ČVUT PRAHA
FAKULTA ELEKTROTECHNICKÁ

DIPLOMOVÁ PRÁCE

2001 Vojtěch Kupča

ČVUT PRAHA
FAKULTA ELEKTROTECHNICKÁ

Teorie a perspektiva kvantových počítačů

2001

Vojtěch Kupča

Teorie a perspektiva kvantových počítačů

Tato diplomová práce se zabývá jedním z nejnovějších odvětví informatiky – kvantovými počítači. Zabývá se základními teoretickými principy, na nichž jsou kvantové počítače založeny a ukazuje jejich schopnosti na typických algoritmech, které byly do dnešní doby navrženy. Na závěr je diskutován stav v oblasti konstrukce reálných kvantových počítačů a jsou učiněny jisté předpovědi o budoucnosti kvantových počítačů.

Theory and Perspectives of Quantum Computers

This Master's thesis deals with today's hot topic in the field of computer science, namely the branch of quantum computing. It explores basic theoretical principles of quantum computers and shows their potential on some of the typical algorithms that were designed so far. Also, the progress in building real quantum computers and some predictions concerning the future are included in the final of the thesis.

Prohlášení

Prohlašuji, že jsem diplomovou práci Teorie a perspektiva kvantových počítačů vypracoval samostatně a použil při tom úplný výčet citací použitých pramenů, které uvádím v referencích na závěr diplomové práce.

Nemám námitky proti půjčování, zveřejnění a dalšímu využití práce, pokud s tím bude souhlasit katedra počítačů FEL-ČVUT.

Vojtěch Kupča 16.ledna 2001

`bashar@centrum.cz`

There's unknown all around at every moment.
That's where you seek knowledge.

–Frank Herbert

Poděkování

Chtěl bych poděkovat všem, kteří mají zásluhu na dokončení této diplomové práce a kteří mi pomáhali svými připomínkami, radami i náměty při obtížích nebo otázkách, na které jsem narazil. Zvláště bych chtěl poděkovat vedoucímu práce Ing. Tomáši Rosovi, který mě svým profesionálním přístupem vedl během této výzkumné činnosti.

Děkuji také rodině, které vděčím za to, že jsem mohl studovat na technické vysoké škole a dokončit tuto práci, která se nesporně týká pozoruhodného odvětví dnešní vědy a techniky.

16.ledna 2001

Obsah

1 Úvod

Skončené 20. století lze bez nadsázky označit za nejpokrokovější v dějinách lidstva. Přestože se zapsalo do dějin i mnoha negativními stránkami, v oblasti poznání a vědy zaznamenalo nejdrtivější postup a utvářelo nebo zpřesňovalo náš pohled na svět. Není tak náhodou, že dnes na začátku roku 2001 se nachází vyspělý svět v brázdě proudících informací, které celkový rozvoj ještě akcelerují. Požadavky na efektivní zpracování informací se rychle během desetiletí množily. Obranou v této záplavě se ve druhé polovině století staly první prototypy počítačů, které měly zprvu usnadnit únavnou práci lidí na složitých výpočtech. Dnes se počítače dostaly do pozice univerzálních nástrojů pro hromadné zpracování informací.

1.1 Limity v konstrukci procesorů

Více informací však nevyhnutelně znamená potřebu větší výpočetní síly. Legendární Mooreův zákon přitom říká, že přibližně každých 18 měsíců se zdvojnásobuje počet tranzistorů, které tvoří jeden čip. Dnes se jich na běžném čipu tísní až 30 milionů[1]. Aby však byla výroba rentabilní, není možné zvětšovat plochu, kterou čip zabírá. To proto, že čím větší jsou plátky křemíku tvořící základní vrstvu čipu, tím větší je pravděpodobnost, že v takovém plátku bude defekt, který učiní čip nepoužitelným. To zákonitě vede ke zmenšování velikosti jednotlivých elementů, jako jsou například tranzistory. To ale také znamená nutnost zjemňování litografické technologie, kterou se na čipu leptají spoje. Dnešní špičková 0,13 mikronová technologie umožňuje propojovat tranzistory šířky 70nm. Technologie 0,11 mikronů má být na světě za několik let. Přesto se obvykle považuje 0,02 mikronová hranice za mez v klasické konstrukci počítačů[2]. To znamená, že kolem roku 2020 by Mooreův zákon přestával dodržovat výše zmíněné kritérium. Co přijde pak? Težko předvídat, ale ve vývojových laboratořích předních výrobců čipů se již dávno vymýšlejí další vylepšení současných technologií ať už jde o 3D čipy, které by měly na sebe naskládat více vrstev spojů nebo fotonické krystaly, jenž mají svými optickými vlákny vést mezi prvky čipu světlo vlnové délky podobné šířce vlákna, až třeba po biočipy, které by využívaly ke zpracování informace přírodou vytvořené nanometrové biologické struktury například v listech rostlin. Taková miniaturizace je zajisté slibná, ale nevyhnutelně směřuje k jedinému konci. A sice, že bude dosažena hranice velikosti jednotlivých molekul a atomů, tj. rozměrů kolem 0,1–0,5 nm. K nutné změně technologie se navíc přidává fakt, že náklady předních výrobců polovodičových komponent na nové výrobní haly se velmi strmě zvyšují, přičemž stejným tempem je tento trend v následujících letech neudržitelný. Pozoruhodné je, že prostá extrapolace těchto charakteristik do dalších let ukazuje na jejich společné dosažení kvantové úrovně kolem roku 2020, kdy má být informace kódována na úrovni částic.

[1] Pentium 4 od Intelu jich má mít v roce 2001 na technologii 0,13 mikronů 42 miliónů – viz prognóza v časopisu *Computer* v referencích.

[2] I když například IBM tvrdí, že jejich budoucí technologie V-Groove za 10–15 let dokáže vytvářet spoje menší než 0,01 mikronu.

Na částicové úrovni ale přestávají platit jindy běžné fyzikální zákony makroskopického světa a na svém významu začíná nabývat do dnešní doby nejpřesnější a nejpodrobnější popis pozorovaného (i nepozorovaného) světa – kvantová mechanika. Když byly kvantové mechanice položeny v roce 1900 Maxem Planckem základy, zřejmě jen málokdo tušil, jaký dopad bude mít tato oblast fyziky na naše pochopení fyzikálního obrazu světa. Na Planckovy závěry totiž navázal později Niels Bohr se svým modelem atomu, v němž byly kvantovány energetické úrovně elektronů v atomu, což dokázalo vysvětlit jev vyzařovaného spektra atomu vodíku a stabilitu atomů. Úspěch Bohra pak o několik let později vedl Heisenberga, Schrödingera, Diraca, Pauliho a další přední fyziky k formulaci prvních základů moderní kvantové mechaniky, založené na aparátu vlnové funkce. Rozhodujícím rozvojem kvantová mechanika prošla poměrně krátce v letech 1923–1927. Shrňme si pro dokreslení situace v první pol. 20. století fundamentální poznatky a principy, které tehdy spatřily světlo světa:

1900: Max Planck – kvantování záření černého tělesa
1905: Albert Einstein – vysvětlení fotoelektrického jevu
1913: Niels Bohr – model atomu s kvantovanými energetickými hladinami
1923: Luis de Broglie – vlnově-částicová dualita
1925: Wolfgang Pauli – vylučovací princip
1925: Werner Heisenberg – maticová mechanika
1926: Erwin Schrödinger – vlnová mechanika
1926: Erwin Schrödinger – potvrzení ekvivalence maticové a vlnové mechaniky a vznik moderní kvantové mechaniky
1926: Max Born – navrhl statistickou interpretaci kvantové mechaniky
1927: Werner Heisenberg – princip neurčitosti
1932: John von Neumann – popis kvant. mechaniky operátorovou algebrou

Ani nás zřejmě nepřekvapí, že kromě von Neumanna dostali všichni za svůj příspěvek k rozvoji kvantové mechaniky Nobelovu cenu. Od té doby prošla kvantová mechanika značným rozvojem i větvením jejích různých specializovaných částí a uplatňuje se dnes také v příbuzných disciplínách, jako jsou například astrofyzika nebo kosmologie.

1.2 Myšlenka kvantového počítače

Někdy v 70. a 80. letech se však začaly objevovat první nápady, týkající se využití kvantové mechaniky v informatice. Dobrou zprávou bylo, že by se dala kvantová mechanika použít i se všemi svými pozitivními dopady. To znamená všemi zvláštními jevy, které jsou jí vlastní. Horší ale bylo, že úvahy o realizaci se v té době zdály vzdálené a težko uskutečnitelné. Na základech *kvantové informatiky* se tehdy podíleli především Charles Bennett, Paul Benioff, David Deutsch a Richard Feynman. Ti postupně definovali abstraktní rámec kvantové informatiky v podobě kvantového Turingova stroje, teorie o kvantové složitosti problémů a konkrétních návrhů funkčního modelu kvantového počítače. Už tehdy bylo zřejmé, že pokud by se jednou podařilo takový počítač postavit, znamenalo by to jistě zásadní průlom ve způsobu, jakým dnes počítače pracují. Prozkoumat možnosti kvantového paralelismu, „nelokální“ povahy reality nebo vlastností přirozeně náhodných jevů představují nepochybně velká lákadla. Cesta k nim je však z několika hlavních důvodů obtížná: jednak je to cesta do opravdového mikrosvěta až k rozměrům velikostí atomů a částic – jistě si dokážeme představit, jaké obtíže musí manipulace s jednotlivými atomy působit; jednak je to výprava k nedeterminismu kvantově-mechanického světa, v němž nejsme (vždy) schopni předvídat následující události. A také je to problematická (až filozofická) otázka měření a dekoherence kvantového systému, tedy vlastností zapřičiňujících, že vidíme svět bez superpozic[3] a jiných klasicky nevysvětlitelných jevů. Přes všechny možné těžkosti (pokud se nevynoří nová nepředvídaná technologická překážka nebo skrytá teoretická chyba) se již dnes dá s velkou nadějí říci, že kvantové počítače bude možné v budoucnosti zkonstruovat. Na otázku jak vzdálená je tato budoucnost by (kromě jiného) měla odpovědět následující práce, která si klade za cíl podat široký přehled problematiky kvantových počítačů a poukázat na jejich využití při řešení reálných problémů. Postupně se seznámíme s teoretickými základy kvantové mechaniky a jejich korespondencí s popisem kvantového počítače. Představíme základní teoretické principy, na kterých je kvantový počítač založen. Zmíníme se o algoritmech, které demonstrují potenciál kvantové informatiky. Budeme hovořit o opravě chyb, které kvantový výpočet nevyhnutelně provází. Na závěr se pokusíme nastínit, v jakém stádiu se nachází experimenty s realizací kvantových počítačů a jaké jsou jejich nejslibnější výsledky.

[3] Kvantový systém je v superpozici, pokud se nenachází ve stavu konkrétní čisté hodnoty (kterou měříme - viz dále). Místo toho je jeho stav „namíchán“ z několika možných výsledných hodnot. Klasickým příkladem je problém tzv. *Schrödingerovy kočky* z roku 1935. Schrödinger popsal lehce nadnesený problém kočky uvězněné v krabici, na niž míří pistole, kterou spouští mechanizmus závislý na náhodném jevu rozpadu radioaktivního atomu s poločasem 1 hodina. Pokud se atom rozpadne, kočka zemře a naopak (pravděpodobnost rozpadu během hodiny je 1/2). Jestliže stav atomu vyjádříme kvantově-mechanicky jako superpozici stavů rozpadlého a nerozpadlého atomu, pak po uplynutí jedné hodiny se stav kočky změní zrovna tak: kočka je nyní živá i mrtvá zároveň! Je tedy v superpozici dvou stavů. Teprve když krabici otevřeme (provedeme měření), zjistíme jen jednu z možných alternativ. Závěr: Superpozice v makrosvětě nepozorujeme, protože měřením superpozice rušíme.

2 Stručný přehled kvantové mechaniky

Abychom mohli správně matematicky kvantový počítač popsat, je zapotřebí zavést základní matematické pojmy a připomenout si některé fundamentální principy kvantové mechaniky. V této části proto nadefinujeme kvantový stav a matematicky popíšeme jeho vývoj. Budeme se zabývat otázkou měření na kvantovém systému a řekneme si, jak matematické formalizmy korespondují s pozorováním kvantově-mechanického světa. Tento úvod si jistě neklade za cíl podat vyčerpávající výklad problematiky Hilbertova prostoru. Spíše se budeme snažit zavést nejdůležitější pojmy, které budeme v průběhu výkladu používat, a které umožní pochopení problémů na technické úrovni. Předpokladem jsou znalosti základních poznatků matematické analýzy a algebry. Pro výklad se jako vhodný jeví přehled Vladimíra Bužka. Čtenářům s hlubším zájmem o Hilbertův prostor se doporučuje například kniha Davida Cohena zmíněná v referencích.

2.1 Základní matematický aparát

Definice 1: Nechť V je množina objektů (vektorů), $\mathbb{C}$ je množina komplexních čísel, „+" je operace součtu a „·" je operace násobení. Pak se čtveřice $(V, \mathbb{C}, +, \cdot)$ nazývá *komplexní vektorový prostor*, jestliže pro zmíněné operace platí: mějme dány libovolné vektory $\vec{x}, \vec{y}, \vec{z} \in V$ a komplexní čísla $a, b, c \in \mathbb{C}$, pak:

$i)$ $\vec{x} + \vec{y} \in V$
$ii)$ $\vec{x} + (\vec{y} + \vec{z}) = (\vec{x} + \vec{y}) + \vec{z}$
$iii)$ $\exists \vec{0} \in V \Rightarrow \vec{x} + \vec{0} = \vec{x}$
$iv)$ $\exists (-\vec{x}) \in V : \vec{x} + (-\vec{x}) = \vec{0}$
$v)$ $\vec{x} + \vec{y} = \vec{y} + \vec{x}$
$vi)$ $a \cdot \vec{x} \in V$
$vii)$ $1 \cdot \vec{x} = \vec{x}$
$viii)$ $(b \cdot c) \cdot \vec{x} = b \cdot (c \cdot \vec{x})$
$ix)$ $c \cdot (\vec{x} + \vec{y}) = c \cdot \vec{x} + c \cdot \vec{y}$
$x)$ $(b + c) \cdot \vec{x} = b \cdot \vec{x} + c \cdot \vec{x}.$

Poznámka: Vektory budeme v následujícím výkladu chápat jako n-rozměrné prvky $\mathbb{C}^n$.

Definice 2: *Komplexní skalární součin* na vektorovém prostoru přiřazuje libovolným dvěma vektorům $\vec{x}, \vec{y} \in V$ komplexní číslo, které zapisujeme $(\vec{x}, \vec{y})$, a které má pro libovolné $\vec{x}, \vec{y}, \vec{z} \in V$ a $a, b \in \mathbb{C}$ tyto vlastnosti:

$i)$ $(\vec{x}, a\vec{y} + b\vec{z}) = a(\vec{x}, \vec{y}) + b(\vec{x}, \vec{z})$
$ii)$ $(\vec{x}, \vec{y}) = (\vec{y}, \vec{x})^*$
$iii)$ $(\vec{x}, \vec{x}) \geq 0$
$iv)$ $(\vec{x}, \vec{x}) = 0 \Leftrightarrow \vec{x} = \vec{0}.$

Prostory, v nichž je definován skalární součin se nazývají *unitární*. Pro případ vektorů z $\mathbb{C}^N$ navíc platí následující: mějme dva vektory $\vec{x}, \vec{y} \in \mathbb{C}^N$. Potom podmínky z definice skalárního součinu jsou splněny pro $(\vec{x}, \vec{y}) = \sum_{i=1}^{N} x_i^* y_i$, kde x_i, y_i jsou příslušné složky obou vektorů.

Dále říkáme, že jsou dva vektory $\vec{x}, \vec{y} \in V$ vzájemně *ortogonální*, pokud je $(\vec{x}, \vec{y}) = 0$. *Ortogonální bází* potom nazýváme množinu lineárně nezávislých vektorů, jejíž jakékoliv dva různé vektory mají skalární součin roven nule. Příkladem může být množina dvou vektorů z $\mathbb{C}^2$, kde $\vec{x}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\vec{x}_2 = \begin{pmatrix} 0 \\ 2 \end{pmatrix}$.

Definice 3: Každý vektor $\vec{x} \in V$ má k sobě přiřazeno číslo $|| \vec{x} || \in \mathbb{R}$, které představuje jeho *normu* (délku). Pro jakékoliv vektory $\vec{x}, \vec{y} \in V$ a číslo $a \in \mathbb{C}$ platí, že:

i) $|| \vec{x} || \geq 0$
ii) $|| a\vec{x} || = | a | \cdot || \vec{x} ||$
iii) $|| \vec{x} + \vec{y} || \leq || \vec{x} || + || \vec{y} ||$.

Triviálně dále platí, že $|| \vec{x} || = 0 \Leftrightarrow \vec{x} = \vec{0}$. Vektorový prostor, jenž má normu se nazývá *normovaný vektorový prostor*. Pokud je v komplexním vektorovém prostoru definován skalární součin, pak lze normu vyjádřit jako:

$$|| \vec{x} || = \sqrt{(\vec{x}, \vec{x})}.$$

Jsou-li složky ortogonální báze jednotkové délky, tj. $|| \vec{x}_i ||^2 = (\vec{x}_i, \vec{x}_i) = 1$, pak se navíc tato báze nazývá *ortonormální*. Ortonormální báze je například $\vec{x}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\vec{x}_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Pomocí skalárního součinu můžeme rovněž rozkládat vektory do báze. Pro ortogonální bázi vektorů $\{\vec{x}_1, \ldots, \vec{x}_n\}$ platí, že libovolný vektor $\vec{y} \in V$ lze vyjádřit jako lineární kombinaci vektorů této báze:

$$\vec{y} = \sum_{i=1}^{n} \lambda_i \vec{x}_i,$$

kde hledáme koeficienty $\lambda_i \in \mathbb{C}$. Pro tyto koeficienty z ortogonality a Definice 2, bodu *i)* plyne, že $(\vec{x}_i, \vec{y}) = \lambda_i (\vec{x}_i, \vec{x}_i)$. Ukažme si rozklad na následujícím příkladu:

Příklad 1: Pokusme se najít rozklad vektoru $\vec{y}$ do báze $\{\vec{x}_1, \vec{x}_2\}$, kde $\vec{y} = \begin{pmatrix} 1 \\ 2i \end{pmatrix}$ a $\vec{x}_1 = \begin{pmatrix} 1+2i \\ 0 \end{pmatrix}$, $\vec{x}_2 = \begin{pmatrix} 0 \\ 1-2i \end{pmatrix}$. Snadno nejprve ověříme, že báze je ortogonální, protože $(\vec{x}_1, \vec{x}_2) = 0$. Hodnota skalárních součinů $(\vec{x}_1, \vec{x}_1) = (\vec{x}_2, \vec{x}_2) = 5$. Z výrazu $(\vec{x}_i, \vec{y}) = \lambda_i (\vec{x}_i, \vec{x}_i)$ vypočítáme koeficienty $\lambda_1 = \frac{1-2i}{5}$, $\lambda_2 = \frac{2i-4}{5}$. Vidíme tak, že vektor $\vec{y}$ lze rozložit jako

$$\vec{y} = \frac{1-2i}{5} \begin{pmatrix} 1+2i \\ 0 \end{pmatrix} + \frac{2i-4}{5} \begin{pmatrix} 0 \\ 1-2i \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 2i \end{pmatrix} = \begin{pmatrix} 1 \\ 2i \end{pmatrix}.$$

Poznámka: Užití ortonormální báze má výhodu v tom, že $\forall \vec{x}_i$ z báze platí $(\vec{x}_i, \vec{x}_i) = 1$, a tedy $\lambda_i = (\vec{x}_i, \vec{y})$.

Definice 4: Posloupnost vektorů $\{\vec{x}_i\}_{i=0}^{\infty}$ normovaného vektorového prostoru se nazývá *Cauchyho posloupnost* pokud $\forall \varepsilon > 0, \exists n_0$ takové, že pro všechny $n, m > n_0$ je $|| \ \vec{x}_m - \vec{x}_n \ || \leq \varepsilon$.

Definice 5: Vektorový prostor V je *úplný*, pokud každá Cauchyho posloupnost vektorů $\vec{x} \in V$ konverguje k vektoru, který je prvkem V.

