ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK VEDOUCÍHO ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	Hidden subgroups and quantum algorithms
Jméno autora:	Matouš Pikous
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra řídicí techniky K13135
Vedoucí práce:	Doc RNDr Jiří Velebil, PhD
Pracoviště vedoucího práce:	Katedra matematiky K13101

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání — náročnější

Hodnocení náročnosti zadání závěrečné práce.

Cílem práce bylo sepsat text, uvádějící čtenáře do problematiky kvantových algoritmů. Jednotícím tématem práce je formulace problému skryté podgrupy, který lze kvantovými počítači řešit v polynomiálním čase. Matematický aparát, nutný k pochopení a vysvětlení (části) takových algoritmů, svým rozsahem a mírou abstrakce značně převyšuje obvyklé curriculum z matematiky na FEL ČVUT.

Splnění zadání — splněno

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Autor zadání práce splnil. V textu seznamuje čtenáře se základními pojmy kvantového počítání: q-bit, unitární matice, kvantový obvod. Dále formuluje Fourierovu transformaci na Abelových grupách a její využití k řešení problému skryté podgrupy. Text je zarámován dvěma pohledy na nejjednodušší kvantový algoritmus (Deutschův algoritmus). Jsou zmíněny i způsoby řešení faktorisačního problému (Shorův algoritmus). Dále je vysvětleno, jak pomocí skrytých podgrup hledat řád prvku a řešit problém diskrétního logaritmu.

Aktivita a samostatnost při zpracování práce — A - výborně

Posuďte, zda byl student během řešení aktivní, zda dodržoval dohodnuté termíny, jestli své řešení průběžně konzultoval a zda byl na konzultace dostatečně připraven. Posuďte schopnost studenta samostatné tvůrčí práce.

Autor při řešení práce postupoval aktivně, vyhledával a četl odbornou literaturu. Při postupu prací se zúčastňoval dohodnutých konsultací. Některá matematická témata bylo nutné projít vícekrát: to bylo dáno vysokou mírou abstrakce.

Odborná úroveň — B - velmi dobře

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Z textu je patrné, že autor ještě nemá zkušenost s psaním odborné práce. Během psaní práce si však autor začal uvědomovat „pravidla hry" a pokoušel se standardu přiblížit. Situaci si autor možná zkomplikoval i tím, že se snažil text psát pro mírně informované laiky (jak otevřeně přiznává v abstraktu). Výsledkem byla snaha o úzkostlivé zavedení všech pojmů, což někdy způsobuje nevyváženost matematické obtížnosti textu. Oceňuji, že se autor snažil i o neformální vysvětlení některých pojmů.

Formální a jazyková úroveň, rozsah práce — A - výborně

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Práce je psána anglicky s minimálním množstvím jazykových chyb. Práce má rozsah 61 stran, je vysázena v TeXu a dodržuje citační a typografické zvyklosti matematických textů.

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK VEDOUCÍHO ZÁVĚREČNÉ PRÁCE

Výběr zdrojů, korektnost citací	A - výborně
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. 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.	
Autor cituje relevantní zdroje na relevantních místech. Autor se snažil o citaci především ustálených a dostupných zdrojů, které studoval osobně.	

Další komentáře a hodnocení
Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.
Práce byla od počátku koncipována jako kompilační. Text s originálními výsledky v oblasti kvantových výpočtů lze v bakalářské práci očekávat jen velmi stěží.

III. CELKOVÉ HODNOCENÍ A NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení.

Téma bakalářské práce hodnotím jako spíše těžké. V textu práce se neobjevuje úsilí, které musel autor věnovat samotnému uvedení do problematiky (matematické základy kvantové mechaniky, základy teorie čísel a některé výsledky z teorie pravděpodobnosti). Výsledný text tedy navazuje na poměrně rozsáhlou teoretickou přípravu.

Kvůli jednotlivým bodům uvedeným v části II tohoto hodnocení předloženou závěrečnou práci hodnotím klasifikačním stupněm A - výborně.

Datum: 31.05.21

Podpis:

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

I. IDENTIFIKAČNÍ ÚDAJE

Název práce:	**Hidden subgroups and quantum algorithms**
Jméno autora:	**Matouš Pikous**
Typ práce:	bakalářská
Fakulta/ústav:	Fakulta elektrotechnická (FEL)
Katedra/ústav:	Katedra řídicí techniky
Oponent práce:	Ing. Rostislav Horčík, Ph.D.
Pracoviště oponenta práce:	Katedra počítačů, ČVUT FEL

II. HODNOCENÍ JEDNOTLIVÝCH KRITÉRIÍ

Zadání — **náročnější**

Hodnocení náročnosti zadání závěrečné práce.

Cílem bakalářské práce bylo nastudovat literaturu týkající se kvantových algoritmů a napsat ucelený text popisující danou problematiku. Zadání hodnotím jako náročnější, protože ke splnění zadání bylo potřeba nastudovat několik partií matematiky od lineární algebry, přes teorii grup a kvantovou Fourierovu transformaci až po vlastní kvantové algoritmy a většina je mimo rozsah bakalářských matematických kurzů na ČVUT FEL.

