

Student: Ludvík Cigna

Název práce: Kvantové počítání na současných kvantových počítačích

Posudek oponenta

Student ve své bakalářské práci pokrývá formou rešerše téma kvantových algoritmů, přičemž se soustředí na detailní analýzu několika vybraných známých případů.

Práce je napsána velmi kvalitně a vypovídá o plném obeznámení studenta s historií, hlavními milníky i nejaktuálnějšími poznatky problematiky. Její šíře neumožňuje zahrnutí všech podrobností do formátu bakalářské práce, nevyhnutelně tedy občas i poměrně podstatné pasáže jsou vynechány, ale vždy alespoň s náznakem myšlenek a především odkazem na patřičnou literaturu.

Práce je v přesném souladu se zadáním rozdělena na pět hlavních kapitol, které se kromě zaměření poněkud liší i charakterem. V části kapitoly 4 student dočasně nahrazuje styl rešerše formátem definice–věta–důkaz. Kapitola 5 je ve své většině již velmi přehledová, i když témata bližší hlavní myšlence celé rešerše, kterou jsou hradlové kvantové algoritmy z hlediska teorie, jsou rozebrány detailněji.

Pokud bych měl mít jednu souhrnnou připomínku, byla by jí nejasná očekávaná úroveň čtenáře. Na jednu stranu je od začátku automaticky předpokládáno obeznámení s matematickými postuláty kvantové teorie (v abstraktní notaci odhlížející od vlnových funkcí a principu korespondence pozorovatelných fyzikálních veličin s operátory), na druhou je v sekci 4.3 věnován čas vůbec definici grupy, homomorfismu apod. Jinde je opět se samozřejmostí odkazováno na elementy teorie složitosti, jako O-notace či NP-těžkost.

Jiné připomínky jsou spíše drobná přehlédnutí s poměrně zřejmým vysvětlením, ale bylo by záhodno o nich studenta informovat.

- Symboly M, N na straně 29 reprezentují jedinou čísla a jedinou množiny.
- U obrázků 3.6, 3.7, 3.9b není nikde již řečeno, že numerické výsledky pocházejí ze simulátoru.
- Strana 54 a dále: „náhodně / zcela náhodně vybraný“ nemá v matematicky psaném textu místo, správný pojem je „vybraný z rovnoměrného rozdělení“.

Požádal bych, zda by student během obhajoby zodpověděl následujících několik dotazů:

1. K Deutsch-Jozsově algoritmu (strana 25): většina binárních funkcí nad $n \geq 2$ bity není ani konstantních ani vyvážených. Jak na ně algoritmus zareaguje?
2. K fázovému zpětnému rázu (strany 22 a 50): stavy $(\alpha |\varphi\rangle) \otimes |\psi\rangle$ a $|\varphi\rangle \otimes (\alpha |\psi\rangle)$ jsou totožné. Jaká je tedy motivace říkat, že se akce „přenesla z druhého qubitu na první“, tedy co je důvodem jeden ze zápisů preferovat před druhým?
3. Ke Groverově algoritmu (strana 29): jaký význam má zvolený příklad problému hledání nejkratší cesty? Jak nám algoritmus pomůže numerickou funkci minimalizovat?
4. K Fourierově transformaci (strana 50): pro n qubitů již obecně Blochova sféra nelze použít. Co tuto vizualizaci umožňuje v obrázku 4.3 a jak jej číst?

Při úspěšné obhajobě s radostí doporučuji ohodnocení známkou **A – výborně**.

V Praze dne 25. 8. 2021

Ing. Václav Potoček, Ph.D.

oponent