Příklad 2: Cauchyho posloupnost se skládá z čísel, jejichž rozdíly se s vyšším indexem čísel posloupnosti zmenšují. Například posloupnost $\{3, 3.1, 3.14, 3.141, 3.1415, \ldots, \pi\}$ je Cauchyho posloupnost racionálních čísel. Vidíme, že prostor racionálních čísel není úplný, protože tato posloupnost konverguje zřejmě k π, jenž není racionální číslo.

Motivací pro zavedení úplnosti Hilbertova prostoru v kvantové informatice je požadavek na vývoj izolovaného kvantového stavu v rámci jednoho Hilbertova prostoru (to znamená, že chceme, aby vývoj stavu konvergoval také do jistého stavu).

Poznámka: Pojem konvergence (limity) vychází ze zavedení metriky prostoru (vzdálenosti mezi dvěma prvky) jako $d(\vec{x}_1, \vec{x}_2) = || \ \vec{x}_2 - \vec{x}_1 \ ||$.

Definice 6: Úplný unitární vektorový prostor se nazývá *Hilbertův prostor* $\mathcal{H}$.

V roce 1932 vyšla v němčině kniha matematika Johna von Neumanna, který v ní popis kvantových systémů zformalizoval.

Postulát 1: Stavy kvantového systému korespondují vektorům Hilbertova prostoru.

V kvantové mechanice se stav zapisuje v tzv. Diracově notaci, která pro zápis vektoru $\vec{x}$ používá ekvivalentu $|x\rangle$ a nazývá jej *ket*. Vektory Hilbertova prostoru (které stále chápeme jako aritmetické) zapisujeme buď v řádku nebo sloupci. Jestliže jsou sloupcové vektory prvky prostoru V, pak řádkové vektory představují prvky tzv. *duálního* prostoru V^*. Duální (konjugovaný) prostor je prostor lineárních funkcí na vektorovém prostoru V. Pokud je pro stavy $|x\rangle, |y\rangle$ definována funkce $f_{|y\rangle} : V \to \mathbb{C}$ jako $f_{|y\rangle}(|x\rangle) = (|x\rangle, |y\rangle)$, pak $f_{|y\rangle}$ je ekvivalentní řádkovému vektoru, který zapisujeme $\langle y|$ a nazýváme *bra*. Lze ukázat, že pro vektory z $\mathbb{C}^n$ představují vektory z V^* komplexně sdruženou transpozici k vektorům z V. S jejich pomocí lze pro dva vektory $\vec{x}, \vec{y}$ odpovídající stavům $|x\rangle$ a $|y\rangle$ definovat skalární součin jako $(|x\rangle, |y\rangle)$, což se obvykle zkracuje na zápis $\langle x|y\rangle$ tvořící závorku (bracket). Shrňme si notaci do následující tabulky:

označení	název	operace	výsledek
$\langle x\|y\rangle$	(vnitřní) skalární součin	řádka × sloupec	skalár
$\|x\rangle\langle y\|$	(vnější) tenzorový součin	sloupec × řádka	matice

Příklad 3: Obecný ket $|x\rangle = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ má příslušný vektor bra $\langle x| = |x\rangle^\dagger = (x_1^*, \ \ldots \ , x_n^*)$, kde symbol $\dagger$ označuje komplexně-sdruženou transpozici.

Příklad 4: Uvažujeme-li tří-složkové vektory $|x\rangle, |y\rangle$, pak skalární součin generuje skalár:

$$\langle x|y\rangle = (x_1^*, x_2^*, x_3^*) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = x_1^* y_1 + x_2^* y_2 + x_3^* y_3.$$

Tenzorový součin generuje v našem případě matici 3×3:

$$|x\rangle\langle y| = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} (y_1^*, y_2^*, y_3^*) = \begin{pmatrix} x_1 y_1^* & x_1 y_2^* & x_1 y_3^* \\ x_2 y_1^* & x_2 y_2^* & x_2 y_3^* \\ x_3 y_1^* & x_3 y_2^* & x_3 y_3^* \end{pmatrix}.$$

Definice 7: Podmnožina prostoru $\mathcal{H}$, která je sama prostorem (ve smyslu Definice 1) se nazývá *podprostor* prostoru $\mathcal{H}$.

Pro každý uzavřený podprostor L v $\mathcal{H}$ existuje jeho komplementární podprostor $L^{\perp}$, který obsahuje prvky kolmé k prvkům L (tj. $\langle x|y\rangle = 0$, pokud je $|x\rangle \in L, |y\rangle \in L^{\perp}$). Navíc každý vektor $|z\rangle \in \mathcal{H}$ lze vyjádřit ve tvaru $|z\rangle = |x\rangle + |y\rangle$, kde $|x\rangle \in L, |y\rangle \in L^{\perp}$. Obecně je možné vyjádřit dekompozici prostoru $\mathcal{H}$ pomocí jeho n ortogonálních podprostorů jako: $\mathcal{H} = L_1 \oplus \ldots \oplus L_n$, kde $\oplus$ představuje direktní součet.

Definice 8: *Lineární operátor* $\boldsymbol{A}$: $\mathcal{H} \to \mathcal{H}$ přiřazuje každému vektoru $|x\rangle \in \mathcal{H}$ vektor $\boldsymbol{A}|x\rangle \in \mathcal{H}$, kde $\forall |x\rangle, |y\rangle \in \mathcal{H}$ a $\forall a, b \in \mathbb{C}$ platí, že $\boldsymbol{A}(a|x\rangle + b|y\rangle) = a\boldsymbol{A}|x\rangle + b\boldsymbol{A}|y\rangle$.

Lineární operátory tedy umožňují transformovat vektory v jednom prostoru. Pokud operátor $\boldsymbol{A}$ působí na vektory duálního prostoru, potom takovou operaci zapisujeme $\langle x|\boldsymbol{A}$. Elementy matice lineárního operátoru můžeme rovněž vyjádřit pomocí bázových vektorů jako $\boldsymbol{A}_{ij} = \langle x_i|\boldsymbol{A}|x_j\rangle$, kde i, j jsou indexy řádků a sloupců a množina $\{x_1, \ldots, x_i\}$ je báze indexovaná stejně jako řádky.

Operátor, který zobrazuje vektory na sebe samy se nazývá *jednotkový* a značí se $\boldsymbol{1}$. Je definován pomocí bázových vektorů $\{\vec{x}_1, \ldots, \vec{x}_n\}$ jako $\boldsymbol{1} = \sum_{i=1}^{n} |x_i\rangle\langle x_i|$. Pro ortonormální bázi se zřejmě jedná o jednotkovou matici.

Definice 9: Operátor $\boldsymbol{A}^{\dagger}$ se nazývá sdružený (adjungovaný) k operátoru $\boldsymbol{A}$, jestliže pro všechny $|x\rangle, |y\rangle \in \mathcal{H}$ platí, že $\langle y|\boldsymbol{A}^{\dagger}|x\rangle = \langle x|\boldsymbol{A}|y\rangle^*$.

Pro popis fyzikálních veličin (pozorovatelných veličin) používá kvantová mechanika zvláštní třídu tzv. *Hermitových operátorů.*

Definice 10: Operátor $\boldsymbol{A}$ se nazývá samosdružený (také Hermitový), jestliže pro všechny $|x\rangle, |y\rangle \in \mathcal{H}$ platí, že $\langle y|\boldsymbol{A}|x\rangle = \langle x|\boldsymbol{A}|y\rangle^*$, tj. $\boldsymbol{A} = \boldsymbol{A}^{\dagger}$.

Definice 11: Lineární operátor $\boldsymbol{A}$ má vlastní vektory $|\lambda\rangle$ a vlastní hodnoty λ, kde $(\boldsymbol{A} - \lambda\boldsymbol{1})|\lambda\rangle = 0$, resp. $\boldsymbol{A}|\lambda\rangle = \lambda|\lambda\rangle$.

Pro výpočet vlastních hodnot si všimněme, že determinant $\det(\boldsymbol{A} - \lambda\boldsymbol{1}) = 0$. V případě Hermitových operátorů, jsou všechny vlastní hodnoty reálné. Ty korespondují všem (také reálným) možným výsledkům měření určité veličiny. Odpovídající vlastní vektory jsou přitom navzájem ortogonální.

Postulát 2: Pozorovatelné fyzikální veličiny se popisují Hermitovými operátory, jejichž reálné vlastní hodnoty odpovídají možným výsledkům měření.

Vlastní vektory Hermitových operátorů operujících na prostoru $\mathcal{H}$ tvoří jeho bázi, tj. všechny vektory $|x\rangle \in \mathcal{H}$ lze vyjádřit jako $|x\rangle = \sum c_i|\lambda_i\rangle$, kde $|\lambda_i\rangle$ jsou vlastní vektory a $c_i \in \mathbb{C}$ jsou příslušné koeficienty.

Definice 12: *Unitární* lineární operátor $\boldsymbol{U}$ provádí zobrazení celého prostoru $\mathcal{H}$ na sama sebe a pro vektory $|x\rangle, |y\rangle \in \mathcal{H}$ platí, že $\langle x|\,\boldsymbol{U}^\dagger\,\boldsymbol{U}|y\rangle = \langle x|y\rangle$.

Poslední podmínka znamená, že aplikace unitárního operátoru nemění skalární součin obou vektorů a můžeme ji také zapsat jako $\boldsymbol{U}^\dagger\,\boldsymbol{U} = \boldsymbol{U}\,\boldsymbol{U}^\dagger = \boldsymbol{1}$.

Nyní máme nadefinovány základní pojmy, které budeme používat. K ostatním se dostaneme při výkladu konkrétních problémů. Protože jsme se zatím kromě důležitých sdělení v postulátech nedozvěděli, jak kvantová mechanika s tímto matematickým formalizmem souvisí, musíme si nyní o tomto vztahu povědět více. Začněme popisem kvantového stavu a problematickou otázkou měření kvantového systému.

2.2 Kvantový stav

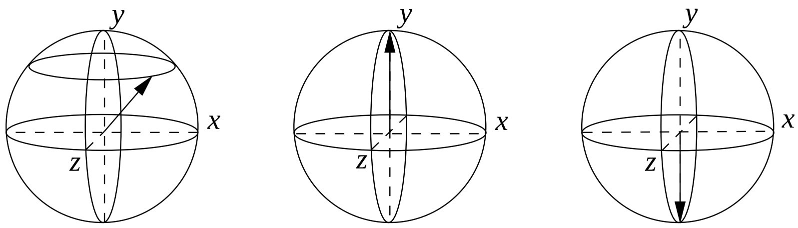
Kvantový stav představuje v kvantové mechanice reprezentaci fyzikální reality. Ta má podle Kodaňské interpretace kvantové mechaniky dvě hlavní části. První je část klasického světa, která odpovídá tomu, jak se na tento svět díváme a jaký jej registrujeme. Druhou součástí je kvantový svět, který není přímo přístupný. Můžeme z něj však pomocí aktu měření extrahovat určité informace. V klasické části nabývá při měření kvantový systém (například energetická hladina elektronu v atomu vodíku nebo spin elektronu) pouze diskrétní hodnoty odpovídající skokům v celkové energii daného systému. Na kvantové úrovni (v kvantové části světa) však mohou sledované veličiny nabývat nekonečně mnoho hodnot odpovídajících nekonečně mnoho kvantovým stavům. Již z těchto poznatků vidíme, že existuje zásadní rozdíl mezi systémem, na němž bylo provedeno měření a takovým, který je izolován od okolí a spojitě se vyvíjí. Spojitý a deterministický vývoj kvantového systému v kvantové mechanice popisuje Schrödingerova vlnová rovnice, jejímž řešením je vlnová funkce odpovídající danému kvantovému systému. Kvantový systém se však může skládat z více vlnových funkcí, o kterých říkáme, že jsou v *superpozici*. To znamená, že kvantový stav je vyjádřen jako součet několika vlnových funkcí. Aby bylo zřejmé jakým příspěvkem se podílí každá vlnová funkce na celkovém stavu, přísluší každému stavu komplexní hodnota tzv. *amplitudy pravděpodobnosti*. Z klasického pohledu nás však zajímá, jak můžeme z takového kvantového systému získat určitou informaci. V této chvíli se dostáváme k otázce měření podrobněji. Měření většinou provádíme tak, že vyšleme foton ke zkoumanému systému. Foton v podobě změny své energie unáší ze systému informaci, kterou zpětně detekujeme. Taková interakce fotonu s kvantovým systémem má však za následek tzv. *kolaps (redukci)* vlnové funkce, která stochasticky přejde do jednoho z možných stavů složeného systému. Každému stavu přísluší výše zmíněná amplituda pravděpodobnosti. Druhá mocnina její absolutní hodnoty udává, s jakou pravděpodobností bude změřen každý z možných stavů. Amplituda pravděpodobnosti může být na rozdíl od klasické pravděpodobnosti také komplexní (a záporná) a dovoluje nám tak čistě kvantovými interakcemi (takovými, které nepředstavují přímé měření) ovlivňovat výsledek měření. Protože měření nemusí vždy vracet numerický výsledek (např. polarizace fotonů – horizontální × vertikální), označuje se měřitelná vlastnost fyzikálního systému jako *pozorovatelná* veličina (observable). Všimněme si, že zavedením amplitud pravděpodobností je charakter kvantového měření pravděpodobnostní, což poukazuje na náhodný element, tvořící základ pozorovaným fyzikálním procesům.

Nyní se zaměřme na to, jak jsou tyto poznatky kvantové mechaniky použitelné v oblasti kvantové informatiky. U klasických počítačů jsme zvyklí reprezentovat bit napěťovými úrovněmi, které dostatečně odlišují 0 od 1. U kvantových počítačů je možné použít některý z dvoustavových kvantových systémů jako je například spin částice (tj. spin 1/2 u leptonů). Takový systém může klasicky nabývat pouze 2 hodnot (stavů): $|+\frac{1}{2}\rangle$ a $|-\frac{1}{2}\rangle$. Tak si lze představit, že bity 0 a 1 zakódujeme pomocí jednoho a druhého spinového stavu. Spin částice je jen jeden z více možných dvoustavových kvantových systémů, které lze použít. Jiné systémy by obstály stejně dobře. Kvantový stav popisujeme vektorem v komplexním lineárním Hilbertově prostoru. Každému prvku báze tohoto prostoru (tj. dimenzi) přísluší jeden vlastní stav, do kterého může kvantový systém při měření přejít. Vlastní stavy jsou přitom vzájemně ortogonální[4]. Nicméně kvantový systém prochází podle Schrödingerovy vlnové rovnice spojitým vývojem stavového vektoru a může tak nabývat nekonečného množství stavů. Libovolný stav (a tím i bod Hilbertova prostoru) můžeme vyjádřit jako součet vlastních stavů (bázových vektorů) násobených komplexními váhovými koeficienty, které představují příspěvek daného bázového vektoru v celkovém stavu. O takovém systému říkáme, že je v koherentní superpozici více stavů vyjádřené jako lineární kombinace bázových vektorů. Pro nejjednodušší případ, kdy chceme vyjádřit kvantový bit jako hodnoty 0 a 1, potřebujeme dva vlastní stavy dvojrozměrného Hilbertova prostoru. Pak takový systém zapisujeme jako:

$$|\psi\rangle = \omega_0|\psi_0\rangle + \omega_1|\psi_1\rangle,$$

kde $\omega_0, \omega_1 \in \mathbb{C}$. Tyto koeficienty odpovídají amplitudám pravděpodobnosti a mají fyzikální význam ve své druhé mocnině absolutní hodnoty, která říká s jakou pravděpodobností naměříme příslušný vlastní stav. Přitom součet pravděpodobností je obecně přes i různých vlastních stavů prostoru $\mathcal{H}^i$ v případě,

[4]Pokud si chceme takový prostor alespoň částečně představit můžeme říci, že vlastním stavům odpovídají osy prostoru, které jsou mezi sebou navzájem kolmé.



Obrázek 1: **Reprezentace dvoustavového systému:** na obrázku vlevo je znázorněn doposud neměřený stav qubitu, v němž jsou v určitém poměru zastoupeny stavy $|0\rangle$ a $|1\rangle$, na prostředním obrázku je pak vlastní stav $|1\rangle$ a vpravo stav $|0\rangle$.

že jsou koeficienty normovány, roven 1:

$$\sum_{i=0}^{n-1} |\omega_i|^2 = 1.$$

Vlastní stavy $|\psi_0\rangle$ a $|\psi_1\rangle$ (odpovídající klasickým bitům) se obvykle označují jako stavy $|0\rangle$ a $|1\rangle$. Pokud tyto vlastní stavy odpovídají bázovým vektorům $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ můžeme psát, že

$$|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle = \begin{pmatrix} \omega_0 \\ \omega_1 \end{pmatrix}.$$

Takový dvoustavový systém, který představuje kvantový bit, nebo-li *qubit*, je možné názorně zobrazit jako vektor v Riemannově kouli s umístěním v počátku souřadnic (viz obrázek). V něm je $|1\rangle$ reprezentována jako vektor směřující k severnímu pólu, $|0\rangle$ k jižnímu. Z úhlu, který vektor svírá se svislou osou je možné vyčíst poměrné zastoupení $|1\rangle$ a $|0\rangle$ ve stavovém vektoru. Úhel, o který je vektor otočen kolem svislé osy se nazývá *fáze*, která nemění poměr $|1\rangle$ a $|0\rangle$, ale je významná vzhledem k jevu *kvantové interference*, o kterém se zmíníme později. Qubit je možné znázornit i v polárních souřadnicích na tzv. Blochově kouli, ve které je stav qubitu vyjádřen pro úhly polárních souřadnic θ, ϕ jako $\cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$. Pro vícestavový kvantový systém je možné výše uvedený výraz pro superpozici zobecnit na

$$|\psi\rangle = \sum_{i=0}^{n-1} \omega_i|\psi_i\rangle.$$

Na závěr této části si pro přehlednost shrňme, jak korespondují pojmy kvantové mechaniky s pojmy kvantové informatiky pro qubit ($\mathcal{H}^2$).

kvantová mechanika	kvantová informatika
vlnová funkce ψ_1 vlastní hodnota a_1	vlastní stav $\|0\rangle$ logická hodnota 0
vlnová funkce ψ_2 vlastní hodnota a_2	vlastní stav $\|1\rangle$ logická hodnota 1
superpozice $\psi_1 + \psi_2$	superpozice $\|0\rangle + \|1\rangle$

2.3 Měření kvantového systému

Jak víme, procesu měření odpovídají Hermitové operátory, jejichž vlastní hodnoty představují možné výsledky měření. To lze popsat operací $\boldsymbol{A}|\psi\rangle = a|\psi\rangle$, kde a je reálná vlastní hodnota odpovídající výsledku měření a $\boldsymbol{A}$ je Hermitový operátor. Existují však pozorovatelné veličiny (a tím i operátory), jejichž vlastní stavy mají stejné vlastní hodnoty a nelze tudíž po měření určit, do kterého vlastního stavu systém přešel. Podle počtu stejných vlastních hodnot příslušejících několika vlastním stavům se vlastní hodnota nazývá n-krát *degenerovaná*. Pro *nedegenerovanou* vlastní hodnotu (jedinečnou pro daný vlastní stav) operátoru $\boldsymbol{A}$ je vlastní stav po měření dán naměřenou hodnotou této pozorovatelné veličiny. U degenerovaných vlastních hodnot ale nevíme, v jakém stavu se systém nalézá, tzn. že ze systému nezískáme žádnou další informaci, přestože jsme jej změřili. Tato nerozhodnost v možných stavech po měření se popisuje tzv. *projekčními operátory*.

Definice 13: $\boldsymbol{P}$ je projekční operátor, jestliže $\boldsymbol{P} = \boldsymbol{P}^\dagger$ a $\boldsymbol{P} = \boldsymbol{P}^2$.

Příklad 5: Příklady projekčních operátorů: $\boldsymbol{P} = \boldsymbol{1}$, $\boldsymbol{P} = |\psi\rangle\langle\psi|$.

Postulát 3: Po měření pozorovatelné veličiny (korespondující operátoru $\boldsymbol{A}$) s výsledkem možné degenerované vlastní hodnoty přechází systém do stavu $\boldsymbol{P}_i|\psi\rangle$, kde $\boldsymbol{P}_i$ je projekční operátor podprostoru L generovaný všemi vlastními vektory $\{|\psi_{ij}\rangle\}$ operátoru $\boldsymbol{A}$, které odpovídají měřené vlastní hodnotě a_i, tj. $\boldsymbol{P}_i = \sum_j |\psi_{ij}\rangle\langle\psi_{ij}|$.

V případě degenerované vlastní hodnoty tak systém zůstává stále v superpozici více vlastních stavů, které odpovídají změřené vlastní hodnotě. Takovým měřením se vlastní stavy s jinou vlastní hodnotou vyloučily. Projekční měření má zásadní význam například u některých kvantových algoritmů, kdy potřebujeme měřením redukovat superpozici stavů v kvantovém registru na jejich určitou podmnožinu.

2.4 Kvantový registr

Až do této chvíle jsme uvažovali pouze jediný osamocený kvantový systém, který představoval jeden qubit. Jak ale víme, klasické počítače jsou vybaveny registry skládajícími se z několika bitových registrů. Takový model, ve kterém je zapotřebí popsat více qubitů, se v kvantové mechanice zapisuje jako *direktní tenzorový součin* více stavů, který zapisujeme pomocí operace $\otimes$. Formálně tak vytváříme nový prostor generovaný tenzorovým součinem. Například pro dva qubity lze psát, že pokud $|\psi_a\rangle \in \mathcal{H}_1$ a $|\psi_b\rangle \in \mathcal{H}_2$, pak $|\psi_a\rangle \otimes |\psi_b\rangle \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Dále platí, že

$$|\psi_a\rangle \otimes |\psi_b\rangle = \begin{pmatrix} \omega_{0a} \\ \omega_{1a} \end{pmatrix} \otimes \begin{pmatrix} \omega_{0b} \\ \omega_{1b} \end{pmatrix} = \begin{pmatrix} \omega_{0a}\,\omega_{0b} \\ \omega_{0a}\,\omega_{1b} \\ \omega_{1a}\,\omega_{0b} \\ \omega_{1a}\,\omega_{1b} \end{pmatrix} = \begin{pmatrix} \omega_{00} \\ \omega_{01} \\ \omega_{10} \\ \omega_{11} \end{pmatrix} = |\psi_{ab}\rangle.$$

Odtud dostáváme sadu nových amplitud pravděpodobností, které odpovídají složeným stavům $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Z toho si lze odvodit novou bázi systému, která má nyní podobu:

$$|00\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |01\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \quad |10\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |11\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

Takový paměťový registr, který se skládá ze dvou qubitů, pak analogicky k zápisu jednoduchého qubitového systému obecně vyjádříme jako $|\psi_{ab}\rangle = \omega_{00}|00\rangle + \omega_{01}|01\rangle + \omega_{10}|10\rangle + \omega_{11}|11\rangle$. Podobně můžeme pokračovat i s registry větší délky: jestliže jsou báze $\mathcal{B}_1, \dots, \mathcal{B}_k$ ortonormálními bázemi prostorů $\mathcal{H}_1, \dots, \mathcal{H}_k$, pak $\mathcal{B} = \bigotimes_{i=1}^{k} \mathcal{B}_i$ je ortonormální bází prostoru $\mathcal{H} = \bigotimes_{i=1}^{k} \mathcal{H}_i$.

V souvislosti s kvantovými registry si někteří fyzici všimli, že složitost simulace kvantových systémů roste exponenciálně s počtem částic (qubitů registru). Napadlo je tedy, zda by zkonstruovaný kvantový počítač nemohl některé exponenciálně složité úlohy řešit efektivněji. Je totiž zřejmé, že kvantový registr v superpozici můžeme chápat jako exponenciálně paralelizovanou verzi paměťového registru, který je schopen pojmout 2^n hodnot současně, kde n je počet qubitů registru. Kvantovou operací nad takovým registrem bychom tak manipulovali 2^n amplitudami zároveň. Tato vlastnost kvantových systémů se označuje jako *kvantový paralelismus* a má rozhodující vliv na efektivitu, s jakou kvantový počítač pracuje.

Na závěr této části se zmiňme o jedné z nejpodivnějších vlastností kvantového světa. Víme, jak vyjádřit jeden nebo více qubitů. Vždy jsou však na sobě jednotlivé qubity zcela nezávislé (popsané oddělenými Hilbertovými prostory). Existují však fyzikální procesy, kterými můžeme připravit registr, jenž nelze vyjádřit jako tenzorový součin dílčích qubitů. V takovém případě říkáme, že jsou qubity *propleteny (entangled)*. Propletení je stav, ve kterém jsou qubity na sobě v nějakém smyslu závislé (jejich stavy jsou přes určitý atribut korelovány). Konkrétně provedením měření na jednom qubitu víme (již bez měření), jaká je hodnota druhého qubitu. Možné případy můžeme pro propletené qubity $|\psi_a\rangle, |\psi_b\rangle$ vyjádřit pomocí pravděpodobností jako

$$\begin{array}{ll} p(|\psi_b\rangle = 1 \mid |\psi_a\rangle = 0) = 0, & p(|\psi_b\rangle = 1 \mid |\psi_a\rangle = 1) = 1, \\ p(|\psi_b\rangle = 0 \mid |\psi_a\rangle = 1) = 0, & p(|\psi_b\rangle = 0 \mid |\psi_a\rangle = 0) = 1. \end{array}$$

Tyto podmínky platí zároveň a odpovídají propletení $|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Propletení dvou qubitů lze také vyjádřit jako $|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, přičemž platí podobné podmínky jako v předchozím případě. Měřením se propletení rozpadá a oba qubity nabývají klasických hodnot.

Příklad 6: Ukážeme si, že propletený stav nelze vyjádřit jako součin dílčích složek. Propletení lze zapsat například jako $|\psi_{ab}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Pokud předpokládáme, že tento stav vznikl tenzorovým součinem stavů $|\psi_a\rangle = \omega_{0_a}|0\rangle +$

$\omega_{1_a}|1\rangle, |\psi_b\rangle = \omega_{0_b}|0\rangle + \omega_{1_b}|1\rangle$, pak pro amplitudy kombinací všech qubitů musí platit, že

$$\begin{array}{llll} |00\rangle: & \omega_{0_a}\omega_{0_b} = \frac{1}{\sqrt{2}}, & |01\rangle: & \omega_{0_a}\omega_{1_b} = 0, \\ |10\rangle: & \omega_{1_a}\omega_{0_b} = 0, & |11\rangle: & \omega_{1_a}\omega_{1_b} = \frac{1}{\sqrt{2}}. \end{array}$$

Pro $|00\rangle$ a $|11\rangle$ musí být koeficienty nenulové, což je v rozporu s dalšími dvěmi podmínkami. Vidíme tak, že propletený stav nelze tenzorovým součinem dílčích qubitů vyjádřit. O fenoménu kvantového propletení budeme podrobněji hovořit v kapitole o kvantové teleportaci, kde se tento jev uplatňuje.

2.5 Vývoj kvantového systému

Vývojem (evolucí) kvantového systému máme na mysli jeho změnu s časem. Nyní je důležité připomenout, že právě zde je zásadní rozdíl mezi pozorovaným a nepozorovaným systémem. V případě, že jej *nepozorujeme*, podléhá stavový vektor spojitému vývoji, který jednoznačně popisuje s tímto systémem související Schrödingerova vlnová rovnice:

$$i\,\hbar\frac{\partial\Psi(t)}{\partial t} = \left(-\frac{\hbar^2}{2m}\Delta + V(t)\right)\Psi(t).$$

Abychom však mohli kvantový systém matematicky ovlivňovat, je zapotřebí definovat vhodné operátory. V kvantové mechanice jsou však dovoleny pouze některé způsoby vývoje systému. Jmenovitě jde o takové vývoje, z jejichž výsledků (výstupů) se dají jedinečně odvodit předchozí stavy (vstupy). To je podmínka tzv. *reverzibility* vývoje kvantového stavu, která plyne z deterministické povahy Schrödingerovy rovnice. Taková reverzibilita je však matematicky možná jen pokud jsou operátory čtvercové *unitární matice*, tj. pokud o takových maticích platí, že $\boldsymbol{U}\,\boldsymbol{U}^\dagger = \boldsymbol{1}$. Pokud jsou stavové vektory normalizovány a jsou to tedy body v kouli o poloměru 1, pak unitární kvantový vývoj s těmito body *rotuje*. Jestliže provedeme následující úpravy

$$|\Psi(t)\rangle = \Psi(t) \qquad \text{a} \qquad \boldsymbol{H}(t) = -\frac{\hbar^2}{2m}\Delta + V(t),$$

lze Schrödingerovu vlnovou rovnici přepsat na

$$i\,\hbar\frac{\partial|\Psi(t)\rangle}{\partial t} = \boldsymbol{H}(t)\;|\Psi(t)\rangle,$$

kde $\boldsymbol{H}(t)$ je *Hamiltonián.* Jak je vidět i z výše uvedené substituce, je Hamiltonián úzce spjat s energií systému a jeho podoba je odvozena od fyzického uspořádání částic nebo molekul, z nichž se systém skládá (mohou ho charakterizovat například veličiny jako síla el.pole nebo směr molekulového dipólového momentu). Hamiltonián se skládá z vektorů vlastních stavů a tvoří bázi v Hilbertově prostoru. Obecně by mohly mít vlastní stavy komplexní vlastní hodnoty, ale protože je Hamiltonián Hermitová matice (tj. $\boldsymbol{H} = \boldsymbol{H}^\dagger$), mají vlastní stavy garantovány reálné vlastní hodnoty, které korespondují možným výsledkům měření nějaké fyzikální veličiny. V Hamiltoniánu jsou, kromě informací o vlastních stavech, obsaženy informace o všech operacích, které během výpočtu použijeme. Jestliže uvažujeme Hamiltonián, který není závislý na čase, tzn. takový, který se po dobu vývoje systému nemění a paměťový registr je na počátku ve stavu $|\Psi(0)\rangle$, má vlnová rovnice řešení

$$|\Psi(t)\rangle = e^{-i\boldsymbol{H}t/\hbar}|\Psi(0)\rangle = \boldsymbol{U}(t)|\Psi(0)\rangle.$$

$\boldsymbol{U}(t) = e^{-i\boldsymbol{H}t/\hbar}$ se nazývá časově závislý *evoluční operátor*, který je vždy unitární matice. Evoluční operátor nám tedy ukazuje, jak se systém dynamicky vyvíjí v čase. Jak by řečeno, v Hamiltoniánu jsou zaznamenány kvantové operace, které popisují výpočet. K vyjádření takové operace na kvantovém systému nám postačuje operátor, kterým násobíme příslušný stav. Například operátor

$$\boldsymbol{U}(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$

můžeme použít s parametrem $\theta = \frac{\pi}{4}$, abychom převedli systém z vlastního stavu $|0\rangle$ do vyvážené superpozice stavů $|0\rangle$ a $|1\rangle$:

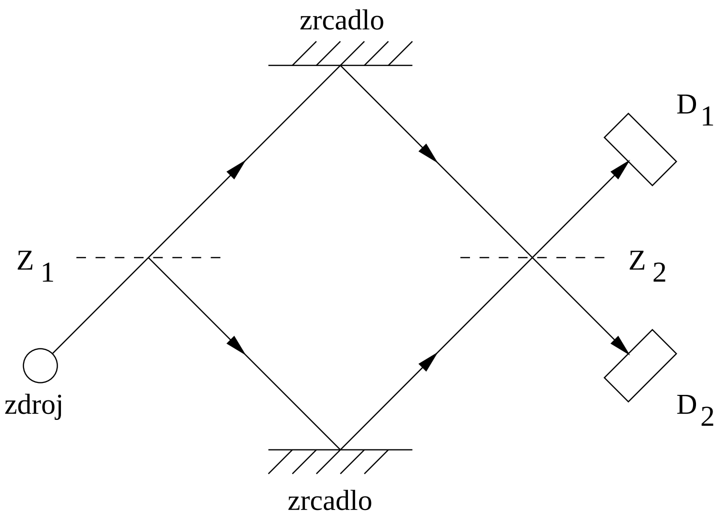
$$\boldsymbol{U}\left(\frac{\pi}{4}\right)|0\rangle = \boldsymbol{U}\left(\frac{\pi}{4}\right)\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Z amplitud pravděpodobností vidíme, že stavy jsou opravdu vyvážené a normalizované, protože $\omega_0 = \omega_1$ a $\omega_0^2 + \omega_1^2 = 1$.

Vraťme se nyní na počátek a připomeňme, že těmito operacemi je možné systém vyvíjet pouze pokud není pozorován (je *dostatečně* izolován od okolí). V případě, že jej však změříme, přejde stochasticky do jednoho z vlastních stavů podle toho, jaké jsou hodnoty jejich amplitud pravděpodobností a podle výsledku našeho měření.

2.6 Kvantová interference

Kvantová interference je jedna z dalších vlastností mikrosvěta, kterou popisuje kvantová mechanika. Odráží se v ní vlastnost kvantového systému existovat v superpozici více stavů. Nejlépe si ji vysvětlíme na příkladu Machova-Zehnderova interferometru, v němž má zdrojem vygenerovaný foton možnost projít více (dvěmi) experimentálními cestami. Představme si přístroj, který se skládá ze zdroje fotonů světla, dvou klasických zrcadel, dvou polopropustných zrcadel (které polovinu intenzity světla propouští a druhou odráží) a dvou detektorů. Konfigurace zařízení je znázorněna na obrázku. Polopropustná zrcadla byla navíc navržena tak, že pokud se na nich paprsek láme, pak se fáze jeho vlny posune o 1/4 vlnové délky. (Právě této fázi odpovídá i fáze vektoru, kterého užíváme k reprezentaci dvoustavového kvantového systému. Je specifikována komplexní složkou amplitudy pravděpodobnosti a geometricky představuje rotaci vektoru v kouli mimo rovinu xy.) To má za následek, že pokud vyšleme ze zdroje spojité světlo, je rozděleno prvním polopropustným zrcadlem Z_1 na dvě části. Část,



Obrázek 2: **Machův-Zehnderův interferometr:** (popis v textu).

která prochází spodní větví je posunuta o $\frac{\lambda}{4}$; při průchodu polopropustným zrcadlem Z_2 ve směru detektoru D_2 je to již o $\frac{\lambda}{2}$. V této chvíli ale potká „neposunutou“ vlnu světla z horní větve. V takovém případě dochází ke klasické interferenci dvou vln. Kvůli posunutí jedné vlny o $\frac{\lambda}{2}$ je tato interference *destruktivní* a na detektoru D_2 nic nenaměříme. Druhá část rozděleného světla se naopak v obou větvích posune po jednom odrazu shodně o $\frac{\lambda}{4}$ a za zrcadlem Z_2 dojde ke *konstruktivní* interferenci, takže celou intenzitu zdrojového světla registrujeme jen na detektoru D_1. Na těchto závěrech není nic překvapivého a plně odpovídají klasické vlnové teorii – podvědomě si zde představujeme fotony jako vlny dělitelné intenzity. Co se však stane, vyšleme-li z generátoru pouze jediný foton? Výsledek experimentu je v tuto chvíli zarážející. Na předchozím výsledku se nic nemění a foton vždy registrujeme v detektoru D_1. Takový výsledek je možné vysvětlit pouze jediným způsobem – foton musel projít oběma rameny současně a na zrcadle Z_2 interferovat sám se sebou – ve směru detektoru D_1 konstruktivně a ve směru D_2 destruktivně. V případě, že ale odstraníme zrcadlo Z_2, nemá elektron na čem interferovat a my jej po odraze na zrcadle Z_1 naměříme se stejnou pravděpodobností buď na detektoru D_1 nebo D_2. Řekněme ale, že se pokusíme foton nachytat tím, že zrcadlo Z_2 umístíme do aparatury pokusu až v době, kdy už prošel zrcadlem Z_1. Napadne nás, že v době nepřítomnosti zrcadla si již částicově se chovající foton vybral právě jednu z cest experimentem a pokud to byla pravě horní, je nyní 50% šance, že projde přidaným zrcadlem přímo do detektoru D_2. To se však neděje a experimentálně bylo potvrzeno, že foton prošel opět oběma rameny naráz a bude vždy naměřen jen v detektoru D_1. Tento experiment dobře potvrzuje nedělitelnou vlastnost kvantových systémů – jejich *vlnově-částicovou dualitu.* S klasickým myšlením bychom chtěli mezi oběmi povahami částic rozlišovat, v kvantově mechanickém světě to však není možné. Dualizmus však uvažujeme do chvíle kolapsu vlnové funkce. Potom si již musíme vybrat jen jednu možnost, podobně jako tomu bylo v popsaném experimentu.

Jiným známým experimentem je průchod elektronu dvojštěrbinou, kdy foton projde oběmi štěrbinami současně a interferuje sám se sebou. Kdybychom si nakreslili mapu pravděpodobností, kde se na stínítku za štěrbinou foton nachází, obdrželi bychom známé interferenční obrazce.

Interference má v kvantovém počítání rozhodující význam při získávání výsledku z kvantového registru. Podobně jako se elektronové vlny navzájem interferenčně skládaly, dochází také mezi jednotlivými qubity registru (po příslušné unitární operaci) ke vzájemným interferenčním působením, což má za následek úpravy amplitud pravděpodobností stavů v superpozici. To umožňuje příznivé stavy (správná řešení) zvýraznit (konstruktivní interference) a nepříznivé potlačit (destruktivní interference).

Na závěr této části si shrňme nejdůležitější poznatky kvantové mechaniky, které se uplatňují v kvantové informatice a jejichž využití je považováno pro určité úlohy za velmi výhodné (je nutné zdůraznit, že kvantové počítače nemohou proměnit obecně nevypočitatelné úlohy ve vypočitatelné, ale dokáží některé vypočitatelné problémy řešit efektivněji).

1. Superpozice: Kvantový stav popsaný vlnovou funkcí, která je řešením příslušné Schödingerovy rovnice, se může nacházet v superpozici, která je součtem příspěvků více vlastních stavů, které odpovídají vlastním vlnovým funkcím. V kvantové informatice zapisujeme obecný stav qubitu jako superpozici $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$. Superpozice je základní vlastnost umožňující **masivní kvantový paralelismus**, který je příčinou exponenciálního zrychlení některých algoritmů.

2. Interference: Při provádění kvantových operací nad superpozicí umožňuje interference měnit amplitudy pravděpodobností vlastních stavů tak, že stav odpovídající řešení má co nejvyšší klasickou pravděpodobnost následného změření.

3. Propletení: Propletení je vlastnost složených kvantových systémů, které mohou existovat ve stavu, jenž nelze vyjádřit jako tenzorový součin jeho složek. Propletení má nelokální povahu a využívá se například u kvantové teleportace nebo u superhustého kódování.

3 Matematické modely počítačů

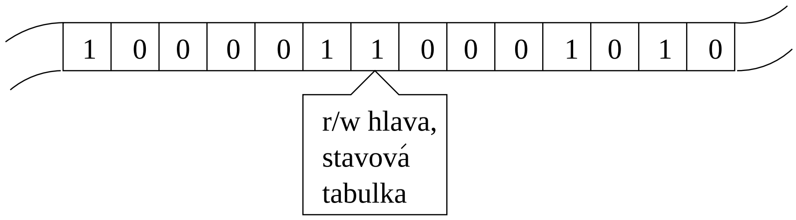
U počítačů jsme ze současných zkušeností zvyklí, že řeší nějaké problémy. V těchto případech se více zaměřujeme na aplikaci a méně nás zajímá teoretický model výpočetních úkonů, které počítač provádí. Již před časem, v roce 1936, se však teoretici Alan Turing, Alonso Church a Kurt Gödel zabývali právě těmito teoretickými základy, na nichž by se dala moderní počítačová věda definovat. Nezávisle na sobě hledali univerzální model, který by z hlediska funkce bez ohledu na fyzikální vlastnosti popsal chování libovolného výpočtu. Každý přišel s vlastním návrhem jak tento problém vyřešit. Později bylo dokázáno, že všechny tři řešení jsou ekvivalentní, přestože každé vychází z rozdílných úvah. Nejčastěji zmiňovaným řešením se stal model Alana Turinga, který byl založen na matematické abstrakci výpočetního stroje, jenž se označuje jako *Turingův stroj*. V této kapitole se proto budeme zabývat matematickými modely počítačů. Nejprve si popíšeme klasický deterministický Turingův stroj, poté se zmíníme o jeho pravděpodobnostní verzi a na závěr uvedeme jeho paralelu v kvantovém světě.

3.1 Klasický Turingův stroj

Motivací pro Turingův stroj se stal v roce 1900 tzv. *Entscheidungsproblem* (rozhodovací problém). V něm německý matematik David Hilbert formuloval problém, ve kterém se ptal, zda existuje mechanický proces, kterým je možno rozhodnout o pravdivosti libovolného matematického teorému nebo výroku. Hilbert se chtěl přesvědčit, zda je například možné vyjádřit kroky matematického důkazu spíše posloupností symbolů, než složitým matematickým aparátem. Toho se chopil Turing a navrhl stroj, který měl simulovat postup matematika při vytváření důkazu. Takový stroj měl několik základních vlastností:

- musel nahradit složitou symboliku matematických kroků. V takovém případě šlo každou konečnou množinu symbolů nahradit pouze dvěma symboly (jako je 0 a 1) a prázdnou mezerou, která by oba symboly oddělovala.
- podobně jako si matematik zapisuje poznámky na papír, má Turingův stroj k zápisu nekonečnou pásku skládající se z buněk, do/ze kterých se symbol zapisuje/čte.
- nad touto páskou je možné provádět za pomocí čtecí hlavy operace čtení, zápisu a posunu pásky (`read, write, shl, shr`).
- protože je možné symboly číst, zapisovat nebo se posunovat po pásce, je pro Turingův stroj důležitý vnitřní stav, ve kterém operaci čtení provádíme (čtený symbol a stav tak určují další akci a přechod do dalšího stavu).

Protože se chování tohoto stroje vyvíjí podle tabulky přechodů, můžeme říci, že každý následující stav lze jednoznačně určit na základě čteného symbolu a aktuálního stavu. Jeho chování je proto *deterministické*. Výpočet začíná tak, že



Obrázek 3: **Deterministický Turingův stroj**

jsou na pásce uložena počáteční data (pokud jsou nějaká) a vlastní kód programu. Hlava je pak uvedena do stavu, který odpovídá načtení kódu programu a stroj tak započne výpočet, přechází mezi stavy a po skončení většinou zapíše výsledek. Vidíme, že takto se chovající model by se dal velmi dobře přirovnat k funkci dnešních počítačů. Přestože moderní technologie nevídaně od 30.let pokročily, Turingův model můžeme k popisu chování počítačů použít bez úprav i dnes. S trochou nadsázky se dá říci, že principiálně se supervýkonný ASCI Red od Intelu rovná jakémukoliv stolnímu počítači. Pomocí Turingova stroje pak bylo dokázáno, že odpověď na počáteční Hilbertovu otázku je záporná. Neexistuje tak mechanický stroj, který by rozhodl pravdivost nebo nepravdivost libovolného matematického výroku.

3.2 Pravděpodobnostní Turingův stroj

V předchozím odstavci jsme se zabývali deterministickou verzí Turingova stroje. Nyní si však představme, že vývoj mezi stavy se řídí podle toho, jaký je výsledek nějakého náhodného jevu – například hodu kostkou. V takovém případě je následující stav určen *stochasticky* výsledkem hodu. Navíc s možností upřednostnit nebo potlačit některé směry vývoje pomocí váhových koeficientů. Na tomto základu je založen *pravděpodobnostní Turingův stroj (PTS)*. PTS je schopen řešit všechny problémy deterministického Turingova stroje a často dokonce dojde k řešení rychleji. U obou typů strojů vlastně balancujeme mezi dvěma póly: jistota, že dojdeme k řešení (pokud existuje) u klasického Turingova stroje stojí proti možnosti, že najdeme správné řešení rychleji u PTS.

Přestože je Turingův stroj matematickým modelem, nezbavil se všech zátěží klasické fyziky a jako takový vychází z jejích poznatků. Se znalostmi kvantové mechaniky však bylo možné ideu PTS upravit a definovat tak model, který popsal proces kvantového výpočtu.

3.3 Kvantový Turingův stroj

Hlavním impulzem pro vznik *kvantového Turingova stroje (KTS)*, bylo v roce 1973 potvrzení Charlese Bennetta, který dokázal jeho reverzibilitu[5]. To nezůstalo bez povšimnutí Paulem Benioffem, kterého napadlo, že by šlo napodobit

[5]Přesněji dokázal, že pro každý vypočitatelný problém existuje 3-páskový Turingův stroj, který je reverzibilní. Reverzibilitě byla věnována pozornost v souvislosti se zahříváním klasických obvodů.

vývoj reverzibilního kvantového systému na Turingově stroji. Na práce Benioffa a později i Richarda Feynmana navázal prvním popisem opravdového KTS v roce 1985 David Deutsch. Kvantová verze měla tyto hlavní charakteristiky a odlišnosti od klasického stroje:

- čtení, zápis a posun pásky se odehrával pomocí kvantově-mechanických interakcí.
- místo čisté 0, 1 a mezery se nyní setkáváme v každé buňce pásky se superpozicí stavů 0 a 1, což si můžeme představit jako vektor v jednotkové kouli; odklon od svislé osy zde určuje podíl zastoupení 0 a 1.
- superpozice zde umožňuje využít kvantový paralelismus – možnost provádět jednu operaci nad více daty současně.

Nejlépe si lze KTS představit jako kvantové zobecnění PTS. Pokud necháme po určitou dobu takový KTS vyvíjet (nebudeme jej měřit), můžeme stav vyjádřit jako součet pravděpodobností výpočetních cest, kterými může stroj projít. U KTS se v jednom kroku nebere pouze jedna náhodně zvolená cesta (jeden následující stav, jako je tomu u PTS), ale výpočet pokračuje v duchu kvantového paralelismu *všemi* možnými cestami naráz. Se vznikem KTS bylo možné zaměřit úsilí na otázky vypočitatelnosti, složitosti a univerzálnosti kvantových počítačů.

Vypočitatelnost je spojena s otázkou, zda je možné o daném problému rozhodnout (nebo nalézt k němu řešení) v konečném čase. Pokud algoritmus, terý by těmto požadavkům vyhověl, neexistuje, nazývá se problém *nevypočitatelný*. Hledání algoritmu k řešení problému vede i k tomu, že například pro generování náhodného čísla žádný klasický algoritmus neexistuje (není možné vygenerovat „opravdu“ náhodné číslo, protože všechny klasické generátory musí být založeny na výpočtu vstupů dle daného předpisu), kdežto u kvantových počítačů takový algoritmus existuje. Vychází totiž ze základní vlastnosti přírody – okamžiku náhodného kolapsu vlnové funkce na vlastní stav při měření kvantového systému. Více se měřením kvantového systému a generováním náhodných číslech budeme zabývat v kapitole o kvantových algoritmech.

Složitost neboli komplexita je druhou vlastností, která nás u kvantových počítačů zajímá. Souvisí s ní efektivita kvantových algoritmů a následně i výkon kvantových počítačů. Aby se dokázalo, že výzkum kvantových počítačů může mít v budoucnosti i praktický dopad, začala se během 90.let vynořovat řada možných aplikací, které využívají superpozice kvantových systémů k uplatnění kvantového paralelismu a tím i vylepšení složitostí dosavadních algoritmů. Jako příklad uveďme známý problém s faktorizací velkých celých čísel na součin prvočísel. Nejlepší známý klasický algoritmus dosahuje exponenciální složitosti, kterou lze (pro obecnou metodu Number Field Sieve) vyjádřit jako: $\mathcal{O}(e^{(L^{\frac{1}{3}}\ \ln^{\frac{2}{3}} L)})$, kde $L = \ln\ n$ a n je celé číslo, jehož rozklad hledáme. Vidíme, že časová náročnost roste velmi rychle s velikostí vstupu. Tento problém je ze skupiny NP problémů (*nondeterministic polynomial*), u nichž existuje efektivní nedeterministický algoritmus, jehož řešení v polynomiálním čase ověřit lze. Řešení takového problému deterministickým algoritmem není kvůli počtu výpočetních kroků schůdné (*tractable*). Nicméně u faktorizačního problému se zatím nepodařilo dokázat, že nemá efektivní algoritmus běžící v třídě složitosti P, tj. v polynomiálním čase, a proto je možné (i když se mnozí domnívají, že nepravděpodobné), že bude takový algoritmus ještě objeven. V roce 1994 se Peteru Shorovi z AT&T Bell Labs podařilo vymyslet kvantový faktorizační algoritmus, jehož složitost je na kvantovém počítači polynomiální. Takové řádové vylepšení znamenalo průlom ve vývoji kvantových algoritmů. Podobně jako se dají roztřídit algoritmy u klasické a pravděpodobnostní verze Turingových strojů, lze definovat i kvantové složitostní třídy. Pro přehlednost byly všechny třídy seřazeny do následující tabulky:

Třída	Popis
P	schůdné algoritmy běžící nejhůře v polynomiálním čase (dále jen PT), příklad: násobení
NP	neschůdné algoritmy; pouze správnost řešení lze ověřit v PT, příklad: faktorizace
NP-úplný	NP problémy vzájemně mapovatelné v PT, příklady: SAT, obchodní cestující, plánování
ZPP	problémy řešitelné s jistotou v průměrně PT na PTS
BPP	problémy řešitelné s $p > 2/3$ v nejhůře PT na PTS
QP	problémy řešitelné s jistotou v nejhůře PT
ZQP	problémy řešitelné s jistotou v průměrném PT
BQP	problémy řešitelné s $p > 2/3$ v nejhůře PT

Tabulka 1: **Třídy složitosti:** první tři klasické, druhé dvě pravděpodobnostní, poslední tři kvantové. SAT je problém splnitelnosti (satisfiability) logické funkce boolovských proměnných.

Univerzálnost je schopnost efektivně simulovat jeden Turingův stroj druhým. Turinga napadlo, že když vytvoří transformační pravidla jednoho Turingova stroje jako program (posloupnost bitů) pro jiný stroj, bude tento stroj schopný simulovat první stroj. Tak vznikla myšlenka, že je možné vytvořit programovatelný počítač – Turingův stroj, jehož programem je nějaký algoritmus. Až v roce 1996 potvrdili Seth Lloyd a Christof Zalka, že univerzálnost platí také u kvantových počítačů. To znamená, že jeden kvantový systém dokáže simulovat jiný.

3.4 Modely kvantových počítačů

Před tím, než je možné vůbec nějaký kvantový počítač vyrobit, je nutné přijít s modelem funkce takového počítače. V roce 1980 přišel Benioff s modelem, který se podobal KTS. Čtecí hlava byla vyměněna za zařízení, které zprostředkovává kvantově-mechanické interakce a ovlivňuje například spiny částic, kterými kódujeme stavy 0 a 1. Vývoj byl nahrazen Hamiltoniánem ve Schrödingerově rovnici. Důležité bylo, že se stroj vyvíjel po pevných krocích. Na konci každého z nich byl klasicky odečten bit z pásky. Mezi kroky se systém kvantově vyvíjel. Klasické měření na konci každého cyklu však neumožnilo využít vlastností kvantových počítačů úplně, protože zničilo křehkou superpozici stavů na pásce. Navíc s použitím časově nezávislého Hamiltoniánu by bylo nesmyslně potřeba znát výsledek výpočtu na počátku, protože by takový Hamiltonián musel obsahovat všechny informace o tom, jak se bude výpočet ubírat a nemohl se dynamicky vyvíjet. Jeho nedokonalost dále souvisí také s velkou vzdáleností, kterou působí čtecí hlava na pásku a nedovoluje navrhnout pouze lokálně působící evoluční operátor s časově nezávislým Hamiltoniánem.

Tyto nedostatky odstranil v roce 1985 Richard Feynman. Popsal výpočet na kvantovém počítači jako posloupnost výpočetních úkonů na logických kvantových branách a jejich zapojení v kombinačním obvodu. Jak bylo dokázáno, je popis výpočtu pomocí kvantových obvodů výpočetně ekvivalentní výpočtu na kvantovém Turingově stroji. Obvod se musel skládat z reverzibilních logických operací (bran). Každá taková operace byla vyjádřena nějakým operátorem $\boldsymbol{A}$. Provedení k operací během výpočtu pak bylo zapsáno jako součin operátoru každé operace. Aby bylo možné vyjádřit Hamiltonián, který by implementoval funkci daného obvodu a zároveň sledoval v jakém stádiu se výpočet nachází, navrhl Feynman přidat ke qubitům reprezentujícím vstupy a výstupy obvodu dalších $k+1$ qubitů, kde k je počet bran obvodu. Tyto qubity slouží vlastně jako čítač programu a informují nás, kolik logických bran již bylo použito, tj. v jakém stádiu se výpočet nachází. Místo, ve kterém se právě nachází výpočet je označeno obsazeným qubitem (s hodnotou 1), který se nazývá *kurzor*. Abychom mohli postupně qubity čítače nastavovat a mazat, je zapotřebí nových operátorů, které by to prováděly. Tyto operátory se označují c a a a nazývají se *kreační* a *anihilační* operátory, které nastavují kurzor na 1, respektive 0. Kdykoliv naměříme kurzor na posledním qubitu, je jasné, že při výpočtu již byly aplikovány všechny brány a výpočet je u konce. Výsledný Hamiltonián má pak tvar:

$$\boldsymbol{H} = \sum_{i=0}^{k-1} \boldsymbol{c}_{i+1} \cdot \boldsymbol{a}_i \cdot \boldsymbol{A}_{i+1} + (\boldsymbol{c}_{i+1} \cdot \boldsymbol{a}_i \cdot \boldsymbol{A}_{i+1})^\dagger.$$

Oba zmíněné operátory tak vlastně pohybují kurzorem dopředu a dozadu, podle použitých bran. S průběhem výpočtu jsou přímo korelovány přes operátory logických funkcí $\boldsymbol{A}$. O všech operátorech budeme blíže hovořit v kapitole o kvantových obvodech.

U Feynmanova modelu se předpokládá, že evoluční operátor umožňuje qubitům interakce na libovolnou vzdálenost. Tento problém (vzhledem k možné implementaci) vyřešil ještě v roce 1985 David Deutsch s jeho lokálním časově nezávislým evolučním operátorem, ovlivňujícím pouze přilehlé qubity. V takovém případě je však potřeba mít časově závislý Hamiltonián.

4 Kvantové obvody

Aby bylo možné kvantový systém udržet v nenarušeném stavu (koherenci), je zapotřebí jej (v ideálním případě) zcela izolovat od okolí. Takovému systému tím znemožníme, aby si s okolím vyměňoval například teplo nebo s ním jinak přímo interagoval. *Landauerův princip* nám říká, že ke smazání jednoho bitu informace z paměti je zapotřebí ze systému vyvést jeden bit entropie. To se obvykle projevuje vyzářením tepla do okolí. Na tomto rozboru vidíme jasnou spojitost mezi energií systému a objemem informací, které jsou v něm uloženy. Jelikož je ale při svém vývoji kvantový systém izolován od okolí, nemůže z něj žádná informace volně unikat. Ztráta informace totiž přímo souvisí s reverzibilitou procesů, které se v systému odehrávají.

4.1 Kvantové brány

V klasickém počítači, složeném z klasických bran jako je $\boldsymbol{AND}$, $\boldsymbol{NAND}$ či $\boldsymbol{OR}$, není vždy reverzibilita mezi vstupy a výstupy zachována. Například u klasického výpočtu víme, že lze libovolnou logickou funkci kombinačního obvodu realizovat pouze použitím univerzální brány $\boldsymbol{NAND}$. Tato brána má ale pro použití u kvantových počítačů tu nevýhodu, že z výstupů nelze jednoznačně určit kombinaci vstupů – brána $\boldsymbol{NAND}$ tedy není reverzibilní. V takovém procesu se ztrácí část informace a systém se tím zahřívá. Obecně lze dokázat, že v klasickém pojetí neexistuje univerzální reverzibilní 2-bitová brána. U kvantových počítačů ale můžeme používat jen ty brány, které podmínku reverzibility (a tím i unitárnosti operací) splňují. Jako první nás asi napadne brána $\boldsymbol{NOT}$. Ta opravdu podmínku reverzibility splňuje. Podobně jsou na tom i brány $\boldsymbol{CNOT}$ a $\boldsymbol{CCNOT}$. Vlastnosti těchto bran jsou shrnuty v tabulce.

brána	jiný název	qubity	funkce
$\boldsymbol{NOT}$		1	$\vert x\rangle \to \vert\overline{x}\rangle$
$\boldsymbol{CNOT}$	controlled $\boldsymbol{NOT}$, $\boldsymbol{XOR}$	2	$\vert x,y\rangle \to \vert x, x\oplus y\rangle$
$\boldsymbol{CCNOT}$	controlled-controlled $\boldsymbol{NOT}$, Toffoliho brána	3	$\vert x,y,z\rangle \to \vert x,y,xy\oplus z\rangle$

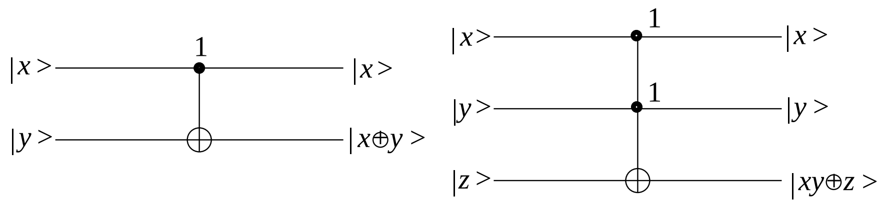
Třetí sloupec tabulky říká, na kolik qubitů daná brána působí. Například Toffoliho brána je 3-qubitová. V maticovém zápisu je

$$\boldsymbol{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \boldsymbol{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Matice $\boldsymbol{CCNOT}$ se podobá $\boldsymbol{CNOT}$, pouze je rozměru 8×8 se submaticí $\boldsymbol{NOT}$ v pravém dolním rohu. Obecně je n-qubitová operace vyjádřena maticí $2^n \times 2^n$. Bránové operace na qubitech se v kvantové informatice obvykle zapisují pomocí kvantových obvodů, které se v čase vyvíjí zleva doprava a každá vodorovná hrana (drát) odpovídá jednomu qubitu. Obecně zakreslíme jedno-qubitovou unitární operaci jak je uvedeno na obrázku.

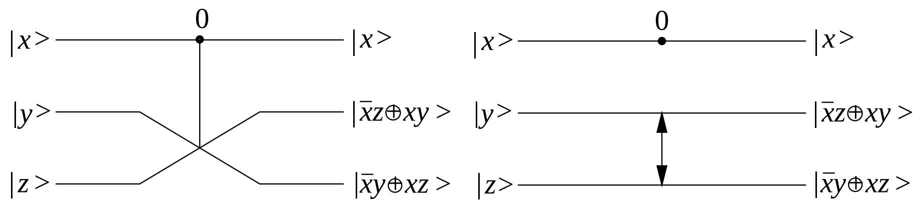
Obrázek 4: **1-qubitová kvantová brána:** Na obrázku vlevo je znázorněna obecná operace působící na jeden qubit $|\psi\rangle$. Jako příklad je vpravo uvedena brána $\boldsymbol{NOT}$.

Dvou- a tří-qubitové operace $\boldsymbol{CNOT}$ a $\boldsymbol{CCNOT}$ jsou znázorněny na následujícím obrázku.



Obrázek 5: **Kvantový obvod $\boldsymbol{CNOT}$ a $\boldsymbol{CCNOT}$:** Tyto brány mají jako kontrolní qubit 1. To znamená, že pokud jsou například u brány $\boldsymbol{CCNOT}$ oba qubity x a y rovny 1, provede se operace na qubitu z.

Jinou důležitou kvantovou bránou je *Fredkinova brána*. Ta prohodí druhý a třetí bit v případě, že první bit je 0. Vidíme, že tak jako v případě $\boldsymbol{CNOT}$ nebo $\boldsymbol{CCNOT}$ je i zde podmíněno provedení operace stavem určitého bitu. Takovým branám se souhrně říká *podmíněné kvantové brány.* Přitom Fredkinova brána je také univerzální a může tak realizovat libovolný logický kombinační obvod. O univerzálnosti se blíže zmíníme v následující podkapitole.

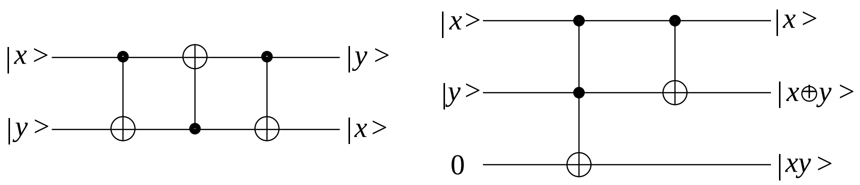


Obrázek 6: **Fredkinova brána:** Má dva alternativní způsoby zápisu (vlevo a vpravo). Fredkinova brána je 3-qubitová a realizuje logickou funkci $|x,y,z\rangle \rightarrow |x, \overline{x}z \oplus xy, \overline{x}y \oplus xz\rangle$.