Splnění zadání — **splněno**

Posuďte, zda předložená závěrečná práce splňuje zadání. V komentáři případně uveďte body zadání, které nebyly zcela splněny, nebo zda je práce oproti zadání rozšířena. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků.

Předložená práce dle mého názoru splnila zadaní. Je zřejmé, že se autor seznámil s potřebnou literaturou a napsal ucelenou práci. Práce nejprve seznamuje čtenáře se základy kvantových výpočtů, tj. zavádí potřebnou notaci, potřebné partie lineární algebry a uvádí postuláty kvantového počítání. Následně čtenáře uvádí do teorie komutativních grup, aby bylo možné formálně definovat problém skryté podgrupy. Většina formálních tvrzení je uvedena i s důkazy. Nakonec práce prezentuje kvantový algoritmus na řešení problému skryté podgrupy. Jako aplikace je následně popsán Shorův faktorizační algoritmus a Deutschův algoritmus.

Zvolený postup řešení — **správný**

Posuďte, zda student zvolil správný postup nebo metody řešení.

Zvolený postup řešení je správný a odpovídá zadaní. Autor prostudoval odpovídající literaturu, sjednotil notaci a napsal přehledový text na dané téma. Struktura kapitol je vhodně zvolena.

Odborná úroveň — **C - dobře**

Posuďte úroveň odbornosti závěrečné práce, využití znalostí získaných studiem a z odborné literatury, využití podkladů a dat získaných z praxe.

Na textu je patrné, že autor nemá zkušenosti se psaním matematických formálních textů, což je nicméně u bakalářského studenta pochopitelné. Text obsahuje řadu drobných nedostatků, které jsou pro čtenáře matoucí, např. používání nedefinovaných symbolů, nejasná notace, neuvedení některých předpokladů či nekorektní důkaz.

Formální a jazyková úroveň, rozsah práce — **B - velmi dobře**

Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku.

Text je napsán dobrou angličtinou a obsahuje jen pár drobných překlepů. Nicméně bylo by dobré sjednotit osobu, ve které je text psán. Autor používá 1. osobu jednotného čísla a zároveň 1. a 2. osobu čísla množného. Text je psán v poměrně neformálním stylu, což ne zcela odpovídá bakalářské práci. Na druhou stranu oceňuji, že se autor pokouší neformálností vtáhnout čtenáře do problematiky.

Výběr zdrojů, korektnost citací — **A - výborně**

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

POSUDEK OPONENTA ZÁVĚREČNÉ PRÁCE

Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení závěrečné práce. Charakterizujte výběr pramenů. Posuďte, zda student využil všechny relevantní zdroje. 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.

Výběr literatury a její citace jsou odpovídající typu práce. Jen mě překvapuje, že práce neuvádí mezi referencemi dvě práce uvedené v zadání, zejména Shorův článek. Autor místo toho odkazuje na knihu. Ta sice může didakticky Shorův algoritmus lépe vysvětlovat, ale je dobré seznámit čtenáře také s originální citací.

Další komentáře a hodnocení

Vyjádřete se k úrovni dosažených hlavních výsledků závěrečné práce, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, publikačním výstupům, experimentální zručnosti apod.

III. CELKOVÉ HODNOCENÍ, OTÁZKY K OBHAJOBĚ, NÁVRH KLASIFIKACE

Shrňte aspekty závěrečné práce, které nejvíce ovlivnily Vaše celkové hodnocení. Uveďte případné otázky, které by měl student zodpovědět při obhajobě závěrečné práce před komisí.

Předloženou závěrečnou práci hodnotím klasifikačním stupněm **B - velmi dobře.**

Celkově hodnotím práci velmi dobře. Oceňuji, že text poskytuje ve sjednocené notaci úvod do problematiky kvantových výpočtů spolu s důkazy potřebných tvrzení z lineární algebry a teorie grup. Oceňuji i řadu neformálních přirovnání a příkladů, které mají problematiku odlehčit a vysvětlit. Na druhou stranu si myslím, že se autorovi nepodařilo splnit svůj cíl a napsat práci, která by byla přístupná studentům se zájmem o problematiku. Od čtenáře totiž vyžaduje jistou zkušenost s algebrou. Bez ní je dle mého mínění text poměrně těžko stravitelný.

Mám následující otázku:
Problém hledání řádu prvku v grupě $Z_n^\times$ byl formulován jako problém skryté podgrupy v grupě $G = (Z, +, -, 0)$. Nicméně uvedená formulace kvantového řešení tohoto problému předpokládá, že $G = (Z_2)^k$. Jak se musí zvolit k, aby kvantový výpočet šel použít k nalezení řádu prvku v $Z_n^\times$?

Datum: 28.5.2021 Podpis: