POSUDEK OPONENTA NA BAKALÁŘSKOU PRÁCI: *LUKÁŠ MEJDRECH, ALGORTIMUS PRO KVANTOVÉ HLEDÁNÍ*

Práce představuje jeden ze známých algoritmů pro (dosud víceméně hypotetický) výpočetní model kvantových počítačů, totiž Groverův algortimus. Téměř polovina práce je věnována úvodu do principů kvantových počítačů a na závěr je zmíněna simulace kvantového počítače počítačem klasickým.

Groverův algortimus je v literatuře bohatě popsán, jedná se tedy o práci ryze kompilační. Náznakem vlastního přínosu je porovnání vhodnosti dvou odlišných popisů fungování algortimu. Ve světle výhrad, které budou následovat, chci zdůraznit, že tento kompilační charakter práce nepovažuji za nevýhodu. Jednak vzhledem k tomu, že se jedná o bakalářskou práci, jednak proto, že kvantové počítače vedou k prolínání několika oborů (fyziky, matematiky a informatiky), a proto je přehledné představení principů kvantového algoritmu, byť známého, dostatečným úkolem.

Konstatuji však, že uchazeč se tohoto úkolu zhostil způsobem málo uspokojivým. Literatura o kvantových počítačích často trpí nešvary plynoucími ze snahy přiblížit komplikovanou teorii populárním způsobem, což je umocněno zmíněným prolínáním několika oborů. To je přesně to, čemu by se podle mého názoru měla bakalářská práce vyhnout a zaměřit se na porozumění a srozumitelnost, spíše než na opakování nejasných, nebo i nepřesných frází.

Moje základní výtka tedy zní: autor mě nepřesvědčil, že tomu, co píše, skutečně rozumí. Ukážu několik míst, ze kterých moje pochybnost vyvěrá. Jedná se o nepřesnosti, které by snad mohly být výrazem nedbalosti, ale v celku vytváří nepříjemný dojem.

(1) Způsob, jakým autor nakládá s komplexními čísly, působí celkově dosti nejistě. Viz:
- V celé práci se hovoří o pravděpodobnosti měření jako o druhé mocnině amplitudy. Ve skutečnosti se jedná o druhou mocninu *absolutní hodnoty* amplitudy.
- Definovat úhel, který svírají komplexní vektory není zvykem. Má autor ve formuli (2.9) skutečně na mysli, že cosinus může nabývat komplexních hodnot?

(2) Tenzorový součin je je v kapitole 2.3 sice definován korektně, ale výklad jeho významu, a tedy i výklad klíčových pojmů kvantového počítání je nekorektní:

a)
- n-qubitový registr neobsahuje 2^n stavů, ale 2^n *základních* stavů,
- a kvantový paralelismus tedy neznamená, že se pracuje s 2^n stavy (to dělá na n bitech i klasický počítač), ale s *lineární kombinací* těchto stavů.

b)
- Není vůbec zmíněn zásadní fakt, že tenzorový součin obsahuje vektory, které nejsou tenzorovým součinem vektorů z výchozích prostorů,
- a to je důvodem zcela nesrozumitelného výkladu propletených stavů. Ten kromě nesrozumitelnosti obsahuje i věcně nesprávná tvrzení: Není (obecně) pravda, že pokud změříme jeden kubit propleteného stavu, nemusíme již měřit hodnotu druhého. Není (obecně) pravda, že měřením kubity opět kolabují do jednoho ze

základních stavů. (Není zde možné popisovat, z jakého zřejmého nedorozumění tato tvrzení vycházejí.)

(3) Pojem *linearita* je na s. 12 vysvětlen chybně.

(4) Operátor R není změnou fáze v dříve definovaném smyslu, která je (mimochodem) také chybná, fází se obvykle rozumí číslo $e^{i\theta}$, nikoli θ. (Důvodem chyby je zřejmě záměna $\mathbb{C}$ a $\mathbb{R}^2$).

(5) Ne zcela srozumitelná je i kapitola 2.5 o měření.

(6) s. 17 nahoře: Jak se měří čas výpočtu kvantového počítače?

(7) s. 17: Ve formuli (3.2.) má být asi v namísto ω.

(8) Odstavec následující po formuli (3.2) je pro mě nesrozumitelný.

(9) s. 17, (3.3.): R je s využitím právě uvedeného značení rovno U_0.

(10) s. 21: Co má znamenat spodní omezení počtu opakování? Pro dosažení jaké pravděpodobnosti?

(11) Formule (3.25) je opsána z knihy R. Špalka a je zcela v rozporu se značením používaným v práci.

Pokud jde o kapitolu 4 o simulaci, miká mi smysl takové simulace. Kvantový počítač provádí deterministické výpočty, jen je provádí rychle. Jaký smysl tedy simulace má? Rozhodujícím momentem, kde se projevuje zvláštnost kvantového výpočtu, je přitom měření, které deterministické není, a je ryze kantovým jevem. O způsobu, jakým se toto simuluje (podle mého názoru klíčová otázka simulace) v práci nic není.

Několik drobných poznámek.

- Anglické slovo pro závorku je *bracket*, ne *braket*.
- Bylo by dobré rozlišovat mezi množinou a uspořádanou n-tici (např. v případě báze).
- Odvození (3.10) je zbytečně krkolomné.
- Ve formuli (3.26) chybí odmocnina.
- Přimlouvám se za to, aby slovo *projektor* zůstalo v češtině vyhrazeno přístrojům dříve nazývaným promítačka.

Celkové hodnocení. Domnívám se, že předložená práce se pohybuje v dolní části požadavků kladených na bakalářskou práci. Doporučuji ji přijmout s hodnocením *dobře*.

Praha 15. června 2007 Štěpán Holub