Další užitečnou bránou je $\boldsymbol{SWAP}$, která spolu prohazuje 2 qubity a provádí tak funkci $|x, y\rangle \to |y, x\rangle$:

$$\boldsymbol{SWAP} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Její obvod je znázorněn s použitím brány $\boldsymbol{CNOT}$ na následujícím obrázku vlevo. Z univerzálních bran je pak možné konstruovat obvody různých funkcí a složitosti. Například lze takto navrhnout reverzibilní 2-qubitovou sčítačku, která provádí funkci $|x, y, 0\rangle \to |x, x \oplus y, xy\rangle$, kde druhý qubit obsahuje sumu a třetí přenos (carry).



Obrázek 7: **SWAP a 2-qubitová reverzibilní sčítačka.**

Kromě klasických kvantových bran však existují také kvantové brány, které klasicky nemohou existovat. Typickým zástupcem je brána $\sqrt{\boldsymbol{NOT}}$ („odmocnina z $\boldsymbol{NOT}$“). Přitom platí, že $(\sqrt{\boldsymbol{NOT}})^2 = \boldsymbol{NOT}$. Tuto podmínku splňuje definice

$$\sqrt{\boldsymbol{NOT}} = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}.$$

Snadno lze ověřit, že je tato operace unitární, tj. že $\sqrt{\boldsymbol{NOT}}\ \sqrt{\boldsymbol{NOT}}^{\dagger} = \boldsymbol{1}$. Použití této brány si uveďme na příkladu výpočtu funkce $\boldsymbol{NOT}$. Podle definice aplikujeme bránu $\sqrt{\boldsymbol{NOT}}$ dvakrát za sebou. Vidíme, že tato operace má celkem 3 stádia – použití první brány, použití druhé brány, skončený výpočet. U Feynmanova modelu kvantového počítače jsou tyto kroky zachyceny ve speciálních qubitech, které tvoří kurzor. Potřebný kvantový registr by se proto skládal ze 4 qubitů: tří kurzorových a jednoho výpočetního, na kterém bychom operaci $\boldsymbol{NOT}$ provedli. Operace první brány by tedy vypadala jako

$$\sqrt{\boldsymbol{NOT}_4} = \boldsymbol{1} \otimes \boldsymbol{1} \otimes \boldsymbol{1} \otimes \sqrt{\boldsymbol{NOT}},$$

Protože se jedná o direktní součin 4 qubitů, bude mít výsledná matice rozměr $2^4 \times 2^4$. Kolem diagonály bude mít rozmístěny submatice $\sqrt{\boldsymbol{NOT}}$. Zkráceně má tato matice tvar

$$\sqrt{\boldsymbol{NOT}_4} = \begin{pmatrix} \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} \end{pmatrix},$$

kde $\boldsymbol{0}$ je nulová submatice 2x2. Celý výpočet pak můžeme zapsat jako

$$\boldsymbol{NOT}_4 = \sqrt{\boldsymbol{NOT}_4}\ \sqrt{\boldsymbol{NOT}_4}.$$

Pokud vyjdeme z počátečního stavu $|1000\rangle$ (tj. že kurzor je na počátku nastaven na prvním qubitu), pak Hamiltonián, kterým popíšeme konfiguraci celého systému včetně kurzoru (a který můžeme dosadit do Schrödingerovy rovnice), je u Feynmanova modelu kvantového počítače roven

$$\boldsymbol{H} = \boldsymbol{c}_1\boldsymbol{a}_0\sqrt{\boldsymbol{NOT}_4} + \left(\boldsymbol{c}_1\boldsymbol{a}_0\sqrt{\boldsymbol{NOT}_4}\right)^\dagger + \boldsymbol{c}_2\boldsymbol{a}_1\sqrt{\boldsymbol{NOT}_4} + \left(\boldsymbol{c}_2\boldsymbol{a}_1\sqrt{\boldsymbol{NOT}_4}\right)^\dagger,$$

kde $\boldsymbol{c}$ a $\boldsymbol{a}$ jsou anihilační a kreační operátory, které jsou definovány jako

$$\boldsymbol{c} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad \boldsymbol{a} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Tyto operátory slouží k nastavování a mazání qubitů kurzoru na hodnoty $|1\rangle$ a $|0\rangle$ podle toho, kam až postoupil výpočet, a tedy kolik již bylo aplikováno bran. Pokud kdykoliv naměříme obsazený poslední (třetí) kurzorový qubit, máme jistotu, že výpočet je u konce. Provázání kurzoru a průběhu vlastního výpočtu zajišťuje právě výše uvedená podoba Hamiltoniánu, která musí reflektovat následnou fyzickou implementaci. U Feynmanova modelu je tvar Hamiltoniánu odvozen od spinových vln, které se šíří řetězcem molekul (to jsou precesní vlny dipólových momentů vzniklé ve feritech, které se ocitly v externím magnetickém poli jiného směru než bylo pole magnetizační). Potom také měřením na kurzoru neovlivňujeme zpětně část registru, v níž probíhá výpočet. Možnosti působení obou operátorů na jeden qubit kurzoru můžeme shrnout takto: $\boldsymbol{c}|0\rangle = |1\rangle$, $\boldsymbol{c}|1\rangle = 0$, $\boldsymbol{a}|0\rangle = 0$, $\boldsymbol{a}|1\rangle = |0\rangle$, kde 0 je nedefinovaný nulový stav. Protože ale potřebujeme specifikovat složitější operaci působící na celý registr, mají v Hamiltoniánu oba operátory indexy určující, který kurzorový qubit je ovlivňován. Například k nastavení druhého qubitu na $|1\rangle$ použijeme operátor $\boldsymbol{c}_1 = \boldsymbol{1} \otimes \boldsymbol{c} \otimes \boldsymbol{1} \otimes \boldsymbol{1}$. Podobně definujeme i ostatní operátory. Všimněme si, že v našem příkladě tyto operátory nikdy neovlivňují poslední qubit, protože ten není součástí kurzoru a probíhá v něm výpočet operace $\boldsymbol{NOT}$.

Nyní, pokud Hamiltonián vypočítáme[6], dostaneme

$$\boldsymbol{H} = \begin{pmatrix} \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \sqrt{\boldsymbol{NOT}}^{\dagger} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}}^{\dagger} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}}^{\dagger} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \sqrt{\boldsymbol{NOT}}^{\dagger} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} & \boldsymbol{0} \end{pmatrix},$$

kde $\boldsymbol{0}$ je nulová submatice 2x2. Pokud jsou počáteční podmínky vlnové funkce $|\Psi(0)\rangle = |1000\rangle$ nebo $|\Psi(0)\rangle = |1001\rangle$, je řešení Schrödingerovy rovnice

$$|\Psi(t)\rangle = e^{-i\boldsymbol{H}t/\hbar}|\Psi(0)\rangle = \boldsymbol{U}(t)|\Psi(0)\rangle,$$

kde $\boldsymbol{H}$ je výše uvedený časově nezávislý Hamiltonián. Z této rovnice nám k úplnému popsání výpočtu zbývá vyjádřit evoluční operátor $\boldsymbol{U}(t)$, který popisuje vývoj systému v čase. To je možné provést několika způsoby. Například přes rozvoj $e^x = 1 + \frac{x^1}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots$. Výsledný evoluční operátor je pak možné použít k (neefektivní) simulaci kvantového výpočtu funkce $\boldsymbol{NOT}$ na klasickém počítači.

Na bráně $\sqrt{\boldsymbol{NOT}}$ jsme si ukázali, jak jsou jednotlivé brány a operátory propojeny s vlastní vlnovou funkcí a jakou v ní hrají úlohu. Také jsme viděli, že ne všechny brány jsou realizovatelné klasicky. Další z čistě kvantových bran jsou například tři jedno-qubitové (osově-) rotační brány $\boldsymbol{R}_x$, $\boldsymbol{R}_y$ a $\boldsymbol{R}_z$ s parametrem θ.

$$\boldsymbol{R}_x = \begin{pmatrix} \cos\theta & i\sin\theta \\ i\sin\theta & \cos\theta \end{pmatrix}, \quad \boldsymbol{R}_y = \begin{pmatrix} i\cos\theta & \sin\theta \\ \sin\theta & i\cos\theta \end{pmatrix}, \quad \boldsymbol{R}_z = \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{-i\theta} \end{pmatrix}.$$

Tyto brány stavový vektor rotují kolem příslušné osy o zvolený úhel. Brány, které provádějí rotaci o $\frac{\pi}{4}$ bez fáze i jsou *Hadamardovy rotační brány*:

$$\boldsymbol{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \boldsymbol{H'} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \quad \boldsymbol{H''} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Tyto brány lze použít například v případě, že chceme uvést stavy $|0\rangle$ nebo $|1\rangle$ do jejich vyvážené superpozice. Podle použité brány získáváme různou fázi.

4.2 Univerzální kvantové brány

Na závěr se vraťme k otázce univerzálnosti kvantových bran. Tak jako existují pro klasické obvody množiny univerzálních operátorů, je možné i u kvantových

[6] Je zřejmé, že řada prvků výsledného Hamiltoniánu bude rovna 0. Například pokud je stav registru zapsán jako $|wxyz\rangle$, pak násobení $\boldsymbol{c}_1\boldsymbol{a}_0\ |wxyz\rangle$ nabývá nulový vektor $\boldsymbol{0}$ kdykoliv je nultý qubit $|0\rangle$ nebo první qubit $|1\rangle$. Podobně si lze výpočet usnadnit u výrazu $\boldsymbol{c}_2\boldsymbol{a}_1$. Komplexně sdružené a transponované části jsou symetrické.

počítačů požadovat univerzalitu. Přitom se snažíme, aby byla tato množina operátorů co nejjednodušší a tím i lépe implementovatelné. Mezi klasickými branami jsou takovými množinami například $\{\boldsymbol{NAND}\}$ nebo $\{\boldsymbol{OR},\ \boldsymbol{NOT}\}$. U kvantových bran bylo dokázáno, že Fredkinova a Toffoliho 3-qubitová brána jsou samy o sobě univerzální[7] (a velmi obtížné na implementaci, protože bychom museli ovládat interakci mezi třemi kvantovými systémy). Davidu DiVincenzovi se však podařilo dokázat, že na rozdíl od klasické informatiky, lze v kvantové informatice vyjádřit libovolný kvantový obvod pouze s využitím 2-qubitových bran. Uvažujeme-li 2-qubitovou bránu $\boldsymbol{CNOT}$[8], pak lze dokázat, že tato brána není samotná univerzální. Může nás však napadnout, že společně s nějakou 1-qubitovou bránou by taková množina univerzální být mohla (což by bylo nadějné vzhledem k méně náročné implementaci 1- a 2-qubitových bran). Jak bylo zjištěno, lze obecnou 1-qubitovou unitární transformaci $\boldsymbol{U}_1$ vyjádřit jako součin čtyř matic 2×2

$$\begin{pmatrix} e^{i\delta} & 0 \\ 0 & e^{i\delta} \end{pmatrix} \cdot \begin{pmatrix} e^{i\alpha/2} & 0 \\ 0 & e^{-i\alpha/2} \end{pmatrix} \cdot \begin{pmatrix} \cos\theta/2 & \sin\theta/2 \\ -\sin\theta/2 & \cos\theta/2 \end{pmatrix} \cdot \begin{pmatrix} e^{i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix},$$

kde první matice je fázový posun vzhledem k δ, druhá a čtvrtá matice jsou rotace o daný úhel kolem z a třetí matice je rotace kolem osy y o úhel θ. Po roznásobení dostáváme

$$\boldsymbol{U}_1(\delta,\alpha,\beta,\theta) = \begin{pmatrix} e^{i(\delta+\alpha/2+\beta/2)}\cos\theta/2 & e^{i(\delta+\alpha/2-\beta/2)}\sin\theta/2 \\ -e^{i(\delta-\alpha/2+\beta/2)}\sin\theta/2 & e^{i(\delta-\alpha/2-\beta/2)}\cos\theta/2 \end{pmatrix},$$

kde δ,α,β a $\theta \in \mathbb{R}$. Například při $\delta = \alpha = \beta = 0$ vytvoříme operátor, který mezi sebou prohazuje qubity $|0\rangle \to -|1\rangle$ a $|1\rangle \to |0\rangle$. Právě pro množinu $\{\boldsymbol{U}_1(\delta,\alpha,\beta,\theta),\ \boldsymbol{CNOT}\}$ Adiano Barenco a jiní dokázali, že je pro konstrukci kvantových obvodů univerzální. Kombinací těchto dvou bran je totiž možné vytvořit Toffoliho univerzální bránu.

Navíc lze univerzalitu 2- a 3-qubitových bran v jistém smyslu zobecnit a vyjádřit jako příslušnou parametrizovanou kvantovou bránu. Například 2-qubitovou univerzální bránu pro bázi $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ poprvé popsal Adriano Barenco:

$$\boldsymbol{A}(\phi,\alpha,\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha}\cos\theta & -ie^{i(\alpha-\theta)}\sin\theta \\ 0 & 0 & -ie^{i(\alpha+\theta)}\sin\theta & e^{i\alpha}\cos\theta \end{pmatrix},$$

kde ϕ,α,θ jsou pevně zvolené iracionální násobky π nebo samy sebe. Ještě před Barencem zobecnili reverzibilní Toffoliho bránu Deutsch a DiVincenzo a pro

[7] Snadno lze ukázat, že Toffoliho brána $\boldsymbol{CCNOT}$ může nahradit například univerzální operaci $\boldsymbol{NAND}$, protože $\boldsymbol{CCNOT}\ |1,1,z\rangle \to |1,1,\overline{z}\rangle$ a $\boldsymbol{CCNOT}\ |x,y,0\rangle \to |x,y,xy\rangle$.

[8] Všimněme si, že některé brány, o nichž jsme se zmínili ($\boldsymbol{CNOT}$, $\boldsymbol{CCNOT}$, Fredkinova, ...) jsou vlastně klasické reverzibilní brány, které jsou jen speciálním případem množiny všech kvantových bran. Reverzibilní bránu lze zkonstruovat z nereverzibilních bran například zkopírováním vstupů na výstup pro zachování informace.

bázi $\{|000\rangle, \ldots, |111\rangle\}$ vymysleli 3-qubitovou univerzální bránu.

$$\boldsymbol{D}(\theta) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & i\cos\theta & \sin\theta \\ 0 & 0 & 0 & 0 & 0 & 0 & \sin\theta & i\cos\theta \end{pmatrix}.$$

Je zřejmé, že $\boldsymbol{D}(\frac{\pi}{2}) = \boldsymbol{CCNOT}$.

5 Kvantové algoritmy

Kvantové počítače byly zpočátku brány jako zajímavá kuriozita, kterou snad bude jednou možné využít až technologie a výzkum postoupí patřičně kupředu. V 80.letech, kdy byly kvantovým počítačům položeny základy, se neobjevil žádný algoritmus, z něhož by bylo zřejmé, že budou kvantové počítače použitelné pro praktické řešení problémů. Hledaly se tedy možné oblasti využití kvantových počítačů, které by zahnaly pochybnosti. O zásadní průlom v konstrukci kvantových algoritmů se zasloužil v roce 1994 Peter Shor z AT&T, který navrhl algoritmus provádějící rozklad celého čísla na jeho prvočinitele. Nejlepší klasické algoritmy tuto úlohu dokáží řešit neefektivně v čase exponenciálně rostoucím s velikostí vstupu. Shorův algoritmus však běží v polynomiálním čase. Takové zlepšení si už zasloužilo větší analýzu a tak se na základě postupu jeho algoritmu začaly vynořovat další praktické algoritmy, které naplňovaly naděje o schopnostech kvantových počítačů. V této kapitole se seznámíme s nejdůležitějšími kvantovými algoritmy, které byly vyvinuty v 90.letech. Budeme také hovořit o jejich dopadu na některá odvětví informatiky jako je například kryptografie v případě Shorova faktorizačního algoritmu. Pokusíme se vždy vyjít z paralely klasického problému a poukázat na jednotlivé odlišnosti kvantového a klasického řešení. Abychom však mohli kvantové algoritmy popisovat, potřebujeme se na úvod seznámit s jedním z hlavních triků, kterým Shor (a později i další) svůj kvantový algoritmus vybavil.

5.1 Kvantová Fourierova transformace

Jak známo, Fourierova transformace mapuje funkce v časové doméně na funkce frekvenčního spektra. Její hlavní vlastností z pohledu kvantové mechaniky je, že mezi qubity vyvolává kvantovou interferenci, která je buď konstruktivní nebo destruktivní. Konstruktivní interference v signálu zvýrazňuje jisté charakteristiky (frekvence) nad charakteristikami jinými. Takovým způsobem uvádí registr do stavu, v němž naměříme jeho hodnoty s *různými* pravděpodobnostmi (tzn. ovlivňuje amplitudy pravděpodobností). A právě tato vlastnost má zásadní vliv na praktickou použitelnost některých algoritmů. Abychom vyhověli požadavku unitárnosti operace definujeme kvantovou diskrétní Fourierovu transformaci (KFT) jako vývoj registru $|a\rangle = |a_0\ a_1 \ldots\rangle$ na $|c\rangle = |c_0\ c_1 \ldots\rangle$ podle :

$$|a\rangle \rightarrow \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a c/q}\ |c\rangle,$$

kde q je počet stavů registru ($0 \leq a < q$) a (a, c) jsou souřadnice prvků unitární matice a jsou rovny $\frac{1}{\sqrt{q}} e^{2\pi i a c/q}$. Tato matice (transformace) je základem faktorizačního algoritmu a nazývá se $\boldsymbol{A}_q$. Její sloupce a řádky jsou indexovány od nuly jako celá čísla odpovídající binárním reprezentacím stavů. Aby bylo možné navrhnout efektivní algoritmy založené na KFT, bylo nutné samotnou KFT vymyslet efektivně. Shor takovou KFT navrhl pro q, které je mocninou dvou ($q = 2^l$). Pro její výpočet potřeboval jen $\mathcal{O}(l^2)$ kvantových bran, kterých jsou dva typy. Jednou je Hadamardova brána definovaná jako:

$$\boldsymbol{H}: \begin{array}{lcl} |0\rangle & \to & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle & \to & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array} \quad \text{neboli} \quad \boldsymbol{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

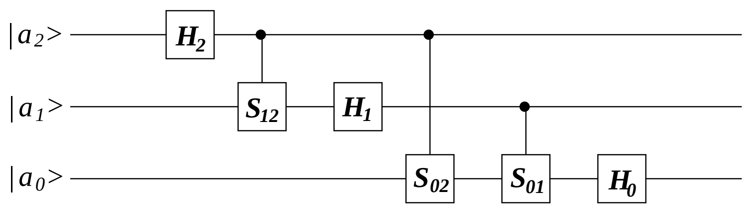
Tato brána vyvíjí stav $|0\rangle$ do vyvážené superpozice všech možných 2^n stavů (pokud je aplikována na n qubitů jako $(\boldsymbol{H} \otimes \boldsymbol{H} \otimes \ldots \otimes \boldsymbol{H})\ |00\ldots0\rangle$ nazývá se Walsh-Hadamardova transformace $\boldsymbol{W}$). Hadamardovu bránu ovlivňující bit na pozici j označujeme $\boldsymbol{H}_j$. Druhou použitou bránou je $\boldsymbol{S}_{j,k}$, která operuje s bity na pozicích j a k:

$$\boldsymbol{S}_{j,k} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\theta_{k-j}} \end{pmatrix},$$

kde $\theta_{k-j} = \pi/2^{k-j}$. K provedení KFT aplikujeme brány v pořadí zleva doprava podle obecného schématu:

$$\boldsymbol{H}_{l-1}\boldsymbol{S}_{l-2,l-1}\boldsymbol{H}_{l-2}\boldsymbol{S}_{l-3,l-1}\boldsymbol{S}_{l-3,l-2}\boldsymbol{H}_{l-3}\ldots\boldsymbol{H}_1\boldsymbol{S}_{0,l-1}\boldsymbol{S}_{0,l-2}\ldots\boldsymbol{S}_{0,2}\boldsymbol{S}_{0,1}\boldsymbol{H}_0.$$

Například pro tři bity ($l = 3$) aplikujeme brány $\boldsymbol{H}_2\boldsymbol{S}_{1,2}\boldsymbol{H}_1\boldsymbol{S}_{0,2}\boldsymbol{S}_{0,1}\boldsymbol{H}_0$. Tato operace vrací registr bitově převrácený, takže pro dokončení KFT je zapotřebí výsledný registr bitově invertovat nebo jej číst z opačné strany, což je již z hlediska implementace jednoduchá operace.



