



Posudek oponenta závěrečné práce

Oponent práce: doc. Ing. Štěpán Starosta, Ph.D.
Student: Bc. Jan-Jakub Fleišer
Název práce: Paralelní faktorizace v technologii CUDA a Metal API
Obor / specializace: Počítačové systémy a sítě
Vytvořeno dne: 5. února 2024

Hodnotící kritéria

1. Splnění zadání

- ▶ [1] zadání splněno
- [2] zadání splněno s menšími výhradami
- [3] zadání splněno s většími výhradami
- [4] zadání nesplněno

Zadání považuji za splněné.

2. Písemná část práce

80 /100 (B)

Práce je dobře strukturovaná a celkově i dobře srozumitelná. Je psána anglicky s nevelkým počtem jazykových chyb (např. český slovosled). Text obsahuje věcné chyby neovlivňující hlavní výsledky práce. Jde především o kapitolu 1, kde je uvedena teorie k eliptickým křivkám, a kde je mnoho nepřesností až chyb - například v 1.1.1 se začne s tělesem K , ale dále je hned R ; křivka je nejprve rovnost a pak množina bodů; operace v 1.1.2 jsou opět nad tělesem K , ale obrázky dávají smysl pouze pro R ; "smoothness" na straně 6 není zavedeno (a mělo by); Z_n s n složeným není těleso (strana 6). Vylepšení by byla vhodná i dále: kapitola 2 na začátku slibuje uvést "parallel regions", ale zavedeny nejsou. Sekce 3.1.2 by dle mého soudu zasloužila pseudokód - hlavní algoritmus je popsán pouze slovně. Obrázek 5.2 je příliš malý nebo nevhodně zvolený do textu.

3. Nepísemná část, přílohy

91 /100 (A)

V první řadě velmi pozitivně hodnotím knihovnu pro počítání s celými čísly s libovolnou přesností pro Apple Metal popsanou v kapitole 4. Zdrojové kódy by zasloužily lepší popis v textu, případně i v příloze. Lze se v nich orientovat a i míra komentářů je rozumná, tj. dají se znovu použít či modifikovat.

4. Hodnocení výsledků, jejich využitelnost

80 /100 (B)

Autor je ke svým výsledkům sám v závěru své práce správně kritický a s jeho závěry zcela souhlasím. Pravděpodobně by bylo zajímavější se místo experimentů s různými verzemi (popsané především v 3.2:1) věnovat některým detailům. Srovnání v tabulce 7.2 s PARI je nerovná soutěž: jak autor sám zmiňuje v 1.5.2, PARI používá kombinaci přístupů, ne jen ECM. S GMP-ECM je to podobné, tato knihovna je silně optimalizovaná. Práce je využitelná jako základ pro další pokračování, které by se ovšem mělo zaměřit do hloubky. Zmíněná knihovna pro Apple Metal je přímo využitelná.

Celkové hodnocení

85 /100 (B)

Práce je rozsáhlá a již díky zadání mám dojem, že její zpracování bylo náročné. Její nevýhodou je široký záběr ve velmi specifické a teoreticky náročné problematice faktorizace pomocí eliptických křivek. To se podepisuje jednak na teoretických částech práce, kde text obsahuje věcné chyby, a také na využitelnosti získaných výsledků. Velmi kladně hodnotím knihovnu pro aritmetiku celých čísel s libovolnou přesností pro Apple Metal.

Otázky k obhajobě

V sekci 7.1. píšete, že zvolená čísla k faktorizaci mají vždy dva rozdílné prvočíselné faktory. Znamená to, že jsou součinem dvou prvočísel? Pokud ano, byla tato prvočísla volena nějak speciálně?

Instrukce

Splnění zadání

Posudte, zda předložená ZP dostatečně a v souladu se zadáním obsahově vymezuje cíle, správně je formuluje a v dostatečné kvalitě naplňuje. V komentáři uveďte body zadání, které nebyly splněny, posudte závažnost, dopady a případně i příčiny jednotlivých nedostatků. Pokud zadání svou náročností vybočuje ze standardů pro daný typ práce nebo student případně vypracoval ZP nad rámec zadání, popište, jak se to projevilo na požadované kvalitě splnění zadání a jakým způsobem toto ovlivnilo výsledné hodnocení.

Písemná část práce

Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. Dále posudte, 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. Posudte správnost používání formálních zápisů obsažených v práci. Posudte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 52/2021, článek 3.

Posudte, zda student využil a správně citoval relevantní zdroje. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami. Zhodnoťte, zda převzatý software a jiná autorská díla, byly v ZP použity v souladu s licenčními podmínkami.

Nepísemná část, přílohy

Dle charakteru práce se případně vyjádřete k nepísemné části ZP. Například: SW dílo – kvalita vytvořeného programu a vhodnost a přiměřenost technologií, které byly využité od vývoje až po nasazení. HW – funkční vzorek – použité technologie a nástroje, Výzkumná a experimentální práce – opakovatelnost experimentů.

Hodnocení výsledků, jejich využitelnost

Dle charakteru práce zhodnoťte možnosti nasazení výsledků práce v praxi nebo uveďte, zda výsledky ZP rozšiřují již publikované známé výsledky nebo přinášející zcela nové poznatky.

Celkové hodnocení

Shrňte stránky ZP, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení nemusí být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích. Obecně platí, že bezvadně splněné zadání je hodnoceno klasifikačním stupněm A.