České vysoké učení technické v Praze
Fakulta jaderná a fyzikálně inženýrská

BAKALÁŘSKÁ PRÁCE

Quantum Algorithms

2007

Václav Potoček

Poděkování

Rád bych tímto poděkoval vedoucímu bakalářské práce, panu prof. Ing. Igoru Jexovi, DrSc., nejen za podnětné konzultace a veškerou podporu při tvorbě této práce, ale především za umožnění okamžitého a bezproblémového přístupu k nejvýznamnějším aktuálním knižním titulům k tématu práce i tématům souvisejícím a k důležitým článkům.

Název práce:
Kvantové algoritmy

Autor: Václav Potoček

Obor: Matematické inženýrství

Zaměření: Matematická fyzika

Druh práce: Bakalářská práce

Vedoucí práce: Prof. Ing. Igor Jex, DrSc., KF, FJFI, ČVUT

Abstrakt: Tato práce seznamuje čtenáře se základy problematiky kvantových algoritmů. Spíše než na detailní popisy jednotlivých známých algoritmů je kladen důraz na vysvětlení celkové podstaty problematiky a vztahu kvantových algoritmů s jejich klasickými protějšky.

Klíčová slova: kvantové algoritmy, prohledávání databáze, Groverův algoritmus, kvantové náhodné procházení

Title:
Quantum algorithms

Author: Václav Potoček

Abstract: This thesis shows basics of quantum algorithm topics. Its purpose is not to describe in detail every single known algorithm of some importance. More likely, emphasis is put in explaining the main concepts and relations of quantum algorithms to their classical counterparts.

Key words: quantum algorithms, database search, Grover's algorithm, quantum random walks

Obsah

Úvod

Tato práce si klade za cíl podat úvod do celkem nové a nadějné oblasti kvantové fyziky, kvantových algoritmů. Kvantové algoritmy jsou obdobou klasických algoritmů, realizovaných v elektronických výpočetních jednotkách – zařízení, které realizuje kvantový algoritmus, se tedy nazývá kvantový počítač. Přes tento honosný název však v době uvedení práce veškeré pokusy, ač prokazující pravdivost teoretických závěrů, probíhají pouze v měřítku laboratorních experimentů.

Od čtenáře se očekává znalost lineární algebry na úrovni prvního ročníku vysoké školy, v rozsahu [1]. V některých místech budeme používat i pokročilejší partie lineární algebry, uvedené např. v [2], jmenovitě Hilbertův prostor, tenzorový součin a stopu lineárního operátoru, pouze však pro prostory konečné dimenze, kde bývají tyto pojmy také součástí sylabu v prvních letech studia matematiky. Znalost základů kvantové mechaniky je výhodou, ale části potřebné pro pochopení tématu budou shrnuty v první kapitole.

V ní jsou uvedeny postuláty kvantové mechaniky v obecném tvaru a později zúžené do jednoduššího, konečnědimenzionálního znění, ve kterém budou plně postačujícími pro většinu následujícího textu. Dále je uvedeno několik dalších termínů a principů, které mají v teorii kvantových algoritmů přímé využití.

Druhá kapitola je již zaměřena na využití kvantové mechaniky pro nalezení blízké analogie logických obvodů. Nejprve se ukáže zobecnění bitu na kvantový bit, qubit, zavedeme princip kvantových hradel jako obdoby klasických digitálních hradel, a ukážeme, jak přes jisté odlišnosti jsme schopni pomocí těchto nástrojů simulovat libovolný digitální obvod.

Ve třetí kapitole ukážeme na několika nejznámějších příkladech možnosti, které poskytuje idea kvantových algoritmů jako výhody oproti klasickým algoritmům. Tato kapitola je však uvažována pouze jako stručný náhled do problematiky, která je jako celek již natolik rozsáhlá, že tato práce se věnuje detailněji jen jedné její úzké části.

Touto částí jsou vyhledávací algoritmy, jejichž základní myšlenky jsou popsány ve čtvrté kapitole. Detailně je pak probrán první vyhledávací algoritmus, jehož autorem je Lov Grover a který vedle kvantové faktorizace tvoří jeden z hlavních pilířů současné znalosti kvantových algoritmů.

V páté kapitole je diskutována poněkud mladší myšlenka převedení myšlenky náhodného procházení do světa kvantových algoritmů a především jeho využití v myšlence vyhledávacích algoritmů, algoritmus vyhledávající na hyperkrychli. Stručně je nastíněna problematika realizace kvantových vyhledávacích algoritmů v optických sítích a uveden příklad na tomto vyhledávacím algoritmu.

Jako přílohy práce jsou uvedeny výpisy zdrojových kódů několika programů, které byly používány k tvorbě grafů a v různých obměnách i k samostatnému zkoumání numerických řešení některých problémů. Důležitější vlastní závěry jsou uvedeny v paragrafech 4.3 a 5.4.

Kapitola 1
Základy kvantové mechaniky

Kvantová mechanika tvoří matematický model, na jehož základě kvantové algoritmy pracují. V prvním a druhém paragrafu této kapitoly tak uvedeme postuláty, na nichž je kvantová mechanika založena. Ve třetím a čtvrtém paragrafu zavedeme prvky formalismu, který budeme dále v rámci této práce využívat. V posledních paragrafech uvedeme některé pokročilejší poznatky teorie vícesložkových systémů, které se tématu práce dotýkají.

1.1 Postuláty kvantové mechaniky

Kvantová mechanika není podle [3] sama fyzikální teorií, pouze matematickým vzorem, na jehož základě jsou založeny jednotlivé teorie nazývané společně kvantovou teorií.

Takové označení ovšem nemusí být zcela jednoznačné – učebnice [4] například uvádí pod stejným názvem jednu z takových fyzikálních teorií, která tvoří obdobu klasické mechaniky. V takové podobě byla kvantová mechanika popsána E. Schrödingerem ve dvacátých letech 20. století. Dalo by se tedy říci, že existují různé stupně matematické abstrakce této formulace. V této práci budeme používat výše naznačenou matematickou formulaci kvantové mechaniky, řízenou sadou postulátů, ve formě, kterou uvádí [3]. Jedná se o sjednocení různých směrů, kterými se kvantová mechanika v době svého vzniku vyvíjela – toto sjednocení, známé od přelomu 20. a 30. let, je prací P. A. M. Diraca a J. von Neumanna.

Uveďme tedy nyní jednotlivé postuláty této formulace, a několik prvních poznámek ke každému z nich.

1. *Stavovým prostorem libovolného izolovaného fyzikálního systému je Hilbertův prostor. Stav systému je pak plně popsán jednotkovým vektorem z tohoto prostoru, stavovým vektorem.*

Dohoda o používání jednotkových vektorů v tomto postulátu je spíše konvencí. Všechny vzorce kvantové mechaniky popisující fyzikální vlastnosti systému (např. předpokládané výsledky pozorování) je totiž možno přeformulovat tak, aby nerozlišovaly mezi daným vektorem a žádným jeho nenulovým násobkem [4], tedy aby bylo možno z nich délku každého použitého vektoru vytknout v nulové mocnině.

Výjimku v předchozímu odstavci tvoří nulový vektor stavového prostoru. Kdybychom z postulátu vyřadili požadavek na jednotkovou délku stavového vektoru, bylo by třeba přidat tvrzení, že nulový vektor nemá fyzikální význam – nepopisuje stav žádného fyzikálního systému. Uvidíme, že časovým vývojem uzavřeného fyzikálního systému nemůže přejít nenulový stavový vektor v nulový a že pokud by jakákoliv jiná situace měla tento důsledek, nebude moci nastat.

Podmínka používání pouze jednotkových vektorů však stále neimplikuje jednoznačnost přiřazení mezi těmito vektory a skutečnými fyzikálními stavy – ve smyslu tvrzení o nerozlišitelnosti mezi vektorem a libovolným jeho nenulovým násobkem existuje stále ještě „volnost“ ve volbě fáze (zvané globální fáze), tedy koeficientu tvaru libovolné komplexní jednotky: stavové vektory ψ a $e^{i\varphi}\psi$ jsou fyzikálně ekvivalentní pro každé $\varphi \in \mathbb{R}$.

Množinu jednotkových vektorů s identifikací vektorů lišících se pouze globální fází můžeme případně popsat matematickou konstrukcí zvanou *projektivní prostor*, což je jistá varieta s dimenzí o 2 menší oproti původnímu prostoru. Tento postup nebudeme příliš využívat, protože opouští hranice použitelnosti lineární algebry (nemá například definovány žádné vektorové operace).

Nakonec v rámci této práce budeme pracovat s konečnědimenzionálními (prehilbertovými) vektorovými prostory, což značně usnadní výklad a matematický formalismus a rovněž zamezí vzniku problémů, které je třeba řešit v jiných aplikacích kvantové mechaniky [4]. Ve zcela výjimečných případech použijeme v krátkých úsecích textu i nekonečnědimenzionální prostor se spočetnou bází (separabilní). V takových případech se budeme spoléhat na intuitivní rozšíření platnosti zavedeného formalismu a rovněž nebudeme dokazovat oprávněnost použitých operací s tím, že čtenář si v případě zájmu dohledá potřebné informace v literatuře, např. [2]. Na taková místa bude předem upozorněno.

2. *Vývoj uzavřeného kvantového systému je dán unitární transformací závisející pouze na počátečním a koncovém čase.*

Tento postulát je třeba chápat tak, že z konstrukce uvažovaného fyzikálního systému vyplývá existence takového unitárního operátoru U na stavovém prostoru, parametrizovaného počátečním a koncovým časem nějakého zkoumaného časového intervalu, že ať byl systém na začátku intervalu ve stavu popsaném kterýmkoliv stavovým vektorem ψ, na konci intervalu bude ve stavu popsaném vektorem $U\psi$.

Důsledkem linearity unitárního operátoru je *princip superpozice*: jestliže časový vývoj stavu systému při různých počátečních podmínkách, popsaných různými stavovými vektory ψ_i v počátečním čase, je popsán vektorovými funkcemi $\Psi_i(t)$, známe i časový vývoj v případě, že počáteční stav systému je popsán libovolnou lineární kombinací

$$\psi = \sum_{i=1}^{n} \psi_i - \tag{1.1 a}$$

– v každém okamžiku bude pak stav systému popsán odpovídající lineární kombinací

$$\Psi(t) = \sum_{i=1}^{n} \Psi_i(t). \tag{1.1 b}$$

Tento postulát je možno ekvivalentně přeformulovat tak, že uzavřený systém se vyvíjí podle diferenciální rovnice

$$\frac{\partial \Psi(t)}{\partial t} = -\frac{i}{\hbar} H(t)\Psi(t), \tag{1.2}$$

kde $\Psi(t)$ je stavový vektor systému v čase t, $\hbar$ redukovaná Planckova konstanta a $H(t)$ hermitovský operátor pro libovolné t [3].[1]

Operátor H, obecně závislý na čase, má ve Schrödingerově reprezentaci kvantové mechaniky přímý fyzikální význam – jak popíšeme níže, je operátorem jistým způsobem odpovídajícím

[1] Jako poznámku uveďme, že pro definici derivace vektorové funkce potřebujeme předpoklad úplného vektorového prostoru, což je však jednou z podmínek Hilbertova prostoru.

energii systému. Nazývá se Hamiltonův operátor nebo Hamiltonián [4]. Zde má také velký význam uvedení redukované Planckovy konstanty v rovnici (1.2). V matematické formulaci se konstanta uvádí z tohoto historického důvodu, jinak by ji bylo možno zahrnout do definice operátoru H.

Při každé unitární operaci se zachovává délka vektoru, což je důvodem, proč je možno v prvním postulátu uvažovat pouze jednotkové vektory, a současně, kdybychom tento požadavek odstranili, proč žádný nenulový vektor nemůže časovým vývojem přejít v nepovolený nulový.

3. *Stavový prostor složeného fyzikálního systému je tenzorovým součinem stavových prostorů jednotlivých komponent. Dále jestliže jednotlivé komponenty očíslujeme čísly* 1 *až* n *a předpokládáme, že* i*-tá komponenta byla připravena ve stavu* ψ_i*, stav složeného systému je* $\psi_1 \otimes \ldots \otimes \psi_n$.

Toto krátké tvrzení (spolu s principem superpozice) v sobě ukrývá zdroj vší síly kvantových počítačů a vůbec není intuitivní. Čtenáře by mohla napadnout i jiná řešení otázky, jak pracovat s vícečásticovými systémy. Připomeňme například, že v klasické mechanice je stavový prostor složeného systému tvořen direktním součtem stavových prostorů jeho komponent.

V paragrafech 1.5 a 1.8 ukážeme některé důležité důsledky, které tento postulát přináší i mimo oblast kvantových algoritmů.

1.2 Kvantové měření

Poslední postulát kvantové mechaniky popisuje výsledky měření stavu fyzikálního systému a vliv měření na jeho časový vývoj. V jednotlivých fyzikálních teoriích na základě kvantové mechaniky je různým způsobem zdůvodňováno, proč by měření mělo systém výrazně ovlivňovat, z matematického hlediska se však jedná pouze o další z postulátů.

4. *Každé kvantové měření je popsáno množinou* $\{M_m\}$ *lineárních operátorů, zvaných měřicí operátory, na stavovém prostoru měřeného systému. Indexy* m *odpovídají různým možným výsledkům měření. Jestliže stav systému okamžitě před provedením měření je* ψ*, pravděpodobnost, že naměříme výsledek* m*, je rovna*

$$p(m) = \|M_m \psi\|^2 \tag{1.3 a}$$

a stav systému v okamžiku ukončení měření je

$$\frac{1}{\|M_m \psi\|} M_m \psi. \tag{1.3 b}$$

Operátory M_m *přitom musí splňovat tzv. rovnici úplnosti*[2]

$$\sum_m M_m^\dagger M_m = I. \tag{1.3 c}$$

[2] Křížkem (†) se v literatuře ke kvantové mechanice značí sdružení.

Všimněme si pravděpodobnostního charakteru měření – dokud měření neprovádíme, je vývoj izolovaného fyzikálního systému plně deterministický proces a díky unitaritě časového vývoje dokonce v každém případě vratný. Tento postulát je jediným bodem, který takové pravidlo porušuje, ale zároveň jediným způsobem zjišťování informací o stavu systému, který kvantová mechanika nabízí.

Vzhledem k tomu, že o operátorech M_m nepožadujeme, aby byly prosté, měření dále není obecně ani vratným procesem. V důsledku toho nemůžeme postupnými měřeními získávat stále detailnější informace o stavu systému. Snadno dokonce ukážeme důležité tvrzení, že žádným měřením není možno spolehlivě vzájemně odlišit dva různé vektory, pokud nejsou ortogonální, v důsledku čehož není možno stav systému nikdy kompletně určit:

Nechť ψ a φ jsou dva neortogonální jednotkové vektory, nechť M_1 a M_2 jsou měřicí operátory tvořící měření, o němž předpokládáme, že dá výsledek 1 pro vektor ψ a 2 pro vektor φ, obojí s jistotou. Tedy

$$\|M_1\psi\| = \|M_2\varphi\| = 1, \tag{1.4 a}$$

současně musí platit

$$\|M_1\varphi\| = \|M_2\psi\| = 0. \tag{1.4 b}$$

Utvořme ortogonální rozklad vektoru φ do podprostorů $[\psi]_\lambda$ a $[\psi]_\lambda^\perp$: $\varphi = \alpha\psi + \beta u$, $|\alpha|^2 + |\beta|^2 = 1$, $\|u\| = 1$, $(u, \psi) = 0$, $\alpha \neq 0$. Díky linearitě M_2 musí platit

$$1 = \|M_2\varphi\| = \|\beta M_2 u\| = |\beta|\|M_2 u\| \leq |\beta|, \tag{1.4 c}$$

což je spor s $|\beta|^2 = 1 - |\alpha|^2 < 1$.

Uvidíme, že nemožnost zjistit kompletní informaci o stavu kvantového systému bude tvořit velkou překážku pro využívání kvantové mechaniky k realizaci výpočtů.

Měřením je ve smyslu předchozích odstavců tedy obecně[3] narušen i unitární časový vývoj systému. To není ve sporu s druhým postulátem z důvodu, že fyzikální systém, na němž provádíme měření, nemůže být uzavřený – musí jistě nějak interagovat s použitým měřicím aparátem.

Jako poslední poznámku k uvedenému znění postulátu uveďme, že rovnice úplnosti, uvedená v tvrzení postulátu, je ekvivalentní požadavku, aby součet pravděpodobností byl roven 1:

$$\sum_m p(m) = \sum_m (M_m\psi, M_m\psi) = \sum_m (\psi, M_m^\dagger M_m \psi) = \left(\psi, \sum_m M_m^\dagger M_m \psi\right). \tag{1.5 a}$$

Protože jednotkový vektor ψ splňuje rovnici $(\psi, \psi) = 1$, bude výraz na pravé straně roven 1 právě tehdy, když bude pro každý jednotkový vektor ψ platit

$$\left(\psi, \left(\sum_m M_m^\dagger M_m - I\right)\psi\right) = 0, \tag{1.5 b}$$

což je ekvivalentní rovnici úplnosti.

Zmiňme, jak by bylo třeba znění postulátu upravit, kdybychom v postulátu 1 nahradili požadavek na používání jednotkových vektorů pouze zákazem nulového vektoru. Definice měřicích

[3] Stále zde připomínáme slovo „obecně“ z důvodu, že definici vyhovuje i měření s jediným měřicím operátorem I, které dá svůj jediný výsledek s jistotou a stav systému nezmění.

operátorů M_m ani rovnici úplnosti není třeba upravovat, ale součet pravděpodobností podle původního znění by vyšel roven dle odvození použitého výše $(\psi, \psi) = \|\psi\|^2$. Toto chování by se tedy opravilo vzorcem

$$p(m) = \frac{\|M_m \psi\|^2}{\|\psi\|^2}. \tag{1.6}$$

Stav po měření zato můžeme uvažovat jednodušší, $M_m\psi$. Z důvodu, že výsledek m, pro který by $M_m\psi$ bylo nulovým vektorem, má z obou definic nulovou pravděpodobnost, nehrozí, že by mohl nulový vektor být stavem po provedení měření, a v původním znění jistě nenastane dělení nulou.

Důležitou skupinu měření tvoří *projektivní měření*: ta jsou popsána jediným hermitovským operátorem, zvaným *pozorovatelná* (veličina). V konečnědimenzionálních prostorech má každý hermitovský operátor H spektrální rozklad[4]

$$H = \sum_{\lambda \in \sigma(H)} \lambda P_\lambda, \tag{1.7}$$

kde $\sigma(H)$ je spektrum operátoru H, λ jsou jeho vlastní čísla a P_λ jsou ortogonální projektory na vlastní podprostory odpovídající vlastním číslům λ. Pro tvrzení původního postulátu budeme uvažovat vlastní čísla λ jako výsledky měření a P_λ jako měřicí operátory. Rovnice úplnosti je splněna díky vlastnostem spektrálního rozkladu.

Projektory ve spektrálním rozkladu splňují rovnost $P_\lambda P_\mu = \delta_{\lambda\mu} P_\lambda$. Po naměření výsledku λ se tak systém dostane do stavu popsaného vektorem

$$\psi' = \frac{1}{\|P_\lambda \psi\|} P_\lambda \psi, \tag{1.8 a}$$

pro který platí

$$P_\mu \psi' = \delta_{\lambda\mu} \psi', \tag{1.8 b}$$

tedy případné okamžitě následující měření stejné pozorovatelné (tedy bez uvažování časového vývoje mezi měřeními) dá stejný výsledek jako první měření s jistotou. Popsaný jev se nazývá *kolaps* do stavu ψ'.

S projektivními měřeními se setkáme především ve Schrödingerově reprezentaci, kde jsou pozorovatelné přiřazeny jednotlivým fyzikálním veličinám. Pozorovatelné jsou konstruovány tak, že vlastní hodnoty λ mají fyzikální rozměr a velikost skutečných výsledků měření odpovídajících fyzikálních veličin. Hamiltonův operátor H, uvedený u druhého postulátu, je například pozorovatelnou odpovídající energii systému a rovnice (1.2) se nazývá Schrödingerova rovnice.

Problematika kvantového měření je mnohem rozsáhlejší a projektivní měření jsou velice dobře prozkoumána, základní poznatky viz [3], [4], v zájmu udržení tématu práce však další detaily uvádět nebudeme.

V teorii kvantových algoritmů budeme používat jistý kompromis mezi uvedenými dvěma formulacemi – měření, jejichž měřicí operátory budou vzájemně ortogonální projektory, nebude

[4] Spektrální rozklad a projektivní měření jsou dobře definovány i v prostorech nekonečné dimenze. Jak však již bylo nejednou řečeno, složitějším matematickým konstrukcím v takovém případě se budeme vyhýbat.

nás však zajímat, jaké hodnotě které fyzikální veličiny výsledek odpovídá. Důležité budou obory hodnot jednotlivých projektorů.

V konečněrozměrných stavových prostorech budeme definovat dva důležité případy kvantového měření:

- Jestliže bude dána ortonormální báze $\{\psi_i\}_{i=1}^n$ stavového prostoru, můžeme uvažovat měření určené všemi n ortogonálními projektory na jednorozměrné podprostory $[\psi_i]_\lambda$. Takové měření dává v případě každého bázového stavu odpovídající výsledek s jistotou a dokáže mezi bázovými stavy jednoznačně rozlišit. Nazývá se *úplné měření* v dané ortonormální bázi.
- Uvažujme případ vícesložkového systému, pro který stavové prostory jednotlivých složek označíme $\mathcal{H}_1$, $\mathcal{H}_2$, ..., $\mathcal{H}_m$, nechť $\{\psi_i\}_{i=1}^n$ je ortonormální báze zvoleného prostoru $\mathcal{H}_k$, $1 \leq k \leq m$. Podle třetího postulátu je stavovým prostorem složeného systému $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \ldots \otimes \mathcal{H}_m$. Označme $I_{\mathcal{H}_j}$ jednotkový operátor na prostoru $\mathcal{H}_j$, označme $P_i \in \mathcal{L}(\mathcal{H}_k)$ ortogonální projektor na $[\psi_i]_\lambda$, $i = 1, \ldots, n$. Ortogonální projektory

$$I_{\mathcal{H}_1} \otimes \ldots \otimes I_{\mathcal{H}_{k-1}} \otimes P_i \otimes I_{\mathcal{H}_{k+1}} \otimes \ldots \otimes I_{\mathcal{H}_m} \tag{1.9}$$

  pak definují měření, které nazveme *měřením na i-tém podsystému*, opět v odpovídající bázi.

Předveďme tvrzení postulátu o měření na příkladě úplného měření: označme ortonormální bázi uvažovaného stavového prostoru stejně jako v předchozích bodech a uvažujme obecnou superpozici

$$\psi = \sum_{i=1}^{n} \alpha_i \psi_i. \tag{1.10 a}$$

Délka vektoru ψ je dle definice ortonormální báze

$$\|\psi\| = \sqrt{\sum_{i=1}^{n} \|\alpha_i\|^2} \tag{1.10 b}$$

a požadavek, aby ψ byl jednotkový vektor, tedy zní

$$\sum_{i=1}^{n} \|\alpha_i\|^2 = 1. \tag{1.10 c}$$

Pravděpodobnost, že měření dá výsledek i odpovídající projektoru na $[\psi_i]_\lambda$, kterou budeme nazývat pravděpodobností naměření i-tého bázového vektoru, je rovna $\|\alpha_i\|^2$. Je tedy druhou mocninou absolutní hodnoty koeficientu lineární kombinace u vektoru ψ_i, kterou budeme nazývat *amplituda* vektoru ψ_i.

Tímto je tedy vymezena sada postulátů, na jejichž platnost se budeme v hlavní části práce spoléhat. Upozorněme však s předstihem, že z fyzikálního hlediska tyto postuláty nejsou zcela obecné – odpovídají jistým ideálním předpokladům o popisovaném systému a možnostech naší znalosti jeho stavu. V paragrafu 1.7 představíme alternativní sadu postulátů, která je za stejných předpokladů matematicky ekvivalentní [3], ale univerzálnější pro praktické použití.

1.3 Diracův formalismus

V lineární algebře se používá mnoho různých způsobů značení jednotlivých matematických objektů. V tomto textu budeme využívat značení obvyklé především v literatuře k teorii kvantové informace, tzv. Diracovu nebo bra-ketovou notaci. Shrňme tedy nyní jeho pravidla.

Vektory, které budeme považovat za nadále nedělitelné (viz níže), budeme značit jako tzv. *kety*: např. $|x\rangle$. Takový symbol má přesně stejný význam jako v jiných notacích x, $\vec{x}$ nebo $\mathbf{x}$, příkladem lineární kombinace vektorů $|x\rangle$ a $|y\rangle$ tak může být $\frac{1}{2}|x\rangle + i|y\rangle$.

Diracova notace nám dává možnost využívat jako „vnitřek" ketu různé skupiny symbolů: běžná jsou písmena latinské i řecké abecedy, číslice i jiné matematické značky (často se setkáme např. s kety $|+\rangle$ a $|-\rangle$), v dalších oblastech kvantové fyziky se používají i jiné značky ($|\uparrow\rangle$, $|vac\rangle$, $|\vec{p}\rangle$ apod.)

Důležitá poznámka je, že v kvantové mechanice se ketové označení ve skutečnosti používá výhradně pro jednotkové vektory – toto pravidlo budeme také důsledně dodržovat. Pokud budeme pracovat s jedním Hilbertovým prostorem, vektory označené čísly $|0\rangle, |1\rangle, \ldots$ budou dále označovat jeho ortonormální bázi a jejich ortogonality budeme využívat bez dalšího připomínání. Upozorněme však předem, že často budeme pracovat s několika Hilbertovými prostory současně a tehdy bude třeba upřesnit, o kterém mluvíme, případně toto pravidlo upravit.

Dalším prvkem Diracovy notace jsou *bra*-vektory. Jestliže označíme kety prvky nějakého vektorového prostoru, dle nejobecnější definice jsou bra vektory z prostoru k němu duálního, tedy spojité lineární funkcionály [2]. Je však známo, že duální prostor k Hilbertovu prostoru je nový Hilbertův prostor s ním izometrický a dále, že prvky obou prostorů lze identifikovat podle Rieszovy věty [1]: ke každému bra-vektoru $\langle\varphi|$ je tak jednoznačně určen jeden ket-vektor $|y\rangle$, že akce $\langle\varphi|$ (jako funkcionálu) na libovolný vektor $|x\rangle$ je dána skalárním součinem:

$$\langle\varphi|(|x\rangle) = (|y\rangle, |x\rangle). \tag{1.11}$$

Říkáme pak, že bra-vektor $\langle\varphi|$ je duální ke ket-vektoru $|y\rangle$. Tento jejich vztah budeme značit tak, že pro „vnitřek" použijeme stejný symbol: $\langle\varphi| = \langle y|$.

První změnou zavedenou použitím Diracovy notace je, že v akci funkcionálu na vektor vynecháme závorky a spojíme svislé linky, čímž vznikne výraz $\langle\varphi|x\rangle$. Podle tvrzení citovaného výše je tedy ekvivalentně $\langle y|x\rangle$ zápisem pro skalární součin vektorů $|x\rangle$ a $|y\rangle$.

Jako další změnu oproti ostatním notacím nebudeme v tomto případě vyžadovat násobení vektoru číslem pouze zleva, matematicky řečeno tedy dodefinujeme operaci násobení číslem zprava se stejným výsledkem. Například výraz $|x\rangle\langle y|z\rangle$ tak je násobek vektoru $|x\rangle$ určený koeficientem $\langle y|z\rangle$.[5] Toto nám umožní zavést výrazy tvaru $|x\rangle\langle y|$[6] tak, že budou působit na vektory zleva a výsledkem bude $|x\rangle\langle y|(|z\rangle) = |x\rangle\langle y|z\rangle$. Snadno nahlédneme, že se tedy jedná o jistou třídu lineárních operátorů.

[5] Ve skutečnosti se budeme opačnému zápisu $\langle y|z\rangle|x\rangle$ vyhýbat, protože označení $|z\rangle|x\rangle$ použijeme později pro tenzorový součin.

[6] Anglicky *outer product*. Tento pojem nebudeme překládat vzhledem k možné záměně s pojmem vnějšího součinu, *exterior product*, z teorie Grassmannových algeber.

Mezi těmito lineárními operátory jsou dále významné operátory tvaru $|x\rangle\langle x|$ – každý takový operátor je ortogonálním projektorem na podprostor $[|x\rangle]_\lambda$. Úplné měření v bázi $\{|i\rangle\}_{i=0}^n$ je tedy určeno množinou měřicích operátorů $\{M_i\}_{i=0}^n$, $M_i = |i\rangle\langle i|$ pro $i = 0, 1, \ldots, n$. Jestliže měření dá i-tý výsledek, řekneme, že jsme systém naměřili ve stavu $|i\rangle$, podobně s měřením na podsystémech.