Obrázek 8: **Obvod kvantové Fourierovy transformace:** pro $l = 3$; rekurzivně lze obvod rozšiřovat podle obecného vzorce. Jak je u kvantových obvodů zvykem, brány se provádějí zleva doprava, což odpovídá uvedenému zápisu. Lze si rovněž všimnout jak brány $\boldsymbol{S}_{j,k}$ operují nad dvěma qubity.

5.2 Klasická kryptografie

Jak jsme se již zmínili, s prvním převratným algoritmem přišel v roce 1994 Peter Shor. A hned se mu podařilo zasáhnout citlivé místo v oblasti počítačové vědy. Nepřímo vyzval k diskusi nad otázkami počítačové bezpečnosti přenášených dat veřejnými komunikačními kanály. Jeho algoritmus totiž v principu dokáže efektivně faktorizovat velké celé číslo, vytvořené například jako součin dvou (velkých) prvočísel. To je problém, na jehož neschůdnosti na klasických počítačích závisí mnoho mechanizmů současné kryptografie (například systém RSA). Pojďme si však nejprve stručně připomenout základní algoritmy, pomocí kterých klasická kryptografie postupuje při zajišťování důvěrnosti přenášených dat.

Jedním ze základních algoritmů je tzv. *One-time pad*. Pokud chtějí dvě strany (Alice a Bob) komunikovat, je zapotřebí se předtím sejít a dohodnout si (náhodně vygenerovat) několik sad tajných klíčů, které budou při komunikaci potřeba. Mohou si například říci, že budou používat 10 sad, každou o 60 klíčích. Dále algoritmus postupuje v těchto krocích:

- Alice si připraví do číselné podoby zkonvertovanou zprávu, kterou si přeje poslat. Vzniká tak zpráva $M = \{m_1, \ldots, m_n\}$.
- Dále si Alice vybere sadu, kterou k šifrování hodlá použít a dostává tak posloupnost klíčů $k_1, \ldots, k_n$.
- Nyní vypočítá ze zprávy šifrovanou posloupnost čísel $C = \{c_1, \ldots, c_n\}$ podle pravidla $c_i = m_i + k_i \pmod{l}$, kde l je počet znaků abecedy (pro binární abecedu je $l = 2$ a sčítaní pak odpovídá operaci XOR).
- Následně pošle Alice Bobovi zašifrovanou zprávu a číslo sady, kterou použila.
- Bob při příjetí zprávy inverzním pravidlem a použitím příslušné sady klíčů zprávu dešifruje podle $m_i = c_i - k_i + l \pmod{l}$. Nakonec zprávu zkonvertuje do textové podoby.

Ve verzi nad binární abecedou se One-time pad označuje jako Vernamova šifra. Tento druh algoritmu je zajímavý tím, že u něj lze za předpokladu kvalitního zdroje klíčů dokázat tzv. *nepodmíněnou bezpečnost*, to znamená odolnost vůči luštění bez ohledu na výpočetní sílu útočníka. Nevýhodou tohoto algoritmu je, že klíč je možné použít jen jednou (jinak se celý systém naopak stává snadno napadnutelným), a že toto heslo musí být stejně dlouhé jako je zasílaná zpráva. Vzniká zde tedy problém s bezpečným přenosem klíče. K řešení těchto nedostatků se používají v současné kryptografii dva hlavní postupy. Jednak je to použití algoritmu, jehož složitost umožňuje zkrátit délku klíče (dnes používané algoritmy jsou například DES, 3DES, AES, Blowfish). Za druhé se přenos uskutečňuje pomocí mechanizmů asymetrické kryptografie [9].

[9] Asymetrická kryptografie je založena na tzv. *jednosměrných funkcích se zadními vrátky*. Tyto funkce lze vypočítat v jednom směru snadno (a rychle – případ šifrování), kdežto opačným směrem (dešifrování) obtížně. Rychlé dešifrování (zadní vrátka) je možné pouze se znalostí určité utajené informace (privátního klíče). Klíč určující funkci pro zašifrování se nazývá veřejný klíč. Zadní vrátka se obvykle vytvářejí pomocí složitých matematických problémů jako jsou faktorizace (na kterou se my zaměříme) nebo diskrétní logaritmy. Problém diskrétních logaritmů je pro konstrukci asymetrických mechanizmů považován za stejně vhodný jako faktorizace. Je obvykle formulován takto: Najděte celé číslo x takové, že $g^x \equiv h \pmod{p}$, kde g a h jsou prvky konečné grupy G_p. Například v G_{17} je řešením $3^x \equiv 13 \pmod{17}$ hodnota $x = 4$. Na složitosti výpočtu diskrétních logaritmů jsou založeny například kryptosystémy ElGamal nebo DSS.

5.3 RSA kryptografie veřejného klíče

Kryptosystém RSA (který v roce 1978 vymysleli Ronald Rivest, Adi Shamir a Leonard Adlemann) je založen na problému faktorizace velkých čísel. Podívejme se na to, jak tento systém řeší přenos zprávy mezi dvěma místy. Nejprve musí přijímající strana (v tomto případě Bob) vygenerovat pár klíčů, z nichž jeden je tzv. *veřejný klíč*, který je k dispozici všem a Bob jej sdělí veřejným kanálem Alici. Alice tímto klíčem zprávu zašifruje (tuto část komunikace může provést kdokoliv). V této chvíli přichází na řadu druhý klíč – *privátní*, který Bob nikomu nesdělil. Alice pošle zašifrovanou zprávu Bobovi, který si ji svým privátním klíčem dešifruje. Aby to však bylo možné, je nutné, aby byly oba klíčem určitým způsobem propojeny. Pojďme se teď na toto spojení podívat podrobněji. Aby byl RSA systém bezpečný, musí být těžké na základě znalosti veřejného klíče a zašifrované zprávy od Alice zjistit otevřenou hodnotu zprávy (to také znamená, že ze znalosti těchto hodnot musí být těžké zjistit klíč privátní). Toho RSA dociluje tím, že spoléhá na neschůdnost faktorizace velkých celých čísel. Řekněme, že Bob chce komunikovat s Alicí. Konkrétní postup při komunikaci se skládá jednak z části generování klíče (první tři body) a části komunikační:

- Bob si nejdříve vybere dvě dostatečně velká prvočísla p a q, která vynásobí a získá číslo $n = p \cdot q$.
- Poté začne počítat dvě celá čísla d a e tak, že za e si zvolí náhodné číslo, které je nesoudělné s číslem $(p-1)(q-1)$. Dále musí vypočítat d z výrazu $ed \equiv 1 \bmod (p-1)(q-1)$.
- Následuje zaslání veřejného klíče Alici jako páru čísel $\{e, n\}$.
- Vytvoření zprávy $M \in \mathbb{Z}_n$.
- Nyní Alice zašifruje zprávu pomocí veřejného klíče jako $C = M^e \bmod n$.
- Tu pak zašle Bobovi, který na základě znalosti svého utajeného privátního klíče dešifruje jako $M = C^d \bmod n$ a potom převede zpět do textové podoby.

Ukažme si celou proceduru na vysvětlujícím příkladu:
Bob si například zvolí $p = 11$ a $q = 13$, dále je $n = p \cdot q = 143$. Jestliže si za e zvolí například číslo 7 (nesoudělné s $(p-1)(q-1)$ a zároveň menší než toto číslo), pak z rovnice $d \cdot 7 \equiv 1 \bmod 120$ je $d = 103$. Tím má Bob k zaslání připraven veřejný klíč (7, 143) a k uschování privátní klíč (103, 143). Veřejným klíčem Alice zašifruje třeba písmeno `x`, které je v našem číselném kódu rovno řekněme 16. Takže je pak $C_p = 16^7 \bmod 143 = 3$. To si Bob dešifruje jako $M = 3^{103} \bmod 143 = 16$, tj. kód písmene `x`. Pro velká čísla nepřipadá prolomení hrubou silou v úvahu, protože k tomu by bylo potřeba zjistit p a q. Pak by byl již výpočet d jednoduchý. Jako bezpečné se dnes obvykle uvažuje použití n v délce 1024 bitů, sestavené ze dvou prvočísel přibližně poloviční délky.

5.4 Shorův faktorizační algoritmus

Jak bylo uvedeno, klasická kryptografie je vzhledem k možnostem počítačů v této chvíli bezpečnou formou zabezpečení přenosu dat. Jak si ale s problémem prolomení metody RSA poradí kvantový počítač? Má jednu velkou výhodu – může totiž využít kvantového paralelismu. Algoritmus Petera Shora na faktorizaci velkých celých čísel právě tuto vlastnost kvantových systémů využívá. Na kvantovém počítači tento algoritmus běží v asymptotickém čase $\mathcal{O}(L^2 \log L \log \log L)$, kde L je počet bitů faktorizovaného čísla. Vidíme, že čas je omezen shora polynomem. Místo, aby algoritmus hledal přímo jednotlivé součinitele, je spíše založen na poznatku, že problém faktorizace čísel se dá převést na problém hledání periody určité periodické funkce. Je-li dáno číslo n, které chceme faktorizovat, je potřeba vytvořit periodickou funkci

$$f_{y,n}(a) = y^a \mathrm{mod}\ n,$$

kde y je náhodné celé číslo nesoudělné s n. Na této funkci je zajímavá její periodicita. Její perioda modulo n se obvykle značí r. Protože je každá r-tá hodnota funkce stejná ($f_{y,n}(a) = f_{y,n}(a+r)$), platí

$$y^r \equiv 1 \bmod n.$$

To lze upravit na tvar

$$(y^{r/2} - 1)(y^{r/2} + 1) \equiv 0 \bmod n.$$

Tento vztah platí pro sudou periodu r (pro lichou se snažíme náhodně vybrat jinou hodnotu y - viz příklad níže). Z tohoto tvaru vidíme, že dělení členů na levé straně rovnice číslem n je bezezbytkové. Proto, pokud není triviálně $y^{r/2} \equiv \pm 1 \bmod n$, pak musí mít některý z členů na levé straně společný faktor s n. Tímto krokem se vlastně úloha převádí na problém hledání největšího společného dělitele (*nsd*) čísel $(y^{r/2} - 1, n)$ a $(y^{r/2} + 1, n)$. Na tento problém existuje algoritmus běžící efektivně i na klasických počítačích. Následující příklad by měl problém objasnit.

Příklad: Řekněme, že chceme faktorizovat číslo 21 na součin jeho prvočinitelů. Pokud je $n = 21$, pak si musíme zvolit $1 < y < 21$ takové, že $nsd\ (y, 21) = 1$. Odpovídající množina čísel y je $\{2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$. Z ní si náhodně zvolíme například $y = 10$. Nyní chceme zjistit periodu funkce $f_{y,n}(a) = 10^a \mathrm{mod}\ 21$. Vidíme, že funkční hodnoty pro celé $a = 1, 2, \ldots$ jsou $10, 16, 13, 4, 19, 1, 10, 16, \ldots$. To znamená, že tato funkce má periodu 6. Tato perioda je sudá a nevrací triviální faktory (Jestliže $y^{r/2} = 1000$, pak chceme ověřit, zda $1000 \stackrel{?}{\equiv} \pm 1 \pmod{21}$. To neplatí, protože $999 \nmid 21$ a $1001 \nmid 21$. Pokud by se tak stalo, museli bychom zvolit jiné y.). Na závěr nalezneme faktory pomocí $nsd\ (1001, 21) = 7$ a $nsd\ (999, 21) = 3$. Všimněme si, že pro $y = 20$ algoritmus neuspěje, protože perioda $r = 2$. Zajímá nás tedy, zda $20 \stackrel{?}{\equiv} \pm 1 \pmod{21}$ a vidíme, že $21 \mid 21$.

Nyní nám zbývá jediný problém – jak vypočítat efektivně periodu r dané funkce. Tento problém není klasicky řešitelný v polynomiálním čase. Shor ale ukázal, že na kvantovém počítači periodu efektivně nalézt lze. Toho dosáhl využitím kvantového paralelismu.

Připravme si kvantový registr, který bude mít 2 části nazvané $R1$ a $R2$, a jehož stav budeme zapisovat $|r1, r2\rangle$.

krok 1: Zvolíme si náhodně y, které je nesoudělné s n. Dále si vybereme q takové, že $2n^2 \leq q \leq 3n^2$.

krok 2: Připravíme kvantový registr do superpozice čísel $|\psi\rangle$ tak, že v $R1$ máme superpozici čísel 0 až $q-1$, a v $R2$ samé nuly. Registr tak přejde do stavu

$$|\Psi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, 0\rangle.$$

krok 3: Z hodnot v $R1$ vypočteme (paralelně) funkční hodnoty funkce $f_{y,n}(a)$ a zapíšeme je do $R2$.

$$|\Psi\rangle = \frac{1}{\sqrt{q}} \sum_{a=0}^{q-1} |a, y^a \bmod n\rangle.$$

krok 4: Nyní změříme pouze část $R2$ registru jako hodnotu k. Tím uvedeme celý registr do superpozice čísel, které mají funkční hodnotu k a představují projekci registru, v němž předtím byly vyváženě zastoupeny všechny hodnoty periodické funkce $f_{y,n}(a)$.

$$|\Psi\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} |a', k\rangle,$$

kde $A = \{a' : y^{a'} \bmod n = k\}$ a $|A|$ je počet prvků množiny A. Použijme nyní příkladu s faktorizací čísla 21 a uvědomme si, v jakém stavu se registr před tímto krokem nacházel. Po 3. kroku byl registr v superpozici $\frac{1}{\sqrt{22}}(|0,1\rangle + |1,10\rangle + |2,16\rangle + |3,13\rangle + |4,4\rangle + |5,19\rangle + |6,1\rangle + \ldots + |21,13\rangle)$. Provedením měření podle kroku 4 se vyselektují pouze stavy příslušející naměřené hodnotě (se stejnou vlastní hodnotou). Podle výsledku měření tak dostaneme jednu z 6 možných superpozic:

změřeno	nový stav
1	$\frac{1}{2}(\|0,1\rangle + \|6,1\rangle + \|12,1\rangle + \|18,1\rangle)$
10	$\frac{1}{2}(\|1,10\rangle + \|7,10\rangle + \|13,10\rangle + \|19,10\rangle)$
16	$\frac{1}{2}(\|2,16\rangle + \|8,16\rangle + \|14,16\rangle + \|20,16\rangle)$
13	$\frac{1}{2}(\|3,13\rangle + \|9,13\rangle + \|15,13\rangle + \|21,13\rangle)$
4	$\frac{1}{\sqrt{3}}(\|4,4\rangle + \|10,4\rangle + \|16,4\rangle)$
19	$\frac{1}{\sqrt{3}}(\|5,19\rangle + \|11,19\rangle + \|17,19\rangle)$

Zdá se, že k odhadu periody z těchto stavů bylo by potřeba první tři kroky několikrát opakovat ke změření několika hodnot. Bohužel to není možné v důsledku různého počátečního offsetu periody u každého výsledku měření. Tento offset nám neumožňuje mít při opakovaných měřeních jistotu, že dosáhneme stejného výsledku a budeme moci periodu určit jednoznačně. To proto, že pravděpodobnosti změření všech 6 výsledků jsou (přibližně[10]) stejné. Aby bylo možné periodu správně určit, je zapotřebí ji nějakým způsobem „zvýraznit“ tak, aby nebyla závislá na počátečním offsetu.

krok 5: Proto nyní provedeme kvantovou Fourierovu transformaci na $R1$ a výsledek vrátíme tamtéž.

$$|\Psi\rangle = \frac{1}{\sqrt{|A|}} \sum_{a' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} e^{2\pi i a' c/q} |c, k\rangle.$$

Fourierova transformace převedla stav registru $|a'\rangle$ na $|c\rangle$, tentokrát již s různými amplitudami. Ty stavy, které se vyskytují v okolí násobků převrácené periody $1/r$ tak naměříme s větší pravděpodobností než ty, které jsou od násobků více vzdáleny. Důležité je, že stav $|a'\rangle$ obsahující problematický offset periody funkce se přesunul do fázového faktoru.

krok 6: Nyní registr změříme s výsledkem c'. Abychom byli schopni určit periodu, je nutné kroky 2 – 6 opakovat do chvíle, než máme k dispozici dostatek vzorků, které jsou s velkou pravděpodobností v okolí různých násobků převrácené periody a které jednoznačně umožňují určit periodu. Pokud tyto násobky označíme λ, pak c' je nějakým násobkem λ výrazu q/r, tj. $c' = \lambda \frac{q}{r}$. Po úpravě dostaneme $c'/q = \lambda/r$, pro $\lambda \in \mathbb{Z}^+$. Odhad, jaký násobek λ byl naměřen, se provádí rozvojem c'/q do řetězcového zlomku.

krok 7: Když je známa hodnota r, jsou již klasicky Eucleidovým algoritmem vypočteny největší společné dělitele $(y^{r/2} - 1, n)$ a $(y^{r/2} + 1, n)$.

Protože je tento algoritmus pravděpodobnostní povahy, není zaručeno, že na konci dostaneme dva užitečné faktory, které nás zajímají. Například špatná volba y v prvním bodě algoritmu může vést k dosažení triviálních řešení rovnice $(y^{r/2} - 1)(y^{r/2} + 1) \equiv 0 \bmod n$.

Vidíme, že Shorův algoritmus je vlastně kombinací dvou metod. Jednak hledání periody funkce $f_{y,n}(a)$ na kvantovém počítači, a jednak hledání největších společných dělitelů dvou čísel na klasickém počítači. Běžící časy obou metod se asymptoticky sčítají pouze na polynomiální složitost. Je možné zhruba odhadnout, že pokud je složitost řádu L^2, pak například faktorizace 768 bitového čísla by při délce jednoho výpočetního kroku kolem 100 cyklů trvalo na 100 MHz kvantovém počítači řádově jednotky sekund. Je jasné, že pokud by se podařilo takový algoritmus použít na skutečném kvantovém počítači, dostali bychom do rukou nástroj na prolamování většiny dnes používaných kryptoschémat. Není divu, že se již několik let o postup ve vývoji kvantových počítačů zajímají instituce, jejichž bezpečnostní systémy jsou založeny na složitosti problémů, jako

[10]V našem příkladě nejsou výsledky 4 a 19 superpozicí 4 stavů, protože se jedná o poslední neúplnou periodu (proto mají amplitudu $1/\sqrt{3}$); pro velká čísla je po měření rozdíl amplitud mezi jednotlivými výsledky nevýznamný.

je faktorizace. O tom, v jakém stádiu se vývoj kvantových počítačů nachází a o tom, jaké překážky klade vědcům vlastní implementace kvantového počítače se zmíníme v závěrečné kapitole. Nyní si ale představme, že žijeme v době, kdy již není kvantový počítač jen „na papíře“ a uvědomme si, jak by se asi změnila kryptografie jakou známe s existencí kvantových počítačů. Běžně by bylo možné výše popsaná kryptoschémata prolomit. Pak by nám nezbývalo nic jiného, než se pokusit kvantových systémů využít k vytvoření nových bezpečných komunikačních schémat, která by byla schopná vzdorovat pokusům o jejich prolomení. Proto zvládnutí kvantové mechaniky pro řešení problémů faktorizace neznamená konec kryptografie. Pouze to určitým způsobem mění podstatu používaných mechanizmů. S jedním z nich se seznámíme dále.

5.5 Kvantová kryptografie

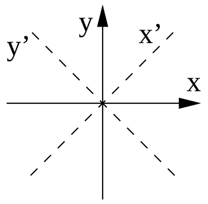
K tomu, abychom odvrátili nebezpečí prolomení současných šifrovacích schémat pomocí kvantových počítačů, je nutné soustředit se na takové problémy, jejichž složitost není potenciální existencí kvantového počítače tak degradována, jako je tomu v případě faktorizační úlohy.

Kromě hledání nových matematických problémů máme v případě kvantové mechaniky možnost využít přímo také problémů spojených s vlastním chováním kvantových systémů. Místo abychom tak použili některý z matematických problémů, o kterém se domníváme, že je se současným technickým vybavením neschůdný, opřeme bezpečnost konstruovaného mechanizmu o nějaký fyzikální děj, o kterém z kvantové teorie víme, že nemůže nastat. Toto nám na první pohled nabízí vyšší úroveň bezpečnosti než klasický matematický přístup, neboť je to sama příroda a její elementární zákony, které ručí za neprolomitelnost takového mechanizmu.

Na druhou stranu však musíme být v takových přístupech velmi obezřetní, protože je nutné důsledně rozlišit děje, které nejsou v přírodě možné z principu od dějů, které jsou sice možné, ale které nejsme zatím schopni technologicky realizovat. Toto je jistě nelehký úkol, který před sebou má teprve se rozvíjející oblast kvantové kryptografie.

Jako příklad zmíněného mechanizmu si zde uvedeme protokol, který v roce 1984 navrhli Charles Bennett a Gilles Brassard. Jejich protokol (BB84) využívá v zásadě dvou kvantových poznatků: teorému o *klonování kvantových stavů* a nemožnosti měření určitých párů veličin současně. Je nutné uvést, že protokol řeší „pouze“ nejcitlivější místo utajené komunikace. A sice výměnu klíčů bez použití důvěryhodné osoby, která by klíče oběma stranám doručila. Pokud jsme totiž schopni (kvantově-) bezpečně distribuovat klíč, pak nám nic nebrání v tom, abychom jako komunikační schéma použili některý z klasických algoritmů (nenapadnutelných kvantovým počítačem), jako je například dříve zmíněný One-time pad.

Aby bylo možné protokol BB84 popsat, je nutné nejprve navrhnout nějaké vhodné technické řešení komunikace mezi oběmi stranami. Již víme, že pro kódování kvantových stavů můžeme kromě spinu použít i jiné dvoustavové kvantové systémy. U protokolu BB84 se nám bude dobře hodit *polarizace* fotonů. Polarizací mohou být v zásadě dva druhy. Jedna je *lineární*, u níž světlo kmitá vždy v jedné rovině, která může být vzhledem k nějaké referenční rovině stočená o určitý úhel. Druhou je *kruhová*, při níž fotony rozlišujeme podle frekvence rotace vektoru elektrického pole v rovině kolmé na směr šíření. Podle směru rotace rozlišujeme mezi pravo- a levotočivou kruhovou polarizací. My si vybereme například lineární polarizaci. Nyní předpokládejme, že Alice a Bob se domluví na způsobu, kterým si budou bity posílat. Za prvé si určí dvě polarizační báze, tj. roviny, ve kterých mohou fotony kmitat. Jedna je vertikálně-horizontální (rektilineární) odkloněná od vodoroviny o 0° nebo 90°. Druhá – diagonálně-antidiagonální – definuje fotony, které oscilují v rovinách stočených o 45° nebo 135°. Aby se dalo mezi bity rozlišit, je potřeba definovat, který foton bude představovat 1, a který 0. Podle obrázku můžeme například říci, že 1 bude x a x' (0° a 45°), 0 pak y nebo y' (90° a 135°). Shrňme tedy, že máme 2 polarizační báze a celkem 4 různé polarizace fotonů.



pol. báze	0	1
$+$	$\updownarrow$	$\leftrightarrow$
$\times$	$\nwarrow$	$\nearrow$

Obrázek 9: **Měřící báze:** Na obrázku jsou znázorněny polarizační báze x, x' pro bit 1 a y, y' pro 0. Symbolicky jsou tyto údaje shrnuty v tabulce.

Měření se v praxi provádí za použití krystalu $CaCO_3$, který nechává horizontálně polarizované fotony projít přímo skrz, kdežto vertikálně polarizované odklání mimo osu příchozích fotonů. Diagonálně polarizované fotony se s poloviční pravděpodobností odkloní (a jejich polarizace se změní na vertikální) a s poloviční projdou přímo (a kmitají horizontálně). Proto nám měření v diagonální bázi neřekne nic o směru polarizace rektilineárních fotonů. Pokud bychom měřící krystal stočili o 45° pro měření diagonální polarizace, vstoupí stejný prvek náhody do měření rektilineárních fotonů. Jinými slovy jsou obě měřící báze k sobě komplementární a žádné měřící zřízení proto nemůže bez narušení stavu fotonu změřit *současně* jeden foton v obou bázích. To koresponduje se závěry Heisenbergova principu neurčitosti, který říká, že určité páry veličin nelze přesně měřit současně.

Vysvětleme si nyní, proč tomu tak je. Jak víme, je akt měření kvantového systému vyjádřen transformační Hermitovou maticí, která zachovává vlastní stav a násobí jej reálným číslem (vlastní hodnotou, tzv. *eigenvalue*). Obecně bychom napsali, že $\boldsymbol{A}|\psi\rangle = a|\psi\rangle$. Řekněme, že kvantový systém je v jednom z vlastních stavů matice $\boldsymbol{A}$. Pokud provedeme s tímto operátorem měření, systém ve vlastním stavu zůstane. Pokud ale budeme měřit takový systém operátorem pro jinou veličinu, například operátorem $\boldsymbol{B}$, pak systém nepředvídatelně (dle amplitud) přejde do jednoho z vlastních stavů popsaných operátorem $\boldsymbol{B}$. Pokud provedeme měření s operátory v opačném pořadí, změní se stav systému dvakrát (z původního souvisejícím s maticí $\boldsymbol{A}$ na stav související s $\boldsymbol{B}$ a zpět). Tato závislost na pořadí měření je odražena v *komutátoru* dvou veličin (jakémsi rozdílu měření veličin v obou pořadích), který je roven

$$[\boldsymbol{A}, \boldsymbol{B}] = \boldsymbol{AB} - \boldsymbol{BA}.$$

Zde se dostáváme zpět k fotonům a jejich měření. Pokud definujeme operátory měření v obou bázích jako

$$\boldsymbol{P}_r = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad \boldsymbol{P}_d = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

kde hodnoty ± 1 odpovídají pozorování fotonů odkloněných či prošlých přímo, pak komutátor zkonstruovaný ve stejné bázi není roven nule. (Stejné báze se docílí otočením jednoho operátoru o $\pi/4$ pomocí rotace $\boldsymbol{U}$.) Z toho plyne závěr, že nelze měřit přesně v obou bázích zároveň. V kvantově-kryptografické praxi to znemožňuje potenciální odposlouchávací osobě (obvykle Evě – *eavesdropper*) na kanále s jistotou určovat hodnoty bitů vysílací strany, pokud se obě strany domluví na použití dvou polarizačních bází. Navíc je Eva omezena teorémem o klonování kvantových stavů. Ten říká, že neznámý kvantový stav není možné klonovat (tj. v Hilbertově prostoru neexistuje pro jedno-qubitový stav $|\psi\rangle$ unitární transformace $\boldsymbol{U}$ taková, že $\boldsymbol{U}|\psi, 0\rangle = |\psi, \psi\rangle$). Myslí se tím to, že si Eva nemůže před měřením stav fotonu „zkopírovat“ a mít tak jeden pro poslání cílové komunikační straně a druhý – identický – pro své měření. To by samozřejmě znamenalo neschopnost její detekce.

Uvažujme nyní situaci, kde Alice je odesílatel a Bob příjemce zprávy. Nejprve si rozeberme jednoduchý příklad, kdy Alice používá pro všechny zaslané bity pouze jednu náhodně zvolenou polarizační bázi, o které Bob ví. Bob takto dokáže jednoznačně určit (v ideálním případě) všechny bity, které k němu doputovaly. Pokud ale bude náhodou na kanále odposlouchávat Eva, je zde 50% šance (v případě, že Eva uhodne polarizační bázi), že budou data kompromitována. Takové schéma je dosti naivní a je třeba jej patřičně vylepšit. Pojďme si proto popsat, jak funguje protokol BB84. Alice chce Bobovi zaslat klíč, kterým by oba později chtěli posílat utajená data. Proto si na své straně Alice nejprve vygeneruje náhodnou sekvenci bitů. Ty začne postupně posílat kvantovým kanálem Bobovi. To ale provádí tak, že opět náhodně mění polarizační bázi na své straně a posílá tak každý foton v jedné ze 4 možných polarizací. Bob tentokrát neví, kterou bázi má použít a proto náhodně střídá báze a provádí na fotonech měření polarizace. Průměrně v 50% případů je úspěšný a trefí se do stejné báze, v jaké daný foton Alice odeslala. Nyní nastupuje fáze, kdy si Bob a Alice veřejným kanálem sdělí, v jakých bázích měřili. U těch bází, v nichž se shodli, je zaručeno (pokud nedošlo k chybám na kanále), že Bob odečetl hodnotu fotonu správně. Dále je část těchto „správných“ bitů porovnáním obětována ke zjištění možného odposlechu. Pokud totiž na kanále odposlouchává Eva, potom neví, kterou bázi má k měření použít a tudíž své měřící báze střídá. To ale způsobuje, že musí někdy posílat Bobovi foton polarizovaný v jiné bázi než poslala Alice. Z toho plyne, že v případě, že Bob náhodou použije stejnou bázi jako Alice, může s pravděpodobností 25% naměřit jinou polarizaci, než Alice poslala a odhalit tak Evu. Celá věc by se měla objasnit z následujícího příkladu:

Alice posílá	$+$	$\updownarrow$	$+$	$\updownarrow$	$+$	$\updownarrow$	$+$	$\updownarrow$	$+$	$\updownarrow$
Eva měří / posílá	$+$	$\updownarrow$	$\times$	$\nearrow$	$\times$	$\nearrow$	$\times$	$\nwarrow$	$\times$	$\nwarrow$
Bob měří	$+$	$\updownarrow$	$+$	$\updownarrow$	$+$	$\leftrightarrow$	$+$	$\updownarrow$	$+$	$\leftrightarrow$

Tato tabulka obsahuje pouze výřez ze všech možností, které mohou nastat. Předpokládejme, že Alice i Bob měří ve správných polarizačních bázích $+$ a odposlouchávající Eva zkouší nastavit svůj detektor ve směrech $+$ nebo $\times$. Každý z těchto směrů představuje 50% případů v uvedené konfiguraci Alice a Boba. V prvním sloupci Eva získá správnou informaci a není přitom odhalena. Ve druhém až pátém sloupci (zbylých 50% případů) nezíská Eva nikdy správnou hodnotu polarizace (protože měří v jiné bázi) a navíc je porovnáním výsledků mezi Alicí a Bobem ve dvou z těchto čtyř případů (tj. v polovině z poloviny všech případů = 25%, viz třetí a pátý sloupec zleva) odhalena. To však bohatě postačuje k tomu, aby bylo srovnáním dostatečného počtu bitů její odposlouchávání potvrzeno. Čím více bitů je srovnáno (a tím i obětováno), tím větší je pravděpodobnost, že bude Eva odhalena. Jestliže je pravděpodobnost odhalení Evy u jednoho bitu 1/4, pak pro n bitů je to $1 - (3/4)^n$. Vidíme, že tato funkce roste exponenciálně k 1. To znamená, že můžeme s libovolnou přesností určit přítomnost Evy. Už pro pouhých 20 testovaných bitů je pravděpodobnost odhalení asi 99,7%. Po dokončení komunikace jsou zbylé neobětované bity použity jako klíč pro následnou tajnou komunikaci, která může používat klasická kryptoschémata. Protokol BB84 je vhodné shrnout do následujícího příkladu:

a)	1	1	0	1	1	1	1	0	1	0	1	0	0	1
b)	$\times$	$+$	$\times$	$+$	$+$	$+$	$\times$	$\times$	$\times$	$+$	$+$	$\times$	$+$	$\times$
c)	$\nwarrow$	$\leftrightarrow$	$\updownarrow$	$\leftrightarrow$	$\leftrightarrow$	$\updownarrow$	$\nearrow$	$\nwarrow$	$\nwarrow$	$\updownarrow$	$\leftrightarrow$	$\nwarrow$	$\updownarrow$	$\nearrow$
d)	$+$	$+$	$+$	$\times$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$\times$	$+$	$+$	$\times$
e)	0	1	0	0	1	1	1	1	1	0	1	1	0	1
f)		OK				OK	OK		OK	OK			OK	OK
g)		1					1						0	
h)		OK					OK						OK	
i)						1			1	0				1

a) Alice generuje náhodně sekvenci bitů. **b)** Potom si náhodně zvolí polarizační báze **c)** a kóduje bity do polarizace fotonů. **d)** Bob si na příjmu také náhodně volí báze, **e)** aby v nich naměřil hodnoty bitů. **f)** Veřejným kanálem si obě strany porovnají báze, v nichž měřili. **g)** Některé bity obětují k odhalení Evy. **h)** Protože Eva není přítomna (jinak by asi 1/4 bitů pozměnila), **i)** je uznán kanál za bezpečný a zbylé neodtajněné bity tvoří klíč.

Závěrem řekněme, že na rozdíl od prolamování současných šifer Shorovým algoritmem, je kvantová kryptografie dnes již laboratorně zvládnutelným principem, i když se pokusy pohybují na hraně technologických možností (ať již jde o přípravu jediného fotonu nebo realizaci založenou na posouvání fáze fotonů podobně jako u kvantového interferometru). Většinou se pro kvantový kanál používá optické vlákno, kterým se posílají jednotlivé fotony. I přes obtížnosti, které konstrukce použitelného kanálu klade, se již podařilo s rychlostmi několika desítek bitů za sekundu na vzdálenosti řádově desítek kilometrů klíč přenést. Přenos na větší vzdálenosti (přes ≈ 50 km) zatím představuje kvůli nemožnosti použití zesilovačů problém.

5.6 Náhodné jevy

V předchozích kapitolách jsme často používali spojení, že někdo něco náhodně vygeneruje nebo náhodně vybere variantu. Téměř jako bychom předpokládali, že na náhodných procesech není nic, co by stálo za hlubší analýzu. Podívejme se však nyní podrobněji na to, co náhodné jevy znamenají na klasickém počítači a jaké jsou možnosti při jejich realizaci na kvantových počítačích.

V některých vědních disciplínách se setkáváme s problémy, které není možné řešit deterministicky a výhodnější je při jejich řešení použít algoritmů využívajících náhodných čísel, která často vedou k řešení rychleji. I v algoritmech, o kterých jsme se zmínili, je často nutné provést náhodnou volbu nebo vygenerovat náhodné číslo. Řekněme si však nejprve, co to vlastně náhodné číslo je. Matematicky je možné o náhodném čísle mluvit, pokud je součástí posloupnosti několika čísel nebo číslic, tj. v určitém kontextu. V takovém případě můžeme například pomocí zkoušek na distribuci a korelaci mezi čísly v posloupnosti rozhodnout, zda lze tuto posloupnost považovat za náhodnou. Protože po klasických počítačích nemůžeme chtít nic jiného, než aby zpracovávaly algoritmicky vstupy a vracely výstupní data, lze vždy pouze skončit u lepšího nebo horšího *generátoru náhodných čísel*. Jistě si dovedeme představit posloupnost, která by prošla oběmi výše uvedenými zkouškami, ale nějaká další zkouška by v posloupnosti odhalila skrytý vzorec. Proto je problém rozhodnutí o náhodnosti posloupnosti ekvivalentní problému o bezztrátové kompresibilitě dané posloupnosti (tzv. Kolmogorova-Chaitinova interpretace). To znamená, že jedině pokud je posloupnost nezhustitelná do kratší podoby, je opravdu náhodná. Ve skutečnosti je problém odhalení náhodnosti (kompresibility) posloupnosti nealgoritmizovatelný, tudíž nevypočitatelný. Z toho rovnou plyne, že není možné klasicky náhodné číslo vygenerovat; vždy je výstupem jen sekvence čísel, vytvořená podle určitého předpisu. Proto dokáží klasické generátory produkovat jen tzv. pseudonáhodná čísla. Ta překvapivě pro řadu problémů postačují, ne však pro všechny.

Abychom měli co srovnávat, podívejme se nyní stručně na některé klasické generátory náhodných čísel a posuďme, jak kvalitní výsledky vracejí. První známou skupinou jsou *lineárně-kongruentní generátory* založené na výpočtu pravidla:

$$N_{k+1} = (l \cdot N_k + m) \bmod M,$$

kde l, m, M jsou celočíselné parametry. Pokud $N_0 \in \langle 0, M)$, pak toto pravidlo generuje čísla z rozsahu $\langle 0, M-1\rangle$. Výstupy těchto generátorů jsou náhodné, avšak periodické s periodou nejvýše M. Perioda je ale velmi závislá na volbě parametrů. Špatná volba znamená malou periodu a časté opakování stejných čísel. Lineárně-kongruentní generátor používá s parametry $l = 1103515245, m = 12345$ a $M = 2^{32}$ například UNIXová funkce `rand()` generující 32-bitová celá čísla. Pro aplikace používající 32-bitový `int` jsou však někdy tyto generátory nedostatečné, protože perioda $2^{32} \approx 10^9$, může být na dnešních počítačích vyčerpána za několik sekund. Aritmetika s dvojtou šířkou, pak může být neúnosně pomalá. Další nevýhodou se později ukázala skutečnost, že skupiny generovaných čísel vykazují geometrický vzorec, který odhaluje test na prostorové rozložení *(scatter plot test)*. Tento problém odstraňují tzv. *kombinované* lineárně-kongruentní generátory, které nepoužívají ke generování pouze jedno předchozí číslo. Výsledek je tvořen součtem dvou pomocných náhodných čísel. Perioda posloupnosti odpovídá $M_1 \cdot M_2$.

$$\begin{aligned} x_i &= (l \cdot x_{i-1} + m_1) \bmod M_1, \\ y_i &= (l \cdot y_{i-1} + m_2) \bmod M_2, \\ N_i &= (x_i + y_i) \bmod max(M_1, M_2). \end{aligned}$$

Na podobném principu jsou založeny také *zpožděné (lagged) Fibonacciho generátory.* Mají však tu výhodu, že náhodné číslo závisí na některém jiném čísle ze stejné posloupnosti a nikoliv na číslech ze dvou pomocných posloupností. Zvyšuje se tím délka periody a snižuje míra korelací mezi prvky posloupnosti.

$$N_i = (N_{i-p} \odot N_{i-q}) \bmod M,$$

kde p a q jsou zpoždění (lags), nabývající nezáporných hodnot do velikosti posloupnosti a $\odot$ je aritmetická operace (jako $+$, $\times$, XOR). Výhodou je, že volbou zpoždění měníme také periodu generovaných čísel. Nicméně je třeba připomenout, že ne vždy je složitý generátor lepší než jednoduchý. Pokud se řeší praktické problémy (například z oblasti simulací), pak často nezbývá nic jiného, než vyzkoušet více generátorů a zvolit ten nejvhodnější[11].

Vidíme, že klasické generátory náhodných čísel mají svoje omezení jak v délce periody, tak v podobě nejrůznějších (často nezjistitelných) korelací mezi čísly. Pokud se podíváme na problém filozofičtěji, pak máme pocit, že je snad jen neschopností počítačů generovat náhodná čísla. A tak nás může napadnout, zda není člověk schopen generovat náhodná čísla. V experimentu D.W.Hagelbargera popsaném Claudem Shannonem, byla zvolená osoba požádána, aby vygenerovala náhodnou posloupnost symbolů $+$ a $-$, kterou analyzoval počítač. Ten se pak na základě rozboru této posloupnosti snažil dopředu uhodnout, jaký následující

[11] Jak jsme již řekli, počítače dokáží vytvářet jen pseudonáhodná čísla, která jsou vytvářena deterministickým algoritmem. V kryptografii nahrazujeme požadavek náhodnosti požadavkem nepredikovatelnosti. Ze znalosti hodnot $x_1, \ldots, x_{n-1}$ nesmí útočník úspěšně určit x_n. Takovéto generátory se vytvářejí např. za pomoci algoritmů blokových šifer, které vytváří náhodné sekvence závislé na klíčích těchto algoritmů, bez nichž je sekvence nepredikovatelná. Pro zpracování opravdu citlivých informací se však i zde vyžaduje generátor založený na fyzikálním principu (viz dále).

symbol si osoba vybere. Počítač byl v předpovídání úspěšný na 55–60%, což znamená, že ani člověk nevolí odpovědi úplně nezávisle. Jak potom ale můžeme připravit okamžik *skutečné* náhody? Odpověď zní: kvantově-mechanicky. Jedině.

