OPONENTSKÝ POSUDEK NA DIZERTAČNÍ PRÁCI

Doktorand: **Ing. Lukáš Charvát**
Název dizertační práce**: AUTOMATED VERIFICATION IN HW/SW CO-DESIGN**
(Automatická verifikace v souběžného procesu návrhu hardware a software).
Obor: Výpočetní technika a informatika.

Předkládaná disertační práce obsahuje 10 kapitol, abstrakt a seznam použité literatury, včetně vlastních publikací. Po hezky zpracovaném úvodu do problematiky návrhu vestavných systémů, zejména verifikačních metod, jsou vlastní přínosy popsány v kapitolách 7 až 9. Tedy podle názvu těchto kapitol jsou postupně popsány metody abstrakce velkých pamětí (Large Memory Abstraction), kontrola popisů procesoru na úrovni RTL a ISA (RTL-ISA Correspondence Checking) a formální analýza pipeline hazardů. Hlavním cílem práce je vylepšení verifikačních technik s tím, že je kladen důraz na automatizovatelnost a dobu verifikace.

1. Aktuálnost námětu dizertační práce z hlediska současného stavu vědy v daném oboru

Téma formální verifikace je stále „hot-topic“ zejména v oblasti návrhu vestavných systémů, které jsou navrhovány pro konkrétní aplikaci za dodržení mnoha omezujících podmínek (např. příkon, spotřeba, spolehlivost apod.) a kde je nutné rozhodnout, co bude implementováno v hardwaru a co v softwaru. Zejména využití programovatelného hardwaru zpřístupnila možnost navrhnout si vlastní procesor (nebo vylepšit nějaké již hotové procesorové jádro). A každý nový návrh je třeba ověřit, pokud možno automatizovaně, v celém stavovém prostoru, a aby to netrvalo příliš dlouho. Takže téma je aktuální a výsledky využitelné.

2. Originalita a přínosy dizertační práce

Cíle disertační práce jsou specifikované jasně, a to navrhnout nové metody verifikace založené na formálním popisu s ohledem na tzv. hardware-software co-design. Proto bylo nutné formalizovat popis všech částí navrhovaného systému. Práce začíná popisem pamětí, což tvoří v dnešní době největší část takového systému a optimalizace a správa paměti vede ke zkvalitnění a mnohdy i ke zrychlení a zjednodušení celého systému. Ovšem pro formální verifikaci bylo třeba i tento paměťový systém formálně (a zjednodušeně) popsat. To je obsahem kapitoly 7. Dále je pro formální popis celého systému důležité dokázat korespondenci mezi RTL popisem a ISA modelem pro všechny instrukce a operandy. Základní originální myšlenka je využití bounded model checkingu (BMC). Experimentální potvrzení bylo realizováno pomocí systému Codasip, což je systém který byl vyvinutý pro návrh procesorů včetně podpůrného softwaru původně na FITu a který je nyní již komerčně využívaný.

Velmi oceňuji to, že výzkum popsaný v disertační práci přináší možnost, jak formálně verifikovat „složitý“ systém tvořený jak hardwarovou tak softwarovou částí a zejména, že se podařilo formálně verifikovat hazardy v již všude používaném pipeliningu. Této problematice je věnována nejobsáhlejší kapitola 9, která využívá SMT řešiče a PSG (processor structure graphs) pro ověření absencí datových a řídících hazardů (RAW, WAR, WAW a CTL hazardy jsou definované v kapitole 9.1.3). Oceňuji i experimentální ověření navržených metod v open-source systému Hades, zřejmě vyvinutém týmem doktorand + školitel + školitel-specialista.

Mám trochu problém s názvem práce a jejím vymezením na oblast vestavných systémů. Omezení popsaná na začátku Kapitoly 6 specifikují již předem typ procesoru, velikost jeho paměti a šířky sběrnic, tedy už konkrétní rozdělení na hardware a software. Cílem HW/SW co-designu je nalezení optimální realizace aplikace tak, aby byl dosažen co nejvýhodnější poměr finálních implementací v hardwaru a v softwaru pro danou aplikaci. Podle mě jde spíš o formální verifikaci návrhu procesorového systému s vybraným ASIPem, tedy ne o optimalizaci hardware-software co-designu jako takového (vestavného systému, typicky nějakého SoC včetně periferií a konkrétního aplikačně závislého programu implementovaného buď v softwaru nebo např. v FPGA, tedy v hardwaru), ani o formální verifikaci

souběžného procesu tohoto návrhu. S tím souvisí i to, že není podle mě nutné omezení na vestavné systémy, zejména když jde „jen“ o procesorovou část těchto systémů.

