FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Posudek oponenta závěrečné práce

Oponent práce:	Ing. Claudio Kozický
Student:	Bc. Ondřej Vladyka
Název práce:	Faktorizace pomocí kvadratického síta
Obor / specializace:	Počítačová bezpečnost
Vytvořeno dne:	14. května 2021

Hodnotící kritéria

1. Splnění zadání

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

2. Písemná část práce

90 / 100 (A)

Autor se v ZP důkladně věnuje všem bodům zadání. V teoretické části jsou poskytnuty veškeré informace potřebné pro pochopení řešené problematiky, vlastnosti naprogramované implementace jsou podrobně popsány a výkonnostní srovnání implementovaných algoritmů je taktéž provedeno důkladně. Kapitoly ZP na sebe logicky navazují.

Anglicky psaný text ZP sice obsahuje drobné jazykové chyby, ale jeho kvalitu bych považoval za nadprůměrnou. Nejčastěji se v textu vyskytují chyby v psaní členů. Nejvýraznější jazykovou chybou je, že autor při odkazování se na kapitoly, obrázky, definice atp. často používá vyjádření jako „in the section X.Y“, ve většině těchto případů by však člen neměl být použit vůbec. Jazykové chyby většinou neměly vliv na srozumitelnost textu.

Zdá se mi, že třetí produkt v poslední rovnici na straně 12 má být pro i od 1 do k, nikoli od 1 do m. V standardním C++11, které autor použil pro implementaci popisovaných algoritmů, se pro použití deklarací knihovny používá direktiva #include a nikoli direktiva #import, jak je napsáno v předposlední větě třetího odstavce na straně 30.

U některých vět, které končí rovnicí, chybí tečky. Např. poslední věta definice 1.8 na straně 5, poslední věta definice 1.15 na straně 6 či první věta na straně 34. Poslední věta kapitoly 3.7.2 na straně 40 je ukončena čárkou.

Na stranách 26 a 27 by v kapitolách 2.5 (Self-initializing quadratic sieve) a 2.6 (Large prime optimization) bylo vhodné citovat zdroj, ze kterého obsažené poznatky pocházejí. K tématu z kapitoly 2.6 se autor vrací na stranách 39 a 40 v kapitole 3.7 a tam už zdroj citován je.

V textu se vzácně vyskytují překlepy. Např. v druhé větě definice 1.9 na stránce 5 je místo „modulo" napsáno „moludo" a v poslední větě předposledního odstavce kapitoly 2.3.1 na straně 16 je napsáno „to check if check if n is". Dále se v textu vyskytuje slovo „lets", které ale mělo být napsáno jako „let's".

V poslední řadě se v textu vyskytují drobné typografické nedostatky. Příklady těchto nedostatků uvádím níže.

V druhém odstavci úvodu autor dává ukončovací dvojitou uvozovku za interpunkci, ale ve zbytku textu dává ukončovací dvojitou uvozovku před interpunkci. Je vhodnější zvolit jeden ze způsobů a používat ho v celém textu.

Dva matematické výrazy, které se nalézají na straně 4, používají mezi operátory nesprávně zarovnanou výpustku (trojtečku). V těchto dvou případech by výpustky měly být zarovnány na střed (např. pomocí maker „\dotsm" a „\dotso" z LaTeXu). V některých matematických výrazech je zřejmě nedopatřením použita hvězdička (*) místo středové tečky (·) (konkrétně v definici 1.9 na straně 5 a v druhém odstavci kapitoly 2.1.1 na straně 10).

Při odkazování se na rovnice (nebo na jiné matematické výrazy) by mělo být číslo rovnice v kulatých závorkách. Např. na straně 11 je napsáno „equation 2.1" místo „equation (2.1)".

V textu občas chybějí nezlomitelné mezery v místech, kde je obvyklé je v Angličtině vkládat. Např. v předposlední větě věty 1.6 na straně 4 mezi slovy „of n", v páté větě posledního odstavce na straně 23 ve vyjádření „congruence 2.5" či v předposlední větě druhého odstavce kapitoly 3.2 na straně 30 ve vyjádření „language [13]". Ve čtvrtém odstavci kapitoly 2.2 na straně 11 je v „50 %" použita obyčejná mezera místo úzké mezery.

3. Nepísemná část, přílohy 100 /100 (A)

Implementaci, kterou autor vytvořil jako součást ZP, se mi podařilo sestavit a spustit podle přiloženého návod. Zdrojový kód v jazyce C++ používá moderní přístupy, je napsán přehledně a je logicky rozčleněn do překladových jednotek. Autor přiložil veškerá potřebná data pro zopakování experimentů popisovaných v ZP.

4. Hodnocení výsledků, jejich využitelnost 95 /100 (A)

Výsledky ZP přehledně ukazují, jak velká čísla lze faktorizovat pomocí jednodušších algoritmů, a pro která je již nezbytné využít pokročilejší algoritmy. Dále je z výsledků patrné, pro jak velká čísla je výhodné faktorizaci řešit paralelně nebo distribuovaně. Zmíněné znalosti jsou využitelné pro další výzkum v oblasti faktorizace.

Celkové hodnocení 95 /100 (A)

Jedná se o výborně vypracovanou ZP, ve které se pouze vyskytují drobné jazykové a typografické nedostatky.

Otázky k obhajobě

V kapitole 3.8.2 popisujete, že pro účely meziprocesové komunikace pomocí MPI serializujete a deserializujete přenášená data do a z řetězců znaků. MPI umožňuje i posílání binárních dat, čímž odpadá potřeba převádět posílaná data do řetězců znaků a zpět. Je nějaká překážka, která by zamezovala upravit Vámi naprogramovanou implementace tak, aby vynechala převod do řetězců znaků a posílala rovnou binární data?

Instrukce

Splnění zadání

Posuďte, 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, posuďte 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 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. Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 26/2017, článek 3.

Posuďte, 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.