k obhajobě.*

Dotaz k obhajobě:

Ve výsledcích referovaných v kapitolách 7 a 8 využíváte verifikační nástroj Cadence SMV. Ten již však není podporován a dokonce není ani veřejně dostupný. Je možné Cadence SMV v uvedeném řetězci nástrojů něčím snadno nahradit? Například nástrojem NuSMV?

Brno 20. prosince 2019 doc. RNDr. Vojtěch Řehák, Ph.D.