3. Publikování výsledků dizertační práce a vědecká erudice

Publikační činnost doktoranda obsahuje 4 články z mezinárodních konferencí (MTV a EUROCAST), jeden příspěvek z doktorandské konference MEMICS a jednu výzkumnou zprávu. To není mnoho, ale témata popsaná v práci byla zveřejněna. Problém je pouze v tom, že nejnovější je z roku 2016.

4. Formální úroveň dizertační práce

Předkládaná práce je po formální stránce napsaná přehledně, dobře čitelnou angličtinou s minimem chyb (občas špatně člen nebo konstrukce věty). Práce obsahuje mnoho definic a vzorců (což se dá podle prezentovaného tématu očekávat). Konstatuji, že vše je dostatečně popsáno a vysvětleno. Struktura práce je z hlediska čitelnosti a logické struktury celkem vyvážená a obsahuje všechny obvyklé části. Trochu nevyvážené podle délky jsou jednotlivé kapitoly. Oceňuji hezky napsaný teoretický úvod, který tvoří 4 kapitoly na 40 stranách, následuje kapitola 6 s popsanými cíli a poté samotné přínosy práce v kapitolách 7, 8 a 9. Nejdelší je kapitola 9 (40 stran), naopak závěr práce, ovšem nazvaný Epilog má jen stránku jednu.

Drobné formální nedostatky jsou např. následující:

- Chtělo by v textu více zdůraznit, která část byla publikovaná a kde.
- Kapitole 9 by slušelo více objasňujících obrázků.
- Chybí state-of-the-art v oblasti verifikace procesorů, nejen popis specifikačních jazyků, vaše odkazy jsou na výsledky z 90. let.

5. Otázky do diskuse:

- Jaký je postup, jestliže budeme chtít využít výsledky disertační práce pro formální verifikace nějakého konkrétního vestavného systému? Existuje nějaký vývojový diagram, co udělat, jaké systémy použít, co napsat a jak v CodALu a kdy?
- Práce/výzkum má/měl za cíl formálně verifikovat nějaký systém s podílem HW a SW, což není jen procesor a paměť, ale i periferie, AD/DA převodníky apod. Počítá se s tím nějak?
- Prosím o upřesnění vlastních přínosů ve srovnání s výsledky dosaženými jinde – pokud existují – viz předchozí bod 4.
- PSG (processor structure graphs) je natolik standardní způsob popisu procesorového systému, že na něj není žádný odkaz nebo jde o originální metodu doktoranda (co např. LNCS 2304)?
- Je vámi navržená metoda verifikace začleněna do systému Codasip? Pokud ano jak?
- Existuje nějaký jiný systém než Codasip, který by vám pomohl s ověřením vašeho přístupu k řešení, s experimenty a formalizací, zejména s ohledem na dodržení času?
- Hlavním tématem práce je formální verifikace. Je možné provést nějaký formální důkaz ekvivalence modelů na úrovni RTL a ISA? V kapitole 8.2 je řečeno, že korespondence je ověřována na úrovni nezávislého provádění každé instrukce. Prosím o vysvětlení.
- Prosím o specifikaci podílů na publikacích, a zejména na realizaci a popisu systému Hades, který byl použitý pro experimentální ověření použitých metod.
- Prosím o doplnění informace, zda máte nějaké další, novější výsledky po odevzdání disertační práce (vaše publikace jsou na konferencích MTC´12, EUROCAST´13, MTV´14, EUROCAST´15 a MEMICS´16)?

Závěrem konstatuji, že předložená práce Ing. **Lukáše Charváta** přes některé výhrady, které by měly být vyjasněny při obhajobě, **odpovídá** obecně uznávaným požadavkům k udělení akademického titulu Ph.D. Předloženou dizertační práci **doporučuji** k obhajobě.

V Praze, 7. ledna 2020

doc. Ing. Hana Kubátová, CSc., oponent
Fakulta informačních technologií, ČVUT v Praze