Ve smyslu předchozího paragrafu budeme často potřebovat ještě označení pro tenzorový součin dvou vektorů (obecně z různých prostorů). I pro ten umožňuje Diracova notace zavést jednoduché konzistentní označení: ve výrazu $|x\rangle \otimes |y\rangle$ vynecháme značku tenzorového součinu a budeme psát $|x\rangle|y\rangle$. Pokud navíc budou násobené vektory prvky stejného prostoru, můžeme dokonce vynechat vnitřní dvojici závorek: $|x\rangle|y\rangle = |xy\rangle$. To je v souladu s tím, že tenzorovým součinem jednotkových vektorů vzniká opět jednotkový vektor.

Všimněme si, že díky příslušným axiomům a definicím a díky dodané komutativitě násobení vektoru a čísla pak můžeme v Diracově notaci provádět různé intuitivní úpravy připomínající roznásobování (či vytýkání):

$$\begin{aligned}
(\alpha\langle x| + \beta\langle y|)|z\rangle &= \alpha\langle x|z\rangle + \beta\langle y|z\rangle \\
\langle x|(\alpha|y\rangle + \beta|z\rangle) &= \alpha\langle x|y\rangle + \beta\langle x|z\rangle \\
\langle x| \circ |y\rangle\langle z| &= \langle x|y\rangle|z\rangle \\
|a\rangle\langle b| \circ |c\rangle\langle d| &= |a\rangle\langle b|c\rangle\langle d| \\
(\alpha|x\rangle + \beta|y\rangle)|z\rangle &= \alpha|x\rangle|z\rangle + \beta|y\rangle|z\rangle \\
&\ldots
\end{aligned} \tag{1.12}$$

V tomto místě upozorněme na výraz tvaru $\langle x|\langle y|$. Z předchozího textu nevyplývá, jak by měl být definován, a bohužel existují dva možné přístupy s různým výsledkem: buď uvažujeme, že výraz vzniknul vynecháním $\otimes$ v $\langle x| \otimes \langle y|$, pak podle definice tenzorového součinu dvou lineárních zobrazení musí platit

$$\langle x|\langle y|(|a\rangle|b\rangle) = \langle x|a\rangle\langle y|b\rangle, \tag{1.13}$$

bližší smyslu předchozího odstavce by však bylo, kdybychom jej definovali jako $\langle y| \otimes \langle x|$, aby platilo

$$\langle x|\langle y|(|a\rangle|b\rangle) = \langle x|\langle y|a\rangle|b\rangle = \langle y|a\rangle\langle x|b\rangle. \tag{1.14}$$

Oba přístupy jsou oprávněné a je na rozmyšlení autora daného textu, který využije. My tuto operaci rovněž budeme příležitostně potřebovat – nechť se tedy u nás chová prvním popsaným způsobem.

1.4 Konečnědimenzionální prostory

Podívejme se stručně, co si můžeme představit pod jednotlivými prvky Diracovy notace v případě konečnědimenzionálních Hilbertových prostorů $\mathbb{C}^n$, které pro nás budou podstatné.

Předpokládejme, že $\mathbb{C}^n$ je prostor *sloupcových* vektorů. To je celkem obvyklá konvence, i když příklad [1] ukazuje, že ne zcela zaručená.

Je třeba stanovit, jak budeme v tomto prostoru reprezentovat bázové vektory $\{|i\rangle\}_{i=0}^{n-1}$. Jistě musíme zachovat podmínku ortonormality. Skalární součin v $\mathbb{C}^n$ však není dán jednoznačně

(může jím být libovolná hermitovská forma s pozitivně definitní diagonálou) a jeho vhodnou volbou bychom mohli zajistit pro libovolně zvolenou bázi, aby byla ortonormální. Stanovme proto, že v prostorech $\mathbb{C}^n$ vždy budeme uvažovat standardní skalární součin. S tím můžeme definovat $|i\rangle = e_{i+1}$:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ \ldots, \ |n-1\rangle = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}. \tag{1.15}$$

Nechť tedy $|x\rangle$ a $|y\rangle$ jsou prvky $\mathbb{C}^n$,

$$|x\rangle = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}, \quad |y\rangle = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}. \tag{1.16 a}$$

Jejich standardním skalárním součinem je pak komplexní číslo

$$\langle x|y\rangle = (|x\rangle, |y\rangle) = \sum_{i=1}^{n} \overline{x_i} y_i. \tag{1.16 b}$$

Vidíme, že stejného výsledku dosáhneme, když vynásobíme matice

$$\begin{pmatrix} \overline{x_1} & \cdots & \overline{x_n} \end{pmatrix} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \tag{1.16 c}$$

a identifikujeme výslednou čtvercovou matici prvního řádu s jejím jediným prvkem. Operace, kterou jsme přitom provedli se sloupcovým vektorem $|x\rangle$, braným jako matice typu $n \times 1$, je kombinací transpozice a komplexního srdužení prvků, tedy analogií *sdružení* pro obdélníkové matice.

Je tedy možné uvažovat duální prostor jako prostor řádkových vektorů a obecně položit

$$\langle x| = \begin{pmatrix} \overline{x_1} & \overline{x_2} & \cdots & \overline{x_n} \end{pmatrix} = |x\rangle^\dagger. \tag{1.17}$$

Skutečnost, že takový tvar pak můžeme dosadit například do výrazů tvaru $|x\rangle\langle y|$, plyne snadno z asociativity násobení matic.

Tenzorový součin Hilbertových prostorů je, jak bychom se dočetli v [2], nový Hilbertův prostor určený jednoznačně až na izometrii. Není tedy dáno jednoznačně, co je tenzorový součin matic. Běžně se používá jeho reprezentace známá jako Kroneckerův součin, viz např. [5]: z matic $\mathbf{A} \in \mathbb{C}^{a,b}$ a $\mathbf{B} \in \mathbb{C}^{c,d}$ utvoříme matici $\mathbf{A} \otimes \mathbf{B} \in \mathbb{C}^{ac,bd}$ v blokovém tvaru

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & a_{12}\mathbf{B} & \cdots & a_{1b}\mathbf{B} \\ \vdots & \vdots & \ddots & \vdots \\ a_{a1}\mathbf{B} & a_{a2}\mathbf{B} & \cdots & a_{ab}\mathbf{B} \end{pmatrix} \tag{1.18}$$

Jestliže tedy uvažujeme Hilbertovy prostory $\mathbb{C}^m$, $\mathbb{C}^n$ a vektory $|x\rangle \in \mathbb{C}^m, |y\rangle \in \mathbb{C}^n$,

$$|x\rangle = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_m \end{pmatrix}, \quad |y\rangle = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}, \tag{1.19 a}$$

můžeme v této reprezentaci říci $|x\rangle|y\rangle \in \mathbb{C}^m \otimes \mathbb{C}^n = \mathbb{C}^{mn}$ a

$$|x\rangle|y\rangle = \begin{pmatrix} x_1y_1 \\ \vdots \\ x_1y_n \\ x_2y_1 \\ \vdots \\ x_my_1 \\ \vdots \\ x_my_n \end{pmatrix}. \tag{1.19 b}$$

Snadno bychom ukázali, že pokud rozepíšeme například výraz $(\mathbf{A} \otimes \mathbf{B})(|x\rangle|y\rangle)$ pro matice $\mathbf{A}$ a $\mathbf{B}$ patřičných rozměrů pomocí Kroneckerova součinu, získáme $(\mathbf{A}|x\rangle) \otimes (\mathbf{B}|y\rangle)$ a podobně.

1.5 Provázané stavy

V tomto paragrafu ukážeme jeden netriviální důsledek postulátu o složených fyzikálních systémech.

Uvažujme fyzikální systém tvořený dvěma podsystémy, abstraktně označenými A a B. Příkladem může být libovolný systém dvou částic, či i tyto podsystémy mohou být samy mnohem komplikovanější. Každý z podsystémů má ve smyslu paragrafu 1.1 přiřazen stavový prostor, který označíme $\mathcal{H}_A$, resp. $\mathcal{H}_B$, a stavovým prostorem celého systému pak je $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Stavové vektory $|\psi\rangle \in \mathcal{H}$ můžeme rozdělit do dvou skupin podle kritéria, zda existují takové $|\alpha\rangle_A \in \mathcal{H}_A$ a $|\beta\rangle_B \in \mathcal{H}_B$, že $|\psi\rangle = |\alpha\rangle_A \otimes |\beta\rangle_B$, či takovou rovnost není možno splnit. Pro netriviální $\mathcal{H}_A$ a $\mathcal{H}_B$ je druhá skupina neprázdná: uvažujme například $\mathcal{H}_A = \mathcal{H}_B = \mathbb{C}^2$ a

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle). \tag{1.20}$$

Zápis takového vektoru v Diracově notaci je

$$|\psi\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{1.21 a}$$

Pokud bychom však uvažovali

$$|\alpha\rangle = \begin{pmatrix} \alpha_1 \\ \alpha_2 \end{pmatrix}, \quad |\beta\rangle = \begin{pmatrix} \beta_1 \\ \beta_2 \end{pmatrix}, \tag{1.21 b}$$

muselo by platit

$$|\psi\rangle = \begin{pmatrix} \alpha_1\beta_1 \\ \alpha_1\beta_2 \\ \alpha_2\beta_1 \\ \alpha_2\beta_2 \end{pmatrix}, \tag{1.21 c}$$

což je ve sporu s tím, že sloupcové vektory tvořené první a druhou dvojicí složek $|\psi\rangle$ jsou lineárně nezávislé.

U vektoru $|\psi\rangle$ tedy nemá smysl říci, že podsystémy A a B by byly ve stavech popsaných nějakými vektory $|\alpha\rangle$ a $|\beta\rangle$, přestože $|\psi\rangle$ je pouze lineární kombinací dvou vektorů ve tvaru tenzorového součinu (*produktových* nebo *faktorizovatelných stavů*), u kterých by taková úvaha možná byla. Stavy, které nejsou faktorizovatelné, se nazývají *provázané stavy* (*entangled states* [3]). Jejich existence je nevyhnutelným důsledkem definice tenzorového součinu.

1.6 Paradox EPR

Provázání je také původcem známého paradoxu EPR [6]. Autoři Einstein, Podolsky a Rosen, jejichž nese jména, se jím snažili ukázat, že pojetí kvantové mechaniky pomocí vlnových funkcí[7] za předpokladu platnosti postulátů uvedených výše vede ke sporům, z nichž jeden detailně popsali.

Tento příklad zde nebudeme uvádět,[8] protože by bylo nutno detailně vysvětlit detaily kvantové mechaniky na Hilbertových prostorech nekonečné dimenze, ukážeme však jeho mnohem jednodušší variantu, kterou se zabýval J. S. Bell. Tento fyzik nejenže ukázal obdobu formulace paradoxu pro mnohem jednodušší fyzikální systémy, které jsou tím blíže experimentálním možnostem, především však zformuloval podmínku známou jako Bellova nerovnost, pomocí jejíhož experimentálního ověření by bylo možno rozsoudit, zda se systém chová ve sporu s kvantovou mechanikou nebo zda byly chybné předpoklady paradoxu. Podívejme se tedy blíže na Bellův příklad:

Jeden velice známý provázaný stav, označovaný z historických důvodů jako *spinový singlet* [3],

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \tag{1.22}$$

má zajímavou vlastnost: jestliže na stavových prostorech obou podsystémů zvolíme stejným způsobem novou bázi $\{|+\rangle, |-\rangle\}$,

$$\left.\begin{aligned} |0\rangle &= \alpha|+\rangle + \beta|-\rangle \\ |1\rangle &= \overline{\beta}|+\rangle - \overline{\alpha}|-\rangle \end{aligned}\right\}, \quad |\alpha|^2 = |\beta|^2 = 1, \tag{1.23}$$

jeho zápis v nové bázi jejich tenzorového součinu má opět tvar

$$\begin{aligned} |\psi\rangle = \frac{1}{\sqrt{2}}\Big(&\alpha\overline{\beta}|{+}{+}\rangle - |\alpha|^2|{+}{-}\rangle + |\beta|^2|{-}{+}\rangle - \beta\overline{\alpha}|{-}{-}\rangle - \\ &- \alpha\overline{\beta}|{+}{+}\rangle - |\beta|^2|{+}{-}\rangle + |\alpha|^2|{-}{+}\rangle + \beta\overline{\alpha}|{-}{-}\rangle\Big) = \\ = \frac{1}{\sqrt{2}}&(|{-}{+}\rangle - |{+}{-}\rangle). \end{aligned} \tag{1.24}$$

Poznamenejme, že pro reálná α a β má uvedená transformace charakter rotace v rovině určené vektory $|0\rangle$ a $|1\rangle$.

Jestliže provedeme na prvním podsystému měření v původní bázi, nastane kolaps vlnové funkce buď do stavu $|01\rangle$ nebo $|10\rangle$. Výsledek sice bude náhodný, ale při následném měření

[7] Vlnové funkce jsou stavovými vektory ve Schrödingerově reprezentaci [4]. Původní znění paradoxu vycházelo z ní, proto v tomto paragrafu budeme používat toto označení.

[8] Celý text původního článku je k nahlédnutí k dispozici zdarma na stránkách časopisu [6]

na druhém podsystému s jistotou naměříme výsledek odpovídající druhému bázovému vektoru. Jestliže bychom vytvořili sérii dvojic částic, každou z nich v tomto provázaném stavu, a prováděli na každé měření popsaným způsobem, pozorovali bychom mezi výstupy korelaci.

Totéž platí, provedeme-li obě měření v nové bázi – systém nyní kolabuje buď do stavu $|+-\rangle$ nebo $|-+\rangle$. V tomto okamžiku však přichází rozumný argument EPR:

Dosud jsme prováděli pouze matematické úvahy. Představme si situaci však z fyzikálního pohledu, a to na příkladě dvou částic. Dle postulátů kvantové mechaniky mohou být v provázaném stavu, ať jsou libovolně vzdálené, a i tehdy, když zabráníme jejich vzájemné interakci. Abychom zabránili všem známým formám interakce, můžeme uvažovat, že se jedná o dva fotony, které se vzájemně vzdalují rychlostí světla, jednotlivé báze nechť pak mají význam natočení detektorů polarizace.

Jestliže provedeme na první částici měření v bázi $\{|0\rangle, |1\rangle\}$, můžeme dle výsledku s určitostí říci, že druhá částice se bude při libovolném následném měření chovat, jako by byla připravena ve stavu $|0\rangle$, resp. $|1\rangle$. *Kdybychom* ale provedli měření v nové bázi $\{|+\rangle, |-\rangle\}$, mohli bychom o stejné částici říci, že je ve stavu $|+\rangle$ nebo $|-\rangle$.

Protože jsme zabránili interakci mezi oběma částicemi, druhá částice se však nemůže „dozvědět“ o tom, jaké měření jsme se rozhodli provést na první částici. Jestliže tedy jsme první částici naměřili například ve stavu $|0\rangle$, druhá již musela nějakým způsobem být na tuto situaci připravena ve stavu $|1\rangle$. *Kdybychom* však první měření provedli v nové bázi a naměřili $|+\rangle$, druhá částice by současně se všemi vlastnostmi stavu $|1\rangle$ musela mít vlastnosti stavu $|-\rangle$, resp. $|+\rangle$. Tyto vlastnosti se však vylučují – kdybychom i na druhé částici provedli měření v původní bázi, stav $|1\rangle$ implikuje nulovou pravděpodobnost naměření $|0\rangle$, zatímco $|-\rangle$ ani $|+\rangle$ ne.

EPR tím argumentovali, že popis fyzikální reality pomocí vlnových funkcí není kompletní, protože druhé částici není možno po oddělení žádnou přiřadit. Všimněme si, že kvantová mechanika netvrdí, že by takové přiřazení mělo být možné – existuje jen stavový vektor celého systému obou částic – pak ale přichází důležitost otázky, jak by stav druhé částice po měření první částice mohl záviset na jeho výsledku, když je efektivně zabráněno přenosu jakékoliv informace.

Prostorové oddělení částic se zdálo být tak silným argumentem, že počaly snahy kvantovou mechaniku pod vlivem tohoto paradoxu nějak opravit nebo vymyslet novou, přesnější teorii. Jednou z uvažovaných možností[9] byla *teorie skrytých proměnných*, která říká, že vlnové funkce tvoří skutečně jen částečný popis stavu fyzikálního systému a především, že proces měření je deterministický a jeho statistický charakter v kvantové mechanice je jen projevem naší neznalosti a neschopnosti ovlivnit dodatečnou informaci.

J. S. Bell však navrhl způsob, pomocí kterého by bylo možno rozsoudit, zda se fyzikální systém chová dle podobných předpokladů, nebo zda se projeví neintuitivní důsledky kvantové mechaniky. Jeho úvaha je především znamenitá tím, že neuvažuje žádné konkrétně formulované teorie – předpokládá pouze, že by bylo možno *jakkoliv* doplnit do nějaké myšlené tabulky výsledky měření, která jsme ve skutečnosti neprovedli, a jednoduchým způsobem vyvodí nerovnost, kterou by pak musely splňovat různé míry korelace mezi jednotlivými položkami.

[9] Další do současnosti uvažovaná řešení, např. přenos informace nazpět v čase, jsou uvedena v [7].

Bellovy předpoklady jsou splněny u teorie lokálních skrytých proměnných, zatímco u kvantové mechaniky nejsou. Další analýza příkladu s různými bázemi $\mathbb{C}^2$ by ukázala, že existují situace, ve kterých kvantová mechanika Bellovu nerovnost porušuje. Závěrem tedy je jednoduché, ač mimořádně významné tvrzení, známé jako *Bellova věta* [8]:

Žádná fyzikální teorie lokálních skrytých proměnných nemůže dát stejné předpovědi jako kvantová mechanika.

S jeho existencí stačilo sestavit odpovídající experiment, naměřit dostatečnou statistiku výsledků a ověřit na konkrétním příkladě platnost Bellovy nerovnosti. Současné závěry těchto experimentů mluví dostatečně přesvědčivě ve prospěch kvantové mechaniky, i když část fyzikálního světa je stále skepická [8].

Je třeba poznamenat, že teorie skrytých proměnných tímto není zavržena, pouze nemůže být lokální ve smyslu, že by částice bylo možno uvažovat fyzikálně zcela izolované, i kdyby s sebou mohly nést libovolné množství informace libovolného druhu.

Celý průběh této diskuse s mnoha dalšími zajímavými náhledy, dodatečnými informacemi a úzce souvisejícími filozofickými otázkami je důsledně popsán v [9]. Autor uvádí i další možná, víceméně filozofická, východiska, z nichž uvedeme například tvrzení, že systém částic tvoří jeden nový nedělitelný fyzikální objekt, tedy například, že pár fotonů nelze myšlenkově rozdělit na „půl-páry“ stejně tak, jako se foton v interferometru nerozštěpí na „polo-fotony“.

Na závěr tohoto paragrafu se zmiňme o čtyřech provázaných stavech z prostoru $\mathbb{C}^2 \otimes \mathbb{C}^2$, které po zmíněných fyzicích nesou název *Bellovy stavy* nebo *EPR stavy*. Mají v teorii kvantové informace (především však mezi kvantovými komunikačními protokoly) široké využití díky své jednoduchostí, díky níž jsme se již i se dvěma z nich seznámili. Jejich definice a obvyklé značení jsou

$$\begin{aligned} |\beta_{00}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\beta_{01}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\beta_{10}\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\beta_{11}\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned} \tag{1.25}$$

Snadno (například z maticového zápisu) bychom se přesvědčili, že se zároveň jedná o zajímavou ortonormální bázi odpovídajícího prostoru.

1.7 Matice hustoty

Pojem *matice hustoty*[10] vzniknul z potřeby popisovat fyzikální systémy, o jejichž stavu máme pouze částečné informace. Je silnější alternativou ke stavovým vektorům, uvedeným v paragrafu 1.1, protože po zavedení v analogii s dosavadním formalismem lze rozšířit i na otevřené fyzikální systémy.

[10] Anglicky *density matrix* nebo *density operator*. Místo přímého překladu druhého z názvů se v české literatuře můžeme setkat s názvem *statistický operátor*.

Matice hustoty je v řeči matematiky pozitivním jaderným[11] lineárním operátorem na daném prostoru se stopou rovnou jedné. V konečnědimenzionálním případě této definici odpovídají lineární operátory, jejichž matice je hermitovská, pozitivní (odpovídá matici pozitivně semidefinitní kvadratické formy) a má stopu rovnu 1.

Obvykle se zavádí při popisu směsí částic: představme si rezervoár stejných kvantových systémů, které ovšem mohou být z hlediska kvantové mechaniky v různých stavech. Nechť $\{|s_i\rangle\}_{i=1}^k$ je konečná[12] množina možných stavů a číslo p_i určuje poměr zastoupení i-tého stavu pro každé $i \in \{1, 2, \ldots, k\}$. Jestliže systém, se kterým budeme pracovat, odebereme z takové směsi, bude s pravděpodobností p_i ve stavu $|s_i\rangle$.

Při zkoumání časového vývoje takového systému můžeme řešení rozdělit do k větví podle tohoto počátečního stavu a u každého výsledku opět uvažovat odpovídající pravděpodobnost p_i. Matice hustoty je naproti tomu jediný matematický objekt, který kompletně popíše tuto situaci a všechny výsledky dá stejné.

Uvažovanému systému přiřadíme matici hustoty ve tvaru

$$\varrho = \sum_{i=1}^{k} p_i |s_i\rangle\langle s_i|. \tag{1.26}$$

Aby ale tento objekt mohl být použitelný, musíme ukázat, jak se vyvíjí s časem a jaké výsledky pro danou matici hustoty dá kvantové měření. To provedeme ve smyslu předchozího odstavce.

Předpokládejme tedy, že uvažovaný systém je v čase t_1 s pravděpodobností p_i ve stavu $|s_i\rangle$, $i = 1, \ldots, n$, a zkoumejme jeho stav v čase t_2. Podle postulátu 2 existuje taková unitární operace U, která každému z uvažovaných počátečních stavů $|s_i\rangle$ přiřadí odpovídající stav $U|s_i\rangle$ v čase t_2. Přiřaďme tedy těmto stavům odpovídající pravděpodobnosti a sestavme v čase t_2 matici hustoty v analogii vzorce (1.26):

$$\varrho' = \sum_{i=1}^{k} p_i \left(U|s_i\rangle(U|s_i\rangle)^\dagger\right) = \sum_{i=1}^{k} p_i U|s_i\rangle\langle s_i|U^\dagger = U\left(\sum_{i=1}^{k} p_i |s_i\rangle\langle s_i|\right)U^\dagger. \tag{1.27}$$

Odtud je zřejmé, že samotná operace U bude udávat přímý vztah i mezi oběma maticemi hustoty:

$$\varrho' = U\varrho U^\dagger. \tag{1.28}$$

Podobným způsobem ukážeme, s jakou pravděpodobností můžeme očekávat které výsledky měření, známe-li matici hustoty. Uvažujme značení dle postulátu 4. Kdyby systém byl ve stavu $|s_i\rangle$, byla by pravděpodobnost naměření výsledku m

$$p(m) = \|M_m|s_i\rangle\|^2 = \langle s_i|M_m^\dagger M_m|s_i\rangle. \tag{1.29 a}$$

[11] Jaderný operátor je operátor, u kterého má smysl obecná definice stopy uvedená v [2]. My se však opět omezíme na konečněrozměrné prostory, kde každý lineární operátor má stopu rovnou stopě jeho matice v libovolné ortonormální bázi.

[12] Pro účely tohoto příkladu. Zobecnění samozřejmě použití matice hustoty neznemožňuje, je jen matematicky náročnější.

Tuto pravděpodobnost je ovšem třeba ještě vynásobit pravděpodobností p_i a přičíst odpovídající příspěvky od ostatních možností. Celkově

$$p(m) = \sum_{i=1}^{k} p_i \langle s_i | M_m^\dagger M_m | s_i \rangle. \tag{1.29 b}$$

Pro podobné zjednodušení tohoto vzorce, jakého jsme dosáhli v minulém odstavci, bude třeba využít trik – na toto číslo pohlédnout jako na stopu matice 1×1 nebo přesněji lineárního operátoru na jednorozměrném prostoru, tedy

$$p(m) = \mathrm{Tr}\left(\sum_{i=1}^{k} p_i \langle s_i | M_m^\dagger M_m | s_i \rangle \right). \tag{1.29 c}$$

Lineární operátor (lineární funkcionál) $\langle s_i|$ pak v této stopě můžeme přesunout na poslední místo díky invarianci výsledku vůči cyklické záměně ve skládání operátorů:

$$p(m) = \mathrm{Tr}\left(\sum_{i=1}^{k} p_i M_m^\dagger M_m |s_i\rangle\langle s_i| \right) = \mathrm{Tr}\left(M_m^\dagger M_m \left(\sum_{i=1}^{k} p_i |s_i\rangle\langle s_i| \right) \right), \tag{1.29 d}$$

čímž máme opět možnost ze vzorce vyčlenit matici hustoty (1.26) jeko celek:

$$p(m) = \mathrm{Tr}(M_m^\dagger M_m \varrho). \tag{1.30}$$

Podobnými úvahami bychom dokázali převést zbývající vzorce z postulátů 3 a 4. Tyto výsledky dávají tušit, že by matice hustoty mohla být definována samostatně, bez jakékoliv závislosti na původních postulátech a úvah o směsích. Jestliže tedy dosadíme do postulátů 2, 3 a 4 odvozené vzorce a postulát 1 nahradíme definicí matice hustoty ze začátku paragrafu, získáme následující sadu postulátů [3], které skutečně tvoří plnou náhradu za postuláty uvedené v paragrafu 1.1.

1'. Stavovým prostorem libovolného izolovaného fyzikálního systému je Hilbertův prostor. Stav systému je pak plně popsán pozitivním jaderným lineárním operátorem ϱ na tomto prostoru se stopou rovnou jedné. Jestliže je systém s pravděpodobností p_i ve stavu ϱ_i, $i = 1, \ldots k$, jeho matice hustoty je $\sum_{i=1}^{k} p_i \varrho_i$.

2'. Vývoj uzavřeného fyzikálního systému je popsán unitární transformací, tedy stav systému ϱ v čase t_1 je svázán se stavem ϱ' v čase t_2 unitárním operátorem U, který závisí pouze na t_1 a t_2, podle vztahu

$$\varrho' = U \varrho U^\dagger. \tag{1.31}$$

3'. Stavový prostor složeného fyzikálního systému je tenzorovým součinem stavových prostorů jednotlivých komponent. Dále jestliže jednotlivé komponenty očíslujeme čísly 1 až n a předpokládáme, že i-tá komponenta byla připravena ve stavu ϱ_i, stav složeného systému je $\varrho_1 \otimes \ldots \otimes \varrho_n$.

4'. Každé kvantové měření je popsáno množinou $\{M_m\}$ lineárních operátorů, zvaných měřicí operátory, na stavovém prostoru měřeného systému. Indexy m odpovídají různým možným výsledkům měření. Jestliže stav systému okamžitě před provedením měření je ϱ, pravděpodobnost, že naměříme výsledek m, je rovna

$$p(m) = \mathrm{Tr}(M_m^\dagger M_m \varrho), \tag{1.32 a}$$

a stav po měření je

$$\frac{1}{\mathrm{Tr}(M_m^\dagger M_m \varrho)} M_m \varrho M_m^\dagger. \tag{1.32 b}$$

Měřicí operátory přitom musí splňovat rovnici úplnosti

$$\sum_m M_m^\dagger M_m = I. \tag{1.32 c}$$

K těmto postulátům uveďme opět několik poznámek:

U směsí jsme se setkali pouze s maticemi hustoty ve tvaru konvexní kombinace projektorů na podprostory dimenze 1 stavového prostoru. Každá taková kombinace vyhovuje požadavkům postulátu 1', jak bychom se snadno přesvědčili z odpovídajících definic. Dá se však ukázat, že ani definice matice hustoty jako pozitivního operátoru se stopou rovnou 1 není obecnější, nejsnáze opět v případě konečné dimenze:

Protože každý pozitivní operátor je hermitovský, pro libovolnou matici hustoty ϱ existuje spektrální rozklad $\varrho = \sum_{i=1}^{k} \lambda_i P_{\lambda_i}$. Jestliže ortogonální projektory P_λ rozepíšeme jako součty ortogonálních projektorů na podprostory dimenze 1 $|x\rangle\langle x|$, můžeme spektrální rozklad psát ve tvaru

$$\varrho = \sum_{j=1}^{l} \lambda_j |x_j\rangle\langle x_j|. \tag{1.33}$$

Protože $\{|x_j\rangle\}_{j=1}^{l}$ pak tvoří ortonormální bázi stavového prostoru, nalezli jsme ortonormální bázi, v níž je ϱ diagonální. Z pozitivity a podmínky na stopu pak rychle plyne, že všechny vlastní hodnoty λ_i leží v intervalu $\langle 0, 1\rangle$ a jejich součet je 1, určují tedy koeficienty konvexní kombinace projektorů $\{|x_j\rangle\langle x_j|\}_{j=1}^{l}$ dávající ϱ.

Tato konvexní kombinace však není určena maticí hustoty jednoznačně: volnost je ponechána v rozkladu projektorů P_λ na součet „jednorozměrných“ projektorů. Například matice hustoty na dvourozměrném prostoru, popsaná v dané ortonormální bázi maticí

$$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}, \tag{1.34}$$

lze z ortogonálních projektorů na jednorozměrné podprostory nakombinovat způsoby

$$\begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix} + \frac{1}{2}\begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix} \tag{1.35}$$

a mnoha dalšími. Jednoznačně je možno zapsat pouze projektory samotné, protože tvoří vrcholy svého konvexního obalu.

Projektory jsou dle úvodní úvahy maticemi hustoty systémů, u nichž známe stav přesně – – odpovídají výběru z rezervoáru, ve kterém všechny systémy byly ve stejném stavu. Stav popsaný maticí hustoty, která je ortogonálním projektorem, se odtud nazývá *čistým stavem*. Ostatní stavy vyhovující postulátu 1' se nazývají *smíšené stavy*.

V tomto místě ještě poznamenejme, že formalismus matice hustoty potřebuje i jinou definici provázaných stavů: řekneme, že stav složeného systému tvořeného n komponentami, popsaný maticí hustoty ϱ, je *separovatelný*, jestliže je konvexní kombinací matic hustoty tvaru $\varrho_1 \otimes \ldots \otimes \varrho_n$, kde ϱ_i je v každém případě nějaká matice hustoty i-tého podsystému pro $i = 1, \ldots, n$. V opačném případě řekneme, že daný stav je *provázaný*.

Matici hustoty má díky své univerzalitě, uvedené na začátku tohoto paragrafu, mnohem více využití než jen pro popis směsí systémů. V kvantové mechanice má další významná použití zejména u neizolovaných systémů, do nichž okolí vnáší šum. Dalším příkladem může být konzistentní popis stavu systému, na němž bylo provedeno měření bez zaznamenání výsledku, čímž nastala velmi podobná situace jako při výběru ze směsi. Pro naše účely však bude nejdůležitější její využití v případě složených fyzikálních systémů, které popisuje následující paragraf.

1.8 Redukovaná matice hustoty

V teorii kvantových algoritmů budeme často potřebovat pracovat s fyzikálním systémem složeným z několika podsystémů. Přestože celý systém je izolovaný, jednotlivé podsystémy nejsou. Ačkoli tedy známe jejich stavové prostory, nelze pro ně nelze zobecnit pojem stavového vektoru, jak ukazuje příklad provázaných stavů. Nad těmito prostory ovšem můžeme s výhodou uvažovat matice hustoty.

Matice hustoty nad stavovým prostorem jedné komponenty složeného systému se nazývá *redukovaná matice hustoty*. Operace, kterou se z matice hustoty celého systému získá, se nazývá *parciální stopa*. V její definici se pro zjednodušení omezíme na případ dvou systémů s konečnědimezionálními stavovými prostory a na bázové vektory množiny lineárních operátorů na tenzorovém součinu těchto prostorů, pro výpočet parciální stopy obecné matice hustoty se dodá požadavek linearity. Nechť tedy systém tvořený podsystémy A a B je ve stavu popsaném maticí hustoty $|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|$, kde $|a_i\rangle$, resp. $|b_i\rangle$ jsou nějaké vektory ze stavových prostorů $\mathcal{H}_A$, resp. $\mathcal{H}_B$ systémů A, resp. B. Redukovaná matice hustoty pro systém A je pak určena výrazem[13]

$$\varrho^A = \mathrm{Tr}_B(|a_1\rangle\langle a_2| \otimes |b_1\rangle\langle b_2|) = (\mathrm{Tr}\,|b_1\rangle\langle b_2|)\;|a_1\rangle\langle a_2| = \langle b_2|b_1\rangle|a_1\rangle\langle a_2|. \tag{1.36}$$

Je otázkou, jak dalece souvisí výsledek této matematické operace se skutečným stavem podsystému A. Snadno se však ukáže, že taková volba redukované matice hustoty je dobrá – pro libovolné měření na systému A dá správný výsledek [3].

Příklad výpočtu redukované matice hustoty ukážeme na dvou příkladech:

– Nechť systém je ve smyslu původního formalismu ve faktorizovatelném stavu $|a\rangle|b\rangle$, $|a\rangle \in \mathcal{H}_A$, $|b\rangle \in \mathcal{H}_B$. Toto odpovídá matici hustoty čistého stavu $\varrho = |a\rangle|b\rangle \otimes \langle a|\langle b| = |a\rangle\langle a| \otimes$

[13] Tr za druhým rovnítkem značí již běžnou stopu matice, třetí rovnítko tedy využívá vlastnosti, že stopa součinu matic je invariantní vůči cyklické záměně.

$|b\rangle\langle b|$. Redukované matice pro oba podsystémy můžeme určit okamžitě dosazením do uvedené definice parciální stopy:

$$\begin{aligned} \varrho^A &= \mathrm{Tr}(|b\rangle\langle b|)\ |a\rangle\langle a| = |a\rangle\langle a|, \\ \varrho^B &= \mathrm{Tr}(|a\rangle\langle a|)\ |b\rangle\langle b| = |b\rangle\langle b|. \end{aligned} \tag{1.37}$$

Jedná se o čisté stavy odpovídající stavovým vektorům $|a\rangle$ a $|b\rangle$.

– Nechť systém je podobně jako výše v čistém stavu popsaném vektorem $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, a tedy maticí hustoty $\varrho = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$. Takový stav je provázaný i dle paragrafu 1.5 i v jazyce matice hustoty. Redukovanou matici hustoty pro systém A můžeme spočítat po členech:

$$\varrho^A = \frac{1}{2}\Big(\langle 0|0\rangle|0\rangle\langle 0| + \langle 0|1\rangle|0\rangle\langle 1| + \langle 1|0\rangle|1\rangle\langle 0| + \langle 1|1\rangle|1\rangle\langle 1|\Big) = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}I. \tag{1.38}$$

Stejná redukovaná matice hustoty vyjde pro systém B a pro libovolný jiný Bellův stav.

Na druhém uvedeném příkladě ukážeme dvě další vlastnosti matice hustoty:

– Redukovaná matice vyšla ve tvaru násobku jednotkové matice. Odpovídající operátor má stejný tvar při vyjádření v libovolné bázi. Každé úplné měření provedené na systému v takovém smíšeném stavu by mělo stejnou pravděpodobnost pro každý možný výsledek. Tento stav se tedy vyznačuje největší možnou neurčitostí.

– Redukované matice hustoty vyjdou ve stejném tvaru $\frac{1}{2}I$ pro oba systémy i v případě kteréhokoliv jiného Bellova stavu, ačkoliv matice hustoty celého systému jsou různé. Znalost redukovaných matic hustoty komponent tedy není postačující pro rekonstrukci matice hustoty složeného systému.

Ve smyslu úvodní věty tohoto paragrafu budeme v rámci této práce pracovat s izolovanými fyzikálními systémy. Většinou tedy nebudeme potřebovat opouštět formalismus stavových vektorů a redukovaná matice hustoty bude pro matici hustoty jediným využitím. U podsystémů budeme příležitostně mezi oběma formalismy přecházet tím, že místo matice hustoty čistého stavu uvedeme některý odpovídající vektor.

Kapitola 2
Kvantová mechanika a zpracování informace

Postuláty kvantové mechaniky je možno použít k simulaci matematických výpočtů podobně jako Booleovu logiku. V této sekci definujeme kvantové obdoby jejích základů – jednotky bitu a logických hradel jakožto matematických operací nad bity. Definujeme kvantové obvody jako analogii logických obvodů – předpisu průběhu digitálního algoritmu. Tato analogie nebude zcela jednoznačná, přesto na konci kapitoly ukážeme, jak jsme schopni libovolný logický obvod nahradit kvantovým protějškem. Mezi prvním a druhým paragrafem je vložena drobná matematická vsuvka určená pro seznámení s definicí a základními vlastnostmi Pauliho matic.

2.1 Dvoudimenzionální prostory

V kvantových algoritmech se nejčastěji setkáme se stavovým prostorem určeným tenzorovým součinem dvoudimenzionálních prostorů. Tento požadavek vzniknul v analogii s klasickými počítačovými algoritmy, které využívají dvojkovou soustavu: jednotkou informace v nich je bit, každá nejmenší paměťová součástka může být ve stavu 0 nebo 1. V kvantových algoritmech se tedy zavedl pojem kvantového bitu, *qubitu*, což je vektor v dvoudimenzionálním prostoru, jehož bázi označíme $\{|0\rangle, |1\rangle\}$.[14] Není to jediná používaná možnost, některé algoritmy využívají i prostory vyšších dimenzí – trojdimenzionální prostory jsou například užitečné pro korekci chyb [3], [10] či v analogii třístavové logiky.

V kvantovém počítači může qubit realizovat například částice s dvěma dobře definovanými energetickými hladinami, částice se spinem $\frac{1}{2}$, foton, jehož budeme sledovat polarizaci, nebo foton v interferometru, který může putovat jednou ze dvou větví. Není však smyslem této práce popisovat jakékoliv detaily realizace kvantového počítače.

V populární literatuře se setkáme s tvrzením, že qubit může být ve stavech $|0\rangle$ a $|1\rangle$ „současně“. Jedná se samozřejmě o vyjádření myšlenky superpozice či tvrzení, že stavový prostor je vektorovým prostorem: existence těchto dvou bázových stavů implikuje fyzikální smysl libovolné jejich nenulové lineární kombinace. Pro laika může být dále překvapivý důsledek skutečnosti, že stavový prostor je komplexní: lineární kombinace, ve kterých $|0\rangle$ a $|1\rangle$ jsou zastoupeny stejně (ve smyslu pravděpodobnosti naměření při úplném měření v této bázi) mohou být $|0\rangle + |1\rangle$, $|0\rangle - |1\rangle$, ale i $|0\rangle + i|1\rangle$, či na místě i může být libovolná jiná komplexní jednotka, a všechny takto vzniklé stavy jsou fyzikálně odlišné.

V případě jednoho qubitu se často uvádí pěkný příklad geometrické reprezentace projektivního stavového prostoru. Všechny fyzikální stavy jednoho qubitu můžeme rozmístit na povrch jednotkové sféry (kulové slupky) zvané Blochova sféra. Taková reprezentace je výhodná z několika důvodů:

– v jednom představitelném obrázku jsou znázorněny všechny paprsky v $\mathbb{C}^2$, tedy všechny možné „poměry“ dvou komplexních čísel, nulový vektor je efektivně vyřazen z úvahy,

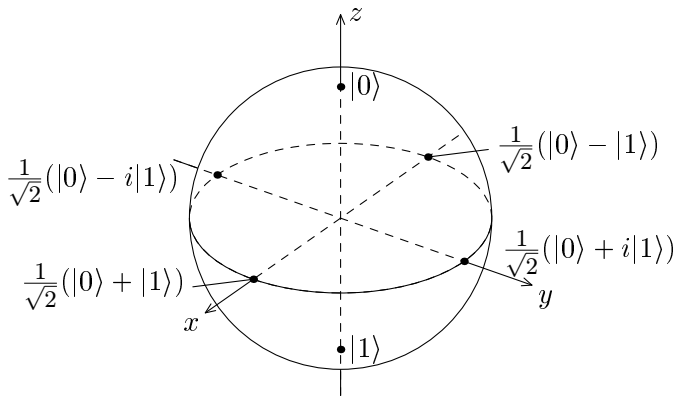
[14] Jedná se zároveň o nejjednodušší netriviální kvantový systém [3].

– každá unitární operace na $\mathbb{C}^2$ odpovídá až na násobení určitou komplexní jednotkou (globální fází obrazu) nějaké speciální ortogonální transformaci v prostoru $\mathbb{R}^3$, do kterého je tato sféra vnořena (tedy jen jejímu natáčení),

– průsečíky libovolné přímky procházející středem se sférou odpovídají dvěma kolmým vektorům,

– při uvažování matice hustoty místo stavových vektorů se tato sféra změní pouze na kouli, jejíž povrch bude odpovídat množině čistých stavů a vnitřek stavům smíšeným, střed bude reprezentovat nejvíce neurčitý stav $\frac{1}{2}I$.

Přesto se Blochova sféra uplatní spíše v jiných oblastech teorie kvantových počítačů, např. v korekci chyb. My ji k výkladu používat nebudeme a případné zájemce odkážeme na [3].



Obr. 1: Blochova sféra

Stavový prostor n qubitů je, jak bylo řečeno, tenzorovým součinem stavových prostorů jednotlivých qubitů. Má tedy dimenzi 2^n a každý vektor v něm by byl popsán 2^n komplexními čísly ($2^n - 2$ v projektivním prostoru). Poznamenejme však, že tento projektivní prostor nemá známu žádnou podobně názornou geometrickou reprezentaci jako Blochovu sféru.

Báze takového stavového prostoru tvořená tenzorovými součiny vektorů $|0\rangle$ a $|1\rangle$ se nazývá *výpočetní báze*, o jejích prvcích budeme mluvit jednoduše jako o bázových vektorech nebo bázových stavech. Pojem *bázové vektory* rozšíříme i na situace jiných tenzorových součinů stavových prostorů, u nichž dopředu uvedeme nějakou pracovní ortonormální bázi nebo budeme uvažovat bázi standardní.

V následujících paragrafech budeme ještě příležitostně bez upozornění využívat *decimální zápis*: na vnitřek ketu tvaru např. $|0101\rangle$, vzniklého ve smyslu paragrafu 1.3 násobným tenzorovým součinem vektorů $|0\rangle$ a $|1\rangle$, pohlédneme jako na zápis čísla ve dvojkové soustavě a nahradíme jej zápisem v soustavě desítkové: $|5\rangle$. Toto značení je ve shodě se skutečností, že vektory $|0\ldots00\rangle$, $|0\ldots01\rangle$, $|0\ldots10\rangle$, …, $|1\ldots11\rangle = |0\rangle$, $|1\rangle$, $|2\rangle$, …, $|2^n - 1\rangle$ tvoří ortonormální bázi prostoru $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$.

2.2 Pauliho matice

V následujícím textu se budeme příležitostně setkávat s trojicí matic známých jako Pauliho matice [3], [4]. Zaslouží si tedy v této kapitole malou vsuvku.

Pauliho matice jsou sadou tří jednoduchých matic 2×2, z nichž každá je současně hermitovská a unitární a jako celek mají mnoho dalších společných vlastností. V kvantové mechanice bychom se s nimi setkali nejčastěji u popisu *spinu* částic, později známých jako „spin-$\frac{1}{2}$ částice“, kde jsou Pauliho matice přímo i jejich lineární kombinace používány jako pozorovatelné s přímým fyzikálním významem. Díky své elementaritě mají Pauliho matice však použití mnohem širší.

Pro nás bude důležitý především jejich explicitní tvar

$$\begin{aligned}\sigma_1 = \sigma_x &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ \sigma_2 = \sigma_y &= \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \\ \sigma_3 = \sigma_z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\end{aligned} \tag{2.1}$$

v textu je budeme nazývat ještě jednodušeji jako X, Y a Z. Mezi Pauliho matice se občas řadí i jednotková matice druhého řádu $\sigma_0 = I$, my ji v následujících bodech však uvažovat nebudeme.

Mezi nejdůležitější vlastnosti Pauliho matic patří:

- druhá mocnina každé z nich je jednotková matice,
- každá má determinant -1, stopu 0 a vlastní čísla 1 a -1,
- každá hermitovská matice 2×2 je reálnou lineární kombinací Pauliho matic a jednotkové matice

a jejich komutační a antikomutační vlastnosti, které zde uvádět nebude třeba.

Kromě zmíněného příležitostného používání Pauliho matic v následujícím výkladu mají ještě další zajímavé souvislosti s tématem kvantových algoritmů, přesněji s předchozím paragrafem:

- Každá matice hustoty jednoho qubitu lze vyjádřit ve tvaru

$$\varrho = \frac{1}{2}I + \sum_{i=1}^{3} n_i \sigma_i, \tag{2.2}$$

  kde (n_1, n_2, n_3) je vektor v $\mathbb{R}^3$ se standardním skalárním součinem mající délku 1 nebo menší. Souřadnice tohoto vektoru přímo odpovídají poloze v Blochově kouli s tím, že čisté stavy jsou popsány právě jednotkovými vektory vyjadřujícími přesně polohu odpovídajícího stavového vektoru na původní sféře.

- Operace X, Y, resp. Z mají na Blochově sféře geometrický význam rotace kolem os x, y, resp. z o $180°$.

2.3 Kvantová hradla

Dalším krokem k přenesení myšlenky klasických digitálních algoritmů do kvantového světa je poskytnout kvantovou analogii logických hradel[15] a dalších prvků číslicových obvodů nebo programů.

Na kvantová hradla budeme pohlížet jako na základní stavební prvky, jejichž kombinací můžeme sestavit požadovaný operátor pro časový vývoj systému: každé z nich bude odpovídat upravenému Hamiltoniánu, podle kterého se uvažovaný systém bude vyvíjet po nějaký omezený časový interval.

Kvantové algoritmy pak budeme popisovat i zakreslovat podobně jako klasické logické obvody: stavový prostor systému n qubitů budeme znázorňovat jako n cest vedoucích zleva doprava, na nichž se budou provádět operace ve formě kvantových hradel. Pořadí zleva doprava bude odpovídat pořadí, v jakém mají jednotlivá hradla působit. Dále u každého qubitu musíme stanovit jeho vstupní hodnotu – stav před provedením algoritmu, a význam výstupní hodnoty – stavu po jeho provedení.

Kvantové hradlo je tedy nějaká unitární operace působící na systém – často však na většinu systému s výjimkou několika qubitů bude působit triviálně. Mluvíme pak o jedno-, dvou-, a tříqubitových hradlech. Značky takových hradel pak budeme v obvodu zakreslovat jen na linkách odpovídajících použitým qubitům.

Každému n-qubitovému kvantovému hradlu bude ve výpočetní bázi stavového prostoru nebo daného podprostoru odpovídat unitární matice řádu 2^n. Podmínka unitarity plyne z postulátů kvantové mechaniky uvedených v první kapitole. Každá unitární matice však naopak odpovídá nějakému myslitelnému časovému vývoji [3].

Při popisu kvantových hradel budeme uvažovat jejich působení na bázové vektory stavového prostoru zúčastněného podsystému. Taková informace je totiž ekvivalentní hledání popsané matice a díky linearitě je postačující pro nalezení obrazu libovolného stavového vektoru.

Nejjednodušší logické hradlo, které má přímou kvantovou analogii, je NOT (negace, invertor) – v klasickém obvodu má jeden vstup a jeden výstup. Jestliže vstupní hodnotou je 0, je výstupem 1 a naopak. V kvantovém světě by takovému chování odpovídalo jednoqubitové hradlo popsané maticí

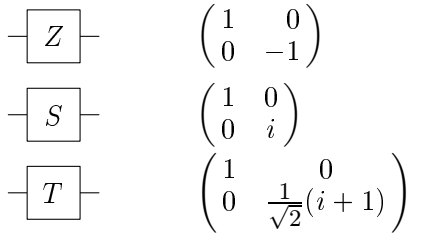
$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},$$

tedy Pauliho maticí X. Taková matice je, jak již víme, unitární, podobně jako každá matice libovolného řádu, která se liší od matice jednotkové pouze permutací řádků. Takové kvantové hradlo se tedy skutečně zavádí, nazývá se dle odpovídající matice hradlem X (případně NOT, N [10]) a v kvantovém obvodu se značí dle obr. 2.

Obr. 2: Zavedená značka pro hradlo X

[15] Termínem *logická hradla* budeme rozumět hradla klasická.

Kvantová mechanika však umožňuje definovat jednoqubitových hradel mnohem více. Mezi další užitečné příklady patří hradla způsobující fázový posun[16] amplitudy $|1\rangle$ vůči $|0\rangle$:



$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 \\ 0 & \frac{1}{\sqrt{2}}(i+1) \end{pmatrix}$$

Obr. 3: Nejčastější jednoqubitová hradla způsobující fázový posun, jejich označení v obvodu a matice

Všimněme si, že mezi těmito obvyklými hradly platí závislosti[17] $S = T^2$, $Z = S^2$, tato redundance však slouží ke zpřehlednění zápisu. Připomeňme také, že Z je další z Pauliho matic – – mohli bychom pro úplnost uvažovat samozřejmě i jednoqubitové hradlo odpovídající zbývající matici Y, my jej ale potřebovat nebudeme.

Ke zmíněným hradlům S a T se ještě setkáme s jejich sdruženými operátory (čili dalšími hradly) $S^\dagger$ a $T^\dagger$, které způsobují fázový posun s opačným znaménkem (připomeňme, že pro unitární operátory je sdružený operátor roven operátoru inverznímu).

Velice důležité je Hadamardovo hradlo, které zobrazuje bázové stavy na superpozice $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ a $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Obr. 4: Hadamardovo hradlo, jeho označení v obvodu a matice

K Hadamardovu hradlu i označením $|+\rangle$ a $|-\rangle$ se ještě mnohokrát vrátíme, nyní v souvislosti s jednoqubitovými hradly poznamenejme jen jednu z jeho důležitých vlastností: $H^2 = I$.

Další logická hradla jsou dvouvstupová, výstupem je však jeden bit. Uvědomme si, že přímou kvantovou analogii žádného takového hradla nemůžeme sestavit, musíme určit význam obou qubitů po provedení operace. Nejpřímější analogii má hradlo XOR, jehož pravdivostní tabulka je

i_1	i_2	o
0	0	0
0	1	1
1	0	1
1	1	0

Tab. 1: Pravdivostní tabulka hradla XOR.
Sloupce i budou označovat vstupní a o výstupní bity.

[16] Řekneme pak, že hradlo mění *relativní fázi* amplitudy $|1\rangle$. Výrok, že dva vektory se liší v relativní fázi, je narozdíl od globální fáze závislý na volbě ortonormální báze, a dva takové vektory jsou fyzikálně rozdílné.

[17] Uvažované jako algebraické vztahy mezi stejně pojmenovanými maticemi.

Pokud k výsledku tohoto hradla ponecháme jednu ze vstupních hodnot, získáme pravdivostní tabulku

i_1	i_2	o_1	o_2
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

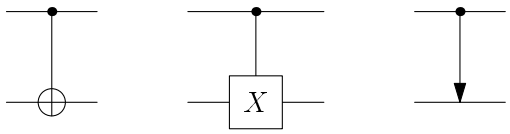
,

Tab. 2: Pravdivostní tabulka hradla CNOT

odpovídající již matici

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Tato matice je opět jakožto permutační matice jistě unitární, popisuje tedy nějaké dvouqubitové kvantové hradlo. To se v literatuře nazývá CNOT [3] nebo CN [10] a v kvantovém obvodu se značí dle obr. 5.



Obr. 5: Různá zavedená značení hradla CNOT

Písmeno C v názvu hradla je zkratkou za „controlled“ nebo jednoduše „control“. Pokud odhlédneme od původního záměru zobecnit hradlo XOR, všimněme si, že CNOT se pro bázové stavy skutečně chová tak, že v závislosti na hodnotě prvního qubitu buď aplikuje na druhý hradlo NOT nebo ne. Takto můžeme „ovládat“ libovolnou jinou operaci (ne nutně jednoqubitovou): přidání ovládacího qubitu k hradlu reprezentovanému maticí U vytvoří matici blokového tvaru

$$\begin{pmatrix} I & 0 \\ 0 & U \end{pmatrix}.$$

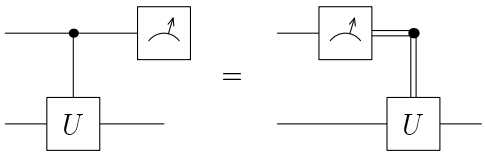
Unitarita matice U se při takovém obložení zachovává.

Často se setkáme ještě s dalšími způsoby definice kvantových hradel, které předvedeme na příkladě CNOT: stejnou informaci, která je obsažena v uvedené pravdivostní tabulce nebo matici, můžeme dále zapsat způsoby

$$\begin{aligned} \text{CNOT} &= |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| = \\ &= |0\rangle\langle 0| + |1\rangle\langle 1| + |3\rangle\langle 2| + |2\rangle\langle 3| = \\ &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \end{aligned} \tag{2.3}$$

Všimněme si důležité skutečnosti, že problém vykonat nějakou operaci v závislosti na tom, jestli je řídicí qubit ve stavu $|1\rangle$, zde neznamená na tomto qubitu provést měření. Je-li tedy například řídicí qubit v superpozici $|0\rangle$ a $|1\rangle$ (není s řízeným provázán), dostane se druhý qubit po provedení takové operace do odpovídající superpozice obou výsledků.

Ve vztahu k poslednímu odstavci uveďme ještě zajímavou skutečnost zmíněnou v [3], že „měření komutuje s ovládáním“. Následující dva algoritmy jsou tedy ekvivalentní, jak se snadno přesvědčíme rozborem jednotlivých případů a jejich pravděpodobností:



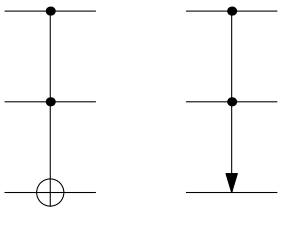
Obr. 6: Komutace měření s řízením

V pravé části obrázku 6 jsou od měření dále čáry vytahovány dvojitě – takto budeme značit jeden bit klasické informace. Místo řízeného hradla se zde tedy jedná jednoduše o provedení či neprovedení hradla U.

Pro dvě nejznámější dvouvstupová logická hradla, AND a OR, stejný postup však nepomůže. Úvahami o tvaru výsledných matic bychom se snadno ujistili, že ani žádným jiným způsobem nemůžeme v případě těchto dvou hradel dosáhnout toho, aby na jednom výstupním qubitu byl přímo výsledek. Kvantové algoritmy zde mají jinou odpověď: lze navrhnout řízené kvantové hradlo, kde řídicí qubit bude nahrazen výsledkem takové operace. Příkladem je tříqubitové Toffoliho hradlo (viz tab. 3 a obr. 7), které na bázové stavy působí tak, že třetí qubit zneguje právě tehdy, když oba první (řídicí) qubity jsou ve stavu $|1\rangle$ (jejich stav se v každém případě zachová).

i_1	i_2	i_3	o_1	o_2	o_3
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Tab. 3: Pravdivostní tabulka Toffoliho hradla

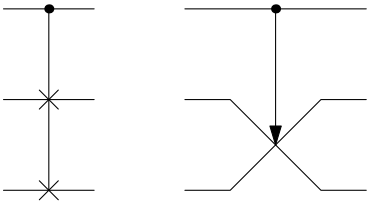


$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Obr. 7: Značení a matice Toffoliho hradla

Můžeme si všimnout, že Toffoliho hradlo je ekvivalentní tomu, kdybychom přidali k hradlu CNOT ještě jeden řídicí bit (nezávisle na tom, že jej již „obsahuje“ – na CNOT pohlížíme v tomto okamžiku jako na obecné dvouqubitové hradlo). Proto se v literatuře, např. [10], setkáme i s označením CCN.

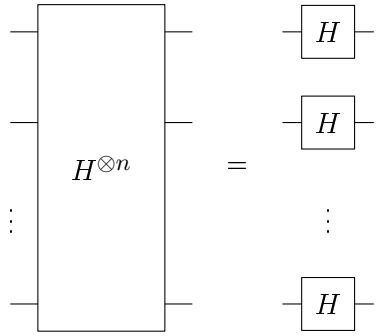
Tříqubitová hradla jsou v kvantových algoritmech, narozdíl od klasických, také velice rozšířena. Dalším častým příkladem je řízená výměna, Fredkinovo hradlo:[18]



$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Obr. 8: Značení a matice Fredkinova hradla

Nakonec uveďme obecně n-qubitové hradlo známé jako Walsh-Hadamardova transformace[19] ([3], [11]). Jedná se vlastně o n Hadamardových hradel působících na každý z qubitů:



Obr. 9: Walsh-Hadamardova transformace

Jednoqubitové operace prováděné na různých qubitech komutují, nemusíme proto uvažovat jejich pořadí. Obvykle není důvod nazývat takto utvořenou operaci novým kvantovým hradlem, ale Walsh-Hadamardova transformace je tak častá, že se tento pojem ustálil.

Matice transformace je, jak bylo řečeno výše, řádu 2^n a její prvky je možno obecně vyjádřit vzorcem

$$H_{i,j} = 2^{-\frac{n}{2}}(-1)^{|(i)_2 \cdot (j)_2|}, \quad i,j \in \{0,1,\ldots,2^n-1\}, \tag{2.4}$$

kde exponent u -1 znamená Hammingovu váhu logického součinu čísel i a j po bitech. *Hammingova váha* nezáporného čísla je počet jedniček v jeho zápisu ve dvojkové soustavě.

Mnoho kvantových algoritmů začíná tak, že všechny qubity uvažovaného systému se předpokládají ve stavu $|0\rangle$ a jako první krok se na ně aplikuje právě Walsh-Hadamardova transformace. Tím se systém dostane do stavu

$$\frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle, \tag{2.5}$$

který budeme nazývat *rovnocennou superpozicí* všech bázových stavů.

[18] Poznamenejme, že T. Toffoli i E. Fredkin pracovali na myšlence reverzibilního programování, ne přímo kvantových počítačů. Tato dvě zmíněná hradla jsou tedy opět kvantovou analogií jejich výsledků.

[19] Či pouze Hadamardova transformace.

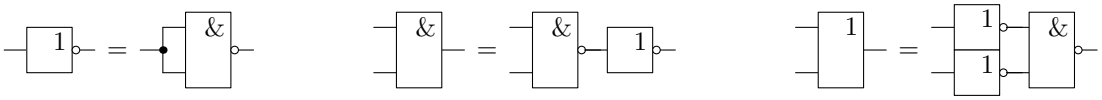
2.4 Univerzální množina hradel

Důležitá otázka je, jaká je podmnožina univerzálních hradel, tedy která hradla postačí pro sestavení celků funkčně shodných s libovolným jiným hradlem. Takový fakt je podstatný především v otázce fyzikální realizace obvodu. Pro logické obvody je známo, že univerzální je hradlo NAND:

i_1	i_2	o
0	0	1
0	1	1
1	0	1
1	1	0

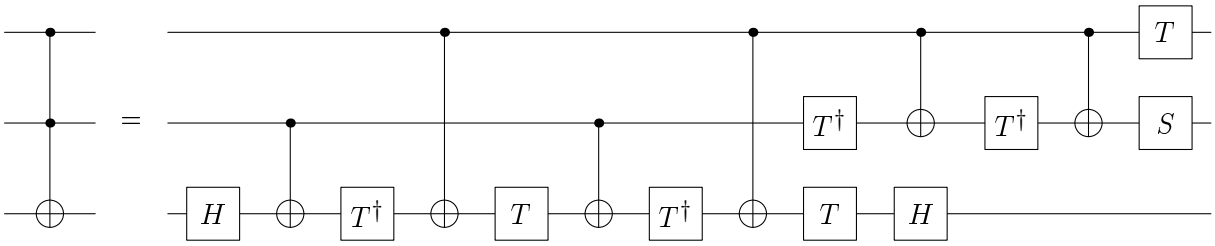
Tab. 4: Pravdivostní tabulka hradla NAND

Základní operace NOT, AND a OR je totiž možno sestavit následujícími způsoby:



Obr. 10: Realizace hradel NOT, AND a OR pomocí NAND

Ukazuje se, že libovolné kvantové hradlo je možno realizovat pomocí hradla CNOT a jednoqubitových operací [3]. V [12] nebo [3] je příklad uveden na Toffoliho hradle:



Obr. 11: Realizace Toffoliho hradla pomocí univerzálních hradel

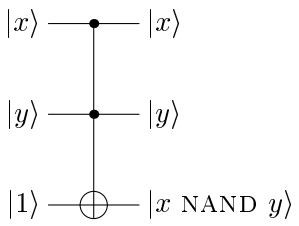
Důležitost Toffoliho a Fredkinova hradla spočívá v tom, že kterékoliv z nich spolu s možností předpokládat existenci pomocných qubitů připravených v daných stavech postačuje pro simulaci libovolného klasického obvodu, jsou tedy univerzální v této oblasti. Výsledkem takové simulace je, že řídicí qubit pro libovolnou operaci bude možno nahradit nejen jednoduchými logickými operacemi na více qubitech, ale výsledkem libovolné Booleovské funkce libovolného počtu proměnných. Takovou konstrukci budeme často využívat. V následujícím paragrafu naznačíme její detaily za použití Toffoliho hradla.

2.5 Simulace klasických obvodů kvantovými hradly

Abychom mohli sestavit kvantový obvod, který by dával stejný výsledek jako daný klasický obvod pro každý bázový stav, je třeba nahradit kvantovými analogiemi všechny prvky, které

se mohou v klasickém případě vyskytovat. Na základě univerzality logického hradla NAND by se mohlo zdát, že postačí najít kvantovou analogii pro něj, ale povšimněme si již v obr. 10, že klasický obvod není tvořen pouze logickými hradly. V kvantové analogii je třeba simulovat ještě rozdvojení vodiče, triviální není ani překřížení dvou vodičů,[20] takovou operaci je však vždy možno bez újmy vynechat.

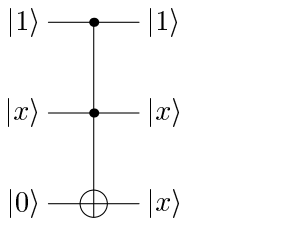
Hradlo NAND můžeme simulovat jediným Toffoliho hradlem, pro výsledek budeme potřebovat využít jeho třetí (řízený) qubit. Tento qubit budeme uvažovat připravený ve stavu $|1\rangle$: jestliže ve stavech $|1\rangle$ budou i oba řídicí qubity, Toffoliho hradlo na něm provede operaci NOT, čímž jej změní na $|0\rangle$, v ostatních tří uvažovaných bázových stavech jej ponechá ve stavu $|1\rangle$, což je přesně požadované chování.



Obr. 12: Simulace hradla NAND pomocí Toffoliho hradla

V případě, že by řízený qubit byl připraven ve stavu $|0\rangle$, stejnou úvahou bychom zjistili, že po průchodu Toffoliho hradlem bude ve stavu $|x$ AND $y\rangle$. Hradlo OR můžeme sestavit za pomoci již popsaného hradla NAND dle obr. 10, když místo NOT použijeme jednoqubitové hradlo X. Toto hradlo by bylo pro menší množinu univerzálních hradel sice také možno nahradit vhodně použitým Toffoliho hradlem, ale ponecháme jej v původním stavu – je obecně jednodušší předpokládat všechny pomocné qubity v obvodu připravené ve stavech $|0\rangle$ a do jiných pomocných stavů je případně převést pomocí jednoqubitových operací.

Toffoliho hradlo s dvěma qubity použitými jako pomocné nám umožní realizovat i obdobu rozdvojení vodiče:



Obr. 13: Simulace odbočky pomocí Toffoliho hradla

Odbočka funguje dle obr. 13 na bázové stavy, ukážeme ale, že zobecnění pro obecnou superpozici $|x\rangle = \alpha|0\rangle + \beta|1\rangle$ neplatí: její použití v obr. 13 by mělo za výsledek stav[21]

$$|1\rangle(\alpha|00\rangle + \beta|11\rangle) \neq |1\rangle(\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle). \tag{2.6}$$

[20] V anglické literatuře se pro tyto dvě operace setkáme s označeními FANOUT a CROSSOVER.

[21] Jako důležitou poznámku uveďme, že se jedná o provázaný stav, přestože výchozí stav nebyl.

Toto na první pohled nevinné zjištění je důsledkem obecně platné věty, že zálohovat stav qubitu pomocí unitární operace není možné, *věty o zákazu klonování* [3]. Ve stručnosti ji dokážeme:

Předpokládejme, že systém složený ze dvou komponent je ve stavu $|x\rangle|s\rangle$ a hledáme unitární transformaci U, která by systém převedla do stavu $|x\rangle|x\rangle$ pro každý stav $|x\rangle$ ze stavového prostoru prvního podsystému ($|s\rangle$ považujme za nějaký univerzální výchozí stav). Nechť takové chování je splněno pro dva stavy, $|\psi\rangle$ a $|\varphi\rangle$:

$$\begin{aligned} U|\psi\rangle|s\rangle &= |\psi\rangle|\psi\rangle \\ U|\varphi\rangle|s\rangle &= |\varphi\rangle|\varphi\rangle. \end{aligned} \tag{2.7}$$

Z předpokladu platnosti obou rovností se musí rovnat i skalární součiny jejich levých a pravých stran. Skalární součin $(U|\psi\rangle|s\rangle, U|\varphi\rangle|s\rangle)$ je však díky unitaritě U roven $(|\psi\rangle|s\rangle, |\varphi\rangle|s\rangle) = \langle\psi|\varphi\rangle\langle s|s\rangle = \langle\psi|\varphi\rangle$, zatímco skalární součin pravých stran je $(|\psi\rangle|\psi\rangle, |\varphi\rangle|\varphi\rangle) = (\langle\psi|\varphi\rangle)^2$. Aby mohly platit současně obě rovnosti, musí tak být skalární součin $|\psi\rangle$ a $|\varphi\rangle$ roven buď 0 nebo 1 a již platnost první rovnosti tak vylučuje platnost druhé pro libovolné $|\varphi\rangle$ kromě případů $|\varphi\rangle = |\psi\rangle$ a $\langle\psi|\varphi\rangle = 0$.

Jejím přímým důsledkem je opět nemožnost zjistit více informací o kvantovém stavu tak, že bychom jej vždy před měřením zálohovali, aby jeho stav během kolapsu nebyl ztracen.

Pro kvantovou simulaci odbočky má věta důsledek, že když zálohujeme úspěšně stavy $|0\rangle$ a $|1\rangle$, pro žádnou jejich netriviální lineární kombinaci odbočka již nemůže fungovat, ať je konstruována jakkoliv.

Upevněním pouze prvního řídicího qubitu ve stavu $|1\rangle$ se Toffoliho hradlo zredukuje na další potřebné hradlo CNOT. Pro zjednodušení zápisu při přepisu klasických obvodů do kvantové analogie je však jednodušší mezi „elementární“ hradla zařadit i CNOT.

Všiměneme si, že v každé části jsme museli zavést pomocné qubity připravené v nějakém konkrétním stavu. Čím více hradel měl klasický obvod, tím obecně více pomocných qubitů by bylo potřeba k jeho simulaci na kvantovém počítači. To může být značným problémem z hlediska fyzikální realizace kvantového algoritmu, proto u konkrétní funkce můžeme uvažovat o jiných způsobech simulace než pouze důsledného používání tohoto postupu.

Jakmile je simulační kvantový obvod sestaven, můžeme se ptát, jak se bude chovat, jestliže místo bázového stavu vyjdeme z nějakého obecného stavu. Celý vývoj stavu během průběhu algoritmu je popsán jednou unitární operací, platí tedy princip superpozice a jestliže na vstupu byla jistá lineární kombinace bázových stavů, získáme na výstupu lineární kombinaci odpovídajících výsledků (opět jakožto bázových stavů), určenou stejnými koeficienty.

Simulovaná funkce tak jistým způsobem spočítá výsledky všech použitých vstupů „najednou“: je-li například kvantový algoritmus navržen tak, aby obrazem $|0\rangle|0\rangle$ bylo $|0\rangle|f(0)\rangle$ a obrazem $|1\rangle|0\rangle$ $|1\rangle|f(1)\rangle$ pro nějaké zobrazení $f : \{0,1\} \to \{0,1\}$, při vstupu $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$ získáme výstup $\frac{1}{\sqrt{2}}(|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle)$. Toto chování se nazývá *kvantový paralelismus* ([10], [3]).

Kvantový paralelismus však nemůžeme využít ke slibovanému urychlení výpočtu přímo. Na uvedeném příkladě vidíme, že měřením nemůžeme získat obě funkční hodnoty současně: kdybychom po algoritmu provedli úplné měření stavu, získali bychom pouze jeden z čitatelů, tedy

pouze jeden z bodů 0 a 1 a funkční hodnotu v něm. Princip, který poskytuje většině kvantových algoritmů jejich výhody oproti algoritmům klasickým, je *interference*. Detaily jejího využití však závisí na konkrétním algoritmu, na příkladě se s ní setkáme v paragrafu 3.4.

V minulém odstavci jsme předpokládali, že pracovní prostor je tvořen jen qubity představujícími vstup pro funkci a jedním qubitem jako místem pro uložení výstupu. Pro zajištění účelu popsaného na konci minulého paragrafu a ve smyslu první části tohoto však bude ve skutečnosti potřeba

- n vstupních qubitů,
- $m + 1$ pomocných qubitů, připravených ve stavu $|0\rangle$,
- 1 cílový qubit, na kterém budeme chtít provést operaci řízenou výsledkem funkce.

Mezi pomocnými qubity jsme zde myšlenkově vymezili poslední pro hodnotu funkce. Nechť tedy počáteční bázový stav, zapsaný v rozdělení na tyto čtyři části, je $|x\rangle|0\rangle|0\rangle|y\rangle$, kde x představuje vstup funkce. Po provedení náhradního kvantového obvodu za obvod počítající požadovanou funkci se tento stav změní na $|x\rangle|g(x)\rangle|f(x)\rangle|y\rangle$, kde jsme $g(x)$ označili výsledek pomocných operací na prvních m pomocných qubitech. V tomto okamžiku můžeme provést libovolnou požadovanou jednoqubitovou operaci na posledním qubitu řízenou posledním pomocným qubitem. Předpokládejme, že se jedná o X, výsledným stavem pak je $|x\rangle|g(x)\rangle|f(x)\rangle|y \oplus f(x)\rangle$.

Pomocné qubity však obecně brání jakékoliv kvantové interferenci výsledků – aby k ní mohlo dojít, musely by se jejich hodnoty u všech čitatelů shodovat, jinak by tyto čitatele byly nutně vzájemně ortogonální. Na počátku algoritmu tomu tak bylo – všechny pomocné qubity jsme jednotně uvažovali ve stavu $|0\rangle$. Ukážeme tedy, že postupem známým jako *uncomputation* [3] jsme schopni je do tohoto stavu vrátit za zachování informace o výsledku funkce.

Každé kvantové hradlo je díky své unitaritě *reverzibilní* – z jeho výstupu je vždy možno získat zpětně a jednoznačně vstupní stav. Libovolný obvod jsme tedy během simulace nahradili obvodem reverzibilním. Všechna hradla použitá pro simulaci klasických obvodů – Toffoliho, X a případně CNOT, mají navíc vlastnost, že toto převrácení lze provést druhou aplikací téhož hradla na výstup (jejich matice ve standardní bázi jsou samy sobě inverzními). Všechna hradla použitá během simulace je tedy možno na stav $|x\rangle|g(x)\rangle|f(x)\rangle|y \oplus f(x)\rangle$ použít znovu, v opačném pořadí, pro získání konečného požadovaného stavu $|x\rangle|0\rangle|0\rangle|y \oplus f(x)\rangle$.

Kapitola 3
Kvantové algoritmy

Minulá kapitola připravila základ, na němž můžeme stavět kvantové algoritmy jakožto algoritmy pracující s registry sestavenými z qubitů a využívající principy kvantové mechaniky, a zabývat se již jen jejich specifickými vlastnostmi.

Teorie kvantových algoritmů se dělí na několik logických celků:

- návrh kvantových algoritmů jako analogie k digitálním algoritmům – realizace výpočtů či algoritmických úloh za využití kvantových hradel,
- kvantové komunikační protokoly a kvantová kryptografie – využití provázání či vlastností kvantového měření pro přenos informace,
- kvantové algoritmy pro korekci chyb – bránění negativního vlivu okolí na průběh výše uvedených algoritmů v neizolovaných fyzikálních systémech,
- matematická teorie kvantové informace a teorie kvantové složitosti,
- úzce související problematika experimentální realizace kvantových počítačů.

Ve všech těchto partiích bylo již dosaženo podstatných pokroků. Tím se problematika kvantových algoritmů stala natolik rozsáhlou, že není v možnostech této práce se zabývat každým z těchto bodů. Ve skutečnosti se ve zbytku textu budeme zabývat pouze prvním z nich, který je pod pojmem *kvantové algoritmy* nejčastěji uvažován.

Kvantové algoritmy začaly být detailně zkoumány poté, co se na několika příkladech ukázalo, že mají v určitých úlohách oproti digitálním algoritmům potenciál dojít k výsledku s výrazně kratší časovou složitostí. Nejdůležitější a nejznámější z těchto příkladů je Shorův algoritmus pro faktorizaci čísel (1994), řešící tento problém v čase polynomickém vzhledem k délce vstupu. Ve světě digitálních algoritmů přitom nejsou známy algoritmy vyžadující kratší než exponenciální čas. Shorově algoritmu věnujeme několik krátkých paragrafů, ale s upozorněním, že se nejedná o hlavní část práce a tak tyto úseky textu podávají pouze zběžný náhled na klíčové body postupu.

Další milník v kvantových algoritmech byl Groverův algoritmus pro vyhledávání v nesetříděné databázi (1996). Ten sice oproti klasické obdobě nabízí pouze polynomické zkrácení časové složitosti, zde však je zřejmé, že žádný digitální algoritmus nemůže takové rychlosti dosáhnout již z principu úlohy. Vyhledávací algoritmy jsou hlavním cílem této práce, Groverově algoritmu se proto věnuje celá příští sekce.

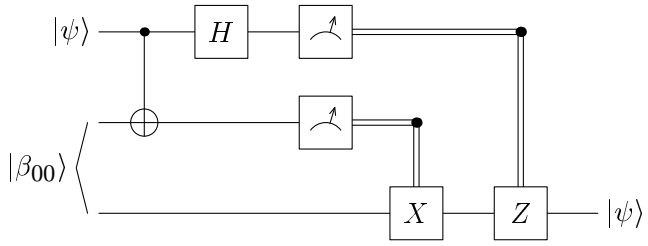
Pro úvod kapitoly byl však zvolen jeden pěkný příklad z jiné oblasti, kvantový komunikační protokol známý pod názvem *kvantová teleportace*.

3.1 Kvantová teleportace

Kvantová teleprotace je algoritmus, na němž předvedeme praktický příklad kvantového obvodu a některé možnosti a principy, se kterými se v kvantových algoritmech setkáváme.

Uváděný název je však bohužel také příkladem značné popularizace terminologie. Tento algoritmus je totiž určen k přenesení libovolné hodnoty jednoho qubitu z jednoho podsystému na jiný bez nutnosti přenosu kvantové informace mezi těmito dvěma částmi zkoumaného systému. Tuto myšlenku brzy upřesníme, ale uvědomme si, že se ani vzdáleně nejedná o žádné přenášení objektů v prostoru.

Je jisté, že dle intuitivní představy by bylo pro rekonstrukci qubitu nutno přenést nekonečné množství klasické informace (stav má dva reálné stupně volnosti), a víme, že navíc tuto informaci nemáme možnost získat měřením. Kvantová teleportace umožňuje využít provázání tak, že pro uskutečnění přenosu kvantového stavu postačí stranám předat si pouhé dva klasické bity.



Obr. 14: Kvantová teleportace

Představme si kvantový obvod podle obr. 14. První dvě částice jsou umístěny u jednoho pozorovatele, který s nimi tak může provádět operace, se kterými jsme se seznámili ve druhé sekci, třetí částice je umístěna u druhého pozorovatele. První částice je v libovolném stavu $\alpha|0\rangle + \beta|1\rangle$, který chceme přenést na třetí částici a předat tak druhému z pozorovatelů, třetí a druhá částice jsou spolu připraveny v provázaném stavu $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Popišme, jak se systém vyvíjí, matematicky: původní stav je

$$|\psi_0\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle). \qquad (3.1\,\mathrm{a})$$

Po první operaci CNOT pak

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle). \qquad (3.1\,\mathrm{b})$$

Hadamardův operátor působící na první částici má výsledek

$$|\psi_2\rangle = \frac{\alpha}{2}(|000\rangle + |100\rangle + |011\rangle + |111\rangle) + \frac{\beta}{2}(|010\rangle - |110\rangle + |001\rangle - |101\rangle). \qquad (3.1\,\mathrm{c})$$

Nyní pouze seskupme členy se stejnými hodnotami prvního a druhého qubitu:

$$|\psi_2\rangle = \frac{1}{2}\left(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right). \qquad (3.1\,\mathrm{d})$$

Jestliže tedy jako další krok provedeme měření na podsystému prvních dvou částic, nastane kolaps vlnové funkce do jednoho z čitatelů. Na prvních dvou částicích naměříme některou ze všech čtyř kombinací 0 a 1, třetí částice se tak dostane do jedné z odpovídajících kombinací

$|0\rangle$ a $|1\rangle$, přičemž tento mezistav, jak bychom okamžitě ověřili, poslední dvě operace na základě výsledků obou měření v každém případě „opraví“ do správného tvaru.

Jak uvádí [3], kvantová teleportace nepopírá ani předpoklad přenášení informace rychlostí větší než c, ani větu o nemožnosti kopírování kvantového stavu. Rychlost přenosu stavu je omezena rychlostí klasického komunikačního kanálu, kterým musíme přenést ke druhému pozorovateli dva bity informace – třetí qubit sám je do té doby zcela nepoužitelný (je jakožto jedna strana provázané dvojice ve zcela neurčitém stavu). Odpovědí na druhou otázku pak je, že po provedení algoritmu neexistují dvě kopie původního stavu – první dva qubity skončí v bázových stavech.

Tento příklad měl však sloužit především jako ukázka, jak málo intuitivní chování kvantového algoritmu může být. Všimněme si například, že až na poslední dvě operace zůstávala třetí částice zcela netknuta a do jednoho ze čtyř stavů výše ji skutečně dostalo „vytknutí ze závorky“. Další zajímavá a méně obvyklá operace je aplikace Hadamardova hradla těsně před měřením, když do té doby byl qubit v bázovém stavu.

3.2 Shorův algoritmus

Shorův algoritmus [13] je bezesporu nejpopulárnějším kvantovým algoritmem. Jeho účelem je řešení problému faktorizace čísel (jejich rozkladu na prvočíselné činitele, v jednodušší podobě však pouze nalezení alespoň jednoho netriviálního dělitele čísla), důležitého především v mnoha odvětvích počítačového zabezpečení. Množství šifrovacích algoritmů totiž spoléhá na fakt, že veškeré známé klasické algoritmy faktorizace čísel mají exponenciální časovou složitost (tzn. počet matematických operací potřebný k jejich průběhu roste zhruba geometrickou řadou v závislosti na délce vstupu, která je zde definována jako počet číslic n faktorizovaného čísla N). Takové algoritmy se obecně nazývají „obtížné“, protože i s malým zvýšením délky vstupu může vzrůst potřebná doba k řešení o několik řádů a tak spolehlivě předstihnout předpokládaný vývoj techniky až do nedohledné doby. Obecně každý algoritmus s exponenciální časovou složitostí je považován za nepoužitelný v případech, kdy délka vstupu není explicitně omezena nějakou malou konstantou, a pro řešení takových problémů jsou vyhledávány algoritmy s polynomiální složitostí.

V případě faktorizace čísel do současné doby nebyl podán teoretický důkaz o tom, že žádný nekvantový algoritmus s polynomiální časovou složitostí nemůže existovat [3], obecně je ale takové tvrzení považováno za velice pravděpodobné. Nalezení takového algoritmu dosud alespoň odolává všem pokusům.

Peter W. Shor však ukázal na přímém příkladu, že polynomiální časové složitosti je možno dosáhnout použitím kvantových algoritmů. (V kvantových algoritmech je časová složitost definována pomocí potřebného počtu univerzálních kvantových hradel, uvedených v paragrafu 2.4.) Taková „hrozba“ pro počítačovou kryptografii zvedla vlnu zájmu o studium kvantových algoritmů, které do té doby byly spíše považovány za okrajovou oblast výzkumu pro menší skupinu teoretických fyziků a informatiků.

Do detailů teorie složitosti v rámci této práce více zasahovat nebudeme. Řekněme jen, že informace, zda algoritmus má polynomiální časovou složitost či nemá, je primární; nejmenší dosažitelný stupeň polynomu, použitelného pro horní odhad, je pak až měřítkem hrubého porovnání

dvou polynomiálně složitých algoritmů, a teprve na dalším místě je přesnější specifikace odhadu pomocí komplikovanějších funkcí jako $\log n$, případně pak konstanta úměrnosti. Ve smyslu těchto pravidel ukážeme specifikaci složitosti Shorova algoritmu až na konci bez hlubšího vysvětlení a pro zajímavost.

Shorův algoritmus vychází nekvantového algoritmu,[22] který převádí problém nalezení netriviálních dělitelů čísla na problém hledání periody celočíselné posloupnosti. Hledání periody je řešeno aplikací diskrétní Fourierovy transformace na vzorek průběhu posloupnosti a právě Fourierova transformace je jediným prvkem celého postupu, který způsobuje v klasickém algoritmu exponenciální časovou složitost. Hlavní přínos Shorovy práce je tedy předvedení, jak je možno realizovat kvantovou obdobu diskrétní Fourierovy transformace pomocí univerzálních kvantových hradel, jejichž počet je polynomicky závislý na délce vstupu.

Kvantová Fourierova transformace má pak několik dalších využití, které popsal Shor i další vědci. Narozdíl od faktorizace čísel se však jedná o řešení více teoretických matematických problémů, např. *diskrétního logaritmu* (odpovídající algoritmus je popsán rovněž ve [13]).

Než popíšeme kvantový algoritmus pro diskrétní Fourierovu transformaci, podívejme se na stručný přehled zbytku algoritmu [14]:

Posloupnost $\{a_k\}_{k=0}^{+\infty}$, jejíž budeme zkoumat periodu, se konstruuje dle vzoru

$$a_k = r^k \bmod N, \tag{3.2}$$

kde r je libovolně zvolené přirozené číslo nesoudělné s N (tedy mající s ním největší společný dělitel rovný 1). Snadno by se ukázalo, že je postačující číslo r volit z rozmezí 2 až $N-1$. Můžeme jej zvolit náhodně a podmínku nejmenšího společného dělitele ověřit. Jestliže vyjde jiný než 1, je netriviálním dělitelem čísla N a úlohu v jednodušší formulaci, uvedené na začátku paragrafu, můžeme považovat za vyřešenou.

Dalším krokem je nalezení periody posloupnosti $\{a_k\}$. Periodicita takové posloupnosti plyne z faktu, že její zadání lze přepsat v rekurentním tvaru

$$a_k = r a_{k-1} \bmod N, \quad k > 1, \tag{3.3}$$

využívajícím pouze jeden předchozí člen, a že obor hodnot posloupnosti je konečná množina (přirozená čísla omezená na interval $\langle 1, N-1\rangle$).[23] Jak bylo uvedeno výše, pro nalezení periody se bude využívat diskrétní Fourierova transformace. Uvidíme, že pro realizaci v kvantovém algoritmu bude vhodné zkoumaný vzorek zvolit jako 2^q prvních hodnot posloupnosti pro nějaké přirozené číslo q. Ukazuje se, že vhodná je taková volba q, aby platilo

$$N^2 \leq 2^q < 2N^2. \tag{3.4}$$

Nalezenou periodu[24] posloupnosti označme p. Algoritmus je dále nepoužitelný, pokud tato perioda je liché číslo – v takovém případě se musí zkusit znovu s jinou volbou r. V pozitivním případě se budeme zabývat hodnotou $a_{\frac{p}{2}}$. Ta musí splňovat kongruenci

$$\left.\begin{aligned} a_p &= a_0 = 1 \\ &= \left(a_{\frac{p}{2}}\right)^2 \bmod N \end{aligned}\right\} \quad \left(a_{\frac{p}{2}}\right)^2 \equiv 1 \bmod N. \tag{3.5}$$

[22] Tento algoritmus byl v době uvedení Shorova algoritmu již znám ([13], [14]).

[23] Ještě by bylo třeba provést důkaz, že opakování bude „platit“ již od prvního členu. Ten uvádět nebudeme, řekneme jen, že v něm se využívá předpokladu nesoudělnosti čísel r a N.

[24] Pod pojmem perioda budeme zásadně rozumět nejmenší periodu.

Rovnost $a_{\frac{p}{2}} = 1$ by byla ve sporu s tím, že periodou posloupnosti je p. Další triviální případ splnění kongruence by mohl nastat, pokud $a_{\frac{p}{2}} = N - 1$. Takový výsledek je však pro pokračování algoritmu nevhodný a znamenal by opět návrat na začátek k jiné volbě r. Budeme tedy předpokládat, že $a_{\frac{p}{2}}$ nemá ani jednu z těchto krajních hodnot.

K zakončení algoritmu se využívá kongruence

$$\begin{aligned} r^p &\equiv 1 \bmod N \\ r^p - 1 &= \left(r^{\frac{p}{2}} - 1\right)\left(r^{\frac{p}{2}} + 1\right) \equiv 0 \bmod N. \end{aligned} \tag{3.6}$$

Z té plyne, že N je dělitelem uvedeného součinu. Protože však nedělí ani jeden z činitelů, což je ekvivalentní omezení hodnot $a_{\frac{p}{2}}$, provedenému v minulém odstavci, musí nutně mít netriviálního společného dělitele s každým z nich.

Průběh algoritmu ukážeme na příkladě: zvolme $N = 143$ a $r = 10$. Prvních několik členů posloupnosti $\{a_k\}_{k=0}^{+\infty}$ je v tomto případě

$$1, 10, 100, 142, 133, 43, 1, 10, 100, \ldots, \tag{3.7 a}$$

perioda je tedy $p = 6$. První kontrola, aby p bylo sudé číslo, proběhne v pořádku, ale $a_{\frac{p}{2}} = a_3 = 142$ je rovno nepovolené hodnotě $N - 1$.

Číslo r bylo tedy zvoleno nevhodně. Pokusme se proto opakovat výpočet s jinou náhodnou volbou, např. $r = 8$. S ní jsou počáteční členy posloupnosti

$$1, 8, 64, 83, 92, 21, 25, 57, 27, 73, 12, 96, 53, 138, 103, 109, 14, 112, 38, 18, 1, 8, \ldots \tag{3.7 b}$$

a platí $p = 20$ a $a_{10} = 12$. Obě kontroly tedy proběhnou úspěšně a díky tomu víme, že 143 má netriviální nejmenší společné dělitele s čísly 12 ± 1. Ty však již tvoří přímo jeho prvočíselný rozklad: $143 = 11 \cdot 13$.

Je zřejmé, že pokračování algoritmu od nalezení periody posloupnosti nevyžaduje žádné postupy z kvantových algoritmů – realizace Shorova algoritmu tak bude sestávat z kvantové a klasické části. Kvantovou část nebudeme i přes možnosti simulace libovolného klasického algoritmu zbytečně rozšiřovat do oblastí, kde klasická výpočetní jednotka poslouží lépe.

V následujícím paragrafu, který je vyčleněn pro popis kvantové Fourierovy transformace, však uvidíme, že některé části výpočtu budeme muset nutně do kvantového algoritmu zařadit.

3.3 Kvantová Fourierova transformace

Kvantová Fourierova transformace je analogií diskrétní Fourierovy transformace. Čtenář bude pravděpodobně seznámen s klasickou Fourierovou transformací, známou pod vzorcem (méně obvyklá znaménková konvence převzata z [15])

$$F(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} e^{2\pi i \omega t} f(t) \mathrm{d}t, \tag{3.8}$$

platným pro Lebesgueovsky integrovatelné funkce f, a se skutečností, že dle tohoto předpisu je možno spojitě dodefinovat Fourierův-Plancherelův operátor, izometrický na prostoru $L^2(\mathbb{R}, \mathrm{d}x)$ [2].

Diskrétní Fourierova transformace je oproti tomu lineární operátor na $\mathbb{C}^n$: n-tici čísel $\{a_i\}_{i=0}^{n-1}$ přiřazuje n-tici $\{A_i\}_{i=0}^{n-1}$ podle předpisu

$$A_j = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} e^{\frac{2\pi i j k}{n}} a_k \tag{3.9}$$

Matice takového operátoru ve standardní bázi má prvky

$$F_{jk} = e^{\frac{2\pi i j k}{n}}, \quad j,k = 0,1,\ldots,n-1. \tag{3.10}$$

Snadno ověříme, že F je unitární: určeme totiž prvky maticového součinu

$$(FF^\dagger)_{jk} = \sum_{l=0}^{n-1} F_{jl}\overline{F_{lk}} = \frac{1}{n}\sum_{l=0}^{n-1} e^{\frac{2\pi i j l}{n}} e^{-\frac{2\pi i l k}{n}} = \frac{1}{n}\sum_{l=0}^{n-1}\left(e^{\frac{2\pi i (j-k)}{n}}\right)^l. \tag{3.11 a}$$

Výsledkem poslední úpravy je částečný součet geometrické řady. Pro případ $j \neq k$ lze použít vzorec

$$\frac{1}{n}\sum_{l=0}^{n-1}\left(e^{\frac{2\pi i (j-k)}{n}}\right)^l = \frac{1 - e^{\frac{2\pi i (j-k)}{n} n}}{n\left(1 - e^{\frac{2\pi i (j-k)}{n}}\right)} = 0, \tag{3.11 b}$$

protože $e^{2\pi i (j-k)} = 1$. Jestliže $j = k$, je koeficient geometrické řady $e^0 = 1$ a platí tak

$$(FF^\dagger)_{jj} = \frac{1}{n}\sum_{l=0}^{n-1} 1 = 1, \tag{3.11 c}$$

celkově tedy

$$(FF^\dagger)_{jk} = \delta_{jk}, \tag{3.11 d}$$

což jsme chtěli dokázat.

Pro účely Shorova algoritmu tak můžeme uvažovat kvantové hradlo F, které bude působit na q qubitech podle odpovídajícího předpisu

$$F|k\rangle = \frac{1}{\sqrt{2^q}} \sum_{j=0}^{2^q-1} e^{\frac{2\pi i j k}{2^q}} |j\rangle : \tag{3.12}$$

obraz obecné superpozice $|\psi\rangle = \sum_{j=0}^{2^q-1} \alpha_k |k\rangle$ pak bude

$$F|\psi\rangle = \sum_{k=0}^{2^q-1} \alpha_k \left(\frac{1}{\sqrt{2^q}} \sum_{j=0}^{2^q-1} e^{\frac{2\pi i j k}{2^q}} |j\rangle\right) = \sum_{j=0}^{2^q-1}\left(\frac{1}{\sqrt{2^q}} \sum_{k=0}^{2^q-1} e^{\frac{2\pi i j k}{2^q}} a_k\right)|j\rangle \tag{3.13}$$

v přímé analogii s (3.9).

Ref. [10] ukazuje, jak jsme takovou unitární operaci schopni realizovat pomocí jedno- a dvouqubitových hradel: zavádí se zde hradlo A_j jako Hadamardovo hradlo působící na j-tý qubit a B_{jk} jako hradlo působící na j-tý a k-tý qubit tak, že změní o $\frac{\pi}{2^{j-k}}$ relativní fázi těch bázových stavů, ve kterých oba tyto qubity jsou ve stavu $|1\rangle$. Pro $j - k = 1$, resp. 2 se tak například jedná o hradla S, resp. T, zavedená v paragrafu 2.3, působící na k-tý qubit a řízená j-tým (uvědomme si však, že v takovém případě není rozdíl v tom, když označení qubitů prohodíme).

Hradlo F získáme, jestliže aplikujeme následující sérii těchto operací:[25]

$$A_1 B_{12} B_{13} \dots B_{1,q} A_2 B_{23} \dots B_{2,q} A_3 \dots A_{q-1} B_{q-1,q} A_q \tag{3.14}$$

následovanou výměnou hodnot prvního a q-tého, druhého a $(q-1)$-tého, ... qubitu. Pokud však budeme hned po aplikaci F chtít provést úplné měření stavu ve výpočetní bázi a pokračovat klasickým výpočtem, je zbytečné tyto výměny zahrnovat do kvantového počítače: postačí provést měření po zmíněné sérii operací a naměřené stavy jednotlivých bitů přečíst v opačném pořadí.

Skutečnost, že (3.14) vede k rychlé Fourierově transformaci, zde již nebudeme hlouběji probírat – tento paragraf je myšlen jako skutečně stručné nahlédnutí na průběh Shorova algoritmu. Poznamenejme pouze, že se jedná o zcela přímou kvantovou interpretaci Cooleyho-Tukeyho implementace rychlé Fourierovy transformace (FFT), která je detailně popsána v [15] nebo [16].

Kvantová mechanika však klade na takovouto implementaci diskrétní Fourierovy transformace dvě silné nevýhody:

- neexistuje obecný způsob, jak „uložit“ do počátečního stavu analyzovaný průběh,
- podobně není možné zjistit výsledný průběh amplitud.

Následující paragraf ukazuje, jak k těmto dvěma bodům přistupuje Shorův algoritmus.

3.4 Fourierova transformace ve Shorově algoritmu

Kvantová část Shorova algoritmu působí na dvou registrech qubitů – tedy uvažujeme stavový prostor vzniklý tenzorovým součinem ze stavových prostorů q a s qubitů, kde q je číslo definované v předminulém paragrafu a s je dostatečně velké, aby $N < 2^s$. Počáteční stav se pro snazší implementaci volí tvaru $|0\rangle|0\rangle$.

Fourierova transformace je ve Shorově algoritmu aplikována na zvláštním vstupu, který má tvar

$$|\Psi_0\rangle = \frac{1}{\sqrt{2^q}} \sum_{k=0}^{2^q-1} |k\rangle|a_k\rangle. \tag{3.15}$$

Přitom transformace se provádí na první sadě q qubitů, která v této superpozici reprezentuje index posloupnosti.

Aby se systém dostal do tohoto stavu z počátečního stavu $|0\rangle\langle 0|$, aplikuje se nejprve Walsh-Hadamardova transformace na prvním registru, který jí převedeme do stavu

$$|\Psi_1\rangle = \frac{1}{\sqrt{2^q}} \sum_{k=0}^{2^q-1} |k\rangle|0\rangle. \tag{3.16}$$

Vzhledem k nemožnosti do tohoto stavu „doplnit zvenku“ předpřipravené hodnoty posloupnosti je bude třeba spočítat v průběhu algoritmu pomocí principu kvantové simulace obvodu, kterým bychom je počítali na klasické výpočetní jednotce. Tato část je mnohem náročnější než

[25] Uvažováno směrem zprava doleva jako skládání operátorů.

Fourierova transformace, a to i v čase, i v potřebě pomocných qubitů [14]. Ty musí být v uvažovaném systému tedy také k dispozici, ale díky předpokladu jejich návratu do původních stavů $|0\rangle$ po výpočtu je jako součást stavového prostoru nemusíme uvažovat.

Příklad realizace výpočtu hodnot posloupnosti potřebné pro Shorův algoritmus pomocí kvantových hradel je uveden v [17].

Jestliže tedy sestrojíme náhradní kvantový algoritmus, který vstup $|k\rangle|0\rangle$ transformuje na výstup $|k\rangle|a_k\rangle$, stačí přivést na vstup superpozici (3.16) a využít tak kvantový paralelismus, abychom na výstupu získali požadovanou superpozici (3.15).

Na tuto superpozici tedy budeme aplikovat kvantový operátor F. Dle rovnice (3.12) se tím stav změní na

$$|\Psi_2\rangle = \frac{1}{2^q} \sum_{k=0}^{2^q-1} \sum_{j=0}^{2^q-1} e^{\frac{2\pi i j k}{2^q}} |j\rangle|a_k\rangle = \frac{1}{2^q} \sum_{j=0}^{2^q-1} \sum_{k=0}^{2^q-1} e^{\frac{2\pi i j k}{2^q}} |j\rangle|a_k\rangle. \tag{3.17}$$

Díky tomu, že posloupnost $\{a_k\}_{k=0}^{+\infty}$ je periodická s periodou $p < N$ a $2^q \geq N^2$, každá dosažená hodnota a_k se ve vzorku vyskytne alespoň N-krát. Tato skutečnost nyní umožní kvantovou interferenci: pravděpodobnost naměření stavu $|j\rangle$ při měření na prvním podsystému ve výpočetní bázi bude

$$\left\| \frac{1}{2^q} \sum_{k=0}^{2^q-1} e^{\frac{2\pi i j k}{2^q}} |a_k\rangle \right\|^2, \tag{3.18}$$

kde koeficienty $e^{\frac{2\pi i j k}{2^q}}$ pro taková k, pro která se shodují a_k, mohou v závislosti na j interferovat konstruktivně i destruktivně.

Ukazuje se, že tato interference výrazně potlačí pravděpodobnost naměření všech j kromě takových, které leží v blízkém okolí[26] celočíselných násobků čísla $\frac{2^q}{p}$, kde p je hledaná perioda [10], [13]. Pravděpodobnost naměření špatného výsledku není nulová, pokud tento zlomek není celé číslo, ale je dostatečně malá, abychom opakovaným průběhem algoritmu mohli eliminovat možnost chyby.

Kvůli vlastnostem kvantového měření však nemůžeme ovlivnit, který z těchto násobků dostaneme. Opakovaným průběhem algoritmu však získáme množství těchto čísel již postačující ke zjištění konstanty p.

Všimněme si, že výsledky celého průběhu algoritmu mají pravděpodobnostní charakter. Jako časovou složitost v takových případech musíme uvažovat počet operací potřebných k překonání jisté předem dané hranice pravděpodobnosti úspěchu – v teoretické informatice se uvažuje hranice $\frac{2}{3}$.

Shor ve svém článku udává odhady časové složitosti jednotlivých částí postupu. Důležitá je především informace, že kvantová Fourierova transformace má složitost $O(q^2) = O(n^2)$ (připomeňme, že n je délka vstupu, tedy úměrná $\log N$), což bychom mohli odhadnout z uvedeného rozpisu na řetězec jedno- a dvouqubitových hradel (ta jsou elementární nebo je lze nahradit konstantním počtem elementárních hradel, stačí je tedy spočítat). Tato složitost vynásobená odhady, kolikrát je pro dosažení dostatečné pravděpodobnosti průběh kvantového algoritmu opakovat, dává konečný odhad $O\left(n^2 \log n \log\log n\right)$.

[26] Největší pravděpodobnost mají celá čísla těmto zlomkům nejbližší, již vzdálenost 1 od této zaokrouhlené hodnoty znamená silný pokles pravděpodobnosti.

Kapitola 4
Groverův algoritmus

V této a následující sekci popíšeme dva základní algoritmy použitelné pro řešení zadání označovaného jako vyhledávání v nesetříděné databázi.

V prvním paragrafu nejprve specifikujeme, jak toto zadání bude znít, a shrneme možnosti jeho řešení v klasickém případě. Uvedeme skutečnost, že kvantové algoritmy umožňují při řešení tohoto problému dosáhnout výrazného časového urychlení, což ukážeme v následujících paragrafech na konkrétních příkladech.

Ve zbytku kapitoly popíšeme historicky první vyhledávací algoritmus, jehož autorem je Lov K. Grover (1996). V jednotlivých paragrafech je detailně matematicky prozkoumám průběh algoritmu, diskutovány některé důležité mezní případy a některé odchylky od původního algoritmu, které mohou pomoci k jeho použitelnosti i při upraveném zadání nebo zvýšit jeho efektivitu.

4.1 Zadání vyhledávacího algoritmu

Je dána nějaká konečná, očíslovaná množina prvků a rozhodovací funkce (orákulum), vázaná podmínkou, že její hodnota je 0 na všech prvcích této množiny kromě jednoho, ve kterém je hodnota funkce 1. Tento prvek budeme nazývat označeným a úkolem je samozřejmě opakovanými dotazy na funkční hodnotu najít jeho index. Množina může být obohacena nějakou dodatečnou strukturu, může tedy tvořit například graf, ale tato struktura neposkytuje žádnou informaci usnadňující nalezení řešení, například ve smyslu jeho „blízkosti“.

Jako názorný příklad aplikace tohoto zadání se uvádí (viz např. [18], [19]) obrácené hledání v telefonním seznamu: máme dáno telefonní číslo, o kterém víme, že bude patřit nejvýše jednomu člověku, a chceme najít tento odpovídající záznam. Seznam je setříděn podle abecedy, ale to nám nijak nepomůže, pokud například najdeme jméno, jehož číslo se liší jen v jediné číslici, odhadnout, kde máme hledat dále.

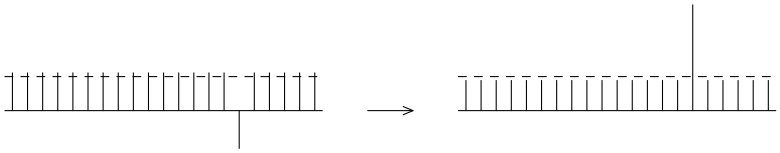
Všimněme si však, že vyslovené zadání nepředpokládá přítomnost žádného objemného paměťového média, které bychom očekávali pod pojmem databáze. Rozhodovací funkce tak musí poskytnout odpověď pouze na základě indexu prvku a veškeré další informace musí být uloženy ve způsobu jejího výpočtu.

Bez použití kvantových algoritmů tak nezbývá jiná možnost, než procházet postupně všechny položky a kontrolovat každou pro shodu. Vzhledem k charakteru tohoto zadání nepřinese vůbec žádné vylepšení ani použití stochastické metody, tj. náhodného výběru dalšího prvku místo procházení po řadě. Uvědomme si, že to je ekvivalentní procházení po řadě po pouhém náhodném proházení prvků. Vzhledem k tomu, že algoritmus se zastaví v okamžiku, kdy náhodně najdeme hledaný prvek, může mít odhad počtu potřebných kroků také jen pravděpodobnostní charakter. V takových případech se u algoritmů uvádí průměrný počet kroků a počet kroků v nejhorším případě, které pro tento postup můžeme odhadnout i intuitivně přibližně na $N/2$, resp. N (N je počet prvků tvořících databázi).

V následujících paragrafech této kapitoly a v kapitole následující ukážeme, že různé kvantové algoritmy mají schopnost za využití kvantové interference řešit tuto úlohu v čase (tedy počtu dotazů na orákulum) úměrném druhé odmocnině z počtu prvků N a navíc s vlastností, že počet kroků bude pro danou velikost seznamu neměnný.

4.2 Popis Groverova algoritmu

Tento algoritmus je navržen k vyhledávání v množině bez jakékoliv dodatečné struktury, tedy v „nesetříděné nestrukturované databázi“. Jeho jádro tvoří jednoduchá, ale mocná myšlenka posilování amplitudy označeného stavu inverzí podle průměru: představme si situaci, že všechny prvky kromě označeného mají stejnou reálnou amplitudu a amplituda označeného prvku je jiné reálné číslo. Jestliže nyní spočítáme aritmetický průměr všech amplitud a následně převrátíme každou z nich na druhou stranu od průměru, pak za jistých podmínek se absolutní hodnota amplitudy označeného prvku zvýší na úkor absolutních hodnot ostatních amplitud. Z jednoduché grafické představy snadno odvodíme, že touto podmínkou je pouze, aby aritmetický průměr ležel mezi nulou a četnější z amplitud.



Obr. 15: Inverze kolem průměru. Jednotlivé prvky grafu jsou detailně popsány v textu.

Velikost databáze, tedy počet prvků prohledávané množiny, je omezen na mocniny dvojky: $N = 2^n$. To umožňuje sestavit n-qubitový systém, jehož bázové stavy budou odpovídat jednotlivým prvkům databáze. Algoritmus bude probíhat tak, že vyjdeme ze stavu, kdy všechny bázové stavy budou mít stejnou amplitudu – o mnoho více nemůžeme obecně požadovat vzhledem k faktu, že nemáme žádné další informace o funkci ani topologii vstupních hodnot. Následně budeme opakovat iteraci sestávající ze dvou kroků: převrácení znaménka amplitudy označeného vstupu a popsaného překlopení podél průměru. Obě tyto operace jsou jistě lineární, odpovídající operátory označme U, resp. D. Jejich další vlastnosti a realizaci pomocí dostupných kvantových hradel ukážeme později. Takto utvořenou iteraci však budeme aplikovat pouze tak dlouho, dokud se absolutní hodnota amplitudy označeného prvku bude zvyšovat – ukážeme, co by se dělo při případných dalších opakováních. Nakonec provedeme úplné měření, jehož výsledkem bude s dostatečně vysokou pravděpodobností právě hledaná vstupní hodnota.

Optimální počet iterací je třeba znát před provedením algoritmu – kvantová mechanika neumožňuje sledovat, jestli už jsme dosáhli dostatečné pravděpodobnosti. Grover ve svém článku dokazuje odhad, že tento počet je třídy $O\left(\sqrt{N}\right)$, existuje však jiný způsob vedení důkazu, uvedený v článku [12] nebo v [3], který umožňuje pro počet iterací najít explicitní vzorec. Předveďme jej i zde.

Počáteční stav označme $|s\rangle = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} |i\rangle$, hledaným vrcholem nechť je bez újmy na obecnosti $|0\rangle$.[27] Difuzní nebo Groverův operátor D je pak možno zapsat ve tvaru

$$D = 2|s\rangle\langle s| - I \tag{4.1}$$

[27] Takový předpoklad zde mnoho zjednodušení nepřinese, ale ve druhém popisovaném algoritmu bude klíčový, je tedy uveden pro jednotnost.

a operátor U jako

$$U = I - 2|0\rangle\langle 0|, \tag{4.2}$$

kde I označuje jednotkový operátor. Ve shodě s Groverovým článkem [18] ukažme nejprve unitatiru obou operací. Pro unitární matici D by muselo platit $D^\dagger D = I$, spočítejme tedy

$$\begin{aligned} D^\dagger D &= (2(|s\rangle\langle s|)^\dagger - I^\dagger)(2|s\rangle\langle s| - I) = (2|s\rangle\langle s| - I)^2 = \\ &= 4|s\rangle\langle s|s\rangle\langle s| - 2|s\rangle\langle s|I - 2I|s\rangle\langle s| + I = 4|s\rangle\langle s| - 2|s\rangle\langle s| - 2|s\rangle\langle s| + I = I. \end{aligned} \tag{4.3}$$

Všimněme si, že tento důkaz nijak nevyužíval toho, který konkrétní projektor je použit na místě $|s\rangle\langle s|$, unitarita U se tedy dokáže zcela stejně.

Dále si všimněme, že vzhledem k tomu, že počáteční stav je $|s\rangle$, žádným provedeným krokem neopustíme reálný lineární obal vektorů $|s\rangle$ a $|0\rangle$. Díky této skutečnosti můžeme pracovat v takovém podprostoru, který má navíc charakter roviny. Před pokračováním odvození však ještě vyřešíme mírně nepřívětivou skutečnost, že vektory $|s\rangle$ a $|0\rangle$ nejsou ortogonální: jejich skalární součin je $\langle s|0\rangle = \frac{1}{\sqrt{N}}$.

Zde můžeme efektivně využít Gramův-Schmidtův ortonormalizační proces. Máme možnost se rozhodnout, který z vektorů v nové bázi ponecháme. Zřejmě nás bude zajímat, jak se bude vyvíjet amplituda $|0\rangle$, nahraďme tedy vektor $|s\rangle$ a výsledek označme $|u\rangle$:

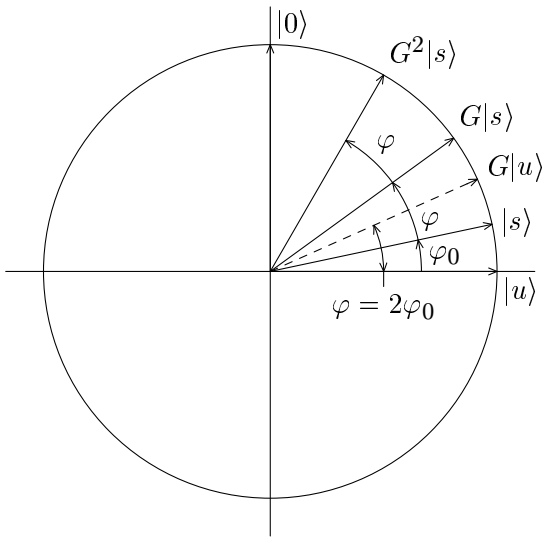
$$|u\rangle = \frac{1}{\||s\rangle - \langle 0|s\rangle|0\rangle\|}(|s\rangle - \langle 0|s\rangle|0\rangle) = \frac{1}{\sqrt{\frac{N-1}{N}}}\left(\frac{1}{\sqrt{N}}\sum_{i=0}^{N-1}|i\rangle - \frac{1}{\sqrt{N}}|0\rangle\right) = \frac{1}{\sqrt{N-1}}\sum_{i=1}^{N-1}|i\rangle. \tag{4.4}$$

Vektory $|u\rangle$ a $|0\rangle$ již tvoří ortonormální bázi pracovního podprostoru. Sestavme tedy izometrii pracovního podprostoru s rovinou, která je identifikuje s jednotkovými vektory ve směru os kartézského systému souřadnic dle obr. 16.

Z lineární algebry víme, že každá ortogonální matice druhého řádu má v rovině buď význam rotace kolem počátku souřadnic o libovolný úhel (v případě, že má determinant $+1$), nebo zrcadlení podle libovolné osy procházející počátkem, pokud má determinant -1. Všimněme si, že operace D i U (zúžené na popsaný podprostor) mají determinant -1 a odpovídají tak zrcadlení. Osou bude v obou případech vlastní podprostor odpovídající vlastnímu číslu 1, což je $[|s\rangle]_\lambda$ pro matici D a $[|u\rangle]_\lambda$ v případě U. Matice odpovídající jedné iteraci $G = DU$ má determinant $+1$ a je tedy tvaru

$$G = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix} \tag{4.5}$$

pro nějaký úhel φ. Ten stačí určit z obrazu libovolného vektoru. Vezměme si tedy pro názornost vektor $|u\rangle$. Protože $U|u\rangle = |u\rangle$, je $G|u\rangle = D|u\rangle$ a $|u\rangle$ se tak zobrazí na vektor, který má dvakrát větší úhel od kladné poloosy než $|s\rangle$. Platí tedy $\varphi = 2\varphi_0$, kde φ_0 je úhel mezi vektory $|u\rangle$ a $|s\rangle$.



Obr. 16: Geometrická reprezentace Groverova algoritmu

Každá provedená iterace tedy zvýší úhel od kladné poloosy o $2\varphi_0$ od počáteční hodnoty φ_0 a úhel po k iteracích je tak roven $(2k+1)\varphi_0$. Cílem Groverova algoritmu je iterace opakovat, dokud amplituda $|0\rangle$ v absolutní hodnotě roste. V této geometrické interpretaci to znamená úhel zvyšovat až k hodnotě $\frac{\pi}{2}$. Následující iterace by totiž amplitudu začaly opět snižovat, až by se přiblížila 0 při úhlu blízkém π, při stále dalším průběhu by se celý proces opakoval.

Optimální počet kroků k_0 by tedy měl splňovat rovnici

$$(2k_0+1)\varphi_0 = \frac{\pi}{2}, \tag{4.6 a}$$

kde pro φ_0 platí $\sin\varphi_0 = \cos(\frac{\pi}{2}-\varphi_0) = \langle s|0\rangle = \frac{1}{\sqrt{N}}$. Z ní určené

$$k_0 = \frac{1}{2}\left(\frac{\pi}{2\varphi_0} - 1\right) \tag{4.6 b}$$

však obecně nebude přirozené číslo, použijeme tedy alespoň co nejbližší počet kroků a tento výsledek zaokrouhlíme. Označíme-li $[x]$ celou část čísla x, bude výsledek podle běžných pravidel zaokrouhlování roven

$$k_0 = \left[\frac{\pi}{4\varphi_0}\right]. \tag{4.6 c}$$

Vzorec můžeme ještě zjednodušit, aproximujeme-li arkussinus ve vzorci $\varphi_0 = \arcsin\frac{1}{\sqrt{N}}$ jeho argumentem. Při menších hodnotách N by se taková aproximace mohla zdát příliš hrubá, ale přímým výpočtem několika prvních odpovídajících hodnot zjistíme, že nový vzorec

$$k_0 = \left[\frac{\pi}{4}\sqrt{N}\right] \tag{4.7}$$

dává stejný výsledek pro každé přirozené N.

Toto odvození nám umožňuje určit i spodní hranici pro pravděpodobnost naměření hledaného vrcholu po tomto optimálním počtu provedených iterací. Vzhledem k platnosti přesného (neaproximovaného) vzorce můžeme s jistotou prohlásit, že úhel $(2k_0+1)\varphi_0$ bude ležet v rozmezí $\langle\frac{\pi}{2}-\varphi_0, \frac{\pi}{2}+\varphi_0\rangle$. Pravděpodobnost naměření stavu $|0\rangle$ pak bude

$$P = \cos^2\left(\frac{\pi}{2} - (2k_0+1)\varphi_0\right) = 1 - \sin^2\left(\frac{\pi}{2} - (2k_0+1)\varphi_0\right) \geq 1 - \sin^2\varphi_0 = 1 - \frac{1}{N}. \tag{4.8}$$

4.3 Groverův algoritmus v krajních případech

Z posledního uvedeného odhadu plyne, že čím větší je databáze, kterou prohledáváme, tím větší pravděpodobnost naměření hledaného vrcholu máme zaručenu. Cílem tohoto paragrafu je naopak popsat, jak se Groverův algoritmus chová při velice malých hodnotách n (připoměňme $N = 2^n$).

Matice Groverova operátoru pro případ $n = 1$ (hledání hodnoty jednoho vstupního bitu) je Pauliho matice X. V každém kroku se tedy změní znaménko amplitudy hledané hodnoty, a poté se amplitudy stavů $|0\rangle$ a $|1\rangle$ zamění. Nedochází tak k žádné interferenci a tedy ani k žádným změnám pravděpodobnosti naměření kterékoliv z hodnot oproti původnímu stavu $|+\rangle$ a Groverův algoritmus je zde zcela nepoužitelný.

Případ $n = 2$ je zcela výjimečný – Groverův algoritmus umožní naměřit správnou hodnotu s jistotou, tedy s nulovou pravděpodobností nesprávné odpovědi, a to po pouhé jediné provedené iteraci. Dosazením do vzorců odvozených výše totiž zjistíme

$$\sin \varphi_0 = \frac{1}{2}, \tag{4.9}$$

tedy $\varphi_0 = \frac{\pi}{6}$ a po jedné iteraci $\varphi = (1 + 2\,.\,1)\frac{\pi}{6} = \frac{\pi}{2}$, což je úhel odpovídající stavu $|0\rangle$. Tento příklad se často uvádí jako ukázka síly kvantových algoritmů – postačilo nám jednou „vyhodnotit“ funkci f, abychom mezi čtyřmi možnými vstupy našli jeden označený. To je v případě klasických algoritmů samozřejmě zcela nepředstavitelné.[28]

Ukážeme, že při žádném vyšším n již nemůže nastat situace, že by po optimálním počtu kroků amplitudy všech bázových stavů kromě hledaného klesly na nuly. Za tímto účelem si představme obr. 16 jako Gaussovu rovinu, tedy sestrojme izomorfismus reálného lineárního obalu vektorů $|u\rangle$ a $|0\rangle$ s prostorem komplexních čísel nad $\mathbb{R}$ daný vztahy $|u\rangle \mapsto 1$ a $|0\rangle \mapsto i$. Vektor $|s\rangle$ se přenese na číslo

$$s = \sqrt{1 - \frac{1}{N}} + \frac{1}{\sqrt{N}} i \tag{4.10}$$

a vektor odpovídající k provedeným iteracím na s^{2k+1}. Abychom dosáhli stavu $|0\rangle$, požadujme, aby s^{2k+1} mělo nulovou reálnou část. Rozepišme jej tedy podle binomické věty:

$$s^{2k+1} = \sum_{l=0}^{2k+1} \binom{2k+1}{l} \sqrt{1 - \frac{1}{N}}^{l} \sqrt{N}^{-(2k+1-l)}\ i^{2k+1-l} \tag{4.11 a}$$

K reálné části zřejmě budou přispívat jen členy určené lichými hodnotami l, ponechme tedy pouze takové a přepišme l na $2m + 1$, kde m bude novým sčítacím indexem:

$$\begin{aligned} \operatorname{Re} s^{2k+1} &= \sum_{m=0}^{k} \binom{2k+1}{2m+1} \sqrt{1 - \frac{1}{N}}^{2m+1} \sqrt{N}^{2m-2k}\ i^{2k-2m} = \\ &= \sum_{m=0}^{k} \binom{2k+1}{2m+1} \sqrt{1 - \frac{1}{N}} \left(1 - \frac{1}{N}\right)^{m} N^{m-k}\ (-1)^{k-m} \end{aligned} \tag{4.11 b}$$

[28] Kvantové „vyhodnocení“ však, jak důsledně upozorňují autoři článku [20], znamená dva průchody klasickou implementací funkce f ve smyslu paragrafu 2.5, tedy v podstatě dvě vyhodnocení klasická. To se obvykle nedodává.

Pravdivost výroku, že tento výraz je nulový, se jistě nezmění, vynásobíme-li jej nenulovým číslem závislým pouze na N a k. Takovou úpravou můžeme získat nutnou podmínku

$$\sum_{m=0}^{k} \binom{2k+1}{2m+1} (N-1)^m \, (-1)^m = 0 \tag{4.11 c}$$

Všechny členy dané m většími než 0 jsou násobky některé kladné mocniny $N-1$. Aby se celý výraz mohl rovnat 0, musí tedy být i první člen dělitelný $N-1$. Tímto členem je přitom pouze číslo $2k+1$, požadujeme tedy

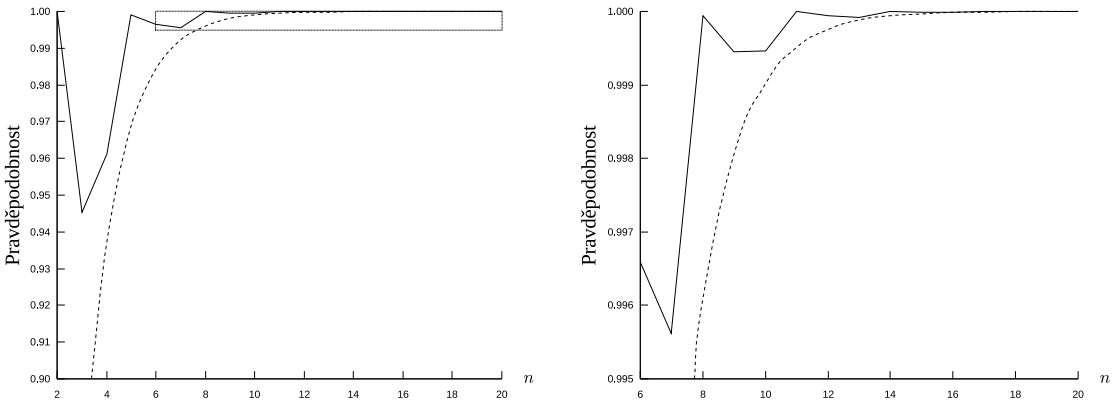
$$N-1 \Big/ 2k+1. \tag{4.11 d}$$

Protože však obě čísla jsou kladná, musí platit $2k+1 \geq N-1$. Tento spodní odhad je však pro $n > 2$ v rozporu s horním odhadem pro optimální počet kroků (4.7) (o horní odhad se jedná proto, že $[x] \leq x$):

$$\begin{aligned} \frac{\pi}{4}\sqrt{N} &\geq k_0 \\ \frac{\pi}{2}\sqrt{N} + 1 \geq 2k_0 + 1 &\geq N-1 \\ \frac{\pi}{2}\sqrt{N} &\geq N-2 \\ \frac{\pi}{2} \geq \sqrt{N} - \frac{2}{\sqrt{N}} \geq \sqrt{N} - 1 &= 2^{\frac{n}{2}} - 1 \end{aligned} \tag{4.12}$$

Snadno ověříme, že pro $n > 2$ je $2^{\frac{n}{2}} - 1 > \frac{\pi}{2}$, což je hledaný spor.

Pro vyšší n již tedy žádné zvláštní případy nenastávají. Pravděpodobnost dostatečně blízkou jednotce však zajistí odhad $P \geq 1 - \frac{1}{2^n}$:



Obr. 17: Groverův algoritmus: pravděpodobnost naměření hledaného vrcholu po optimálním počtu iterací. Vpravo je zvětšený výsek s jemnějším měřítkem svislé osy. Čárkovaně je znázorněn spodní odhad $1 - 2^{-n}$.

4.4 Variace Groverova algoritmu

Groverův algoritmus je použitelný i v případě, že vyhledávacímu kritériu vyhovuje více než jeden z prvků databáze, musíme však vědět předem, kolik takových existuje. Označme tento počet t a množinu všech označených prvků T.

Odvození provedeme zcela analogicky jako v předchozím paragrafu. Vektor $|0\rangle$ však nahradíme vektorem

$$|t\rangle = \frac{1}{\sqrt{t}} \sum_{i \in T} |i\rangle. \tag{4.13}$$

Skalární součin $\langle s|t\rangle$ je roven

$$\frac{1}{\sqrt{Nt}} t = \sqrt{\frac{t}{N}}, \tag{4.14}$$

vektor $|u\rangle$ získaný ortonormalizačním procesem tedy

$$|u\rangle = \frac{1}{\sqrt{N-t}} \sum_{\substack{i=0 \\ i \notin T}}^{N-1} |i\rangle. \tag{4.15}$$

Všechny následující úvahy mohou po této náhradě zůstat nezměněny s tím, že $\sin\varphi_0 = \langle s|t\rangle = \sqrt{\frac{t}{N}}$, vzorec pro optimální počet kroků se tedy změní pouze na

$$k_0 = \frac{\pi}{4}\sqrt{\frac{N}{t}}. \tag{4.16}$$

Jiné silné zobecnění Groverova algoritmu uvádí článek [21]. V něm autoři definují obecný algoritmus pro posilování amplitudy označených stavů a později zobecní i operátory D a U tak, že amplituda $|s\rangle$, resp. $|t\rangle$ se může násobit i jinou komplexní jednotkou než -1. Operátory používané v Groverově algoritmu jsou podle této logiky jednotkovému operátoru „nejvzdálenější“, takže takováto úprava může zvětšit počet potřebných iterací. Její vhodnou volbou však můžeme dosáhnout jistoty naměření hledaného vrcholu tak, že „zpomalíme“ poslední iteraci, čímž v uvedené geometrické reprezentaci dosáhneme finálního natočení o potřebný úhel menší než φ.

Takovou úpravu uvádí na konkrétním příkladě článek [22]: zde se uvažuje pouze vyhledávání s více označenými prvky. Jestliže tvoří právě jednu čtvrtinu ze všech prvků databáze, naměříme s jistotou jeden z nich právě po jedné iteraci, stejně jako v původním algoritmu pro $N = 4$. Jestliže je však označených prvků ještě více, vychází nezaokrouhlená hodnota k_0 menší než 1 a již provedením první iterace by se stavový vektor dostal za optimální hranici. Zpomalením této jedné iterace způsobem uvedeným v předchozím odstavci však můžeme zajistit výsledek stejný jako v případě $t = \frac{N}{4}$.

4.5 Realizace hradel v Groverově algoritmu

Podobně jako v případě Shorova algoritmu by bylo třeba ještě ukázat, jak je možno operátory D a U realizovat pomocí jednodušších kvantových hradel.

Připomeňme, že operátor D je roven $2|s\rangle\langle s| - I$, kde $|s\rangle$ je rovnocenná superpozice všech stavů $|i\rangle_{i=0}^{2^n-1}$. Dále dle paragrafu 2.3 je $|s\rangle$ obrazem $|0\rangle$ při Walsh-Hadamardově transformaci $H^{\otimes n}$ a platí $(H^{\otimes n})^2 = I$. Pro dosažení akce operátoru D, fázového posunu složky odpovídající ortogonální projekci do podprostoru $[|s\rangle]_\lambda$ vůči projekci do jeho ortogonálního doplňku, tedy

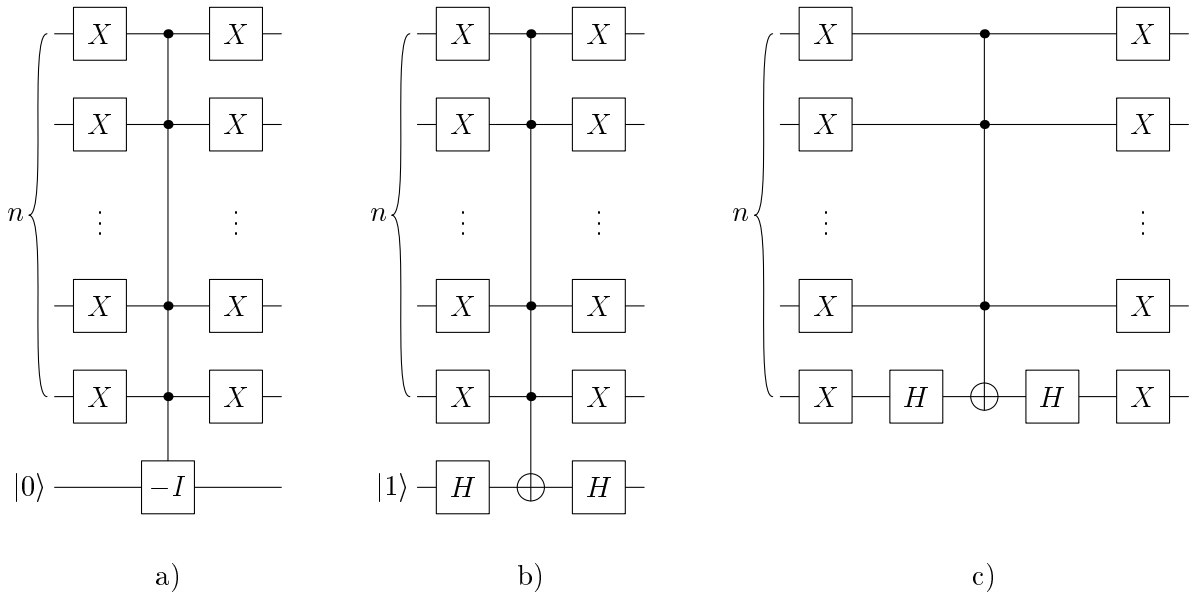
stačí ekvivalentně totéž udělat s ortogonální projekcí do podprostoru $[|0\rangle]_l$ a tuto operaci z obou stran obložit operátory $H^{\otimes n}$:

$$D = 2|s\rangle\langle s| - I = H^{\otimes n}(2|0\rangle\langle 0| - I)H^{\otimes n} \tag{4.17}$$

Dále využijeme možnosti zanedbat globální fázi vektoru, díky níž je hradlo $2|0\rangle\langle 0| - I$ fyzikálně ekvivalentní hradlu $I - 2|0\rangle\langle 0|$. Tím jsme úlohu převedli na problém konstrukce hradla, které na všechny bázové vektory kromě $|0\rangle$ působí jako jednotkový operátor a vektoru $|0\rangle$ změní znaménko. To se velice podobá jednobitovému hradlu $-I$ řízenému současně negacemi všech qubitů, jak ukazuje obr. 18 a) (připomeňme, že pro změnu znaménka stavového vektoru postačí změnit znaménko libovolného činitele v tenzorovém součinu), toto hradlo se liší potřebou jednoho pomocného qubitu.

Řízené hradlo $-I$ je však stále vzdálené množině univerzálních hradel. Abychom se více přiblížili hradlům popsaným v paragrafu 2.3, ukážeme, že jsme jej schopni nahradit řízeným hradlem X, které můžeme nazvat *zobecněné Toffoliho hradlo*. Změna znaménka totiž nastane při působení X na vektor $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, protože je vlastním vektorem X příslušejícím vlastnímu číslu -1. Stačí tedy pomocný qubit předpokládat připravený ve stavu $|1\rangle$ a aplikovat na něj Hadamardovo hradlo (dvakrát kvůli navrácení do původního stavu).

Rozumnou úvahou však můžeme ušetřit i potřebu pomocného qubitu. Stejně jako $|-\rangle = H|1\rangle$ je vlastním vektorem X příslušejícím vlastnímu číslu -1, je $|+\rangle = H|0\rangle$ vlastním vektorem příslušejícím vlastnímu číslu 1. Kdybychom tedy v obr. 18 b) předpokládali pomocný qubit připravený ve stavu $|0\rangle$, celý zobrazený obvod by představoval jednotkový operátor. Všimněme si, že místo pomocného qubitu tak lze použít kterýkoliv z n původních qubitů po operaci X: změna znaménka nastane pouze tehdy, když byl před operací X ve stavu $|0\rangle$ a všechny ostatní, řídicí, qubity také. To je ovšem přesné znění původního zadání. Výsledný náhradní obvod pro $I - 2|0\rangle\langle 0|$ tedy ukazuje obr. 18 c).



Obr. 18: Realizace Groverova operátoru pomocí univerzálních hradel –
– odvození náhradního obvodu pro pomocný operátor $I - 2|0\rangle\langle 0|$

Dále ukážeme, jak je možno zobecněné Toffoliho hradlo, použité na obr. 18 c), realizovat pomocí „běžného“ Toffoliho hradla, které již budeme považovat za elementární (jeho přepis

pomocí univerzálních kvantových hradel ukazuje obr. 11 v paragrafu 2.4). Jedná se o operaci řízenou hodnotou $(n-1)$-bitové výrokové formy, což jsme schopni obecně realizovat postupem naznačeným v paragrafu 2.5. Představíme řešení ukázané v [12], které tento postup v podstatě přesně sleduje a potřebuje $n-2$ pomocných qubitů připravených ve stavech $|0\rangle$. Pro přehlednost jej výjimečně popíšeme slovy.

V prvním Toffoliho hradle použijeme 1. a 2. qubit jako řídící a 1. pomocný qubit jako cílový. Protože byl ve stavu $|0\rangle$, jeho stav bude následně $|x_1 \text{ AND } x_2\rangle$, kde $|x_1\rangle$, resp. $|x_2\rangle$ jsou stavy 1., resp. 2. qubitu. Nyní použijeme tento qubit a 3. z původní sady jako řídicí a další pomocný jako cílový pro druhé Toffoliho hradlo. Stav druhého pomocného qubitu pak bude $|x_1 \text{ AND } x_2 \text{ AND } x_3\rangle$. K tomuto výsledku opět „přidáme“ 4. qubit a tak dále, až po $n-2$ krocích (Toffoliho hradlech) bude poslední pomocný qubit ve stavu odpovídajícímu konjunkci všech původních hodnot, které jsme chtěli použít jako řídicí. Nyní tedy postačí tento qubit použít jako řídicí pro hradlo CNOT a následně všechny pomocné operace provést znovu v opačném pořadí pro návrat pomocných qubitů do původních stavů.[29]

Operátor U je v Groverově algoritmu orákulem. Má opět charakter výrokové formy, při jejímž splnění požadujeme změnu znaménka odpovídajícího bázového stavu. Způsobem popsaným v paragrafu 2.5 jsme za pomoci nějakého počtu pomocných qubitů tento problém převést až na změnu znaménka řízenou jedním qubitem, o které podobnou úvahou jako při odvození obr. 18 b) zjistíme, že je ji možno realizovat pomocí hradla CNOT a jednoho pomocného qubitu. Podobné zjednodušení jako u obr. 18 c) pochopitelně již možné není.

Z uvedeného postupu je zřejmé, že pro realizaci hradla D budeme potřebovat $O(n)$ univerzálních kvantových hradel. Definice hradla U nemá n jako parametr, proto pro ni nemá smysl tvořit žádný podobný odhad. Již toto však znamená, že ve smyslu počtu provedených univerzálních hradel nebude časová složitost Groverova algoritmu $O\left(2^{\frac{n}{2}}\right)$, ale $O\left(n2^{\frac{n}{2}}\right)$. Číslo n je však úměrné pouze logaritmu počtu prvků databáze N, takže odhad se „příliš nezhoršil“. Nový odhad můžeme označit $\tilde{O}\left(\sqrt{N}\right)$, kde $\tilde{O}(f(n))$ znamená $O(f(n)p(\log f(n)))$ pro nějaký polynom p [12].

4.6 Vztah Groverova algoritmu a problému nerozlišitelnosti neortogonálních stavů

Na závěr sekce o Groverově algoritmu uveďme následující drobnou úvahu.

Při přemýšlení o posilování amplitudy vyhledávaného stavu by mohlo nastat podezření, zda zvyšování pravděpodobnosti naměření správného výsledku není ve sporu v poučkou, že žádné měření nemůže spolehlivě odlišit blízké stavy. Je však třeba si povšimnout, že v Groverově algoritmu žádný pokus o takové měření nepoužíváme. Při hledání označeného vstupu provádíme zcela běžné projektivní měření v bázi $\{|i\rangle\}_{i=0}^{N-1}$ a ve skutečnosti se snažíme rozlišit mezi málo odlišnými unitárními operacemi, které k měřenému stavu vedly od původního stavu $|s\rangle$.

[29] Pozorný čtenář si jistě povšimne, že jeden pomocný qubit je možno ještě ušetřit – poslední pomocné Toffoliho hradlo může působit již na cílový qubit. Postup se zkrátí o použití hradla CNOT a opakování tohoto Toffoliho hradla.

Kapitola 5
Prohledávání, sítě a náhodné chození

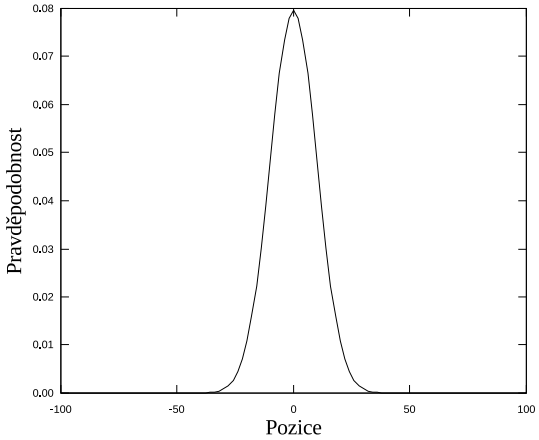
Tato sekce popisuje kvantovou obdobu k zajímavému principu využívanému v některých klasických algoritmech: náhodnému procházení. První paragraf shrnuje popis a základní poznatky o náhodné procházce na přímce, druhá navrhuje kvantovou obdobu tohoto algoritmu. Ukazuje se však, že výsledky obou přístupů jsou radikálně odlišné. Kvantová náhodná procházka má především vlastnost mnohem rychlejšího dosažení kterékoliv polohy – této vlastnosti je možno využít pro jiný přístup k řešení problému vyhledávání v nesetříděné databázi. Od třetího paragrafu dále je tedy popisován kvantový vyhledávající algoritmus využívající tento přístup a některé jeho variace.

5.1 Náhodné procházení

Náhodná procházka je postup, při kterém sledujeme pohyb objektu po vrcholech nějakého grafu. Pohyb se děje po krocích – v každém kroku objekt přejde právě po jedné hraně vycházející z vrcholu, ve kterém právě stojí, přičemž výběr z možných hran je prováděn náhodně. Jako příklad může posloužit „hra“, při které „hráč“ chodí po přímce tak, že hází mincí a podle výsledku hodu postoupí buď jeden krok dopředu nebo nazpět.

Jestliže nasimulujeme množství takových náhodných procházek po přímce, vycházejících ze stejného bodu, a vždy po daném počtu kroků N označíme aktuální polohu objektu, získáme pravděpodobnostní rozdělení. Toto rozdělení bude omezené na interval $\langle -N, N \rangle$, tyto hranice odpovídají konstantnímu pohybu v jednom směru. Dále každá druhá poloha bude mít nulovou pravděpodobnost: díky tomu, že v každém okamžiku je třeba udělat právě jeden krok, po každé iteraci se změní parita polohy. Po sudém počtu kroků jsou tedy nedosažitelné polohy, jejichž vzdálenost od počátečního místa je lichá, a naopak.

V obr. 19 jsou tedy vyznačeny a propojeny jen polohy s nenulovou pravděpodobností. Toto pravděpodobnostní rozdělení připomíná tvarem Gaussovo rozdělení, které je jeho limitním případem (jedná se o tzv. binomické rozložení).



Obr. 19: Pravděpodobnostní rozdělení koncových bodů klasické náhodné procházky po přímce po 100 iteracích

Dobrou mírou otázky, jak daleko se při náhodném procházení objekt dostane po N krocích, je střední kvadratická odchylka tohoto rozdělení. Ta je v tomto případě přímo rovna odmocnině z počtu kroků.

5.2 Kvantové náhodné procházení

Kvantovou obdobou tohoto základního příkladu se zabývá mnoho prací, např. [19], [23] nebo [24]. Intuitivně bychom mohli předpokládat, že poloze na přímce budou odpovídat bázové stavy $|i\rangle, i \in \mathbb{Z}$ nekonečněrozměrného stavového prostoru, že náhodný výběr bude možno nahradit utvořením superpozice možných výsledků a náhodnost že ponecháme procesu měření. Snadno se však ukáže, že požadavkům unitarity, symetrie vůči posunutí po přímce a tomu, aby obrazem každého bázového stavu byla lineární kombinace pouze dvou přilehlých, vyhovují jen triviální případy operací, které představují pohyb pouze v jednom směru. Toto zjištění je v literatuře označováno jako „No-Go Lemma“ (podrobnější popis a diskuse mnohem volnějších předpokladů viz [25]).

Řešením tohoto problému je umožnit závislost této operace ještě na výsledku předchozího „hodu“.[30] To se realizuje tak, že výše uvedený stavový prostor rozšíříme tenzorovým součinem ještě o prostor „mince“ $\mathcal{H}_C = \mathbb{C}^2$. Jedna iterace pak bude tvaru

$$U = SC, \tag{5.1}$$

kde C je nějaká unitární operace působící pouze na prostoru mince $\mathcal{H}_C$, $C = I \otimes C_1$. C_1 budeme uvažovat jako matici z prostoru $\mathbb{C}^{2,2}$ a dále vektory standardní báze $\mathcal{H}_C$ označíme $|\rightarrow\rangle$ a $|\leftarrow\rangle$.

Operaci S definujeme pomocí její akce na bázové vektory celého prostoru $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_C$:

$$\begin{aligned} S|n\rangle|\rightarrow\rangle &= |n+1\rangle|\rightarrow\rangle \\ S|n\rangle|\leftarrow\rangle &= |n-1\rangle|\leftarrow\rangle \end{aligned} \tag{5.2}$$

Jak bylo řečeno v úvodu práce, přesnou korektnost takového vyjádření a definici unitárního zobrazení v nekonečnědimenzionálním prostoru nebudeme diskutovat.

Matice C_1 je omezena pouze požadavkem unitarity a jejímy různými volbami můžeme dosáhnout různých průběhů algoritmu. Nejblíže analogii s původním, klasickým příkladem se dostaneme v případě, kdy absolutní hodnoty jejích prvků budou stejné, tj. $\frac{1}{\sqrt{2}}$. Algoritmus by totiž tehdy na klasický případ zkolaboval, kdybychom po každé iteraci provedli úplné měření stavu.[31] Příkladem matice splňující zmíněné požadavky je Hadamardova matice

$$C_1 = H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \tag{5.3}$$

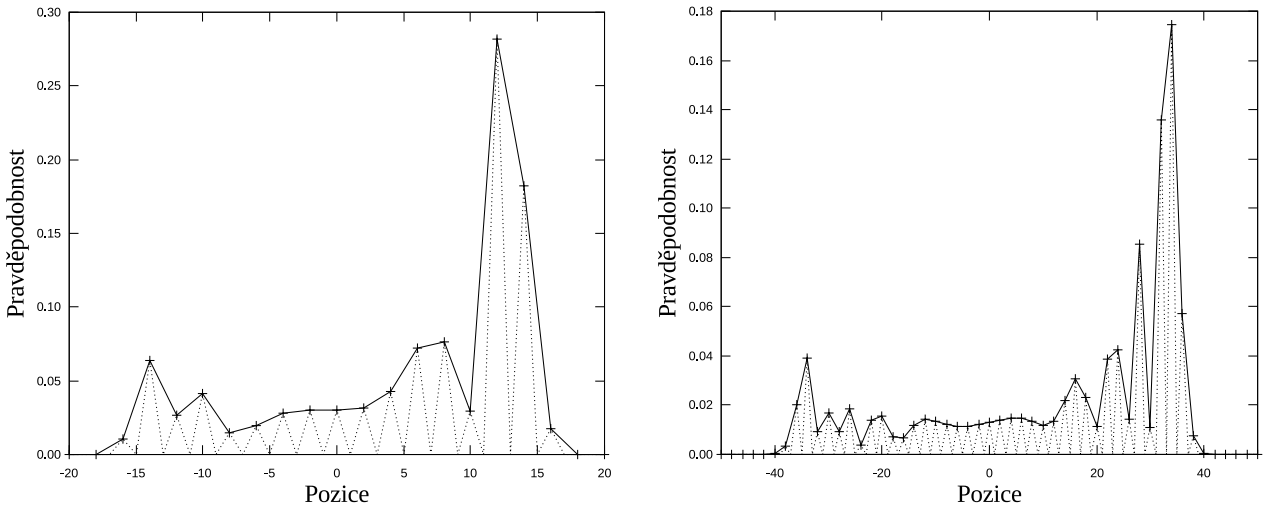
podle které se počáteční stav $|0\rangle|\rightarrow\rangle$ bude vyvíjet následovně:

$$\begin{gathered} \tfrac{1}{\sqrt{2}}(|1\rangle|\rightarrow\rangle + |-1\rangle|\leftarrow\rangle) \\ \tfrac{1}{2}(|2\rangle|\rightarrow\rangle + |0\rangle|\leftarrow\rangle + |0\rangle|\rightarrow\rangle - |-2\rangle|\leftarrow\rangle) \\ \tfrac{1}{2\sqrt{2}}(|3\rangle|\rightarrow\rangle + |1\rangle|\leftarrow\rangle + 2|1\rangle|\rightarrow\rangle - |-1\rangle|\rightarrow\rangle + |-3\rangle|\leftarrow\rangle) \\ \dots \end{gathered} \tag{5.4}$$

[30] Autorem argumentu No-Go je přímo autor zmíněného článku [25], uvedené řešení se připisuje J. Watrousovi [26]

[31] Stejného výsledku můžeme snáze dosáhnout měřením na prostoru $\mathcal{H}_C$ vždy mezi operacemi C a S.

Kdybychom po první nebo druhé iteraci provedli měření na prostoru $\mathcal{H}_S$, nepozorovali bychom žádný rozdíl vůči klasickému příkladu. Ve třetím řádku se však začíná projevovat asymetrie v pravděpodobnostech naměření $|1\rangle$ a $|-1\rangle$. Amplitudy ve směru „od nuly“ totiž v jednom případě zinterferovaly konstruktivně a v jednom destruktivně. Obr. 20 ukazuje pravděpodobnostní rozdělení po větším počtu iterací, jmenovitě 20 a 50.



Obr. 20: Průběh pravděpodobnosti při kvantové náhodné procházce po přímce po 20 a 50 iteracích

Na první pohled je zřejmé, že toto pravděpodobnostní rozdělení nijak nepřipomíná klasické binomické rozložení, předvedené na obr. 19. Zachovává se však argument s mezemi $-N$ až N, určenými N-násobným provedením operátoru S, a podmínka parity polohy. Proto je v obr. 20 spojen plnou čarou až každý druhý bod. V následujících ilustracích již vynechané body nebudou uvažovány. Všimněme si však, že i v hrubším měřítku je propojující čára silně zvlněna.

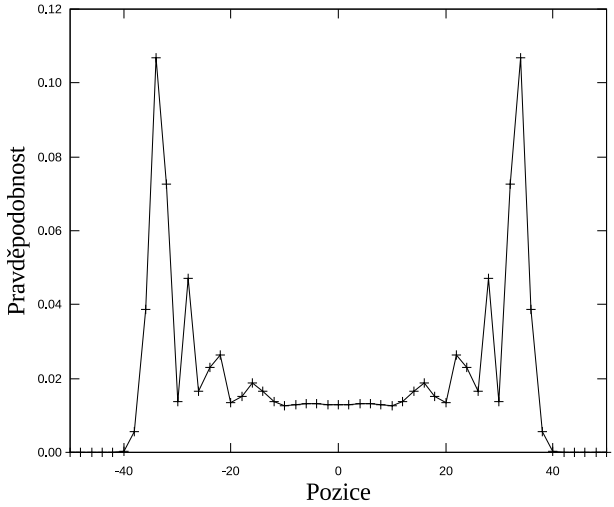
Při odhlédnutí od této nepravidelnosti ukazuje rozdělení dva výrazné vrcholy, které se od sebe navzájem vzdalují s rostoucím počtem iterací zhruba lineární rychlostí. Tyto vrcholy leží přibližně na polohách $\pm\frac{1}{\sqrt{2}}N$ (např. ± 34 pro $N = 50$, ± 702 pro $N = 1000$). Rozdělení je navíc asymetrické, vrchol na pravé straně obr. 20 je mnohem vyšší než vrchol vlevo. Pravděpodobnost za hranicí těchto vrcholů je až ke dříve zmíněné hranici $\pm N$ nenulová, ale velice silně tlumená.

Díky tvaru a popsaným vlastnostem rozdělení roste lineární rychlostí i střední kvadratická odchylka. Toto je důležitý rozdíl oproti klasickému případu, protože daná poloha je s dostatečnou pravděpodobností dosažena v kvadraticky kratším čase než u klasické náhodné procházky. V následujícím paragrafu ukážeme, jak kvantová náhodná procházka na jiném grafu využije podobné vlastnosti k podobnému urychlení řešení vyhledávacího problému, jako poskytuje Groverův algoritmus.

S počáteční podmínkou $|0\rangle|\leftarrow\rangle$ by situace byla podobná jako s původně uvažovaným počátečním stavem $|0\rangle|\rightarrow\rangle$, pravděpodobnostní rozložení by bylo jen zrcadlově otočené vzhledem k poloze odpovídající $|0\rangle$. Vzhledem k tomu, že ani jeden případ neopustí reálný lineární obal bázových vektorů $\mathcal{H}$, můžeme volbou počáteční podmínky

$$\frac{1}{\sqrt{2}}(|0\rangle|\rightarrow\rangle + i|0\rangle|\leftarrow\rangle) \tag{5.5}$$

dosáhnout současné existence obou pozorovaných jevů s prostým součtem pravděpodobností, jak ukazuje obr. 21.

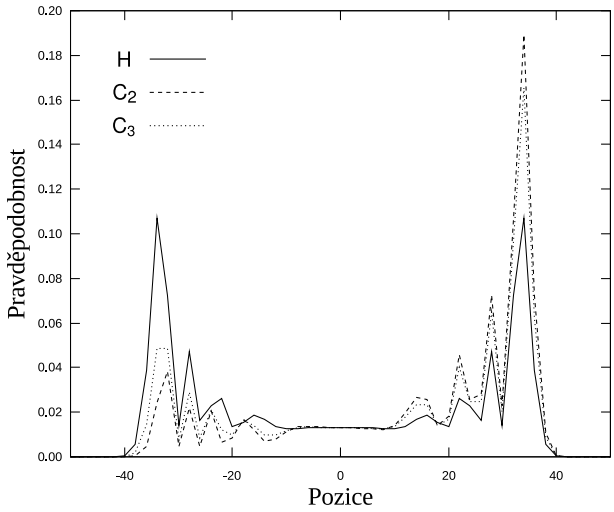


Obr. 21: Průběh pravděpodobnosti při kvantové náhodné procházce na přímce –
– symetrická počáteční podmínka, 50 iterací

Velice zajímavé je, že celkový charakter výsledku příliš nezávisí na volbě matice C_1, pokud je splněna podmínka stejných absolutních hodnot jejích prvků: obr. 22 ukazuje případy

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad C_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \quad C_3 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{2}(i+1) \\ \frac{-1}{\sqrt{2}} & \frac{1}{2}(i+1) \end{pmatrix} \tag{5.6}$$

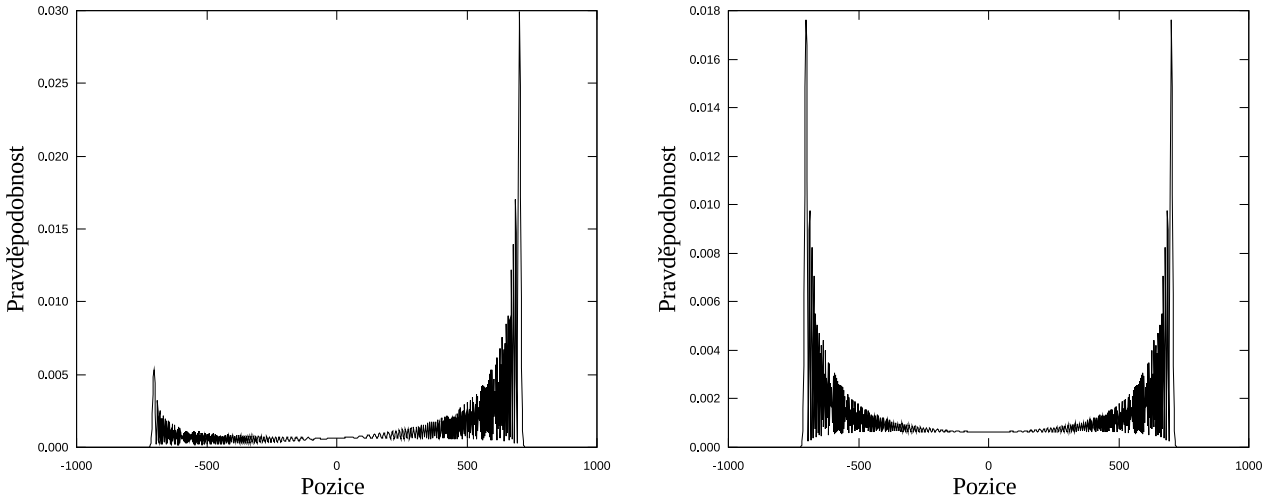
se stejnou volbou počátečního stavu $\frac{1}{\sqrt{2}}(|0\rangle|{\rightarrow}\rangle + i|0\rangle|{\leftarrow}\rangle)$. Všimněme si však, že na této volbě závisí, zda daná počáteční podmínka povede k symetrickému nebo asymetrickému vývoji.



Obr. 22: Výsledky různé volby matice C po 50 iteracích

Pro zajímavost ukažme ještě, jak pravděpodobnostní rozdělení vypadá po značně velkém

počtu iterací:



Obr. 23: Průběh pravděpodobnosti pro $C_1 = H$ a $N = 1000$
při nesymetrické a symetrické počáteční podmínce

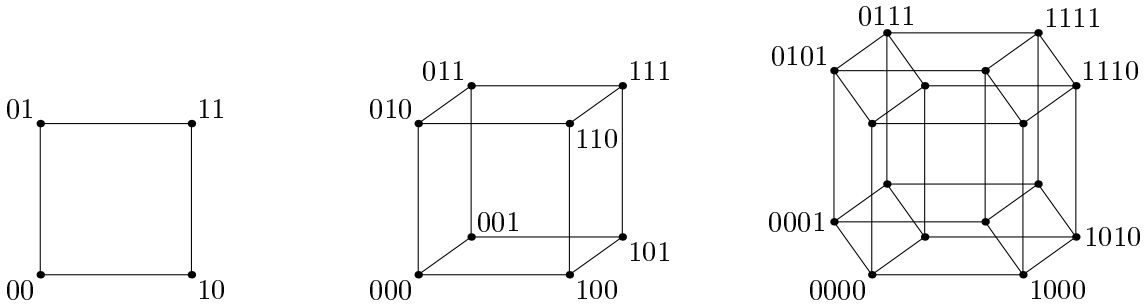
5.3 Vyhledávání na hyperkrychli

Myšlenku kvantových náhodných procházek je možno aplikovat ve vyhledávacích algoritmech. Dobře prozkoumán [27] je algoritmus určený k řešení podobného zadání jako Groverův algoritmus – vyhledávání v nesetříděné databázi o velikosti $N = 2^n$. Tentokráte však budeme předpokládat, že prvky jsou uspořádany do vrcholů n-rozměrné hyperkrychle. Jedná se tedy o databázi mající nějakou vnitřní strukturu, která ale nalezení označeného vrcholu nijak neusnadňuje.

Na vrcholech hyperkrychle, kterým opět přiřadíme význam bázových vektorů $\{|i\rangle\}_{i=0}^{N-1}$ stavového prostoru n qubitů, nyní však ve shodě s obr. 24, necháme probíhat kvantovou náhodnou procházku. Stejně jako v případě přímky využijeme pomocný prostor $\mathcal{H}_C$, který však zde bude mít dimenzi n a operace S bude definována vztahy

$$S|i\rangle|d\rangle = |i \oplus 2^d\rangle|d\rangle \quad \text{pro každé } i \in \{0, 1, \ldots, N-1\}, d \in \{0, 1, \ldots, n\}. \tag{5.7}$$

Značka $\oplus$ zde znamená XOR po bitech, předchozí řádek má tedy význam negace d-té číslice n ve dvojkové soustavě čili krok po přilehlé hraně rovnoběžné s $(d+1)$-tou souřadnou osou.



Obr. 24: Hyperkrychle dimenzí 2, 3 a 4. Vrcholy jsou popsány řetězci n bitů –
– dva vrcholy jsou spojeny hranou právě tehdy, když se liší právě v jednom bitu.

U bázových vektorů $\mathcal{H} = \mathcal{H}_S \otimes \mathcal{H}_C$ tak budeme mluvit o *prostorové* a *směrové části*. Operace C bude v tomto vyhledávacím algoritmu nadále působit pouze na směrovou část vektoru, ale nebude již tvaru $I \otimes C_1$: v různých vrcholech necháme působit různé „mince". Pro všechny vrcholy kromě označeného volíme minci, která má stejnou matici jako difuzní operátor D pro $N = n$:

$$C_1 = 2|s_d\rangle\langle s_d| - I = \begin{pmatrix} \frac{2}{n} - 1 & \frac{2}{n} & \cdots & \frac{2}{n} \\ \frac{2}{n} & \frac{2}{n} - 1 & \cdots & \frac{2}{n} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{2}{n} & \frac{2}{n} & \cdots & \frac{2}{n} - 1 \end{pmatrix}, \tag{5.8}$$

$$|s_d\rangle = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle, \tag{5.9}$$

v označeném vrcholu pak pouze $C_2 = -I$. Celkově tedy

$$C = I \otimes C_1 - |i_0\rangle\langle i_0| \otimes (C_1 + I) \tag{5.10}$$

Počáteční stav algoritmu je rovnocenná superpozice všech bázových stavů $\mathcal{H}$:

$$|\psi_0\rangle = \frac{1}{\sqrt{Nn}} \sum_{i=0}^{N-1} \sum_{d=0}^{n-1} |i\rangle|d\rangle. \tag{5.11}$$

Na tento stav budeme podobně jako u Groverova algoritmu aplikovat předem daný počet iterací tvaru $U = SC$, představujících průběh kvantové náhodné procházky. Poté provedeme měření na prostoru $\mathcal{H}_S$. Ukazuje se, že kvantová náhodná procházka spolu s vhodně zvoleným počtem iterací opět zajistí zvýšenou pravděpodobnost naměření označeného vrcholu.

Řešení průběhu algoritmu se dá, podobně jako u Groverova algoritmu, značně zjednodušit. Předpokládejme opět, že hledaným vrcholem je $|0\rangle$ – toho můžeme vždy dosáhnout vhodným přeznačením vrcholů (za dodržení popsaných pravidel). Jestliže přiřadíme nějaké označení rovnocenným superpozicím bázových stavů $\mathcal{H}$ majících stejnou Hammingovu váhu prostorové části (tedy vzdálenost od hledaného vrcholu v počtu kroků po hranách hyperkrychle) a směrovou část odpovídající při operaci S buď zvýšení nebo snížení Hammingovy váhy, ukážeme, že po celý průběh algoritmu stavový vektor opět neopustí (reálný) lineární obal tohoto souboru vektorů.

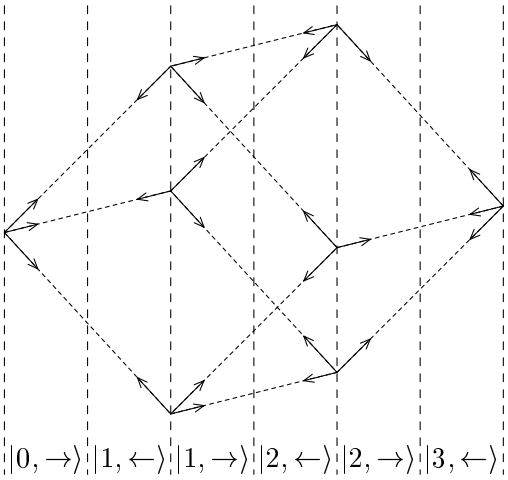
Ve smyslu předchozího odstavce tedy označme

$$\begin{aligned} |x,+\rangle &= \frac{1}{\sqrt{p_{x,+}}} \sum_{\substack{i=0 \\ |i|=x}}^{N-1} \sum_{\substack{d=0 \\ |i\oplus 2^d|=x+1}}^{n-1} |i\rangle|d\rangle, \qquad x = 0,\ldots,n-1, \\ |x,-\rangle &= \frac{1}{\sqrt{p_{x,-}}} \sum_{\substack{i=0 \\ |i|=x}}^{N-1} \sum_{\substack{d=0 \\ |i\oplus 2^d|=x-1}}^{n-1} |i\rangle|d\rangle, \qquad x = 1,\ldots,n \end{aligned} \tag{5.12}$$

Vektory $|x,\pm\rangle$ jsou jistě vzájemně kolmé a jejich normalizaci zajistíme volbou čísel $p_{x,\pm}$. Ta udávají počet použitých bázových vektorů. Určíme je následovně: podmínky první sumy v obou případech dávají $\binom{n}{x}$ možností pro směrovou část vektoru. Počet možností d ve druhé ze sum nezávisí na konkrétní hodnotě i, pouze na $|i| = x$, tímto počtem se tedy $\binom{n}{x}$ bude násobit.

V prvním případě je roven počtu nul v $(i)_2$, ve druhém počtu jedniček, tedy $n-x$, resp. x, což dává

$$\begin{aligned} p_{x,+} &= \binom{n}{x}(n-x) = \frac{n!}{x!(n-x-1)!} \\ p_{x,-} &= \binom{n}{x}x = \frac{n!}{(x-1)!(n-x)!} = p_{x-1,+} \end{aligned} \quad . \tag{5.13}$$



Obr. 25: Náhodná procházka na hyperkrychli: grafické znázornění bázových vektorů $\mathcal{H}$ a jejich vybraných „vrstev“

Především pro počáteční stav $|\psi_0\rangle$ platí

$$\begin{aligned} |\psi_0\rangle &= \frac{1}{\sqrt{Nn}}\sum_{i=0}^{N-1}\sum_{d=0}^{n-1}|i\rangle|d\rangle = \frac{1}{\sqrt{Nn}}\left(\sum_{x=0}^{n-1}\sqrt{p_{x,+}}|x,+\rangle + \sum_{x=1}^{n}\sqrt{p_{x,-}}|x,+\rangle\right) = \\ &= \frac{1}{\sqrt{Nn}}\sum_{x=0}^{n-1}\sqrt{p_{x,+}}(|x,+\rangle + |x+1,-\rangle) = \frac{1}{\sqrt{N}}\sum_{x=0}^{n-1}\sqrt{\tbinom{n-1}{x}}(|x,+\rangle + |x+1,-\rangle). \end{aligned} \tag{5.14}$$

Podívejme se na akci operátoru C a S na označené kombinace.

Je zřejmé, že pro každý vektor $|i\rangle|d\rangle$, který je zastoupen v lineární kombinaci $|x,+\rangle$, splňuje $S|i\rangle|d\rangle$ podmínky určené sumami popisujícími $|x+1,-\rangle$ a naopak. Z vyjádření vektorů $|x,+\rangle$ a $|x,-\rangle$, prostoty S a rovnosti $p_{x,+} = p_{x+1,-}$ pak rychle plyne

$$\begin{aligned} S|x,+\rangle &= |x+1,-\rangle \\ S|x,-\rangle &= |x-1,+\rangle \end{aligned} \tag{5.15}$$

pro každé $x \in \{0,1,\ldots,n-1\}$.

Nechť $x > 0$ a $|i| = x$. Protože hledaným vrcholem je 0, na vektor $|i\rangle|d\rangle$ působí C jako $I \otimes C_1$:

$$C|i\rangle|d\rangle = |i\rangle(C|d\rangle) = |i\rangle\left(\frac{2}{n}\sum_{e=0}^{n-1}|e\rangle - |d\rangle\right) \tag{5.16}$$

Přitom pro $n-x$ hodnot čísla e platí $|i\oplus 2^e| = x+1$ a pro zbylých x platí $|i\oplus 2^e| = x-1$. Je tedy

$$\begin{aligned}
C|x,+\rangle &= \frac{1}{\sqrt{p_{x,+}}} \sum_{\substack{i=0\\|i|=x}}^{N-1} \sum_{\substack{d=0\\|i\oplus 2^d|=x+1}}^{n-1} \left(\frac{2}{n} \sum_{e=0}^{n-1} |i\rangle|e\rangle - |i\rangle|d\rangle \right) = \\
&= \frac{2}{n\sqrt{p_{x,+}}}(n-x) \sum_{\substack{i=0\\|i|=x}}^{N-1} \sum_{e=0}^{n-1} |i\rangle|e\rangle - |x,+\rangle = \\
&= \frac{2(n-x)}{n\sqrt{p_{x,+}}} \sum_{\substack{i=0\\|i|=x}}^{N-1} \sum_{\substack{e=0\\|i\oplus 2^e|=x+1}}^{n-1} |i\rangle|e\rangle + \frac{2(n-x)}{n\sqrt{p_{x,+}}} \sum_{\substack{i=0\\|i|=x}}^{N-1} \sum_{\substack{e=0\\|i\oplus 2^e|=x-1}}^{n-1} |i\rangle|e\rangle - |x,+\rangle = \\
&= \frac{2(n-x)}{n\sqrt{p_{x,+}}} \sqrt{p_{x,+}}|x,+\rangle + \frac{2(n-x)}{n\sqrt{p_{x,+}}} \sqrt{p_{x,-}}|x,-\rangle - |x,+\rangle = \\
&= \frac{n-2x}{n}|x,+\rangle + \frac{2\sqrt{x(n-x)}}{n}|x,-\rangle
\end{aligned} \tag{5.17}$$

Podobným výpočtem bychom odvodili

$$C|x,-\rangle = \frac{2\sqrt{x(n-x)}}{n}|x,+\rangle + \frac{2x-n}{n}|x,-\rangle, \tag{5.18}$$

pak zbývá jen triviální případ $C|0,+\rangle = -|0,+\rangle$.

Uvažme dále, jak jsme schopni z amplitud vektorů $|x,\pm\rangle$ určit zpětně pravděpodobnosti výsledků měření na původním prostoru.

Skalární součin bázového vektoru $|i\rangle|d\rangle$ je nulový se všemi vektory $|x,\pm\rangle$ kromě takového, pro který platí $x = |i|$ a $|i\oplus 2^d| = x\pm 1$, s nímž je roven $\frac{1}{\sqrt{p_{x,\pm}}}$. Bude tedy platit

$$P_{|i\rangle|d\rangle} = \frac{1}{p_{x,\pm}} P_{|x,\pm\rangle}, \tag{5.19 a}$$

kde $P_{|x,\pm\rangle}$ značí druhou mocninu absolutní hodnoty amplitudy odpovídajícího vektoru $|x,\pm\rangle$. Více než úplné měření na $\mathcal{H}$ nás však bude zajímat měření na prostoru $\mathcal{H}_S$, zkoumejme tedy výraz

$$P_{|i\rangle} = \sum_{d=0}^{n-1} P_{|i\rangle|d\rangle} = \frac{n-x}{p_{x,+}} P_{|x,+\rangle} + \frac{x}{p_{x,-}} P_{|x,-\rangle} = \frac{1}{\binom{n}{x}} \left(P_{|x,+\rangle} + P_{|x,-\rangle} \right). \tag{5.19 b}$$

Pravděpodobnost naměření kteréhokoliv bázového stavu tedy závisí jen na Hammingově váze $|x|$ jeho prostorové části. Součet pravděpodobností $P_{|x,+\rangle} + P_{|x,-\rangle} = P_x$ má pak bezprostřední význam celkové pravděpodobnosti naměření *některého* bázového vektoru s Hammingovou vahou x (kterých je celkem $\binom{n}{x}$). Vzhledem k tomu, že jsme nedefinovali vektor $|0,-\rangle$, je pravděpodobnost naměření $|0\rangle$ v $\mathcal{H}_S$ přímo rovna $P_{|0,+\rangle}$.

Nejenže tedy při výpočtu průběhu algoritmu postačí místo nN amplitud bázových vektorů $|i\rangle|d\rangle$ počítat amplitudy těchto $2n$ významných kombinací, současně se problém převedl z kvantové náhodné procházky na hyperkrychli na problém velice podobný kvantové náhodné procházce na přímce s různými mincemi v různých polohách.

Analogie bude úplná, pokud zavedeme nové Hilbertovy prostory $\mathcal{H}'_S = \mathbb{C}^{n+1}$, $\mathcal{H}'_C = \mathbb{C}^2$ a $\mathcal{H}' = \mathcal{H}'_S \otimes \mathcal{H}'_C$, kde ortonormální bázi $\mathcal{H}'_S$ označíme běžným způsobem a ortonormální bázi $\mathcal{H}'_C$ kety $|\leftarrow\rangle$ a $|\rightarrow\rangle$ a mírně upravíme zúžení operací S a C odvozené výše:

$$\begin{aligned} S'|i\rangle|\rightarrow\rangle &= |i+1\rangle|\rightarrow\rangle, \quad i = 0, \ldots, n-1, \\ S'|i\rangle|\leftarrow\rangle &= |i-1\rangle|\leftarrow\rangle, \quad i = 1, \ldots, n, \\ S'|0\rangle|\leftarrow\rangle &= 0, \quad S'|n\rangle|\rightarrow\rangle = 0, \end{aligned} \tag{5.20 a}$$

$$C' = \sum_{i=1}^{n} |i\rangle\langle i| \otimes \begin{pmatrix} \frac{2}{n}\sqrt{x(n-x)} & 1 - \frac{2x}{n} \\ \frac{2x}{n} - 1 & \frac{2}{n}\sqrt{x(n-x)} \end{pmatrix} - |0\rangle\langle 0| \otimes I. \tag{5.20 b}$$

Jestliže identifikujeme vektory $|i\rangle|\rightarrow\rangle$ s $|x,-\rangle$ a $|i\rangle|\leftarrow\rangle$ a $|x,+\rangle$, snadno se přesvědčíme, že jedna iterace $U' = S'C'$ má v $\mathcal{H}'$ stejný účinek jako $U = SC$ v $\mathcal{H}$. „Krajní“ vektory $|0\rangle|\rightarrow\rangle$ a $|0\rangle|\leftarrow\rangle$ nemají v $\mathcal{H}$ protějšky (prostor $\mathcal{H}'$ má dimenzi $2n+2$), ale lineární obal všech ostatních bázových vektorů je vůči U' invariantní a touto identifikací izometrický lineárnímu obalu vektorů $|x,+\rangle$ a $|x,-\rangle$.

Upozorněme ještě, že lineární operátor S' není unitární. Prostor $\mathcal{H}'$ je však pouze pomocná matematická konstrukce a od U' tak unitaritu nepožadujeme.

Ani přes takové zjednodušení není průběh algoritmu řešitelný analyticky podobně jednoduše jako v případě Groverova algoritmu. Výpočet je naopak velice komplikovaný, využívá několika pomocných tvrzení a zanedbání a jeho výsledek je přibližný. Kompletní postup je obsahem většiny článku [27]. Uvedeme tedy jen jeho výsledky.

Pro dostatečně velká n má pravděpodobnost naměření hledaného vrcholu v počtu iterací podobně oscilující charakter jako u Groverova algoritmu. Délka jedné půlvlny, tedy optimální počet iterací, je přibližně

$$k_0 = \left\lceil \frac{\pi}{2}\sqrt{2^{n-1}} \right\rceil \tag{5.21}$$

(pro nezaokrouhlenou hodnotu platí odhad $t_f = \frac{\pi}{2}\sqrt{2^{n-1}}(1 + O(1/n))$, jedná se tedy o spodní odhad tím lepší, čím vyšší je n).

Pravděpodobnost dosažená po tomto počtu iterací je

$$p = \frac{1}{2} - O\left(\frac{1}{n}\right), \tag{5.22}$$

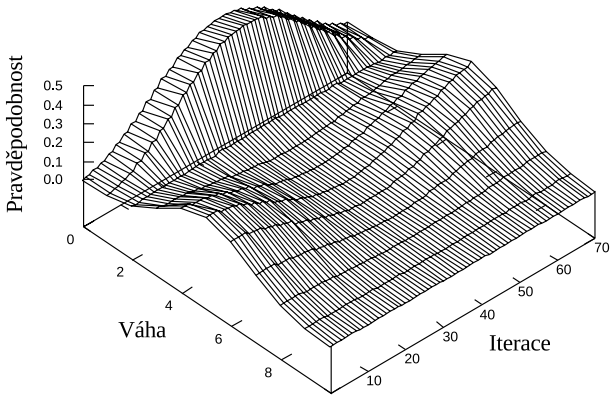
tedy její limitou pro velká n není 1, ale pouze $\frac{1}{2}$.

Numericky aproximovaný průběh pravděpodobností P_x během dvou půlvln je znázorněn na obr. 26. Všimněme si několika zajímavostí:

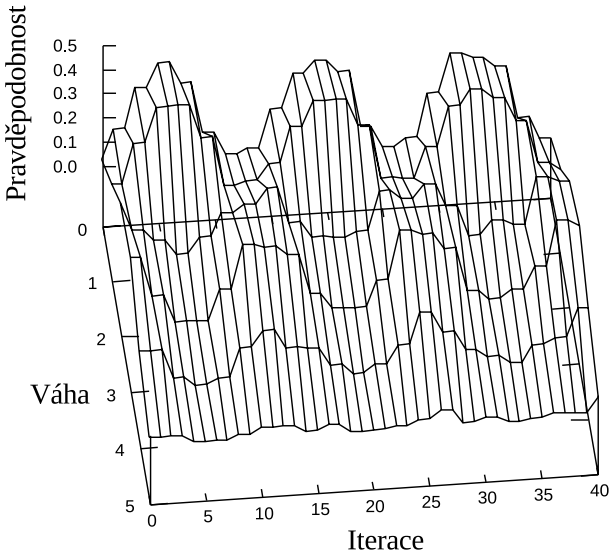
- Pravděpodobnost, podobně jako v Groverově algoritmu, se přerozděluje ve prospěch hledaného vrcholu a po překročení optimálního počtu iterací periodicky zpět k původnímu stavu. Tentokrát však nepřejde do hledaného vrcholu všechna, narazí na horní hranici $\frac{1}{2}$. Stejně výrazný vrchol pravděpodobnosti je současně v P_1, tedy struktura databáze se projeví tak, že je značná pravděpodobnost naměření některého přilehlého vrcholu místo hledaného.
- Na první pohled si jednoduchým způsobem vyměňují dominanci dvě pravděpodobnostní rozložení, podobně jako vektory $|u\rangle$ a $|0\rangle$ v Groverově algoritmu. Při bližším prozkoumání však

zjistíme, že sinusové spojnice v počtu iterací jsou jemně zvlněny, průběh je tedy komplikovanější. Obr. 27 ukazuje, že v případě malého n jsou odchylky od tohoto pohledu značné.

K oběma těmto bodům se podrobněji vyjadřuje následující paragraf.



Obr. 26: Průběh pravděpodobnosti P_x v závislosti na Hammingově váze x a počtu provedených iterací, $n = 10$.



Obr. 27: Obdoba obr. 26 pro menší databázi: $n = 5$. Obrázek je natočen pro snadnější pohled na průběhy jednotlivých P_x.

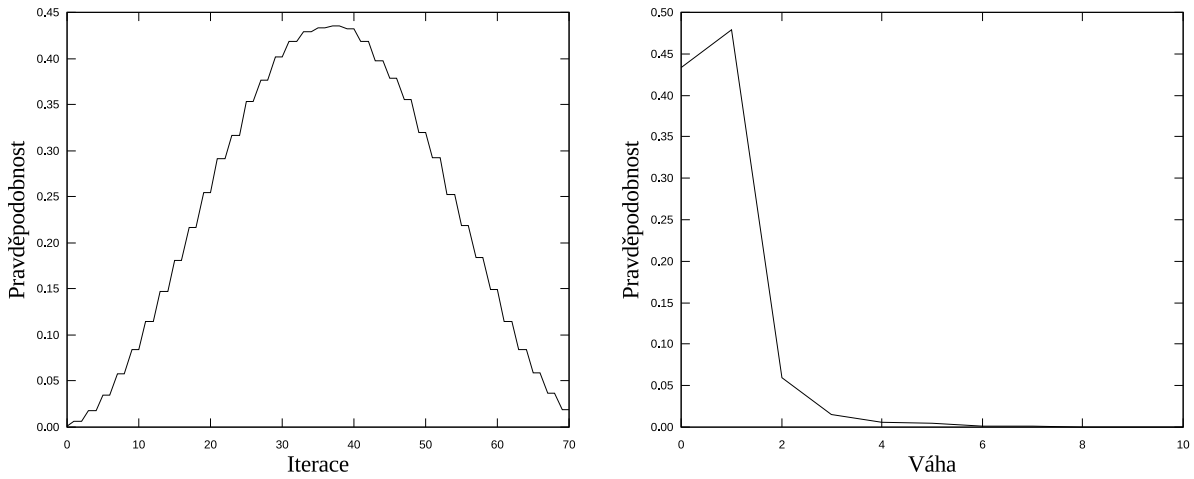
5.4 Další vlastnosti prohledávání na hyperkrychli

Při detailnějším pohledu na obr. 27 si můžeme povšimnout, že každá z pravděpodobností P_x je vždy stejná po dvojicích následujících kroků. Obr. 28 ukazuje názorně takové chování pravděpodobnosti P_0 pro $n = 10$. Že se nejedná o náhodné pozorování nebo důsledek volby malého n, se snadno přesvědčíme. Nejprve však budeme potřebovat několik dodatečných definic:

Operátor mince C v zápisu (5.20 b) má tvar jednoduššího operátoru $I \otimes C_1$ s poruchou. Označme tedy

$$\begin{aligned} C_0 &= I \otimes C_1 \quad \text{a} \\ U_0 &= SC_0. \end{aligned} \tag{5.23}$$

Okamžitě bychom ukázali, že $|\psi_0\rangle$ je vlastním vektorem C_0 i S příslušejícím vlastnímu číslu 1.



Obr. 29: Vlevo: průběh pravděpodobnosti P_0 v závislosti na počtu provedených iterací. Vpravo: průběh pravděpodobnosti P_x v závislosti na Hammingově váze x po optimálním počtu kroků. V obou případech je voleno $n = 10$.

Označme dále Q_1 lineární obal množiny všech bázových vektorů $\mathcal{H}$, jejichž prostorová část má sudou Hammingovu váhu, a Q_2 jeho ortogonální doplněk do $\mathcal{H}$. Označme dále $|s_1\rangle$ a $|s_2\rangle$ ortogonální rozklad $|\psi_0\rangle$ do Q_1 a Q_2.

Vzhledem k tomu, že jedno provedení S na libovolném bázovém vektoru změní paritu jeho prostorové části a C_0 ani C ji neovlivní, musí U_0 i U zobrazovat Q_1 do Q_2 a naopak. Protože však $|\psi_0\rangle = |s_1\rangle + |s_2\rangle$ je vlastním stavem U_0 příslušejícím vlastnímu číslu 1, není jiná možnost, než že $U_0|s_1\rangle = |s_2\rangle$ a $U_0|s_2\rangle = |s_1\rangle$. Protože však akce U_0 a U se z bázových stavů liší jen na $|0\rangle|{\rightarrow}\rangle$, který patří do Q_1, platí také $U|s_2\rangle = |s_1\rangle$.

Výchozí stav vyhledávacího algoritmu $|\psi_0\rangle$ tedy můžeme zapsat jako $|s_2\rangle + U|s_2\rangle$, po k iteracích přejde na $U^k|s_2\rangle + U^{k+1}|s_2\rangle$. Tyto součty stále ukazují ortogonální rozklad do Q_1 a Q_2 a je zřejmé, že stav po každé iteraci se v jednom čitateli shoduje s předchozím a ve druhém s následujícím, čímž je dosaženo popsaného chování.

Toto zjištění má jeden velice závažný důsledek: Označme $P_x^{(k)}$ pravděpodobnost P_x při provedení měření po k iteracích. Je součtem druhých mocnin absolutních hodnot amplitud $|x,+\rangle$ a $|x,-\rangle$ a tedy větší nebo rovna než kterýkoliv z těchto čitatelů. Podívejme se na vztah $P_1^{(k-1)}$ a $P_0^{(k)}$. Na stav po $k-1$ iteracích působí nejprve operace C. Ta však nezmění součet $P_{|1,+\rangle}^{(k-1)}$ a $P_{|1,-\rangle}^{(k-1)}$, jak bychom snadno ověřili z (5.17) a (5.18). Následná operace S přenese amplitudu $|1,-\rangle$ na $|0,+\rangle$, kde bude jediným původcem pravděpodobnosti $P_0^{(k)} = P_{|0,+\rangle}^{(k)}$ a tedy musí platit $P_0^{(k)} \leq P_1^{(k-1)}$.

Určení vztahu mezi $P_0^{(k)}$ a $P_1^{(k+1)}$ je ještě jednodušší: při operaci C se u amplitudy $|0,+\rangle$ pouze změní znaménko, načež ji operace S přenese na amplitudu $|1,-\rangle$. Protože však $P_1^{k+1} = P_{|1,+\rangle}^{(k+1)} + P_{|1,-\rangle}^{(k+1)}$, bude i $P_1^{(k+1)} \geq P_{|1,-\rangle}^{(k+1)} = P_{|0,+\rangle}^{(k)}$.

Podle dřívějšího odstavce se však $P_1^{(k)}$ rovná buď $P_1^{(k-1)}$ nebo $P_1^{(k+1)}$, což znamená, že $P_1^{(k)} \geq P_0^{(k)}$ nezávisle na k.

Protože však po optimálním počtu iterací je pravděpodobnost P_0 podle (5.22) rovna $\frac{1}{2}-O(\frac{1}{n})$ a pravděpodobnost P_1 může být jedině ještě větší nebo rovna, jejich součet musí být $1-O(\frac{1}{n})$. To znamená, že pro dostatečně vysoká n máme téměř jistotu, že vrchol, který naměříme, bude buď přímo hledaným vrcholem nebo s ním bude spojen hranou (bude mít vzdálenost 1). Důležitá je pak ovšem otázka, jestli je taková informace k něčemu užitečná. Ukažme si sílu tohoto závěru na příkladě. Zvolme $n = 30$. Optimální počet iterací v tomto případě vychází asi 36 tisíc. Po takto dlouhém experimentu máme pravděpodobnost pouze 0,482, že vrchol, který naměříme, je hledaným vrcholem. Pokud není, můžeme celý výpočet opakovat a zvýšit tak pravděpodobnost nalezení správného výsledku na 0,731 a tak dále. Pokud však zkusíme ověřit ještě přilehlé vrcholy, za cenu pouhých 30 (v nejhorším případě) dalších dotazů na orákulum nalezneme správný vrchol s pravděpodobností 0,980!

Nakonec bychom mohli podobně jako v paragrafu 4.3 diskutovat, jak se chová tento vyhledávací algoritmus pro malá velice malé hodnoty n. Výsledkem analýzy několika prvních iterací je, že selhává pro $n = 1$, ale ještě také pro $n = 2$, od $n = 3$ dále se chová očekávaným, jednotným způsobem. Podobný zvláštní případ jako u Groverova algoritmu zde nenastává. Dalším rozdílem oproti Groverově algoritmu je, že odhad optimálního počtu iterací (5.21) není přesný, pro větší spolehlivost při menších n by tedy bylo lepší algoritmus nejprve numericky simulovat a zjistit, po kolika iteracích je pravděpodobnost naměření označeného vrcholu nejvyšší.

5.5 Podobné vyhledávací algoritmy

V literatuře jsou popsány dobře i další vyhledávací algoritmy založené na kvantovém náhodném procházení po pravidelných grafech. V tomto paragrafu se o nich však opět zmíníme pouze výčtem. Obecně se dochází k výsledku, že za vhodného použití kvantových algoritmů je možno vyhledat označený prvek v nesetříděné databázi o velikosti N s časovou složitostí $O(\sqrt{N})$ nebo $\tilde{O}(\sqrt{N})$.

Článek [28] popisuje vyhledávání na čtvercové mřížce o rozměrech $\sqrt{N} \times \sqrt{N}$ a zobecňuje výsledky i na pravoúhlé sítě vyšších dimenzí.

Dále se definuje *spojitá náhodná procházka*, která neprobíhá po krocích. Je v klasickém obraze limitním případem situace, kdy zkracujeme časový interval mezi kroky za cenu přidělení jisté rostoucí pravděpodobnosti, že objekt zůstane na místě. Z tohoto modelu je opět odvozena kvantová analogie, která nevyužívá kvantových hradel, ale popisuje vývoj systému pomocí Hamiltoniánu. Vztahy mezi tímto diskrétním a spojitým modelem nejsou dosud zcela pochopeny [29], zajímavé například je, že spojitá procházka nepotřebuje pomocný prostor mince.

Analýzou složitosti spojitých analogií Groverova algoritmu, vyhledávání na hyperkrychli i na mřížkách vyšších dimenzí se zabývá článek [30].

5.6 Procházení na obecných grafech, optické sítě

Klasickou náhodnou procházku jsme definovali tak, že jejím působištěm je libovolný graf.[32] Kvantové analogie jsme naproti tomu dosud diskutovali pouze na grafech, které se vyznačovaly

[32] Obecně se uvažují pro jednoduchost pouze neorientované grafy.

značnou strukturální jednoduchostí – přímka i hyperkrychle jsou grafy *regulární*, v každém jejich vrcholu se setkává stejný počet hran. Pravoúhlé sítě mají takovou vlastnost alespoň ve většině svých vrcholů a v krajních vrcholech mají hran méně.

Otázkou je, jak bychom mohli rozšířit popsanou myšlenku kvantového náhodného procházení s mincí (*coined quantum random walk*, CQRW) jednotným způsobem na obecné grafy, o jejichž globálních vlastnostech nemáme podobné informace. Odpověď na ni zatím není známa [26].[33]

Takovou otázku je schopen řešit poslední algoritmus, který v této práci popíšeme, nazývaný občas v analogii *scattering quantum random walk*, SQRW [31]. Jeho základem je (v současné době myšlený) experiment, ve kterém necháváme putovat fotony po optické síti, což je zařízení principiálně podobné interferometru. Ukážeme, že tento algoritmus je v případě regulárních grafů zobecněním CQRW.

Tento algoritmus byl poprvé popsán v [26]. Jeho technickým podkladem jsou lineární optické prvky zvané *multiporty*, teoreticky popsané v práci [32]. Jedná se o zobecnění polopropustného zrcadla pro n vstupně-výstupních cest.

Polopropustné zrcadlo, anglicky přesněji zvané *beam splitter*, je charakterizováno dvěma parametry, koeficienty odrazu r a prostupnosti t, $|r|^2+|t|^2=1$. Jestliže na zrcadlo dopadne foton přicházející z jedné strany, řekněme zleva, transformuje se jeho stav $|{\rightarrow}\rangle_i$ na lineární superpozici stavů odpovídajících průchodu a odrazu s těmito koeficienty:

$$|{\rightarrow}\rangle_i \mapsto t|{\rightarrow}\rangle_o + r|{\leftarrow}\rangle_o. \tag{5.24 a}$$

Jestliže bude foton dopadat z druhé strany, jeho stav bude podle základů kvantové optiky [33] ortogonální k $|{\rightarrow}\rangle_i$, výsledný stav však očekáváme opět v superpozici stavů $|{\rightarrow}\rangle_o$ a $|{\leftarrow}\rangle_o$. Protože od lineární operace, která na zrcadle probíhá, budeme očekávat unitaritu, musí být tato superpozice ortogonální k (5.24 a). Tak získáme až na volnost ve volbě globální fáze vztah

$$|{\leftarrow}\rangle_i \mapsto \overline{t}|{\leftarrow}\rangle_o - \overline{r}|{\rightarrow}\rangle_o. \tag{5.24 b}$$

Multiport má, jak bylo řečeno výše, n vstupů a výstupů. Očíslujme pevně tyto optické cesty čísly 1 až n a označme zatím abstraktním vektorem $|i\rangle_i$ stav fotonu, který putuje po i-té z nich směrem do multiportu, a $|i\rangle_o$ směrem z multiportu ven. Akci multiportu na vzájemně ortogonální vstupní stavy budeme hledat ve tvaru

$$|i\rangle_i \mapsto r|i\rangle_o + t\sum_{\substack{j=1\\ j\neq i}}^{n}|j\rangle_o = \sum_{j=1}^{n} C_{ij}|j\rangle_o \tag{5.25}$$

Podmínka na unitaritu takového zobrazení, aplikovaná podobně jako výše, dá tentokrát podmínky pro t a r tvaru [26]

$$\begin{aligned}(n-1)|t|^2+|r|^2&=1\\ (n-2)|t|^2+2\,\mathrm{Re}\,\overline{t}r&=0.\end{aligned} \tag{5.26}$$

Taková podmínka je však současně podmínkou unitarity matice s prvky $\{C_{ij}\}_{i,j=1}^{n}$. Na tuto matici předpokládané transformační vztahy kladou požadavky, aby všechny její diagonální prvky

[33] Pokud známe maximální stupeň vrcholu v grafu – největší počet hran, který z některého jeho vrcholu vychází, obecné metody jsou známy [19].

měly hodnotu r a mimodiagonální t. Uvědomme si, že kromě triviálních příkladů násobků jednotkové matice nějakou globální fází jsme se seznámili ještě s jednou maticí, která těmto požadavkům vyhovuje: viz (5.8).

Pro realizaci kvantové náhodné procházky na obecném grafu reprezentujeme každý vrchol multiportem s počtem vstupů rovným stupni vrcholu. Každý výstup multiportu vede do jiného multiportu a tyto spojnice odpovídají hranám grafu.

Prostor mince v tomto algoritmu nebude potřeba – je nahrazen informací, po které optické dráze foton do, resp. z daného multimetru přichází, resp. odchází.

V algoritmu SQRW předpokládáme, že stavový prostor je definován svou ortonormální bází, tvořenou vektory označenými $|xy\rangle$, kde x a y značí dva vrcholy uvažovaného grafu propojené hranou. Pod každým takovým vektorem budeme rozumět foton putující z multiportu odpovídajícího x do multiportu odpovídajícího y.

Předpokládáme dále, že cesta fotonu po libovolné hraně trvá vždy stejnou časovou jednotku. Budeme tedy uvažovat, že během této jednotky se stav systému v zavedeném formalismu nemění, a vstupem do další takové fáze se změní skokově. Tento vývoj proto nejlépe budeme popisovat operátorem časového vývoje U s parametry t_1 voleným během první fáze a t_2 během následující. Tento operátor je určen obrazy bázových vektorů:

$$U|xy\rangle = \sum_{j=1}^{n} C_{ij}^{(y)} |yz_j\rangle, \tag{5.27}$$

kde $\mathbf{C}^{(y)}$ je matice multiportu ve vrcholu y, i je číslo výstupu tohoto multiportu ve smyslu označení (5.25), vedoucího k x, a z_j je multiport, ke kterém dle stejného označení vede výstup očíslovaný j.

Zkusme, jak by v takto zavedených podmínkách bylo možno najít analogii vyhledávacího algoritmu na hyperkrychli z paragrafu 5.3. Pro hyperkrychli řádu n bude tedy třeba 2^n multiportů, označených čísly 0 až 2^n, každý s n výstupy. Propojeny budou, stejně jako vrcholy hyperkrychle, multiporty, jejichž číselná označení se ve dvojkové soustavě liší právě v jednom bitu. Jednotlivé výstupy multiportů očíslujeme tak, že i-tý výstup multiportu x povede k multiportu $x \oplus 2^i$, nechť $i = 0, 1, \ldots, n-1$. Všimněme si vlastnosti takového číslování, že stejná optická cesta má u multiportů na obou koncích stejné číselné označení.

Všem multiportům kromě jednoho, odpovídajícího označenému vrcholu, přiřaďme matici (5.8) (jinými slovy $r = \frac{2}{n} - 1$, $t = \frac{2}{n}$), označenému vrcholu matici $-I$, tedy $t = 0$ a $r = -1$.

Ukážeme, že průběhy obou algoritmů se stanou ekvivalentními, jestliže identifikujeme vektory $|x\rangle|d\rangle$ z paragrafu 5.3 s vektory $|x, x \oplus 2^d\rangle$, zavedené v tomto paragrafu, pokud iteraci původního algoritmu myšlenkově přetvoříme z $U = SC$ na tvar $U = CS$.

Jedna taková iterace pak totiž působí na bázový stav

$$CS|x\rangle|d\rangle = C\left(|x \oplus 2^d\rangle|d\rangle\right) = \sum_{j=0}^{n-1} C_{dj}^{x \oplus 2^d} |x \oplus 2^d\rangle|d\rangle, \tag{5.28 a}$$

zatímco unitární vývoj přiřazeného bázového stavu $|x, x \oplus 2^d\rangle$ v SQRW algoritmu za jednotku času je podle (5.27)

$$U|x, x \oplus 2^d\rangle = \sum_{j=0}^{n-1} C_{dj}^{x \oplus 2^d} |x \oplus 2^d, x \oplus 2^d \oplus 2^d\rangle = \sum_{j=0}^{n-1} C_{dj}^{x \oplus 2^d} |x \oplus 2^d, x\rangle. \qquad (5.28\,\mathrm{b})$$

Vektor $|x \oplus 2^d, x\rangle$ byl přitom identifikován s vektorem $|x \oplus 2^d\rangle|d\rangle$.

Pro úplnou ekvivalenci algoritmů by bylo ještě třeba udat odpovídající počáteční stav v CQRW. Obecně se totiž uvažuje, že foton uměle vyšleme do jedné z optických cest, to ale v udané identifikaci rovnocenné superpozici všech bázových stavů v původním algoritmu neodpovídá. Přes stejný operátor časového vývoje by tak oba systémy vykazovaly odlišný průběh stavu.

Je zřejmá jedna okamžitá výhoda algoritmu CQRW. Experimentální realizace hradla (5.10) bude velice snadná díky tomu, že jednotlivým polohám odpovídají fyzicky různé multiporty, a můžeme tak jednoduše každé poloze přiřadit, který je potřeba. Tato výhoda je za cenu exponenciální prostorové náročnosti, která v případě experimentálního sestavení CQRW algoritmu přesně podle uvedeného návodu umožnila jeho využití jen v případech drobných n.

Závěr

Cílem práce bylo popsat úvod do problematiky kvantových algoritmů. Není však v možnostech rozsahu jedné podobné práce popsat větší množství algoritmů tak podrobně, jak jsem se pokusil alespoň u Groverova algoritmu a vyhledávání na hyperkrychli, pro udržení rozumného rozsahu práce musely být informace o ostatních algoritmech podány buď velmi útržkovitě, nebo zkráceny na pouhé zmínky o jejich existenci. Detaily kvantové mechaniky by také potřebovaly důslednější rozbor a uvedení uvedení více definicí a zákonitostí např. v paragrafu o kvantovém měření. Přesto doufám, že práce svůj účel splnila v rámcích svých možností dobře.

Přílohy

Jako přílohy uveďme výpisy zdrojových kódů několika počítačových programů, které byly využívány ke tvorbě grafů v práci obsažených. Zdrojové kódy jsou psány v programovacím jazyce C a pro překlad vyžadují překladač implementující standard ISO 9899-1990.

A.1 Program grover

Tento jednoduchý program slouží k nalezení pravděpodobnosti naměření hledaného vrcholu v Groverově algoritmu po optimálním počtu iterací. Vzhledem k tomu, že se jedná pouze o dosazení do vzorce, mohl být nahrazen použitím libovolného tabulkového procesoru – program je tedy uváděn vedle ostatních dvou spíše pro úplnost – ale v této formě byl inspirací ke zkoumání problematiky paragrafu 4.3.

```
#include <stdio.h>
#include <math.h>

const int Nm = 20;  // Délka tabulky

int main() {
  int n, N;
  for(n = 2; n <= Nm; n++) {
    N = floor(M_PI/4*pow(2.0, n/2.0));
    printf("%i %.6f %.6f\n", n, pow(sin((2*N+1)*asin(pow(2.0, -n/2.0))), 2),
        1-pow(2.0, -n));
  }
  return 0;
}
```

A.2 Program `qrw-line`

Tento program simuluje kvantovou náhodnou procházku na přímce. Počet iterací N musí být uveden na počátku, tomu pak je přizpůsobena délka pracovního pole. Výstupem je výčet pravděpodobností naměření na každé poloze po tomto počtu iterací.

```
#include <stdio.h>
#include <math.h>
#include <complex.h>

#define N 50         // Počet iterací
#define V M_SQRT1_2  // Převrácená hodnota odmocniny ze 2
#define C c2         // Výběr mince z možností níže

int main() {
  double complex fld[2*N+1][2] = {{0}};         // Pracovní pole
  double complex c2[2][2] = {{V, V}, {V, -V}},  // Mince používané v obr. 22
          c3[2][2] = {{V, I*V}, {I*V, V}},
          c4[2][2] = {{V, (I+1)/2.0}, {-V, (I+1)/2.0}};
  double complex t;
  int i, j;
  fld[N][0] = I*V;                 // Počáteční stav: amplituda "vlevo"
  fld[N][1] = V;                   // a "vpravo"
  for(i = 0; i < N; i++) {         // Operace C
    for(j = 1; j < 2*N; j++) {
      t = C[0][0]*fld[j][0] + C[0][1]*fld[j][1];
      fld[j][1] = C[1][0]*fld[j][0] + C[1][1]*fld[j][1];
      fld[j][0] = t;
    }
    for(j = 0; j < 2*N; j++)       // Operace S
      fld[j][0] = fld[j+1][0];
    for(j = 2*N; j > 0; j--)
      fld[j][1] = fld[j-1][1];
  }
  for(j = 0; j < 2*N+1; j++)       // Výpis pravděpodobností
    printf("%i %.6f\n", j-N, pow(cabs(fld[j][0]), 2) +
        pow(cabs(fld[j][1]), 2));
  return 0;
}
```

A.3 Program `qrw-cube`

Tento program simuluje algoritmus vyhledávající na hyperkrychli. Využívá k tomu zjednodušení zavedené v paragrafu 5.3. Jeho výstupem je tabulka pravděpodobností použitá pro vykreslení obr. 26 a 27.

```
#include <stdio.h>
#include <math.h>

#define N 10                    // Rozměr hyperkrychle

double binom(int a, int b) {  // Binomické koeficienty
  double v = 1.0;             // Tento výpočet není příliš efektivní,
  int i;                      // ale funguje i pro velká N
  if(b < 0 || b > a) return 0;
  for(i = 0; i < b; i++)
    v = v * (a-i) / (b-i);
  return v;
}

int main() {
  double fld[N+1][2], c, s, t;          // Pracovní pole
  int i, it, m, st, o;
  for(i = 0; i <= N; i++) {             // Výchozí stav
    fld[i][0] = sqrt(binom(N-1, i) / pow(2, N));
    fld[i][1] = sqrt(binom(N-1, i-1) / pow(2, N));
  }
  m = M_PI/2/M_SQRT2*pow(2, N / 2.0);   // Optimální počet kroků
  if(m > 1000)           // Pokud je příliš velký, budeme vypisovat
    st = m / 100;        // pouze každou stou řádku
  else
    st = 1;
  for(it = 0; it <= 2*m; it++) {        // Délka dvou půlvln
    fld[0][0] = -fld[0][0];             // Operace C
    for(i = 0; i <= N; i++) {
      c = 1 - 2.0*i/N;
      s = 2.0 / N * sqrt(i * (N-i));
      t = c*fld[i][0] + s*fld[i][1];
      fld[i][1] = s*fld[i][0] - c*fld[i][1];
      fld[i][0] = t;
    }
    for(i = 0; i < N; i++) {            // Operace S
      t = fld[i][0];
      fld[i][0] = fld[i+1][1];
      fld[i+1][1] = t;
```

```
    }
    if(!(it % st))                    // Výpis pravděpodobností P_x
      for(i = 0, o = 0; i <= N; i++) {
        c = pow(cabs(fld[i][0]), 2) + pow(cabs(fld[i][1]), 2);
        printf("%.6f ", cabs(c));
      }
    puts("");
  }
  return 0;
}
```

Použitá literatura

[1] Pytlíček, J. *Lineární algebra a geometrie.* Skripta ČVUT, Vydavatelství ČVUT, Praha, 2002. 122 s.

[2] Blank, J., Exner, P., Havlíček, M. *Lineární operátory v kvantové fyzice.* Karolinum, Praha, 1993. 678 s.

[3] Nielsen, M. A., Chuang, I. L. *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, UK, 2000. 676 s.

[4] Hlavatý, L. *Slabikář kvantové mechaniky.* Skripta ČVUT, nevydáno, 2006

[5] Wikipedia, the free encyclopedia. *Tensor product.* <http://en.wikipedia.org/wiki/Tensor_-products> [rev. 17. 4. 2007, cit. 6. 5. 2007]

[6] Einstein, A., Podolsky, B., Rosen, N. *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?* Phys. Rev., 47, s. 777–780, 1935, k nahlédnutí bezplatně na <http://prola.aps.org/abstract/PR/v47/i10/p777_1> [cit. 11. 7. 2007]

[7] Wikipedia, the free encyclopedia. *EPR paradox.* <http://en.wikipedia.org/wiki/EPR_-paradox> [rev. 26. 6. 2007, cit. 11. 7. 2007]

[8] Wikipedia, the free encyclopedia. *Bell's Theorem.* <http://en.wikipedia.org/wiki/Bell%27s_-theorem> [rev. 27. 6. 2007, cit. 11. 7. 2007]

[9] Peres, A. *Quantum Theory: Concepts and Methods.* Kluwer Academic Publishers, Dordrecht, NL. 1989. 446 s.

[10] Berman, G. P., Doolen, G. D., Mainieri, R., Tsifrinovich, V. I. *Introduction to Quantum Computers.* World Scientific Publishing, Singapore, 1998. 187 s.

[11] Wikipedia, the free encyclopedia. *Hadamard transform.* <http://en.wikipedia.org/wiki/-/Hadamard_transform> [rev. 16. 6. 2007, cit. 30. 6. 2007]

[12] Lavor, C., Manssur, L. R. U., Portugal, R. *Grover's Algorithm: Quantum Database Search.* arXiv:quant-ph/0301079

[13] Shor, P. W. *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer.* arXiv:quant-ph/9508027v2

[14] Wikipedia, the free encyclopedia. *Shor's algorithm.* <http://en.wikipedia.org/wiki/Shors_-algorithm> [rev. 11. 6. 2007, cit. 14. 7. 2007]

[15] Virius, M. *Základy algoritmizace.* ČVUT, Praha, 1995. 179 s.

[16] Wikipedia, the free encyclopedia. *Cooley-Tukey FFT algorithm.* <http://en.wikipedia.org/-/wiki/Cooley-Tukey_FFT_algorithm> [rev. 12. 6. 2007, cit. 14. 7. 2007]

[17] Beckman, D. et al. *Efficient networks for quantum factoring.* arXiv:quant-ph/9602016v1

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

[19] Kempe, J. *Quantum random walks – an introductory overview.* Contemporary Physics, 44, s. 307–327, 2003

[20] Boyer, M., Brassard, G., Høyer, P., Tapp, A. *Tight bounds on quantum searching.* arXiv:-:quant-ph/9605034v1

[21] Brassard, G., Høyer, P., Mosca, M., Tapp, A. *Quantum Amplitude Amplification and Estimation.* arXiv:quant-ph/0005055v1

[22] Chi, D. P., Kim, J. *Quantum Database Searching by a Single Query.* arXiv:quant-ph/ /9708005v1

[23] Ambainis, A. *Quantum walks and their algorithmic applications.* arXiv:quant-ph/0403120

[24] Nayak, A., Vishvanath, A. *Quantum walk on the line.* arXiv:quant-ph/0010117

[25] Meyer, D. A. *On the absence of homogenous scalar unitary cellular automata.* arXiv:quant-ph/9604011v2

[26] Hillery, M., Bergou, J., Feldman, E. *Quantum walks based on an interferometric analogy.* arXiv:quant-ph/0302161v1

[27] Shenvi, N., Kempe, J., Whaley, K. *Quantum Random Walk Search Algorithm.* arXiv:quant-ph/0210064

[28] Ambainis, A., Kempe, J., Rivosh, A. *Coins Make Quantum Walks Faster.* arXiv:quant-ph/ /0402107

[29] Kendon, V. *Quantum walks on general graphs.* arXiv:quant-ph/0306140

[30] Childs, A. M., Goldstone, J. *Spatial search by quantum walk.* arXiv:quant-ph/0306054v2

[31] Košík, J., Bužek, V. *Scattering model for quantum random walks on hypercube.* arXiv:quant-ph/0410154v2

[32] Jex, I., Stenholm, S., Zeilinger, A. *Hamiltonian theory of a symmetric multiport.* Opt. Commun. 117, 95 (1995)

[33] Paul, H. *Introduction to Quantum Optics: From Light Quanta to Quantum Teleportation.* Cambridge University Press, Cambridge, UK, 2004. 254 s.

Prohlášení

Prohlašuji, že jsem svou bakalářskou práci vypracoval samostatně a použil jsem pouze literaturu uvedenou v přiloženém seznamu.

Nemám závažný důvod proti užití tohoto skolního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne ....
podpis