Hodnocení vedoucího závěrečné práce

České vysoké učení technické v Praze **Fakulta informačních technologií**

Student: Bc. Dominik Plíšek
Vedoucí práce: Dr.-Ing. Martin Novotný
Název práce: Řešení problému diskrétního logaritmu použitím index calculu na GPU
Obor: Počítačová bezpečnost

Datum vytvoření: 6. 6. 2017

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
1. Náročnost a další komentář k zadání	***1=mimořádně náročné zadání,*** *2=náročnější zadání,* *3=průměrně náročné zadání,* *4=lehčí, ale ještě dostatečně náročné zadání,* *5=nedostatečně náročné zadání*

Popis kritéria:
Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.)

Komentář:
Úkolem práce bylo řešení rozsáhlých řídkých soustav lineárních rovnic v modulární aritmetice, což je jeden z kroků algoritmu Index Calculus. Předložená diplomová práce má rešeršní a výzkumný charakter. Bylo potřeba nastudovat velké množství zdrojů.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
2. Splnění zadání	***1=zadání splněno,*** *2=zadání splněno s menšími výhradami,* *3=zadání splněno s většími výhradami,* *4=zadání nesplněno*

Popis kritéria:
Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Komentář:
Zadání bylo splněno beze zbytku. Byly splněny i části, které nebyly výslovně požadovány.

Autor nejprve seznamuje čtenáře s algoritmem Index Calculus. Následně se zaměřuje na problém řešení řídkých soustav lineárních kongruencí, tedy na problém řídkých matic v modulární aritmetice. Popisuje tři faktorizace, a sice Choleského faktorizaci, LU faktorizaci a QR faktorizaci. Tyto faktorizace jsou použitelné, pokud pracujeme nad reálnými nebo komplexními čísly. Pro práci v modulární aritmetice je použitelná pouze LU faktorizace, jak autor zdůvodňuje.

LU faktorizaci v modulární aritmetice autor následně implementoval, a to jak pro CPU, tak pro GPU. Jak vyplývá z provedených měření, použití GPU v případě Index Calculu nepřináší žádné výhody, neboť nelze efektivně využít paralelismu - matice jsou příliš řídké. Vzhledem ke komunikační režii, kdy je potřeba přenášet do GPU rozsáhlé matice, dokonce došlo při použití GPU k prodloužení celkového času výpočtu.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 4:*
3. Rozsah písemné zprávy	***1=splňuje požadavky,*** *2=splňuje požadavky s menšími výhradami,* *3=splňuje požadavky s většími výhradami,* *4=nesplňuje požadavky*

Popis kritéria:
Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části.

Komentář:
Diplomová práce je obsahově bohatá, má 101 stran. Jak bylo zmíněno výše, jedná se především o rešeršní práci. Práce poskytuje čtenáři přehled o používaných metodách a diskutuje a zdůvodňuje jejich aplikovatelnost či neaplikovatelnost pro problém řešení řídkých soustav lineárních rovnic v modulární aritmetice. Nezaznamenal jsem žádné zbytečné části.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
4. Věcná a logická úroveň práce	*100 (A)*

Popis kritéria:
Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře.

Komentář:
Struktura práce je bezchybná, autor logicky postupuje od stanovení problému až k jeho řešení. V textu nechybí zdůvodnění jednotlivých kroků, tedy, proč v konkrétním kroku se zabývá daným dílčím problémem.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
5. Formální úroveň práce	*95 (A)*

Popis kritéria:
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

Komentář:
V práci jsem velmi vzácně zaznamenal drobné překlepy, sirotky na koncích řádků a drobné typografické nepřesnosti, např. symbol pro logaritmus "log" je občas psán kurzívou.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
6. Práce se zdroji	*100 (A)*

Popis kritéria:
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

Komentář:
Jak jsem se zmínil v úvodu, autor musel nastudovat velké množství literatury, v referencích cituje 24 pramenů. Autor se o tom v textu nezmiňuje, ale mezi jeho zdroji byly i hodiny videozáznamů přednášek prof. Davise. Musel nastudovat a pochopit i zdrojové kódy cizích autorů.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
7. Hodnocení výsledků, publikační výstupy a ocenění	*100 (A)*

Popis kritéria:
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

Komentář:
- Autor zdokumentoval tři metody faktorizace (Choleského, LU, QR) a zdůvodnil, proč v případě modulární aritmetiky lze použít pouze LU faktorizaci
- Autor vytvořil balíček pro řešení metody Index Calculu. Balíček je spustitelný jak čistě pod CPU, tak s využitím grafické karty (GPU).
- Autor provedl měření, kdy porovnal běh algoritmu na GPU a na CPU. Na základě naměřených hodnot zjistil, že doba zpracovnání na GPU je delší nežli doba zpracování na CPU, a to vzhledem ke komunikační režii a k charakteru úlohy.

Hodnotící kritérium:	*Způsob hodnocení - nehodnotí se*
8. Komentář o využitelnosti výsledků	

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

Komentář:
Zdá se, že zatím neexistuje práce, která by se zabývala použitelností jednotlivých metod faktorizace (Choleského, QR, LU) v případě modulární aritmetiky. Je-li tomu tak, pak se jedná o pionýrskou práci.
Další významný poznatek spočívá ve zjištění, že grafické karty (GPU) jsou pro problém Index Calculu nevhodné.
Domnívám se, že oba tyto dílčí výsledky by, každý zvlášť, měly být publikovány.

Hodnotící kritérium:	*Způsob hodnocení - následující škálou 1 až 5:*
9. Aktivita a samostatnost studenta v průběhu řešení	9a: ***1=výborná aktivita,*** *2=velmi dobrá aktivita,* *3=průměrná aktivita,* *4=slabší, ale ještě dostatečná aktivita,* *5=nedostatečná aktivita* 9b: ***1=výborná samostatnost,*** *2=velmi dobrá samostatnost,* *3=průměrná samostatnost,* *4=slabší, ale ještě dostatečná samostatnost,* *5=nedostatečná samostatnost*

Popis kritéria:
Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven (9a). Posuďte schopnost studenta samostatné tvůrčí práce (9b).

Komentář:
Je obdivuhodné, že autor zvládne živit rodinu a zároveň vypracovat takto náročnou a hodnotnou práci.

Hodnotící kritérium:	*Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):*
10. Celkové hodnocení	*100 (A)*

Popis kritéria:
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

Text hodnocení:
Doporučuji, aby komise předloženou diplomovou práci navrhla na cenu děkana.

Podpis vedoucího práce: