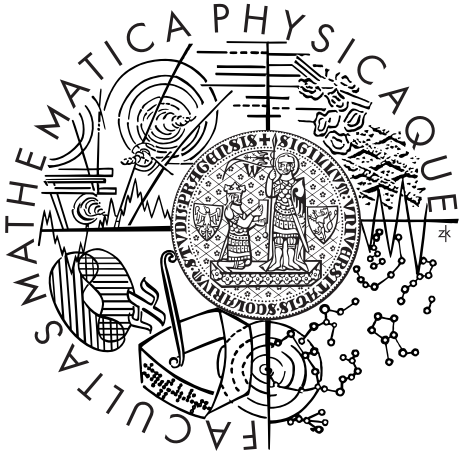
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Lukáš Charamza

Adiabatické kvantové počítání

Ústav částicové a jaderné fyziky

Vedoucí bakalářské práce: prof. RNDr. Pavel Cejnar, Dr., DSc.
Studijní program: Fyzika
Studijní obor: obecná fyzika

Praha 2014

Děkuji svému vedoucímu prof. Pavlu Cejnarovi za jeho ochotu a čas, které mi věnoval. Bez jeho cenných rad a připomínek by tato práce nikdy nevznikla.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Adiabatické kvantové počítání

Autor: Lukáš Charamza

Katedra: Ústav částicové a jaderné fyziky

Vedoucí bakalářské práce: prof. RNDr. Pavel Cejnar, Dr., DSc.

Abstrakt: V této práci jsou shrnuty principy kvantového počítání. Konkrétně se zaměřujeme na adiabatické kvantové počítače, jejichž princip vysvětlujeme a ukazujeme na několika konkrétních příkladech. Pro vysvětlení principu adiabatických kvantových počítačů zavádíme adiabatický teorém. Nastiňujeme také možnost využití speciálního hamiltoniánu podle Berryho, který umožňuje libovolně zrychlit adiabatickou evoluci. V závěrečné části práce vysvětlujeme pojem fázových přechodů a rozebíráme souvislost mezi adiabatickým kvantovým počítáním a kvantovými fázovými přechody, kde ukazujeme, že kvantový výpočet se škáluje polynomiálně s počtem qubitů jen pro kvantové fázové přechodu druhého a vyšších řádů.

Klíčová slova: Kvantové počítání, adiabatický teorém, kvantové fázové přechody

Title: Adiabatic quantum computation

Author: Lukáš Charamza

Department: Institute of Particle and Nuclear Physics

Supervisor: prof. RNDr. Pavel Cejnar, Dr., DSc.

Abstract: In this thesis we summarize the principles of quantum computing. We specifically consider adiabatic quantum computing, whose principles are explained and shown on several examples. To explain the principle of adiabatic quantum computing we review the adiabatic theorem. We also outline possibility of using a particular Hamiltonian by Berry, which enables us to evolve system adiabatically in arbitrarily short time. In the final part of this thesis, we explain the concept of quantum phase transitions. We discuss a relationship between quantum phase transitions and adiabatic quantum computing and show that adiabatic quantum computing scales polynomially with the number of qubits only for quantum phase transitions of second or higher order.

Keywords: Quantum computing, adiabatic theorem, quantum phase transitions

Obsah

Úvod

Klasické počítače, od těch stolních po mobilní telefony, se staly každodenní součástí našich životů. Pomáhají nám při komunikaci a při řešení složitých problémů snad ve všech odvětvích vědy, používáme je pro práci i pro zábavu. Je však důležité si uvědomit, že počítače nejsou všemocné a mají své nepřekonatelné limity. Už v 60. letech minulého století si lidé začali uvědomovat, že miniaturizace, tedy skládání čím dál více transistorů do čím dál menších součástek, nebude moci pokračovat věčně. I když by tento problém šel vyřešit stavěním větších strojů, nakonec se vzrůstajícím výkonem narazíme na Landauerův princip, který v roce 1961 popsal Rolf Landauer v článku [1]. Landauerův princip, důsledek druhého zákona termodynamiky říká, že s každou provedenou nereverzibilní operací počítač musí uvolnit jisté nenulové množství tepla.

Další bariérou mezi počítači a dokonalostí je jejich digitální podstata. Při simulaci skutečného světa na počítači jsme omezeni jeho konečnou přesností.

Jestliže tedy chceme i nadále pokračovat ve vývoji počítačů, je nutné vycházet z jiných principů. Těmito novými principy jsou například biomolekulární počítače, navržené L. M. Adlemanem [2]; či kvantové počítače, navržené R. P. Feynmanem [3]. Právě kvantovým počítačům je věnována tato práce.

V dnešní době existuje několik ekvivalentních [4] návrhů, jak kvantový počítač sestrojit. Prvním z nich jsou hradlové kvantové počítače. Tyto jsou svojí činnosti podobné našim klasickým počítačům, akorát místo klasických bitů (které mohou nabývat hodnot pouze 0 a 1), pracují s qubity (které mohou nabývat superpozice stavů 0 a 1, což zjednodušeně řečeno znamená, že pracují s oběma hodnotami najednou). Nad těmito qubity počítač provádí jednoduché logické operace, řazené za sebou do tzv. kvantových logických obvodů.

Druhým návrhem jsou adiabatické kvantové počítače. Adiabatické kvantové počítače taktéž pracují s qubity, ale s těmito nepracují pomocí logických operací. Místo toho pozvolným upravováním vnějších podmínek převedou qubity ze základního stavu do stavu odpovídajícího řešení daného problému.

V této práci se pokusíme shrnout teorii, která stojí za adiabatickými kvantovými počítači od základních principů známých již téměř sto let po nejnovější poznatky. Tuto teorii se také pokusíme demonstrovat na praktických příkladech jako je SAT problém, což je typický příklad NP-úplného problému, tedy problému obtížně řešitelného na klasickém počítači. Dalším uvedeným příkladem bude vyhledávání v databázi, kde si ukážeme algoritmus typický pro hradlové kvantové počítače i pro adiabatické kvantové počítače.

V kapitole 1 této práce se podíváme na historii kvantového počítání a zavedeme základní pojmy. V kapitole 2 nejprve zavedeme adiabatický teorém, teoretický základ fungování adiabatických kvantových počítačů. Poté se budeme přímo věnovat adiabatickým kvantovým počítačům, vysvětlíme si princip jejich fungování, který si ukážeme na výše uvedených problémech. Na konci kapitoly 2 uvedeme myšlenku M. V. Berryho, která částečně umožňuje vyhnout se omezením vyplývajících z adiabatického teorému. V kapitole 3 je proveden podrobnější rozbor podmínek adiabatického počítání s využitím teorie kvantových fázových přechodů.

1. Historie a základní principy kvantového počítání

1.1 Základní pojmy

Než začneme sledovat vývoj kvantových počítačů, je vhodné některé koncepty vytrhnout z jejich historického kontextu. Některé z nich totiž byly používány mnohem dřív, než byly formálně zavedeny. V tomto úvodu samozřejmě není možné shrnout vše známé o kvantovém počítání. Podrobnější výklad poskytuje učebnice [5], z jejíhož textu tato práce částečně vychází.

(Kvantový) počítač. Téměř na každé stránce této práce je možno nalézt nějakou zmínku o klasickém, či kvantovém počítači. Pojem klasický počítač nás v dnešní době asi příliš nezaskočí. Ale klasické počítače, sestavené z tranzistorů, také využívají principů kvantové fyziky. Čím se tedy liší od těch kvantových?

Na začátku výpočtu dáme počítači určitou sekvenci bitů (vstup), se kterou on na základě předem daných pravidel pracuje. Bit, základní jednotka informace, může nabývat dvou hodnot: 1, nebo 0. Na konci výpočtu nám počítač vrátí jinou sekvenci bitů (výstup). Veškeré výpočty, které počítač provádí, jsou ryze nekvantové. Neprojevuje se zde tedy žádná vlastnost kvantové fyziky. A můžeme sice k sestavení určitého počítače využívat kvantových jevů, nejsme k tomu však nuceni a stačí nám jevy z klasické fyziky. Například tranzistory lze nahradit elektronkami či relé.

Naopak kvantový počítač využívá kvantových jevů — superpozice, provázanost — přímo. Informaci v něm nereprezentuje bit, ale qubit. Qubit je dvoustavový kvantový systém a je možné jej reprezentovat například jako $\frac{1}{2}$-spin. Vlastní stavy qubitu označujeme $|1\rangle$ a $|0\rangle$. V maticové reprezentaci mají qubity podobu

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{1.1}$$

Konkrétní qubit se může nacházet v superpozici

$$|\psi\rangle = \alpha\,|1\rangle + \beta\,|0\rangle\,; \quad |\alpha|^2 + |\beta|^2 = 1. \tag{1.2}$$

Název qubit navrhl Benjamin Schumacher ve své práci z oblasti kvantové teorie informace z roku 1995 [6]. Slovo qubit, navzdory zvyklostem anglického jazyka čteno [kju:bit], je slovní hříčkou na prastarou jednotku délky cubit.

(Kvantový) registr. V průběhu výpočtu si počítač musí pamatovat mezivýpočty. Za tímto účelem si je ukládá do paměti, tzv. *registru*. Stejným způsobem pracuje i kvantový počítač, ale informace uložené v kvantovém registru je oproti tomu klasickému více.

U qubitů se totiž projeví kvantová provázanost. Z teoretického hlediska kvantovým registrem rozumíme stav $|\Psi\rangle$ provázaných qubitů $|\psi_i\rangle$, $i = 1, \cdots, n$. Výsledný stav $|\Psi\rangle$ systému n qubitů $|\psi_i\rangle$ leží v Hilbertově prostoru $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$ ($\mathcal{H}_i$ je Hilbertův prostor qubitu $|\psi_i\rangle$) a má tvar

$$|\Psi\rangle = \alpha_1\,|0\rangle\,|0\rangle \overset{n}{\cdots} |0\rangle + \alpha_2\,|0\rangle\,|0\rangle \cdots |0\rangle\,|1\rangle + \cdots + \alpha_{2^n}\,|1\rangle\,|1\rangle \cdots |1\rangle\,. \tag{1.3}$$

Vidíme tak, že systém n qubitů popisuje 2^n čísel α_1 až α_{2^n}, a nikoliv pouze n, jako je tomu u klasických bitů.

Logický člen. Logický člen, známý také pod názvem hradlo, či logická brána, je prvek v počítači reprezentující logickou operaci nad množinou bitů. Příkladem logického členu je například člen AND, který má na vstupu dva bity a na výstupu jeden bit. Výstupní bit nabývá hodnoty 1, pokud oba vstupní bity nabývají hodnoty 1. Ve všech ostatních případech nabývá výstupní bit hodnoty 0.

Podobně můžeme uvažovat i o kvantových logických členech. Ovšem vzhledem ke komplikacím způsobených dekoherencí, se jimi budeme zabývat v sekci věnované Landauerově principu 1.2.

Logický obvod. Přestože lze sestrojit logický člen reprezentující libovolnou operaci, je pro výrobce snazší konstruovat pouze několik základních typů logických členů. Další operace se poté vykonávají jako sekvence několika logických členů, které pracují s podmnožinami dané množiny bitů. Takovou sekvenci nazýváme logickým obvodem.

Typickým příkladem logického obvodu je sčítačka. Sčítačka je binární obdobou klasického sčítání. Tato lze složit například z logických členů XOR, AND a OR.

Obdobně lze sestavovat i kvantové logické obvody. Kvantovými logickými obvody se nebudeme přímo zabývat. Jejich podrobnější vysvětlení a ukázky je možno nahlédnout v [5], či [7].

1.2 Landauerův princip a dekoherence

Počátky kvantového počítání. Nyní, když jsme si shrnuli základní pojmy, podívejme se na historický vývoj kvantových počítačů. Zbytek této kapitoly bude věnujme vývoji hradlových kvantových počítačů s důrazem na vysvětlení souvisejících pojmů v jejich historickém kontextu. Tento historický vývoj bude směřovat ke vzniku adiabatických kvantových počítačů, kterým se budeme věnovat v následujících kapitolách.

S příchodem 60. let 20. století začali lidé uvažovat nad omezeními klasických počítačů. Jako symbolický počátek těchto úvah můžeme brát přednášku Richarda Feynmana „There's plenty of room at the bottom“ z prosince roku 1959 [8]. Feynman zde vyslovil svojí představu o stále menších strojích a o uchovávání informace na menších a menších nosičích. Na druhou stranu však také zmínil omezení této miniaturizace, jednotlivé atomy. A skutečně za 50 let, která od této přednášky uběhla, jsme byli svědky stále menších tranzistorů, až v roce 2009 byl proveden experiment, kdy jako tranzistor posloužila jediná molekula benzenu, tedy 12 atomů [9].

Landauerův princip. Krátce poté, v roce 1961, Rolf Landauer publikoval myšlenku [1], dnes známou jako „Landauerův princip“, že každá nevratná operace pracující s informací produkuje entropii, která se projeví vzrůstem tepla okolí. Nevratná operace je taková, která nejde provést opačným směrem, tedy z jejích výstupů nejsme schopni získat vstupy. Příkladem takové operace je třeba sčítání. Ze dvou čísel jejich sečtením získáme jedno číslo. Z tohoto výsledku už ovšem

nejsme schopni reprodukovat původní dvě čísla. Klasické počítače provádějí právě takové nevratné operace, což klade omezení na minimální množství energie, kterou spotřebují pro provedení výpočtu.

Landauerův princip se podařilo experimentálně ověřit v roce 2012 [10]. Ztráta informace byla reprezentována vymazáním jedno-bitové paměti. Jako paměť v experimentu posloužila částice v potenciálu $U(x)$ se dvěma minimy pro $x = x_0 < 0$, kterému odpovídá hodnota paměti 0, a pro $x = x_1 > 0$, kterému odpovídá hodnota paměti 1, oddělenými hradbou vysokého potenciálu $x = 0$. Na počátku experimentu byla částice náhodně umístěna do jednoho z bodů x_0, x_1. Vymazání paměti bylo realizováno snížením hradby po dobu t mezi těmito minimy a zapůsobením slabou silou F) ve směru rostoucího x. Autorům článku se podařilo ukázat, že při limitě $F \to 0$ a $t \to \infty$ se teplo uvolněné tímto procesem skutečně blíží Landauerově limitě $-k_B T \ln 2$. Zde k_B je Boltzmannova konstanta.

Vratné brány. Aby se vyhnuli omezujícím důsledkům Landauerova principu, začali informatici vymýšlet *reverzibilní* (vratné) logické brány. Vratná brána je taková, že ke každému jejímu výstupu lze jednoznačně přiřadit vstup a naopak. Vratnost této operace zaručí, že se neztrácí informace, tedy neroste entropie a plně vratný počítač by tedy mohl pracovat za dodávání minimální energie. Kromě obyčejné NOT-brány, tedy negace, jsou příkladem vratných bran ještě takzvané CNOT-brány a CCNOT-brány známé, podle svého vynálezce Tommase Toffoliho, jako *Toffoliho* brána.

Brána CNOT má na vstupu dva bity: 1. kontrolní a 2. určený pro negaci, jehož hodnota se prohodí právě tehdy když nabývá kontrolní bit hodnoty 1. Na výstupu jsou oba vstupní bity, kde druhý nabývá hodnoty podle výše uvedeného pravidla.

Brána CCNOT funguje podobně jako CNOT, ale místo jednoho kontrolního bitu používá kontrolní bity dva, a třetí bit se změní, pouze pokud oba nabývají hodnoty 1. Na výstupu jsou pak všechny tři tyto bity. Tato brána je univerzální. To znamená, že libovolný výpočet (například sečtení dvou binárních čísel) lze provést pomocí vhodné kombinace několika CCNOT bran.

Dekoherence. Landauerův princip má mnohem větší důsledky při kvantových výpočtech. Ztráta informace ze systému, a tedy růst entropie, se projeví dekoherencí. Jestliže jsme si na počátku připravili kvantový systém v čistém stavu $|\psi\rangle$ a vložili ho na vstup kvantovému počítači, který provádí nějakou nevratnou operaci, přejde tento čistý stav $|\psi\rangle$ na smíšený stav. Tím ovšem počítač přestává být kvantový a zbylý výpočet je pouze pravděpodobnostní — již nedochází k interferenci jednotlivých stavů.

K dekoherenci může dojít i ve vratném kvantovém počítači, pokud je špatně odstíněn od okolí. Například kontakt s nekoherentním rezervoárem, či prolétající foton, mohou systému narušit koherenci. Toto je jeden z největších problémů konstrukce kvantových počítačů. Jednak se nemůžeme v průběhu výpočtu podívat, co už máme spočítáno, a také musíme kvantový počítač dostatečně chladit a izolovat.

1.3 První náznaky kvantových počítačů

Kvantový simulátor. Impulzem k počínajícím úvahám o kvantových počítačích byla fyzikální simulace. V roce 1981 Richard Feynman přednesl řeč, jejíž přepis vyšel v [3], o nemožnosti simulace kvantových systémů na klasických počítačích. Podstata problému je následující. Snažíme se popsat systém k částic, které se mohou vyskytovat v n stavech. Stavem myslíme například spin nebo diskretizovanou polohu v prostoru. Částice se v různých stavech vyskytují s různými pravděpodobnostmi, a pro popis systému musíme zadat pravděpodobnost každému možnému výskytu těchto částic. Pro n stavů a k částic musíme tedy zadat dohromady n^k čísel. To znamená, že za každou částici, kterou bychom chtěli do našeho modelu přidat, bychom museli počítač n-krát zvětšit. Tento exponenciální nárůst je zřejmě nepřekonatelnou překážkou. Pro představu si uveďme příklad. Na dnešním počítači bychom byli schopni v paměti držet informaci maximálně o zhruba 26 částicích, a to jen tehdy, pokud by nás zajímal pouze jejich $\frac{1}{2}$-spin.

Je možné si všimnout analogie tohoto exponenciálního nárůstu s exponenciálním nárůstem informace popisující kvantový registr. Proto je nutné pro popis kvantových systémů použít kvantový počítač. Na té samé přednášce Feynman navrhl model takového kvantového počítače – simulátoru, na kterém by se fyzikální simulace daly provádět. Toto můžeme považovat za jistý milník v historii kvantových počítačů. Do této doby se kvantová fyzika uvažovala spíše jako zdroj potíží, a od této doby se začíná přemýšlet, jak ji využít. Feynmanův kvantový simulátor je uskupení mnoha dvou-stavových systémů (qubitů, které ovšem v té době ještě nebyly známy pod tímto názvem). Nad každým z nich máme čtyři operátory

$$a = \text{annihilační} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \tag{1.4}$$

$$a^* = \text{kreační} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \tag{1.5}$$

$$n = \text{počtu částic} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \tag{1.6}$$

$$\mathbb{I} = \text{identity} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{1.7}$$

Feynman byl přesvědčený, že tento simulátor je schopný modelovat libovolný konečný, diskrétní systém bosonů.

Kvantový Turingův stroj. V roce 1985 David Deutsch navrhl *kvantový Turingův stroj* [11], hypotetický počítač, který je schopný simulovat libovolný kvantový algoritmus.

Deutschův stroj $\mathcal{Q}$ se, obdobně jako klasický stroj, skládá z registru, paměťové pásky, zapisovací hlavy a přechodové funkce. Registr je M-tice dvou-stavových veličin $\hat{r}_i$

$$\hat{\boldsymbol{r}} = \{\hat{r}_i\}, \quad i \in \{0, 1, \cdots, M-1\} \tag{1.8}$$

a paměťová páska je nekonečná, uspořádaná množina dvou-stavových veličin $\hat{p}_i$

$$\hat{\boldsymbol{p}} = \{\hat{p}_i\}, \quad i \in \mathbb{Z}. \tag{1.9}$$

Zapisovací hlava je reprezentována operátorem $\hat{x}$, jehož spektrum jsou všechna celá čísla $x \in \mathbb{Z}$. Jedná se tedy o ukazatel na místo v paměti o indexu x.

Tyto tři veličiny dohromady tvoří stavový vektor obsahující veškerou informaci o stavu stroje $\mathcal{Q}$. Daný stav označujeme

$$|\boldsymbol{r}, \boldsymbol{p}, x\rangle = |r_0, r_1, \cdots, r_{M-1}; p_0, p_1, \cdots; x\rangle\,. \tag{1.10}$$

Přechodová funkce je reprezentována unitárním operátorem $\hat{U}$. Tato funkce popisuje jednotlivý výpočetní krok. V závislosti na aktuálním stavu registru a paměti převede systém do nového stavu a posune zapisovací hlavu o jeden stupeň doleva, či doprava. $\hat{U}$ popisujeme maticí definovanou předpisem

$$\langle \boldsymbol{r}', \boldsymbol{p}', x'|\hat{U}|\boldsymbol{r}, \boldsymbol{p}, x\rangle = \left[\delta_{x'}^{x+1} U^{+}(\boldsymbol{r}', p_x'; \boldsymbol{r}, p_x) + \delta_{x'}^{x-1} U^{-}(\boldsymbol{r}', p_x'; \boldsymbol{r}, p_x)\right] \prod_{y \neq x} \delta_{p_y}^{p_y'} \tag{1.11}$$

Funkce $U^{\pm}$ jsou libovolné takové, aby operátor $\hat{U}$ byl unitární. $\delta_{x'}^{x\pm1}$ reprezentují posun hlavy pouze o jeden krok. Součin $\delta_{p_y}^{p_y'}$ zajišťuje, že v daném kroku se neprojeví jiná místa v paměti, než na která hlava $\hat{x}$ právě ukazuje.

Zákon o neklonování. Mezitím v roce 1982 William Wootters a Wojciech Zurek přišli se zákonem o neklonování [12], který říká, že obecně nelze vytvořit identickou kopii daného kvantového stavu. Ukažme si, proč není možné takovou kopii vytvořit.

Uvažujme stav $|\psi\rangle$, který chceme klonovat, ale jehož konkrétní podobu neznáme. Snažíme se nějaký jiný stav $|\phi\rangle$ převést do stavu $|\psi\rangle$. Jde nám tedy o zobrazení

$$|\psi\rangle\,|\phi\rangle \to |\psi\rangle\,|\psi\rangle\,, \tag{1.12}$$

které zprostředkuje operátor $\hat{U}$. Tedy pro libovolná $|\psi\rangle$ a $|\phi\rangle$ musí $\hat{U}$ splňovat

$$\hat{U}\,|\psi\rangle\,|\phi\rangle = |\psi\rangle\,|\psi\rangle\,. \tag{1.13}$$

Takové zobrazení ovšem není lineární, což po operátorech v kvantové fyzice požadujeme. Uvažujme totiž stavy $|\psi_1\rangle$ a $|\psi_2\rangle$. Pak

$$\hat{U}\,(|\psi_1\rangle + |\psi_2\rangle)\,|\phi\rangle = (|\psi_1\rangle + |\psi_2\rangle)\,(|\psi_1\rangle + |\psi_2\rangle)\,, \tag{1.14}$$

ale také

$$\hat{U}\,|\psi_1\rangle\,|\phi\rangle + \hat{U}\,|\psi_2\rangle\,|\phi\rangle = |\psi_1\rangle\,|\psi_1\rangle + |\psi_2\rangle\,|\psi_2\rangle\,. \tag{1.15}$$

Tedy

$$\hat{U}(|\psi_1\rangle + |\psi_2\rangle)\,|\phi\rangle \neq \hat{U}\,|\psi_1\rangle\,|\phi\rangle + \hat{U}\,|\psi_2\rangle\,|\phi\rangle\,. \tag{1.16}$$

Nemožnost klonovat kvantové stavy ohrozila rozkvétající vývoj kvantových počítačů. V klasických počítačích totiž využíváme klonování (kde ho známe spíše jako kopírování) neustále. Pokud si zkopírujeme nějakou informaci a později se s původní kopií něco stane, můžeme poté podle nové kopie starou opravit. V kvantovém počítači toto ovšem udělat nemůžeme, a pokud dojde například k dekoherenci, ztratíme důležitá data, či průběh výpočtu.

1.4 První algoritmy a experimenty

Shorův algoritmus. V roce 1994 přišel Peter Shor s významným kvantovým algoritmem, publikovaným v článku [13]. Tento algoritmus využívá *kvantové Fourierovy transformace* a slouží ke zjišťování periodičnosti funkce a toho následně ke zjištění dělitelů čísla. Konkrétní podobu a průběh algoritmu je možno vidět v [13].

Experimentální CNOT brána Ve stejném roce, kdy Shor přišel se svým algoritmem, Ignacio Cirac a Peter Zoller navrhli experimentální uspořádání kvantové CNOT brány. Toto uspořádání o rok později sestavili Christopher Monroe et al. v NIST v Coloradu. V souvislosti s počítačem Monroeova týmu můžeme tedy nadneseně hovořit o prvním kvantovém počítači, který byl sestaven.

Univerzální kvantová brána. V odstavci o Landauerově principu 1.2, jsme hovořili o univerzalitě CCNOT brány pro klasické počítače. Tato brána ovšem není univerzální pro kvantové počítače. Neumí totiž z vlastních stavů vyrobit jejich superpozici a také neumí posouvat vzájemnou fázi stavů. V článku [14] hovoří David P. DiVincenzo o univerzalitě trojice bran:

1. Dvou qubitová CNOT brána, o které jsme se zmiňovali v kapitole 1.2.
2. Jedno qubitová Hadamardova brána. Tato převádí stav $|0\rangle$ na $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ a stav $|1\rangle$ na $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Slouží tedy k vytváření superpozice z vlastních stavů.
3. Jedno qubitová „fázová“ brána. Tato ponechá stav $|0\rangle$ nezměněný a stav $|1\rangle$ změní na $e^{i\theta}|1\rangle$. Vytváří tedy fázový posuv stavů v qubitu o θ.

Díky jejich univerzalitě jsme pomocí kombinace těchto tří bran schopni reprodukovat libovolný kvantový algoritmus.

Groverův algoritmus. To si můžeme naznačit na Groverově algoritmu, pojmenovaném po svém objeviteli L. Groverovi [15]. Groverův algoritmus slouží k vyhledávání v databázi. Databází rozumíme N-tici prvků. Konkrétní význam prvků není pro algoritmus podstatný a můžeme tedy bez újmy na obecnosti uvažovat N-tici různých čísel 0 až $N-1$. Vyhledávání v databázi je potom proces, který nám řekne pozici daného čísla v databázi.

V případě klasického počítače procházíme databázi prvek po prvku a ptáme se, zdali je daný prvek ten, který hledáme. Tento dotaz můžeme charakterizovat funkcí $f(k)$

$$f(k) = \begin{cases} 1 & \iff k \text{ je hledaný prvek} \\ 0 & \iff k \text{ není hledaný prvek} \end{cases} \tag{1.17}$$

Takové prohledávání v průměru projde polovinu prvků databáze, než najde hledaný prvek. Složitost klasického algoritmu je tedy $\mathcal{O}(N)$.

V kvantovém případě využijeme superpozice k tomu, abychom se podívali na všechny prvky najednou, což nám umožní algoritmus zrychlit.

Ukažme si nyní princip Groverova algoritmu. K uchování informace o tom, na jakou pozici v databázi se díváme, potřebujeme kvantový registr o n qubitech.

Počet n qubitů je určen vztahem $2^n = N$ Dále budeme mít ještě 1 qubitový registr, jehož význam bude patrný později. Všechny qubity jsou na počátku algoritmu ve stavu $|0\rangle$. Prvním krokem algoritmu bude všechny qubity uvést do superpozice vlastních stavů. K tomu použijeme Hadamardovo hradlo, které zobecníme pro m qubitů následujícím způsobem

$$H^{\otimes m} |00\cdots\rangle = (H|0\rangle)^{\otimes m} = \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)^{\otimes m} = \frac{1}{\sqrt{2^m}} \sum_{i=0}^{m-1} |i\rangle , \tag{1.18}$$

kde $|i\rangle$ označuje stav reprezentující číslo i ve dvojkové soustavě. A symbol $\otimes m$ v exponentu značí tenzorový exponent, tedy $|x\rangle^{\otimes m} = |x\rangle \otimes |x\rangle \otimes \overset{m}{\cdots} \otimes |x\rangle$.

V tuto chvíli se chceme obdobně jako v klasickém algoritmu dotázat, zdali je daný prvek tím hledaným. K tomu poslouží operátor $\hat{U}_f$ související s funkcí $f(k)$.

$$\hat{U}_f |i\rangle |j\rangle = |i\rangle |j \oplus f(i)\rangle , \tag{1.19}$$

kde $|i\rangle$ je stav prvního registru a $|j\rangle$ je stav druhého registru. Symbol $\oplus$ značí součet $j + f(i) \mod 2$. Podívejme se nyní, jak tento operátor působí na stav $|j_s\rangle = \frac{|0\rangle+|1\rangle}{2}$

$$\hat{U}_f |i\rangle |j_s\rangle = \frac{\hat{U}_f |i\rangle |0\rangle + \hat{U}_f |i\rangle |1\rangle}{\sqrt{2}} = \frac{|i\rangle |f(i)\rangle - |i\rangle |1 \oplus f(i)\rangle}{\sqrt{2}} = (-1)^{f(i)} |i\rangle |j_s\rangle . \tag{1.20}$$

Tedy pokud bude první registr v superpozici, označené $|\psi_s\rangle$ získané zobecněným Hadamardovým hradlem podle rovnice (1.18), bude $\hat{U}_f$ působit následujícím způsobem

$$|\psi_s'\rangle = \hat{U}_f |\psi_s\rangle |j_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{n-1} \hat{U}_f |i\rangle |j_s\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{n-1} (-1)^{f(i)} |i\rangle |j_s\rangle . \tag{1.21}$$

Tedy operátor $\hat{U}_f$ označí prvek hledaný v databázi tím, že změní znaménko jemu odpovídající vlnové funkce. Toto provede nezávisle na velikosti databáze vždy v konstantním čase. Tím ovšem algoritmus ještě není u konce. Kdybychom totiž nyní chtěli získat informaci o pozici prvku, museli bychom na prvním registru provést měření. Ovšem otočení znaménka u jedné z bázových funkcí nijak nezmění pravděpodobnosti výsledných měření.

Proto dále používáme ještě operátor $2|\psi_s\rangle\langle\psi_s| - \mathbf{1}$. Jeho působením na $|\psi_s'\rangle$ dostáváme

$$(2|\psi_s\rangle\langle\psi_s| - \mathbf{1})|\psi_s'\rangle = (2|\psi_s\rangle\langle\psi_s| - \mathbf{1})\left(|\psi_s\rangle - \frac{2}{\sqrt{2^n}}|i_0\rangle\right) = \frac{2^{n-2}-1}{2^{n-2}}|\psi_s\rangle + \frac{2}{\sqrt{2^n}}|i_0\rangle , \tag{1.22}$$

kde jsme využili, že při označení hledaného prvku jako i_0 lze $|\psi_s'\rangle$ zapsat jako $|\psi_s\rangle - 2\frac{1}{\sqrt{2^n}}|i_0\rangle$. Působením tohoto operátoru jsme tedy zvýšili v registru zvýšili amplitudu hledaného stavu $|i_0\rangle$.

Tuto amplitudu dále můžeme zvětšovat opakovaným působením operátorů $\hat{U}_f$ a $2|\psi_s\rangle\langle\psi_s| - \mathbf{1}$. Lze ukázat, viz původní článek [15], že pokud tuto dvojici operátorů aplikujeme $\frac{\pi\sqrt{N}}{4}$ krát, bude se pro $N \gg 1$ pravděpodobnost naměření stavu $|i_0\rangle$ blížit 1. Groverův algoritmus má tedy složitost $\mathcal{O}(\sqrt{N})$.

Kvantová oprava chyb. Dalším důležitým objevem, se kterým přišel Peter Shor [16] byla kvantová oprava chyb. Dříve jsme hovořili o nemožnosti klonovat kvantový stav, z čehož plynula nemožnost použít klasických opravných kódů v kvantových počítačích. Shorova metoda spočívá v rozložení informace z jednoho qubitu na kvantově provázaných 9 qubitů. To mu umožňuje později změřit jakým způsobem se daný qubit změnil (aniž by změřil původní či nový, chybný stav) a provést na něm opačnou změnu.

1.5 Pokroky poslední doby

Pokroky v oblasti hradlových kvantových počítačů. Na první experimentální počítače navazovali na počátku 21. století další experimenty. Tyto z velké části nepřinášejí do oblasti kvantových počítačů žádný průlomový objev a pouze objevují nové metody uchovávání qubitů, provádění výpočtů apod., případně vylepšují stávající „počítače“ a stavějí jejich větší podoby. Ke každému novému paradigmatu se navíc začínají objevovat skeptici, kteří říkají, že daný postup ve skutečnosti není kvantovým počítačem. I přesto se zájem vědecké veřejnosti o kvantové počítače neustále zvyšuje, a začíná být čím dál problematičtější se ve všech novinkách orientovat. Pro zájemce o problematiku existuje průběžně aktualizovaná mapka [17], která se snaží shrnout objevy poslední doby.

Idea adiabatických kvantových počítačů. Dosud jsme mluvili pouze o *hradlových* kvantových počítačích. Hradlové kvantové počítače jsou obdobou klasických počítačů ve smyslu, že qubity prohánějí jednotlivými logickými bránami (hradly), a tím sledují daný algoritmus. V roce 2001 ovšem přišli E. Farhi et al. s *adiabatickým kvantovým počítačem*. Adiabatické kvantové počítače se od hradlových principem výpočtu značně liší, a tím přinášejí alternativní možnosti konstrukce. V dalším textu se budeme právě adiabatickými počítači zabývat. Pokusíme se shrnout základní principy jejich fungování a jejich výhody i nevýhody a limitace. Jako motivaci zakončeme náš průřez historií výrobkem firmy D-Wave Systems, která prohlásila, že vytvořila adiabatický kvantový počítač o 512 qubitech.

2. Adiabatické kvantové počítání

2.1 Adiabatický teorém

Časový vývoj vlastních stavů. Podstatou adiabatických výpočtů je adiabatický teorém, který říká, že pro hamiltonián $\hat{H}(g)$ závisející na parametru g, který se dostatečně pomalu mění s časem $g = g(t)$ zůstává systém ve vlastním stavu $|\psi_i(g)\rangle$. Zde i je index daného stavu, $i \in \left\{0, 1, \cdots, \dim(\hat{H}(g))\right\}$.

Při odvozování tohoto tvrzení budeme sledovat postup z knihy [18]. Závislost veličiny na parametru uvádějme pro přehlednost v horním indexu. Uvažujme vývoj systému popsaného hamiltoniánem $\hat{H}^g$, který je ve stavu $|\Psi^g\rangle$. V průběhu odvozování pamatujme, že parametr g je funkcí času, i když tuto závislost dále explicitně neuvádíme. V každém čase t můžeme stav $|\Psi^g\rangle$ rozepsat do aktuálních vlastních stavů hamiltoniánu

$$|\Psi^g\rangle = \sum_j \alpha_j^g \left|\psi_j^g\right\rangle. \tag{2.1}$$

Budeme vyšetřovat časový vývoj koeficientů α_j^g. Z nestacionární Schrödingerovy rovnice pro funkci Ψ^g dostáváme dosazením z (2.1) výraz

$$i\hbar \sum_j \dot{\alpha}_j^g \left|\psi_j^g\right\rangle + i\hbar \sum_j \alpha_j^g \frac{\mathrm{d}}{\mathrm{d}t}\left|\psi_j^g\right\rangle = \sum_j \alpha_j^g E_j^g \left|\psi_j^g\right\rangle. \tag{2.2}$$

Nyní využijeme ortogonality stavů $\left|\psi_j^g\right\rangle$ a přenásobíme tuto rovnost bravektorem $\langle\psi_i^g|$. Tím dostáváme

$$i\hbar\dot{\alpha}_i^g + i\hbar \sum_j \alpha_j^g \left\langle \psi_i^g \middle| \frac{\mathrm{d}}{\mathrm{d}t}\psi_j^g \right\rangle = \alpha_i^g E_i^g. \tag{2.3}$$

Při vyšetřování sumy v rovnosti (2.3) uvažujme dva případy.

Nejprve případ, kdy $j = i$. V takovém případě nás zajímá hodnota výrazu $\langle\psi_i^g|\frac{\mathrm{d}}{\mathrm{d}t}\psi_i^g\rangle$. Povšimněme si následujících vztahů, plynoucích z vlastností skalárního součinu, a faktu že $\langle\psi_i^g|\psi_i^g\rangle = 1$,

$$\frac{\mathrm{d}}{\mathrm{d}t}\langle\psi_i^g|\psi_i^g\rangle = \left\langle \frac{\mathrm{d}}{\mathrm{d}t}\psi_i^g \middle| \psi_i^g \right\rangle + \left\langle \psi_i^g \middle| \frac{\mathrm{d}}{\mathrm{d}t}\psi_i^g \right\rangle = 2\mathrm{Re}\left\langle \psi_i^g \middle| \frac{\mathrm{d}}{\mathrm{d}t}\psi_i^g \right\rangle = 0, \tag{2.4}$$

ze kterých plyne, že zúžení vektoru ψ_i^g a jeho derivace je ryze imaginární funkce. Zavedeme pro ní označení $i\phi^g$, kde $\phi^g \in \mathbb{R}$.

$$\left\langle \psi_i^g \middle| \frac{\mathrm{d}}{\mathrm{d}t}\psi_i^g \right\rangle = i\phi^g. \tag{2.5}$$

Dále prozkoumejme případ, kdy $j \neq i$. Vyjděme ze stacionární Schrödingerovy rovnice, která platí v každém pevném čase t pro funkce ψ_j^g

$$\hat{H}^g \left|\psi_j^g\right\rangle = E_j^g \left|\psi_j^g\right\rangle. \tag{2.6}$$

Jejím derivováním podle parametru g získáme rovnost

$$\frac{\mathrm{d}\hat{H}^g}{\mathrm{d}g}\left|\psi_j^g\right\rangle + \hat{H}^g\left|\frac{\mathrm{d}\psi_j^g}{\mathrm{d}g}\right\rangle = \frac{\mathrm{d}E_j^g}{\mathrm{d}g}\left|\psi_j^g\right\rangle + E_j^g\left|\frac{\mathrm{d}\psi_j^g}{\mathrm{d}g}\right\rangle. \tag{2.7}$$

Nyní zúžíme tuto rovnost bravektorem $\langle\psi_i^g|$ (pamatujeme přitom, že $j \neq i$, tedy $\langle\psi_i^g|\psi_j^g\rangle = 0$) a dostáváme

$$\left\langle\psi_i^g\right|\frac{\mathrm{d}\hat{H}^g}{\mathrm{d}g}\left|\psi_j^g\right\rangle + E_i^g\left\langle\psi_i^g\right|\frac{\mathrm{d}\psi_j^g}{\mathrm{d}g}\right\rangle = E_j^g\left\langle\psi_i^g\right|\frac{\mathrm{d}\psi_j^g}{\mathrm{d}g}\right\rangle \tag{2.8}$$

Z čehož dostaneme

$$\left\langle\psi_i^g\right|\frac{\mathrm{d}}{\mathrm{d}t}\psi_j^g\right\rangle = \dot{g}\left\langle\psi_i^g\right|\frac{\mathrm{d}}{\mathrm{d}g}\psi_j^g\right\rangle = \dot{g}\frac{\left\langle\psi_i^g\right|\frac{\mathrm{d}}{\mathrm{d}g}\hat{H}\left|\psi_j^g\right\rangle}{E_j^g - E_i^g} \tag{2.9}$$

Dosazením vztahů (2.5) a (2.9) do (2.3) dostaneme soustavy diferenciálních rovnic pro parametry α_i

$$\dot{\alpha}_i^g = \left(-\frac{i}{\hbar}E_i^g + i\dot{g}\phi^g\right)\alpha_i^g + \dot{g}\sum_{j\neq i}\frac{\left\langle\psi_i^g\right|\frac{\mathrm{d}}{\mathrm{d}g}\hat{H}^g\left|\psi_j^g\right\rangle}{E_j^g - E_i^g}\alpha_j^g \tag{2.10}$$

Adiabatická aproximace. Adiabatická aproximace znamená, že se parametr g mění s časem dostatečně pomalu, tj $\dot{g}$ je malé. Dostatečně malé znamená, že

$$\dot{g}\tau \ll \sum_{j\neq i}\frac{\left|E_j^g - E_i^g\right|}{\left\langle\psi_i^g\right|\frac{\mathrm{d}}{\mathrm{d}g}\hat{H}^g\left|\psi_j^g\right\rangle} \tag{2.11}$$

Kde τ je čas po který by nemělo dojít k přechodu. Prozatím nebudeme tutu podmínku hlouběji zkoumat. Vrátíme se k ní v sekci 2.2.

V případě, že platí (2.11), můžeme v rovnici (2.10) zanedbat člen se sumou. Výsledná diferenciální rovnice má řešení

$$\alpha_i(t) = \alpha_i(0)\exp\left(-\frac{i}{\hbar}\int_0^t E_i(g(t'))\mathrm{d}t' + i\int_0^g \phi(g')\mathrm{d}g'\right) \tag{2.12}$$

Z toho lze udělat následující závěr. Pokud je splněna podmínka adiabatické aproximace a systém je na počátku evoluce ve stavu $|\Psi(0)\rangle = |\psi_i(0)\rangle$, zůstává po celou dobu této evoluce systém ve stavu $e^{i\kappa}|\psi_i(t)\rangle$. Fáze κ skrývající v sobě integrály z výrazu (2.12) v sobě obsahuje dvě části — dynamickou a geometrickou fázi.

Dynamická fáze. První z nich je dynamická fáze. Dynamická fáze je známá i z řešení Sch. rovnice pro časově nezávislý hamiltonián, kde má podobu $e^{-\frac{i}{\hbar}E_i t}$. Skutečně, pokud budeme uvažovat $\hat{H}(t) = \text{konst.}$, bude i $|\psi_i(t)\rangle = \text{konst.}$, $\phi = \text{konst.}$ a $E_i = \text{konst.}$ a námi získaná změna fáze se zjednoduší na tvar odpovídající stacionárním vlnovým funkcím.

Geometrická fáze. Druhá je geometrická fáze, známá jako *Berryho fáze*. Tato fáze žádným způsobem nezávisí na čase, ani na rychlosti/pomalosti probíhající evoluce.

2.2 Adiabatický kvantový počítač

Obecné principy. Při kvantovém výpočtu na hypotetickém adiabatickém kvantovém počítači si připravíme nejprve nějaký počáteční hamiltonián $\hat{H}_i$ (například vhodným nastavením elektromagnetického pole), a systém převedeme do základního stavu tohoto hamiltoniánu. $\hat{H}_i$ volíme tedy takový, pro který je dosažení základního stavu jednoduché. Dále budeme uvažovat konečný hamiltonián $\hat{H}_f$, jehož základní stav je námi hledané řešení. Konkrétní tvary hamiltoniánů $\hat{H}_i$ a $\hat{H}_f$ závisejí na daném problému a jeho implementaci.

Průběh výpočtu symbolizuje hamiltonián $\hat{H}(g)$ závislý na parametru $g(t) \in [0; 1]$ ve tvaru

$$\hat{H}(g) = (1-g)\hat{H}_i + g\hat{H}_f. \tag{2.13}$$

Ve shodě s adiabatickou aproximací předpokládejme, že platí (2.11).

Uveďme si nyní několik příkladů jak sestavit hamiltoniány a reprezentovat stavy pro některé problémy, kde by se kvantové počítání mohlo uplatnit.

2.2.1 SAT problém.

Formulace problému. Jeden z problémů, které je vhodné na adiabatických kvantových počítačích řešit, je problém vyhovění (anglicky satisfiability, SAT problem). Snažíme se najít n-tici bitů, která splňuje předem dané klauzule typu *první bit ano nebo druhý bit ano, ale třetí bit ne* apod. Qubity v tomto případě budeme reprezentovat pomocí interagujících $\frac{1}{2}$-spinů. Každému z původních bitů b_i nyní odpovídá qubit $|z_i\rangle$, kde $z_i = 0, 1$.

Rozmysleme si nyní, jak vypadají hamiltoniány $\hat{H}_i$ a $\hat{H}_f$.

Koncový hamiltonián $\hat{H}_f$. Koncový hamiltonián odpovídající konkrétnímu problému budeme uvažovat jako součet dílčích hamiltoniánů $\hat{H}_{f,k}$,

$$\hat{H}_f = \sum_k \hat{H}_{f,k}, \tag{2.14}$$

které odpovídají jednotlivým klauzulím k. Klíčový požadavek, který na hamiltonián $\hat{H}_f$ klademe, je, aby jeho základní stav odpovídal námi hledanému řešení. Toto můžeme splnit pomocí hamiltoniánů $\hat{H}_{f,k}$, které na n-tici qubitů působí následujícím způsobem

$$\hat{H}_{f,k} |z_1\rangle |z_2\rangle \cdots |z_n\rangle = h_k(z_1, z_2, \cdots, z_n) |z_1\rangle |z_2\rangle \cdots |z_n\rangle . \tag{2.15}$$

Funkce h_k jsou takové, které splňují

$$h_k = 0 \quad \Longleftrightarrow \text{ bity vyhovují klauzuli } k, \tag{2.16}$$

$$h_k > \epsilon \quad \Longleftrightarrow \text{ bity nevyhovují klauzuli } k. \tag{2.17}$$

Zde $\epsilon > 0$. Na volbě hodnoty ϵ závisí vzdálenost energetických hladin. Je tedy vhodné zvolit dostatečně velké ϵ. Tato závislost je ovšem konstantní. Později si ukážeme, že přiblížení hladin pro SAT problém závisí polynomiálně, či dokonce exponenciálně na počtu qubitů. Není tedy z výpočetního hlediska nutné se hodnotou ϵ příliš zabývat. To zvláště protože tato určuje sílu interakce mezi jednotlivými qubity a s její rostoucí hodnotou roste i energetická složitost daného výpočtu.

Čísla h_k jsou jistou penalizací pro qubity nevyhovující dané klauzuli. Ve skutečnosti je lepší uvažovat, že daná klauzule určuje jistou interakci mezi qubity. Například klauzuli u: „první a druhý qubit“ odpovídá interakční hamiltonián

$$\hat{H}_{f,u} = \frac{1}{2}(\mathbf{1} - \sigma_z^1\sigma_z^2) + \frac{1}{2}(\mathbf{1} + \sigma_z^1) + \frac{1}{2}(\mathbf{1} + \sigma_z^2) \tag{2.18}$$

Počáteční hamiltonián $\hat{H}_i$. Koncový hamiltonián v sobě obsahuje interakce mezi qubity. Tyto interakce odpovídají jednotlivým klauzulím. Po počátečním hamiltoniánu naopak požadujeme, aby žádné interakce neobsahoval.

Počáteční hamiltonián $\hat{H}_i$ tedy odpovídá vnějšímu poli, které na qubity působí

$$\hat{H}_i = \sum_j \frac{1}{2}\left(\mathbf{1} - \sigma_x^{(j)}\right), \tag{2.19}$$

kde sčítáme přes všechny qubity j.

Je důležité, aby směr tohoto vnějšího pole byl jiný, než směr, ve kterém chceme qubity měřit po provedení výpočtu. Zde jsme zvolili směr x, neboť qubity měříme ve směru z. K tomuto problému se vrátíme na konci této sekce o SAT problému, až si řekneme o podmínce adiabatičnosti.

Celkový hamiltonián pro SAT tedy v průběhu výpočtu vytváří interakce mezi qubity. Systémy s takovou vlastností vykazují kvantové fázové přechody. Kvantové fázové přechody jsou neanalytičnosti ve spektru daného hamiltoniánu. O tom, že fázové přechody by mohly být překážkou pro adiabatické počítání hovoří kapitola 3.

Podmínka adiabatičnosti Podívejme se nyní podrobněji na podmínku adiabatičnosti (2.11) pro SAT problém. Přestože bychom mohli nadále uvažovat podmínky kladené na parametr g, lepší představu nám dá celkový čas T, po který se bude systém vyvíjet.

Protože přesné odvození podmínky adiabatické aproximace je komplikované, uveďme si zde pouze typickou podobu této podmínky

$$T \gg \hbar \sum_{j \neq i} \frac{\left\langle \psi_i^g \middle| \frac{\mathrm{d}}{\mathrm{d}g}\hat{H}^g \middle| \psi_j^g \right\rangle}{(E_j^g - E_i^g)^2} \tag{2.20}$$

Tato podoba platí pouze pro dostatečně hladké hamiltoniány, jak ukazuje článek [19], kde lze nalézt i odvození této konkrétní podoby. Při adiabatickém kvantovém počítání závisí hamiltonián na parametru lineárně, tedy je dostatečně hladký a v dalším budeme tedy uvažovat tvar podmínky (2.11).

Podívejme se nyní, co pro adiabatické počítání tato podmínka znamená. V čitateli v (2.20) vystupují čísla menší než vlastní hodnoty operátoru $\frac{\mathrm{d}\hat{H}}{\mathrm{d}g}$. Neboť

operátory $\hat{H}_f$ a $\hat{H}_i$ nezávisejí na g, platí

$$\frac{\mathrm{d}\hat{H}}{\mathrm{d}g} = \hat{H}_f - \hat{H}_i. \tag{2.21}$$

Tedy čitatel v (2.20) řádově odpovídá vlastním hodnotám hamiltoniánů $\hat{H}_f$ a $\hat{H}_i$. Tyto jsou dány součtem vlastních hodnot hamiltoniánů $\hat{H}_{f,k}$ resp. $\hat{H}_{i,k}$, jejichž vlastní hodnoty nepřekročí počet qubitů, kterých se týkají. Čitatel tedy řádově odpovídá počtu m klauzulí.

Ve jmenovateli vyšetřujeme vzdálenost energetických hladin. Může se stát že pro nějaká j', i' platí $E_{j'} = E_{i'}$. V takovém případě čas evoluce $T \to \infty$. Tato situace nastává pouze pro speciální symetrické hamiltoniány a hovoří o ní „teorém o nekřížení".

O vzdálenostech $E_j - E_i \neq 0$ budeme hovořit v kapitole 3. Zde pouze uveďme, že se energetické hladiny při adiabatických výpočtech mohou silně blížit. Toto blížení je v některých případech úměrné počtu qubitů. Vzdálenost $E_j - E_i$ je tedy pro rozbor adiabatického počítání klíčová.

Teorém o nekřížení. Podívejme se nyní, proč je křížení hladin vzácné. Zaměřme na situaci, kdy máme hamiltonián se dvěma energetickými hladinami[1]. Takový můžeme zapsat maticí

$$\hat{H} = \begin{pmatrix} a(s) & c(s) \\ \bar{c}(s) & b(s) \end{pmatrix}. \tag{2.22}$$

Při hledání vlastních čísel $E(s)$ takové matice dojdeme k rovnici

$$(a(s) - E(s))(b(s) - E(s)) - c(s)\bar{c}(s) = 0 \tag{2.23}$$

s řešeními

$$E_{1,2}(s) = \frac{a + b \pm \sqrt{(a+b)^2 - 4(ab - c\bar{c})}}{2} \tag{2.24}$$

Aby došlo ke křížení hladin, musí platit $E_1 = E_2$, tedy $\sqrt{(a-b)^2 + 4\left|c\right|^2} = 0$. Tato podmínka může být splněna pouze při splnění

$$(a-b)^2 = 0 \tag{2.25}$$

$$\left|c\right|^2 = 0 \tag{2.26}$$

Což jsou dvě podmínky, které musí platit zároveň. Máme ovšem pouze jeden parametr, který můžeme měnit a splnění obou podmínek je vzácné. Hladiny se tedy nekříží.

Výjimkou je situace, kdy

$$c(s) = 0, \quad \forall s \tag{2.27}$$

Což je případ, kdy hamiltonián vykazuje určitou symetrii. V případě adiabatického kvantového počítání se může taková symetrie objevit, pokud nemáme dostatek klauzulí pro jednoznačné určení systému.

Příkladem toho budiž dvou qubitový problém s klauzulí „Jeden nebo druhý qubit, ale ne oba zároveň". Taková klauzule umožňuje stavy $|01\rangle$ a $|10\rangle$, přičemž oba budou mít stejnou energii. To ovšem není problém pro adiabatický výpočet. Změřením qubitů získáme jedno z možných řešení.

[1] Argument o nekřížení hladin se dá zobecnit i pro více hladinové systémy, jako je ukázáno například v [21].

Směr pole v $\hat{H}_i$. Protože koncový hamiltonián bude obsahovat Pauliho matice σ_z, bude vhodné, aby počáteční hamiltonián obsahoval matice v jiném směru. Například σ_x. Této problematice je věnován odstavec v článku [20]. Autoři uvažují jedno-qubitový problém, který je splněn, pokud tento qubit nabývá hodnoty 1. Takovému problému odpovídá koncový hamiltonián

$$\hat{H}_f = \frac{1}{2}(1 + \sigma_z) \tag{2.28}$$

Volbou počátečního hamiltoniánu

$$\hat{H}_i = \frac{1}{2}(1 - \sigma_z) \tag{2.29}$$

dostáváme hamiltonián vývoje

$$\hat{H}(g) = (1-g)\frac{1}{2}(1-\sigma_z) + g\frac{1}{2}(1+\sigma_z) = \begin{pmatrix} g & 0 \\ 0 & 1-g \end{pmatrix}. \tag{2.30}$$

Pozorujeme, že pro $g = \frac{1}{2}$ se vlastní čísla matice samy sobě rovnají, dochází ke křížení a není možné provést systém adiabatickou evolucí.

2.2.2 Vyhledávání v databázi.

V kapitole 1 jsme si ukázali Groverův algoritmus pro vyhledávání v databázi, který by fungoval na hradlových kvantových počítačích. V této sekci si ukážeme jiný přístup ke kvantovému vyhledávání v databázi — využívající adiabatické evoluce. V kapitole 3 ukážeme, že tento adiabatický algoritmus má časovou složitost $T = \mathcal{O}(\sqrt{k})$, kde k je velikost prohledávané databáze.

Koncový hamiltonián. Výsledkem vyhledávacího algoritmu by měl být stav, jehož změření nám dá jeden konkrétní stav. Označme tento stav $|v\rangle$. Kde v je index prvku v databázi. Pak $|v\rangle$ obdobně jako v kapitole 1 je takový stav, jehož qubity odpovídají danému indexu. Hamiltonián, pro který je tento stav základním stavem je

$$\hat{H}_{Gf} = 1 - |v\rangle \langle v|. \tag{2.31}$$

Počáteční hamiltonián. O řešení Groverova problému nemáme žádné předchozí informace. Chceme tedy, aby v počátečním hamiltoniánu byly všechny možnosti zastoupeny rovnoměrně. Uvažujme tedy počáteční hamiltonián

$$\hat{H}_{Gi} = 1 - |s\rangle \langle s| \tag{2.32}$$

kde $|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$ je superpozice všech čísel reprezentovaných odpovídajícími qubity.

Z hamiltoniánů $\hat{H}_{Gf}$ a $\hat{H}_{Gi}$ sestavíme, ve shodě s obecným adiabatickým algoritmem postulovaným v této kapitole, hamiltonián

$$\hat{H}_G = (1-g)\hat{H}_{Gi} + g\hat{H}_{Gf}. \tag{2.33}$$

2.3 Berryho hamiltonián

Zrychlení adiabatické evoluce. M. V. Berry si v článku [22] všímá, že pomalu se měnící hamiltonián $\hat{H}$ lze nahradit jiným hamiltoniánem $\hat{H}_B$, který systém provede stejnou evolucí, ovšem v libovolně krátkém čase.

Sestrojení. Shrňme si zde Berryho úvahy, které vedou k vytvoření takového hamiltoniánu.

V sekci 2.1 jsme sledovali vývoj základního stavu $\alpha_j |\psi_j(t)\rangle$ časově závislého hamiltoniánu $\hat{H}(t)$. Zjistili jsme, že při adiabatické aproximaci se koeficienty α_j vyvíjejí podle (2.12). Nyní hledáme hamiltonián $\hat{H}_B$, pro který budeme tento vývoj sledovat i při nesplnění podmínky adiabatické aproximace. Tedy takový hamiltonián, pro který platí Schrödingerova rovnice

$$i\hbar\frac{\partial}{\partial t}\alpha_j |\psi_j\rangle = \hat{H}_B\alpha_j |\psi_j\rangle \tag{2.34}$$

pro α_j dané vztahem (2.12).

K tomu si všímáme platnosti operátorové rovnosti

$$i\hbar\frac{\partial}{\partial t}\hat{U} = \hat{H}_B\hat{U} \tag{2.35}$$

platné pro libovolný unitární operátor $\hat{U}$, a hamiltonián $\hat{H}_B$ určený operátorem $\hat{U}$ jako

$$\hat{H}_B = i\hbar\left(\frac{\partial}{\partial t}\hat{U}\right)\hat{U}^\dagger. \tag{2.36}$$

Zde $\hat{U}^\dagger$ je hermitovsky sdružený operátor k $\hat{U}$.

Volbou

$$\hat{U} = \sum_j \exp\left(-\frac{i}{\hbar}\int_0^t \mathrm{d}t' E_n(t') - \int_0^t \mathrm{d}t' \left\langle \psi_n(t') \middle| \frac{\partial}{\partial t'}\psi_n(t') \right\rangle\right) |\psi_n(t)\rangle \langle\psi_n(0)| \tag{2.37}$$

dostáváme $\hat{H}_B$, který vede stavy $|\psi_j\rangle$ přesně podle vztahu (2.34).

$$\hat{H}_B = \sum_n |\psi_n\rangle E_n \langle\psi_n| + i\hbar\sum_n \left(\left|\frac{\partial}{\partial t}\psi_n\right\rangle\left\langle\psi_n\right| - \left\langle\psi_n\left|\frac{\partial}{\partial t}\psi_n\right\rangle\right|\psi_n\rangle\langle\psi_n|\right), \tag{2.38}$$

kde dále využitím vztahu (2.9) a rozepsáním $|\frac{\partial}{\partial t}n\rangle$ do vlastních stavů $\hat{H}$ dostaneme

$$\left|\frac{\partial}{\partial t}\psi_n\right\rangle = \sum_m |\psi_m\rangle\left\langle\psi_m\left|\frac{\partial}{\partial t}\psi_n\right\rangle\right. = \sum_{m\neq n} |\psi_m\rangle \frac{\langle\psi_m \,|\, \frac{\partial}{\partial t}H \,|\, n\rangle}{E_m - E_n} + |\psi_n\rangle\left\langle\psi_n\left|\frac{\partial}{\partial t}\psi_n\right\rangle\right. . \tag{2.39}$$

A tedy

$$\hat{H}_B = \sum_n |\psi_n\rangle E_n \langle\psi_n| + i\hbar\sum_{m\neq n}\sum_n \frac{|\psi_m\rangle\langle\psi_m|\frac{\partial}{\partial t}\hat{H}|\psi_n\rangle\langle\psi_n|}{E_m - E_n} = \hat{H} + \hat{H}'. \tag{2.40}$$

Tedy nový hamiltonián $\hat{H}_B$ lze zapsat jako součet původního hamiltoniánu $\hat{H}$ a jisté korekce $\hat{H}'$. Všímáme si, že korekce $\hat{H}'$ nabývá tvaru, který odpovídá členu zanedbanému adiabatickou aproximací. To ovšem znamená, že můžeme adiabatickou evoluci libovolně zrychlit, ovšem potřebujeme k tomu korekci hamiltoniánu v řádu odpovídajícímu požadovanému zrychlení.

3. Kvantové fázové přechody a adiabatické počítání

3.1 Kvantové fázové přechody

V minulé kapitole jsme hovořili o adiabatickém kvantovém počítání. Na příkladu SAT problému jsme poukázali na fakt, že v adiabatickém kvantovém počítání dochází k přechodu od systému neinteragujících qubitů k systému qubitů interagujících. Systémy interagujících spinů vykazují fázové přechody, kterým bude věnována tato kapitola. Důvodem našeho zájmu je fakt, že při kvantových fázových přechodech dochází k blížení hladin. Navíc velikost tohoto blížení je odvislá od velikosti systému. S rostoucím počtem qubitů se hladiny při kvantových fázových přechodech stále více blíží. Toto může být překážkou pro adiabatické kvantové počítání.

V této kapitole se pokusíme nejprve vysvětlit, co kvantové fázové přechody jsou, a ukázat si důvody jejich vzniku v interagujících systémech na Lipkinově modelu. Poté provedeme rozbor blížení hladin při kvantových fázových přechodech.

Definice. Řekneme, že hamiltonián závisející na nějakém parametru ξ vykazuje kvantový fázový přechod (dále jen KFP), jestliže se při změně parametru ξ objeví neanalytičnost základního stavu tohoto hamiltoniánu. Ke kvantovým fázových přechodům dochází jen v limitě $N \to \infty$, kde N charakterizuje velikost systému — počet qubitů.

Podobně jako pro klasické fázové přechody zavádíme pro KFP Ehrenfestovu klasifikaci. KFP n-tého řádu znamenají nespojitost n-té derivace energie systému. Podívejme se nyní na Lipkinův model, který vykazuje fázové přechody prvního a druhého řádu.

3.2 Lipkinův model

Lipkinův hamiltonián ve spinové reprezentaci. Fázové přechody si ukážeme na Lipkinově modelu ze dvou důvodů: Prvním důvodem je, že Lipkinův model v námi použité reprezentaci odpovídá systému interagujících spinů. Druhým důvodem je, že Lipkinův model vykazuje fázové přechody prvního i druhého řádu.

Zaveďme si operátory celkového spinu

$$\hat{J}_{\{x,y,z\}} = \sum_i \hat{S}^i_{\{x,y,z\}}, \tag{3.1}$$

kde $\hat{S}^i$ je i-tý qubit, reprezentovaný spinem. Index i běží přes všechny qubity. Velikost celkového spinu $\hat{J}^2 = \hat{J}_x^2 + \hat{J}_y^2 + \hat{J}_z^2$ nabývá hodnoty $j(j+1)$. V Lipkinově modelu se $\hat{J}^2$ zachovává. Budeme se tedy pohybovat v podprostoru $j = \frac{N}{2}$, kde N je počet qubitů.

Dále si ještě zaveďme operátory

$$\hat{J}_{\pm} = \hat{J}_x \pm i\hat{J}_y. \tag{3.2}$$

Uvažujme Lipkinův hamiltonián ve tvaru

$$\hat{H}^{\eta,\chi} = \hat{H}(\eta,\chi) = \eta\left(1 - \frac{\hat{J}_z}{j}\right) - \frac{1-\eta}{2}\left(\frac{2\hat{J}_x}{j} + \chi\left(1 - \frac{\hat{J}_z}{j}\right)\right)^2 \tag{3.3}$$

Budeme se zabývat změnou základního stavu tohoto Hamiltoniánu v závislosti na změnách parametrů η a χ. Konkrétně sledujme směr spinu $\hat{J} = (\hat{J}_x, \hat{J}_y, \hat{J}_z)$. Za tímto účelem zaveďme sférické souřadnice $\hat{\theta}$ s vlastními hodnotami $\theta \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ a $\hat{\phi}$ s vlastními hodnotami $\phi \in (0, 2\pi)$, ve kterých vyjádříme spinové operátory $\hat{J}_x$, $\hat{J}_y$ a $\hat{J}_z$.

$$\begin{aligned} \hat{J}_x &= j\cos\hat{\phi}\sin\hat{\theta} \\ \hat{J}_y &= j\sin\hat{\phi}\sin\hat{\theta} \\ \hat{J}_z &= j\cos\hat{\theta} \end{aligned} \tag{3.4}$$

V dodatku A můžeme nahlédnout, že aby platily komutační relace

$$[\hat{J}_z, \hat{J}_{\pm}] = \pm\hat{J}_{\pm}, \tag{3.5}$$

musí souřadnice $\hat{\theta}$ a $\hat{\phi}$ splňovat komutační relaci

$$[\cos\hat{\theta}, \hat{\phi}] = -i\frac{1}{j}. \tag{3.6}$$

O veličinách $\cos\hat{\theta}$ resp. $-\hat{\phi}$ můžeme uvažovat jako o zobecněné souřadnici resp. hybnosti. V takovém případě má celkový spin význam převrácené Planckovy konstanty.

Lipkinův hamiltonián ve sférických souřadnicích. V nově zavedených souřadnicích $\hat{\theta}$ a $\hat{\phi}$ nabývá $\hat{H}^{\eta,\chi}$ tvaru

$$\begin{aligned} \hat{H}^{\eta,\chi} = {} & \eta - \eta\cos\hat{\theta} - 2\cos^2\hat{\phi}\sin^2\hat{\theta} + 2\eta\cos^2\hat{\phi}\sin^2\hat{\theta} + \chi\cos\hat{\phi}\sin\hat{\theta} \\ & - \eta\chi\cos\hat{\phi}\sin\hat{\theta} - \chi\cos^2\hat{\phi}\sin\hat{\theta} + \eta\chi\cos\hat{\phi}\sin\hat{\theta} + \frac{1}{2}\chi^2 \\ & - \frac{1}{2}\chi^2\eta - \chi^2\cos\hat{\theta} + \eta\chi\cos\hat{\theta} + \frac{1}{2}\chi^2\cos^2\hat{\theta} - \frac{1}{2}\eta\chi^2\cos^2\hat{\theta} \end{aligned} \tag{3.7}$$

KFP nastávají v limitě $N \to \infty$, což v našem případě znamená i $j \to \infty$. Pak ovšem $[\cos\hat{\theta}, \hat{\phi}] = 0$ a dostáváme klasickou limitu. Při vyšetřování KFP nás tedy zajímají stacionární body klasického hamiltoniánu shodného s hamiltoniánem (3.7), kde ovšem jsou souřadnice $\hat{\theta}$ a $\hat{\phi}$ nahrazeny jejich klasickým ekvivalentem. K určení stacionárních bodů potřebujeme znát derivace tohoto klasického hamiltoniánu, ty jsou spočtené v dodatku B.

KFP druhého řádu. První případ, který budeme rozebírat, je případ $\chi = 0$ a $\eta \in [0, 1]$. Při hledání extrému řešíme rovnice

$$4(1-\eta)\cos^2\phi \sin\theta\cos\theta - \eta\sin\theta = 0 \tag{3.8}$$
$$4\cos\phi\sin\phi\sin^2\theta - 4\eta\cos\phi\sin\phi\sin^2\theta = 0 \tag{3.9}$$

Z druhé rovnice dostáváme podmínku $\cos\phi = 0 \vee \sin\phi = 0 \vee \sin\theta = 0$. Z první rovnice dostáváme podmínku $\sin\theta = 0 \vee \cos\theta = \frac{\eta}{4(1-\eta)\cos^2\phi}$.

Obě podmínky najednou jsou splněny ve dvou případech

1. V prvním případě je $\sin\theta = 0$, tedy $\theta = 0$ a ϕ je libovolné.
2. Ve druhém případě je $\sin\phi = 0$, tedy $\phi \in \{0, \pi\}$. Pro θ poté máme $\cos\theta = \frac{\eta}{4(1-\eta)}$, tedy $\theta = \arccos\frac{\eta}{4(1-\eta)}$, což má smysl pouze pro $\eta < 0{,}8$.

Při vyšetřování, pro které θ nabývá energie globálního minima, si pomůžeme grafem 3.1, kde vykreslíme hodnotu energie pro hodnoty $\theta_1 = 0$ a $\theta_2 = \arccos\frac{\eta}{4(1-\eta)}$. V grafu 3.1 je možné si povšimnout, že energie nabývá minimum pro θ_2 pro $\eta < 0{,}8$ a v θ_1 pro $\eta > 0{,}8$.

V bodě $\eta = 0{,}8$ má tedy energie základního stavu nespojitou druhou derivaci, což je příznačné pro fázové přechody druhého řádu. Můžeme tušit, že se tato nespojitost nějakým způsobem projeví při adiabatické evoluci ($\dot{\eta}$ malé) systému. Podrobně se tímto budeme zabývat v sekci 3.3.

KFP prvního řádu. Ve druhém případě naopak budeme držet pevné $\eta = 0{,}4$ a měnit budeme χ mezi hodnotami -1 a 1. V tomto případě je analytický rozbor energie složitější, a zde si uvedeme pouze výsledky.

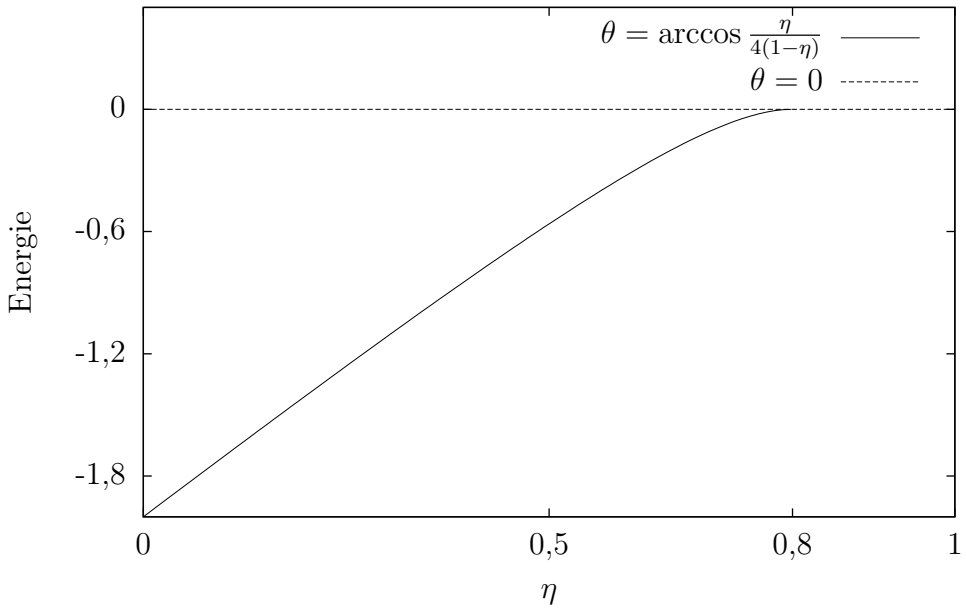
Tato energie nabývá dvou minim, v bodech $(\theta, \phi) = \left(\pm\arccos\frac{\eta(1-\chi)+\chi^2}{(1-\eta)(4+\chi^2)}, 0\right)$. S rostoucím χ hodnota energie v jednom minimu roste a v druhém klesá. To je patrné z grafu 3.2. Hodnoty v těchto minimech se rovnají pro $\chi = 0$. V tomto bodě má globální minimum energie nespojitou první derivaci — dochází k KFP prvního řádu.

3.3 KFP a přiblížení hladin.

Energetická minima. Všímali jsme si kvalitativních změn v energiích odpovídajících Lipkinově modelu. Tyto změny jsou typické pro všechny KFP. Nyní se budeme zabývat energetickými hladinami takového systému a časem potřebným pro adiabatickou evoluci.

Pro adiabatické počítání vyžadujeme, aby systém zůstával v základním stavu, tedy stavu o minimální energii. V předchozí sekci jsme si povšimli prudkých změn v energii systému, když počet částic $N \to \infty$. V praxi samozřejmě nebudeme nikdy počítat s nekonečným počtem částic. Mohlo by se tedy zdát, že se nás KFP netýkají.

Ve skutečnosti ovšem již pro N konečná pozorujeme jisté jevy, které jsou jakousi předzvěstí KFP. Tyto jevy jsou provázeny těsným přiblížením energetických hladin v závislosti na N. Nyní se pokusíme tato přiblížení vysvětlit a kvantifikovat. To nám umožní rozebírat časovou složitost kvantových adiabatických algoritmů z pohledu KFP podle článku [23].



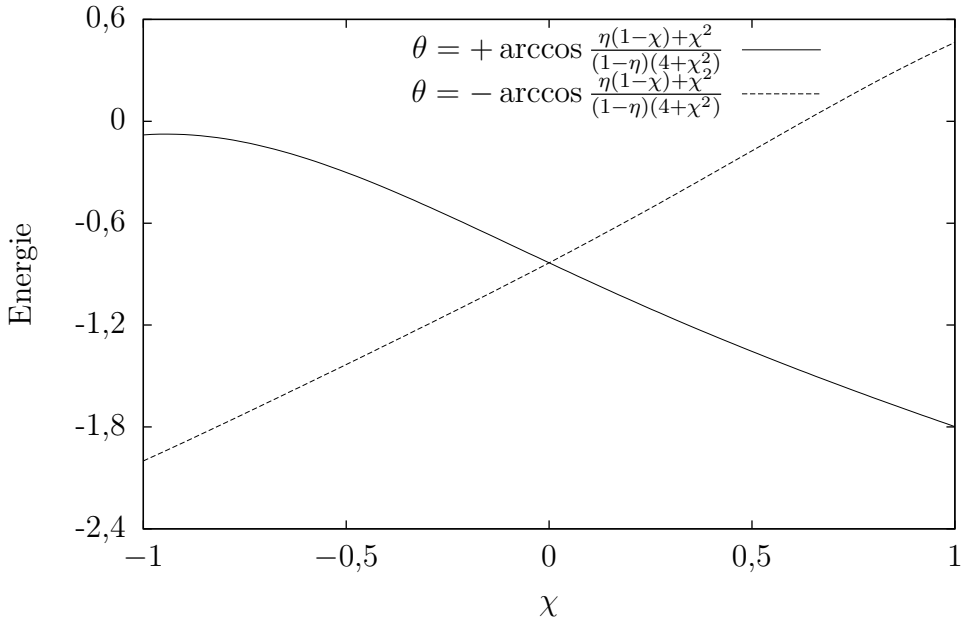
Obrázek 3.1: Klasická energie, odpovídající Lipkinově modelu v případě $\chi = 0$ v závislosti na parametru η. Křivky odpovídají směrům momentu setrvačnosti $\boldsymbol{J}$, pro které energie nabývá extrémů. V bodě $\eta = 0{,}8$ přestává být minimálním směr $\theta = \arccos \frac{\eta}{4(1-\eta)}$, a minimálním se stává směr $\theta = 0$, který pro interval $[0; 0{,}8)$ byl maximem.

KFP prvního řádu. KFP 1. řádu odpovídá závislost energie jako je naznačeno v grafu 3.4. Tato závislost má dvě lokální minima. V jednom z těchto minim nabývá systém nižší hodnoty energie. Energie zde má globální minimum. Když měníme parametr χ, energie tohoto minima začíná růst, zatímco energie druhého minima klesá. Pro určitou hodnotu parametru se poloha globálního minima prudce změní z původní na polohu v druhém lokálním minimu. Pokud systém má zůstat v minimu energie, musí dojít k prudké změně stavu. Systém tedy musí protunelovat bariérou oddělující tato dvě minima.

I pro konečné N, kdy nedochází k fázovému přechodu jsme svědky podobného jevu. Předpokládejme veličinu, obdobnou veličině $\hat{\theta}$ z Lipkinova modelu, která charakterizuje dvě odlišná minima energie. Označme ji $\hat{x}$. V reprezentaci určené souřadnicí x bude vlnová funkce $\psi(x)$ popisující systém nabývat nejvyšších hodnot v okolí bodu, ve kterém má klasická energie minimum. Toto si můžeme představit jako kvantovou částici v potenciálu. Pro určitou hodnotu parametru χ přestane tato částice být v základním stavu. Aby se opět dostala do základního stavu, musí protunelovat bariérou.

WKB aproximace určuje transmisní koeficient T_{WKB} této částice jako $T_{\text{WKB}} = e^{-\frac{C}{\hbar}}$. Zde C je konstanta závisející na průběhu tunelovaného potenciálu a energii částice. Tato tedy závisí na typu úlohy, kterou na adiabatickém kvantovém počítači řešíme a nezávisí na počtu qubitů. Na počtu qubitů ovšem v našich úlohách závisí $\hbar = \frac{1}{j} = \frac{2}{N}$. Pozorujeme tedy, že čas potřebný pro adiabatické kvantové počítání roste v systémech vykazujících KFP prvního řádu exponenciálně s počtem částic.

Lepší představu pro adiabatické kvantové počítání dává článek [24], který ro-



Obrázek 3.2: Klasická energie odpovídající Lipkinově modelu v případě $\eta = 0{,}4$. Sledujeme vývoj energie v závislosti na parametru χ v bodech $\theta = \pm$, která odpovídají minimům této energie. V bodě $\chi = 0$ vidíme, že pro udržení systému v globálním minimu musí dojít k náhlé změně úhlu θ. Dochází tedy k fázovému přechodu prvního řádu.

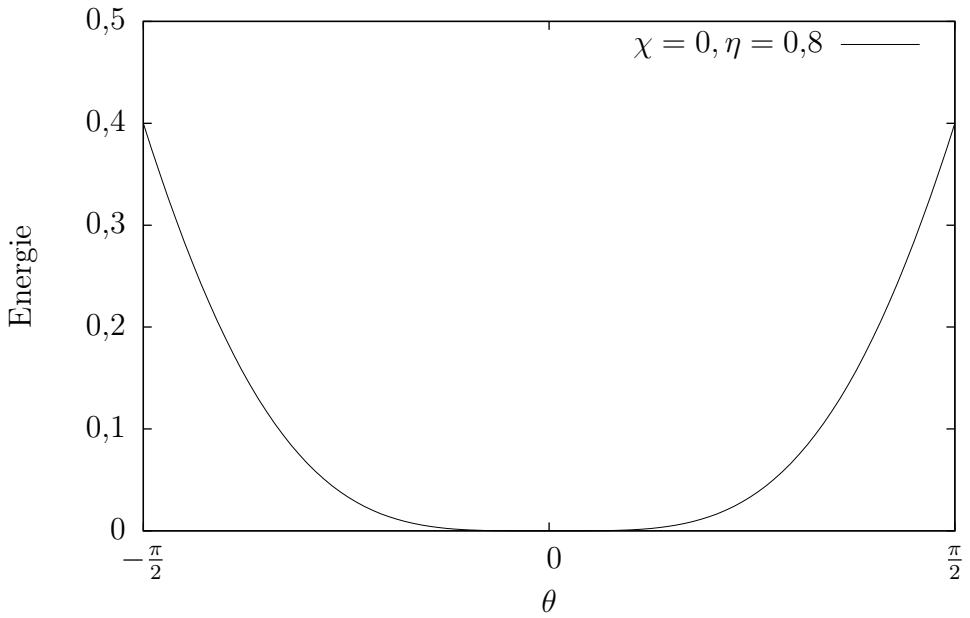
zebírá přiblížení hladin při KFP prvního řádu. V tomto článku autoři ukazují, že přiblížení hladin (pro hodnotu parametru χ kdy jsou hodnoty energie ve stacionárních bodech shodné) závisí na počtu částic exponenciálně, což je v souladu s našim přibližným odvozením. Skutečně tedy čas T potřebný pro adiabatickou evoluci roste jako $T = \mathcal{O}(e^{cN})$, kde c je konstanta typická pro konkrétní systém.

KFP 1. řádu vykazuje například kvantový adiabatický algoritmus pro vyhledávání v databázi. Pro něj konkrétně $c = \frac{1}{2}$, jak ukazuje článek [25]. Tedy časová složitost tohoto algoritmu je $T = \mathcal{O}(e^{\frac{N}{2}})$. Zde N je počet spinů, který ovšem kóduje $k = 2^N$ prvků databáze. Časová složitost vyjádřená pomocí počtu prvků databáze je tedy $T = \mathcal{O}(\sqrt{k})$.

KFP druhého řádu. KFP 2. řádu odpovídá závislost potenciálu jako je naznačeno v grafu 3.3[1]. V článku [26] je ukázáno, že potenciál KFP 2. řádu odpovídá kvartickému oscilátoru. U kvartického oscilátoru, na rozdíl od oscilátoru harmonického, nejsou energetické hladiny ekvidistantní, ale jejich vzdálenost roste s rostoucí energií. Nejnižší hladiny jsou ovšem blízko sebe. Jejich vzdálenost naopak klesá s rostoucím N. V článku [26] je ukázáno, že tato závislost na N je polynomiální (konkrétně $N^{-\frac{1}{3}}$. Náznak odvození této závislosti je v dodatku C.

Na rozdíl od KFP prvního řádu se ovšem u KFP druhého řádu k sobě přiblíží více hladin. Z algebraického škálování spektra $E_i - E_j \propto N^{-\frac{1}{3}}$ dostáváme z podmínky adiabatičnosti (2.20), že čas potřebný pro adiabatický kvantový výpočet

[1]Striktně řečeno v grafu není vynesen potenciál, ale energie. Uvážíme-li ovšem, že potenciál v grafu je vynesen pro $\phi = 0$, o kterém jsme řekli, že odpovídá hybnosti, můžeme předpokládat, že je v grafu skutečně potenciál závislý pouze na souřadnici.

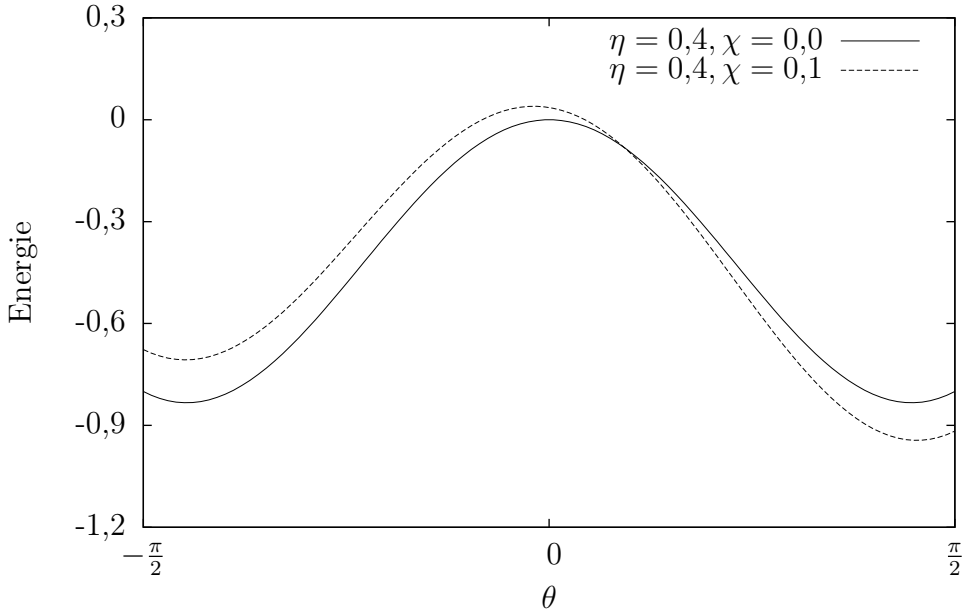


Obrázek 3.3: Klasická energie odpovídající Lipkinově modelu v případě $\chi = 0$ v závislosti na směru celkového momentu setrvačnosti $\boldsymbol{J}$. Zde $\phi = 0$, $\eta = 0{,}8$ a měníme θ. V okolí nuly vidíme přechod od energie s jedním minimem v nule, k energii se dvěma minimy od nuly stejně vzdálených.

roste s počtem qubitů přibližně jako $N^{\frac{5}{3}}$, což je polynomiální závislost.

Ukázali jsme tedy, alespoň na jednoduchém příkladu Lipkinova modelu, že KFP 2. řádu jsou pro adiabatické kvantové počítání výhodnější, než KFP 1. řádu.

V kapitole 2.3 jsme viděli, že komponenta $\hat{H}'$ Berryho hamiltoniánu, určená vztahem (2.40), obsahuje ve jmenovateli rozdíly energií. Je tedy zřejmé, že exponenciální nebo polynomiální škálování s počtem qubitů N se týká i Berryho hamiltoniánu v bodě KFP prvního nebo druhého řádu.



Obrázek 3.4: Klasická energie odpovídající Lipkinově modelu v případě $\eta = 0{,}4$ v závislosti na směru celkového momentu setrvačnosti $\boldsymbol{J}$. V grafu jsou vyobrazeny dvě křivky pro různé hodnoty parametru χ. Je patrné, že pro $\chi = 0$ má energie dvě minima o stejné hodnotě. Pro $\chi > 0$ hodnota jednoho minima začíná růst, naopak hodnota druhého minima klesat. Pro $\chi < 0$ bychom pozorovali, že hodnota prvního minima klesá a hodnota druhého minima roste. V této situaci dochází k fázovému přechodu prvního řádu.

Závěr

V této práci jsme shrnuli poznatky o kvantových počítačích. V první kapitole jsme diskutovali převážně hradlové kvantové počítače, jejichž princip jsme ilustrovali na Groverově algoritmu. Pomocí tohoto algoritmu jsme ukázali hlavní důvod využívání kvantových počítačů — zrychlení některých konkrétních výpočtů oproti klasickým počítačům.

V druhé kapitole se věnujeme hlavnímu tématu této práce, adiabatickým kvantovým počítačům. Bylo dokázáno, že adiabatické a hradlové kvantové počítače jsou z pohledu výpočetní složitosti polynomiálně ekvivalentní. Z fyzikálního hlediska se však jedná o zcela odlišné přístupy ke konstrukci kvantového počítače. Na začátku druhé kapitoly jsme si odvodili adiabatický teorém, klíčovou myšlenku adiabatického počítání: Systém, který je na začátku evoluce v základním stavu hamiltoniánu, zůstane v tomto základním stavu po celou dobu evoluce, je-li tato evoluce dostatečně pomalá. Poté jsme si již vysvětlili základní princip adiabatického kvantového počítače, a ukázali dva konkrétní příklady využití: SAT problém a vyhledávání v databázi.

Poukázali jsme na fakt, že adiabatickému počítači odpovídá systém interagujících spinů, který při provádění kvantového výpočtu často vykazuje kvantové fázové přechody. Že jsou tyto fázové přechody možnou překážkou kvantového počítání, jsme si ukázali ve třetí kapitole. Nejprve jsme si uvedli, co kvantové fázové přechody jsou a ukázali si je na Lipkinově modelu. Poté jsme se zabývali fázovými přechody prvního a druhého řádu. Ukázali jsme, že fázové přechody druhého řádu jsou pro adiabatické kvantové počítání méně problematické, neboť při nich je blížení energetických hladin polynomiálně závislé na počtu qubitů. U kvantových fázových přechodů prvního řádu je tato závislost exponenciální.

V práci jsme též okrajově diskutovali využití Berryho hamiltoniánu při adiabatickém kvantovém počítání. Ukázali jsme, že pomocí tohoto hamiltoniánu umíme výpočet zrychlit, ovšem za cenu dodání komplikovaných interakcí do systému qubitů. Navíc v případě průchodu KFP prvního resp. druhého dochází k exponenciálnímu resp. polynomiálnímu nárustu síly těchto interakcí.

A. Komutační relace

Požadujeme splnění relace

$$\left[\hat{J}_z, \hat{J}_\pm\right] = \pm\hat{J}_\pm. \tag{A.1}$$

Dosazením z definičních vztahů (3.4) do levé strany rovnice (A.1) dostaneme pro $\pm\hat{J}_\pm$

$$\pm\,\hat{J}_\pm = j^2\left[\cos\hat{\theta}, e^{\pm i\hat{\phi}}\sin\hat{\theta}\right] = j^2\left[\cos\hat{\theta}, e^{\pm i\hat{\phi}}\right]\sin\hat{\theta}. \tag{A.2}$$

Rozepsáním $e^{\pm i\hat{\phi}}$ do Taylorovy řady dostaneme

$$\begin{aligned}
\pm\hat{J}_\pm &= \left[\cos\hat{\theta}, \sum_{n=0}^{\infty}\frac{(\pm i\hat{\phi})^n}{n!}\right]\sin\hat{\theta} = j^2\sum_{n=0}^{\infty}\frac{(\pm i)^n}{n!}\left[\cos\hat{\theta}, \hat{\phi}^n\right]\sin\hat{\theta} = \\
&= j^2\sum_{n=0}^{\infty}\frac{(\pm i)^n}{n!}\left[\cos\hat{\theta}, \hat{\phi}\right]n\hat{\phi}^{n-1}\sin\hat{\theta} = j^2\left[\cos\hat{\theta}, \hat{\phi}\right]\sum_{n=1}^{\infty}\frac{(\pm i)^n}{(n-1)!}\hat{\phi}^{n-1}\sin\hat{\theta} = \\
&= j\left[\cos\hat{\theta}, \hat{\phi}\right](\pm i)je^{\pm i\hat{\phi}}\sin\hat{\theta} = j\left[\cos\hat{\theta}, \hat{\phi}\right]i(\pm\hat{J}_\pm),
\end{aligned} \tag{A.3}$$

kde jsme předpokládali $\left[\left[\cos\hat{\theta}, \hat{\phi}\right], \hat{\phi}\right] = 0$. Z (A.3) plyne vztah

$$\left[\cos\hat{\theta}, \hat{\phi}\right] = -i\frac{1}{j}. \tag{A.4}$$

B. Derivace Lipkinova hamiltoniánu

Klasický Lipkinův hamiltonián ve sférických souřadnicích θ, ϕ má tvar

$$\begin{aligned} H^{\eta,\chi} &= \eta - \eta\cos\theta - 2\cos^2\phi\sin^2\theta + 2\eta\cos^2\phi\sin^2\theta + \chi\cos\phi\sin\theta \\ &\quad - \eta\chi\cos\phi\sin\theta - \chi\cos^2\phi\sin\theta + \eta\chi\cos\phi\sin\theta + \frac{1}{2}\chi^2 \\ &\quad - \frac{1}{2}\chi^2\eta - \chi^2\cos\theta + \eta\chi\cos\theta + \frac{1}{2}\chi^2\cos^2\theta - \frac{1}{2}\eta\chi^2\cos^2\theta \end{aligned} \tag{B.1}$$

Tomu odpovídají derivace

$$\begin{aligned} \frac{\partial H^{\eta,\chi}}{\partial\theta} &= \eta\sin\theta - 4\cos^2\phi\sin\theta\cos\theta + 4\eta\cos^2\phi\sin\theta\cos\theta \\ &\quad + \chi\cos\phi\cos\theta - \eta\chi\cos\phi\cos\theta - \chi\cos^2\phi\cos\theta + \eta\chi\cos^2\phi\cos\theta \\ &\quad + \chi^2\sin\theta - \eta\chi\sin\theta - \chi^2\sin\theta\cos\theta + \eta\chi^2\sin\theta\cos\theta \end{aligned} \tag{B.2}$$

$$\begin{aligned} \frac{\partial H^{\eta,\chi}}{\partial\phi} &= 4\cos\phi\sin\phi\sin^2\theta - 4\eta\cos\phi\sin\phi\sin^2\theta - \chi\sin\phi\sin\theta \\ &\quad + \eta\chi\sin\phi\sin\theta + 2\chi\cos\phi\sin\phi\sin\theta - 2\eta\chi\cos\phi\sin\phi\sin\theta \end{aligned} \tag{B.3}$$

$$\begin{aligned} \frac{\partial^2 H^{\eta,\chi}}{\partial\theta\partial\phi} = \frac{\partial^2 H^{\eta,\chi}}{\partial\phi\partial\theta} &= 8\cos\phi\sin\phi\cos\theta\sin\theta - 8\eta\cos\phi\sin\phi\cos\theta\sin\theta \\ &\quad - \chi\sin\phi\cos\theta + \eta\chi\sin\phi\cos\theta + 2\chi\cos\phi\sin\phi\cos\theta \\ &\quad - 2\eta\chi\cos\phi\sin\phi\cos\theta \end{aligned} \tag{B.4}$$

$$\begin{aligned} \frac{\partial^2 H^{\eta,\chi}}{\partial\theta^2} &= \eta\cos\theta - 4\cos^2\phi\cos^2\theta + 4\cos^2\phi\sin^2\theta + 4\eta\cos^2\phi\cos^2\theta - \\ &\quad - 4\eta\cos^2\phi\sin^2\theta - \chi\cos\phi\cos\theta + \eta\chi\cos\phi\sin\theta + \\ &\quad + \chi\cos^2\phi\sin\theta - \eta\chi\cos^2\phi\sin\theta + \chi^2\cos\theta - \eta\chi\cos\theta - \\ &\quad - \chi^2\cos^2\theta + \chi^2\sin^2\theta + \eta\chi^2\cos^2\theta - \eta\chi^2\sin^2\theta \end{aligned} \tag{B.5}$$

$$\begin{aligned} \frac{\partial^2 H^{\eta,\chi}}{\partial\phi^2} &= 4\cos^2\phi\sin^2\theta - 4\sin^2\phi\sin^2\theta - 4\eta\cos^2\phi\sin^2\theta + 4\eta\sin^2\phi\sin^2\theta - \\ &\quad - \chi\cos\phi\sin\theta + \eta\chi\cos\phi\sin\theta + 2\chi\cos^2\phi\sin\theta - \\ &\quad - 2\chi\sin^2\phi\sin\theta - 2\eta\chi\cos^2\phi\sin\theta + 2\eta\chi\sin^2\phi\sin\theta \end{aligned} \tag{B.6}$$

C. Škálování kvartického oscilátoru

Uvažujme hamiltonián soustavy qubitů, který má v reprezentaci kolektivní souřadnice x (například projekce spinu do osy z v Lipkinově modelu) tvar

$$\hat{H} = N\left(\frac{\hbar^2}{2M}\frac{\mathrm{d}^2}{\mathrm{d}x^2} + ax^4\right), \tag{C.1}$$

kde M, a jsou konstanty, N je počet qubitů a Planckova konstanta $\hbar$ se vyjádří jako $\hbar = N^{-1}$.

Provedeme substituci $x \mapsto \bar{x} = N^{\kappa}x$, čímž dostaneme

$$\hat{H} = \frac{N^{2\kappa-1}}{2M}\frac{\mathrm{d}^2}{\mathrm{d}\bar{x}^2} + N^{1-4\kappa}a\bar{x}^4. \tag{C.2}$$

Volbou exponentu $\kappa = \frac{1}{3}$ dostáváme

$$\hat{H} = N^{-\frac{1}{3}}\left(\frac{1}{2M}\frac{\mathrm{d}^2}{\mathrm{d}\bar{x}^2} + a\bar{x}^4\right), \tag{C.3}$$

odkud vidíme, že vzdálenosti hladin ve spektru se škálují jako $N^{-\frac{1}{3}}$.

I když tvar hamiltoniánu v reálných případech KFP bývá složitější, vztahy (C.1) a (C.3) jsou často dobrou aproximací.

Seznam použité literatury

[1] Landauer R., *Irreversibility and heat generation in the computing process.* IBM Journal of Research and Development, vol. **44** (2000) 261-269

[2] Adleman L. M. *Molecular computation of solutions to combinatorial problems.* Science vol. **266** (1994) 1021–1024

[3] Feynman R. P. *Simulating physics with computers.* (přepis přednášky) International Journal of Theoretical Physics, vol. **21** (1981) 467-488

[4] Aharonov D., van Dam W., Kempe J., Landau Z., Lloyd S., Regev O. *Adiabatic Quantum Computation is Equivalent to Standard Quantum Computation* SIAM Journal of Computing, vol. **37** (2007) 166-194

[5] Nielsen M. A., Chuang I. L. *Quantum Computation and Quantum Information.* Cambridge University Press, (2000)

[6] Schumacher B., *Quantum coding.* Physical Review A, vol. **51** (1995) 2738–2747

[7] Brandejs H., *Kvantové výpočty v mnohočásticové fyzice.* Bakalářská práce MFF UK, (2014)

[8] Feynman R. P. *There's Plenty of Room at the Bottom.* (přepis přednášky) Caltech Engineering and Science, vol. **23:5** (1960) 22-36

[9] Song H., Youngsang K., Jang Y. H., Jeong H., Reed M. A., Takhee L. *Observation of molecular orbital gating.* Nature vol. **462** (2009) 1039-1043

[10] Bérut A., Arakelyan A., Petrosyan A., Ciliberto S., Dillenschneider R., Lutz E. *Experimental verification of Landauer's principle linking information and thermodynamics.* Nature, vol. **483** (2012) 187–189

[11] Deutsch D. *Quantum theory, the Church-Turing principle and the universal quantum computer.* Proceedings of the Royal Society of London A, vol. **400** (1985) 97-117

[12] Wootters W. K., Zurek W. H. *A single quantum cannot be cloned.* Nature vol. **299** (1982) 802-803

[13] Shor P. W. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* arXiv:quant-ph/9508027

[14] DiVincenzo D. P. *Two-bit gates are universal for quantum computation.* Physical Review A vol. **51** (1995) 1015-1022

[15] Grover L. K. *A fast quantum mechanical algorithm for database search.* arXiv:quant-ph/9605043

[16] Shor P. W. *Scheme for reducing decoherence in quantum computer memory.* Physical Review A vol. **52** (1995) 2493-2496

[17] Hughes R. internetový zdroj. `http://qist.lanl.gov/qcomp_map.shtml`

[18] Cejnar P. *A Condensed Course of Quantum Mechanics.* Karolinum, (2013) 147-148

[19] Comparat D. *General conditions for a quantum adiabatic evolution.* arXiv:quant-ph/0607118

[20] Farhi E., Goldstone J., Gutmann S., Sipser M. *Quantum computation by adiabatic evolution.* arXiv:quant-ph/0001106

[21] Kloc M. *Quantum critical phenomena in finite systems.* Diplomová práce MFF UK, (2013)

[22] Berry M. V. *Transitionless quantum driving.* J. Phys. A: Math. Theor. vol. **42** (2009)

[23] Schützhold R., Schaller G. *Adiabatic quantum algorithms as quantum phase transitions: First versus second order.* Physical Review A vol. **74** (2006) 60304-60307

[24] Vidal J., Arias J. M., Dukelsky J., García-Ramos J. E. *Scalar two-level boson model to study the interacting boson model phase diagram in the Casten triangle.* Physical Review C vol. **73** (2006) 054305-054309

[25] Roland J., Cerf N. J. *Quantum search by local adiabatic evolution.* Physical Review A vol. **65** (2002) 42308-42314

[26] Dusuel S., Vidal J., Arias J. M., Dukelsy J., García-Ramos J. E. *Continuous unitary transformations in two-level boson system* Physical Review C vol. **72** (2005) 064332-064348

Seznam použitých zkratek

SAT	satisfiability problem
NP	non-polynomial
CNOT	controlled not
CCNOT	controlled controlled not
KFP	kvantový fázový přechod
WKB	Wentzel–Kramers–Brillouin