Zcela přirozeně k tomu můžeme použít základní vlastnost přírody – chvíli náhodného kolapsu vlnové funkce v jeden z vlastních stavů kvantového systému v momentě měření. Pojďme si tedy přiblížit poměrně jednoduchý algoritmus, kterým může kvantový počítač generovat skutečná náhodná čísla. Pokud budeme uvažovat fyzikální systém představující qubit ve stavu $|0\rangle$, pak úkolem bude jej připravit do vyvážené superpozice stavů $|0\rangle$ a $|1\rangle$. Toho docílíme aplikováním unitárního operátoru $\boldsymbol{U}$ s rotací o $\pi/4$.

$$\boldsymbol{U}\left(\frac{\pi}{4}\right)|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

V této chvíli je systém připraven na měření. Při měření přejde systém náhodně do jednoho z vlastních stavů této superpozice. Pokud chceme generovat vícebitová náhodná čísla je potřeba připravit dost qubitů k reprezentaci těchto čísel a následně vytvořit operací přímého tenzorového součinu jeden více-qubitový registr, který poté změříme. Ukažme si tyto kroky na jednoduchém příkladu: Řekněme, že chceme vygenerovat číslo z rozsahu $0-15$.

- Nejprve si připravíme čtyři izolované qubity ve stavu $|0\rangle$.
- Aplikací $\boldsymbol{U}\left(\frac{\pi}{4}\right)$ upravíme stav každého qubitu na vyváženou superpozici $|0\rangle$ a $|1\rangle$, tj. $\left\{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\ \frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\right\}$.
- Poté přímým součinem vytvoříme z jednotlivých qubitů jeden paměťový registr, tj. $\frac{1}{4}\big(|0000\rangle + \ldots + |1111\rangle\big)$.
- Nakonec takto připravený registr změříme, čímž superpozice náhodně zkolabuje do jednoho z možných stavů $|0000\rangle, \ldots, |1111\rangle$.

Existují tedy aplikace, které klasický počítač z principu nezvládá, kdežto kvantový ano. Nicméně pro generování náhodných čísel se dnes už nemusíme nutně upínat ke klasickému počítači, neboť již existují generátory (TRNG - True Random Number Generators) využívající kvantovou mechaniku. Dříve šlo zejména o fyzikální procesy založené na radioaktivním rozpadu prvků. Počet těchto rozpadů detekovala Geiger-Müllerova trubice, která výsledky následně převáděla do počítače. Podle intervalů měření šlo generovat náhodná čísla různých rozložení. Nevýhodou však byla většinou malá rychlost generování. Častěji se dnes proto jako TRNG používají kvantově mechanické děje na polovodičových přechodech. Velmi častá je detekce náhodného prvku ze šumu, který je možné naměřit na PN přechodech polarizovaných v závěrném směru. Klasický PC tak vlastně už dnes používá jako periferii silně degenerovaný kvantový počítač.

6 Kvantová teleportace

Obraťme nyní pozornost k další z pozoruhodných vlastností kvantového světa. Tou je jev *kvantové teleportace*. Význam slova teleportace je nám dobře znám ze science fiction a většinou si pod ním představujeme bezztrátový přenos hmoty prostorem, jehož výsledkem je rekonstrukce objektu na jiném místě. V této kapitole si ukážeme, jak teleportaci chápe kvantová mechanika a popíšeme si také úskalí, která její implementace v praxi má.

6.1 Teleportace jednoho qubitu

Jak známo, Heisenbergův princip neurčitosti nedovoluje změřit přesně všechny charakteristiky kvantového systému současně. Tím bychom ale hned v úvodu možné diskuze o teleportaci zcela eliminovali, protože by nebylo možné získat informaci o celém kvantovém systému před tím, než bychom jej přenesli. To se ale změnilo roce 1993, kdy skupina předních kvantových teoretických informatiků dospěla k formulaci *teleportace stavu* kvantového systému s využitím další z vlastností kvantového světa, a sice fenoménu propletení (entanglement) kvantových stavů. Fyzikálně mají propletené částice korelován nějaký atribut, který se při jejich vzniku zachovává. Příkladem takového atributu je spin nebo polarizace. Jestliže má jedna částice spin nahoru, pak druhá má s jistotou spin dolů a naopak. Při měření na jedné částici dojde ke kolapsu vlnové funkce systému v celém prostoru a k přechodu do jednoho z možných vlastních stavů. Tím se jednoznačně určí, která z částic má spin dolů a která nahoru. Téměř magická povaha propletení vyvolává mezi fyziky řadu otázek. Zejména je s podivem, že lze bez přítomnosti výměnných částic ovlivňovat částici, která je třeba na opačné straně vesmíru. Očekávali bychom, že v kauzálním kontaktu mohou být jen místa, mezi nimiž existuje časoprostorové spojení omezené rychlostí světla. Nicméně kvantová mechanika v tomto ohledu směřuje rázně ke konceptu *nelokální reality*. Tento koncept byl dlouho odmítán, protože Einsteinovi připadalo nemožné, aby kvantová mechanika porušovala principy lokálnosti, kterými se řídí relativistická fyzika. Tento problém byl později nazván EPR (Albert Einstein, Boris Podolsky, Nathan Rosen) paradox. Zabýval se otázkou, zda již v momentě vzniku nemohou mít částice předem určeny výsledky měření. A to i s možností, že neznáme všechny aspekty popisu kvantového světa a tudíž existují skryté proměnné, které by dopředu udržovaly informaci o stavu částic (což by ukazovalo na neúplnost kvantové mechaniky). Fyzikové se poté snažili tento paradox vyvrátit a teoretickým experimentem (který byl pak několikrát v praxi potvrzen) dokázali, že obě částice nabývají hodnoty daného atributu až v momentě měření a náhodného přechodu do vlastního stavu korelovaného se stavem druhé částice[12]. Stavu propletení se také jinak říká EPR stav nebo EPR efekt.

Propletení je možno připravit různými fyzikálními postupy. Například se k tomu

[12] V roce 1960 ukázal John Bell, že existuje experiment, kterým lze vyvrátit existenci skrytých proměnných a potvrdit nelokální realitu. Experiment po něm dostal název Bellovy nerovnosti.

používá krystal β-BaB_2O_4. Jestliže do tohoto krystalu namíříme ultrafialový foton, pak se někdy po průchodu přemění na dva fotony s nižší energií, jeden polarizovaný vertikálně, druhý horizontálně. Pokud však foton prochází místem krystalu, kde jsou výskyty obou polarizací v „rovnováze“, pak dojde ke vzniku dvou fotonů, jejichž polarizace jsou neurčité, avšak komplementární. Matematicky je propletení stav, který nelze vyjádřit jako direktní součin jednotlivých stavů složek.

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \qquad \text{nebo} \qquad |\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle).$$

Předpokládejme, že Alice má nějakou částici A v neznámém kvantovém stavu $|\psi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$, kde $|\omega_0|^2 + |\omega_1|^2 = 1$, a chce tento stav poslat Bobovi. Víme, že změřit částici nemůže, protože by tím křehký kvantový stav porušila. Jediné co ji zbývá, je stav teleportovat. K tomu ale bude muset využít triku s propletením stavů částic. Nejprve si Alice a Bob připraví propletený EPR pár dvou částic B a C jako $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice si z tohoto páru ponechá částici B, Bobovi zašle částici C. Alice pak spojí svoji částici A a propletený pár do systému tří částic

$$|\varphi\rangle = |\psi\rangle \otimes |\phi\rangle = \frac{1}{2}(\omega_0|000\rangle + \omega_0|011\rangle + \omega_1|100\rangle + \omega_1|111\rangle).$$

K provedení teleportace musí nyní Alice provést měření na sloučeném stavu obou částic. Toto měření je speciální tím, že musí být provedeno v tzv. Bellově bázi pouze pro částice A a B (což způsobí pouze jiné vyjádření stavu $|\varphi\rangle$), jejíž čtyři stavy tvoří úplnou ortonormální bázi částic A a B. Tato báze má tvar $\{|\Psi^-\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Phi^+\rangle\}$, kde

$$|00\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle), \qquad |01\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle),$$

$$|10\rangle = \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle), \qquad |11\rangle = \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle).$$

Protože lze výše uvedený zápis stavu $|\varphi\rangle$ přepsat na

$$|\varphi\rangle = \frac{1}{\sqrt{2}}(\omega_0|00\rangle \otimes |0\rangle + \omega_0|01\rangle \otimes |1\rangle + \omega_1|10\rangle \otimes |0\rangle + \omega_1|11\rangle \otimes |1\rangle),$$

je možné první dva qubity převést do Bellovy báze a $|\varphi\rangle$ vyjádřit jako

$$|\varphi\rangle = |\Phi^+\rangle\frac{1}{\sqrt{2}}(\omega_0|0\rangle + \omega_1|1\rangle) + |\Psi^+\rangle\frac{1}{\sqrt{2}}(\omega_1|0\rangle + \omega_0|1\rangle)$$

$$+|\Phi^-\rangle\frac{1}{\sqrt{2}}(\omega_0|0\rangle - \omega_1|1\rangle) + |\Psi^-\rangle\frac{1}{\sqrt{2}}(\omega_1|0\rangle - \omega_0|1\rangle).$$

Pokud nyní Alice změří v Bellově bázi první dva qubity stavu $|\varphi\rangle$, obdrží se stejnou pravděpodobností 1/4 jeden ze 4 možných výsledků, tj. některý ze stavů

$|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle$. Protože jsou však částice propleteny, změní se přitom projekcí i stav Bobovy částice na jeden ze stavů

$$\frac{1}{\sqrt{2}}(\omega_0|0\rangle + \omega_1|1\rangle),\ \frac{1}{\sqrt{2}}(\omega_1|0\rangle + \omega_0|1\rangle),\ \frac{1}{\sqrt{2}}(\omega_0|0\rangle - \omega_1|1\rangle),\ \frac{1}{\sqrt{2}}(\omega_1|0\rangle - \omega_0|1\rangle).$$

Všimněme si, že Alice svým měřením prvních dvou qubitů neodkryla nic konkrétního o stavu částice A, kterou chce teleportovat. Místo toho pouze odhalila, kterou kombinaci sloučených stavů všech tři částic u sebe má. Rozhodující tak byla před měřením skutečnost, že jsme přechodem do nové báze „promíchali“ předtím oddělený stav částice A (první qubit stavu $|\varphi\rangle$) s propleteným párem částic B a C (druhý a třetí qubit).

V tuto chvíli má u sebe Bob jeden ze čtyř možných teleportovaných stavů. Pouze v jednom případě jsou však správně zachovány amplitudy, ostatní výsledky jsou různě rotovány. Proto přichází chvíle, kdy se Alice s Bobem spojí klasickým komunikačním kanálem a sdělí mu, jaký výsledek naměřila. Bob tuto klasickou (2-bitovou) informaci použije k tomu, aby na stav částice C aplikoval příslušnou rotaci. K tomu použije následující tabulku.

měření Alice	rotace Boba	měření Alice	rotace Boba
$\|\Phi^+\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\|\Psi^+\rangle$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\|\Phi^-\rangle$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	$\|\Psi^-\rangle$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Poznamenejme, že je to právě komunikace klasickým kanálem, která znemožňuje posílat informace nadsvětelnou rychlostí. Bez informace o měření Alice by Bob nemohl s jistotou říci, že má stav částice A. Zároveň je zřejmé, že je naplněn také teorém o klonování kvantových stavů tím, že stav částice A je při teleportaci zničen.

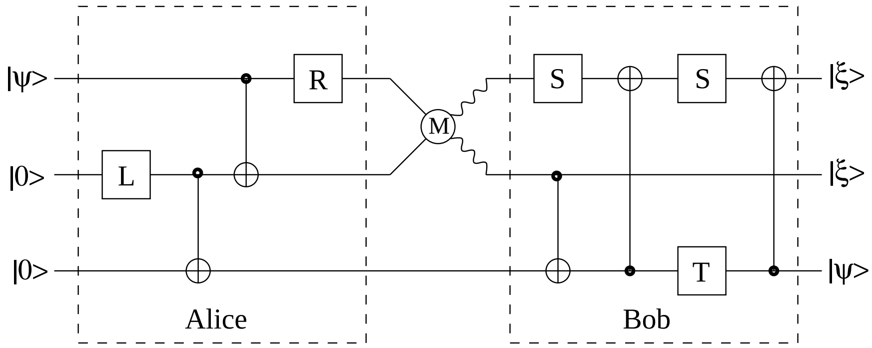
6.2 Kvantový teleportační obvod

Aby bylo možné teoretický základ teleportace realizovat, je nutné navrhnout kvantový obvod, který by to dokázal. Gilles Brassard vytvořil obvod, který umí teleportovat qubit s použitím bran působících nejvýše na dva qubity. Brassardův obvod je znázorněn na obrázku.

Obvod se skládá z dvou-qubitové brány ***XOR*** a dále z jedno-qubitových bran:

$$\boldsymbol{R} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \qquad \boldsymbol{L} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

Tyto brány jsou operátory rotace na qubitech a z vlastních stavů generují superpozice stavů (odpovídají Hadamardovým branám ***H'*** a ***H"***). Brány ***S*** a ***T***



Obrázek 10: **Brassardův teleportační obvod:** Obvod je rozdělen na dvě části. Jedna část tvoří obvod Alice a obsahuje bránu $\boldsymbol{L}$, která ji umožňuje proplést částice B a C. Bránou $\boldsymbol{R}$ pak proplete stav $|\psi\rangle$ s částicemi B a C. Následně provede Bellovo měření M částic A a B, jehož výsledek oznámí dvěma bity Bobovi (vlnovky). Stavy částic A a B měřením zkolabují a částice C přejde do jednoho ze čtyř možných stavů. Bob využije informace od Alice jako vstupy do své části obvodu a pomocí bran $\boldsymbol{S}$ a $\boldsymbol{T}$ provede nutné rotace k úpravě stavu částice C. Brány $\boldsymbol{XOR}$ jsou označeny symbolem $\oplus$.

provádí na qubitech fázový posun.

$$\boldsymbol{S} = \frac{1}{\sqrt{2}} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \qquad \boldsymbol{T} = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}.$$

Na závěr nás může zajímat odpověď na otázku, k čemu se může kvantová teleportace hodit. Je zřejmé, že teleportování stavu znemožňuje i teoretické odposlouchávání přenosu, protože informace žádným komunikačním kanálem neputuje. Navíc Alice ani nemusí tušit, kde se právě Bob se svou propletenou částicí nachází, protože stačí, aby například vysílačem rozeslala klasickou zprávu do všech směrů. Také pro implementaci kvantového počítače je teleportace zajímavé téma s ohledem na přenášení qubitů mezi částmi kvantového procesoru. Protože kvantová teleportace je pouze protokol popisující zaslání kvantového stavu, nesouvisí přímo s existencí kvantového počítače, a proto je její realizace možná již dnes. První úspěšné teleportace na mikro- i makroskopické vzdálenosti byly provedeny v letech 1997 a 1998.

7 Kvantová oprava chyb

Až do této chvíle jsme uvažovali ideální kvantový systém. Ten se vyznačuje tím, že jej z vnějšku nic nenarušuje a také vnitřně se vyvíjí konzistentně. Avšak zcela izolovat nějakou částici od svého okolí není technicky možné. Jakýkoliv kontakt s okolními částicemi (tedy i částicemi pole) totiž způsobuje tzv. *dekoherenci* kvantového stavu, což prakticky představuje provázání částice s okolím a tím i nežádoucí chybovou změnu kvantového stavu. Navíc dekoherence není jediným procesem vedoucím k chybám. Například spontánní přechod qubitu, realizovaného stavem elektronu, mezi vybuzeným a základním stavem má za následek překlopení qubitu do komplementárního stavu (podle reprezentace $|0\rangle \rightarrow |1\rangle$ nebo $|1\rangle \rightarrow |0\rangle$), což je doprovázeno vysláním fotonu příslušné energie, která je tak ze systému uvolněna do okolí (*vyzařování energie*). Další nepříznivé vlivy mohou zahrnovat i vliv kosmického záření vysokých energií nebo částice okolního plynu. A tak se v 90.letech v mnoha odborných pracích rozpoutala diskuze o schůdnosti realizace kvantových počítačů. Ta vedla ke vzniku problematiky věnující se detekci a opravě chyb, k nimž dochází během kvantového výpočtu – tzv. *kvantové opravě chyb (quantum error correction)*.

7.1 Dekoherence

Ještě nedávno nebylo zcela jasné, zda bude možné kvantový výpočetní systém vůbec sestrojit. Zdálo se nemožné, aby se za krátký moment než systém dekoheruje, provedl rozumný výpočet. Dekoherence má totiž stejný efekt, jako bychom provedli měření a tím vlastně zahodili možné superpozice stavů a případné interference mezi nimi již v průběhu výpočtu. Vzhledem k implementaci jsou pak nepříjemné doby, za které k dekoherenci dochází. V běžném prostředí, jež prostupují nejrůznější pole a částice je tato doba v závislosti na teplotě a velikosti systému (10^{-8} m) asi 10^{-20} s. Pokud se podaří kvantový systém co nejlépe izolovat od prostředí, je možné tyto časy prodloužit použitím různých druhů kvantových systémů. Například použití metody uvězněných iontů (*trapped ions*) dovoluje provést během doby než systém dekoheruje (asi 10^{-1} s) až 10^{13} operací.

Dekoherence se popisuje pomocí operátorů hustých matic, které mají k sobě asociovány tzv. *smíšené stavy*. Smíšené stavy popisují systém, o němž nemáme úplnou informaci a přesně nevíme v jakém čistém stavu (tj. v jakém konkrétním kvantovém stavu popsaném buď vlastním stavem nebo superpozicí) se právě nachází. Takový popis se může hodit právě v momentě, kdy kvantový systém něco ruší a nepředvídatelně mění jeho stav. Součet klasických pravděpodobností přes možné čisté stavy tvořící smíšený stav, je roven 1. Husté matice tak obsahují informace o možných čistých stavech[13]. Například pro stav $|\phi\rangle = \omega_0|0\rangle + \omega_1|1\rangle$

[13] Například informace o střední hodnotě určité sledované veličiny, časovém vývoji smíšeného systému nebo pravděpodobnostech přechodů do vlastních stavů sledované veličiny (dostáváme zde jakýsi dvouúrovňový systém pravděpodobností – jednak klasické pravděpodobnosti existence čistých stavů v rámci smíšeného stavu a jednak kvantové pravděpodobnosti vlastních stavů v čistých stavech).

je hustá matice:

$$\rho = |\phi\rangle\langle\phi| = \begin{pmatrix} |\omega_0|^2 & \omega_0\omega_1^* \\ \omega_0^*\omega_1 & |\omega_1|^2 \end{pmatrix}$$

Dekoherence eliminuje prvky, které jsou mimo diagonálu. To zaručuje časově závislá hustá matice

$$\rho_t = \begin{pmatrix} |\omega_0|^2 & e^{-t/\tau}\omega_0\omega_1^* \\ e^{-t/\tau}\omega_0^*\omega_1 & |\omega_1|^2 \end{pmatrix},$$

kde τ se nazývá *dekoherenční čas*. Elementy $\omega_0\omega_1^*$ a $\omega_0^*\omega_1$ tak exponenciálně konvergují k nule. Jak se dnes zdá, dekoherenci zatím nelze úplně zabránit. Proto jsou v této chvíli úvahy o univerzálním kvantovém počítači, který by byl neomezeně stabilní, poněkud předčasné (přestože existují optimistické náznaky možných řešeních). Je však jasné, že tyto systémy budou muset být tolerantní k chybám a mít velmi sofistikované samoopravné mechanizmy. Podívejme se nyní na možnosti, které kvantová oprava chyb má.

Matematicky je možné chyby v kvantovém systému popsat pomocí několika operátorů, jejichž lineární kombinací lze vyjádřit libovolnou chybu. Těmito operátory jsou *Pauliho spinové matice*:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \boldsymbol{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Každá matice působící na nějaký stav $|\psi\rangle = \begin{pmatrix} \omega_0 \\ \omega_1 \end{pmatrix}$ a určitým způsobem ho modifikuje (kromě matice identity $\boldsymbol{I}$). Tyto modifikace jsou shrnuty v následující tabulce.

operátor	chybová operace	výsledek operace
σ_x	inverze bitu	$\begin{pmatrix} \omega_1 \\ \omega_0 \end{pmatrix}$
σ_y	inverze bitu a fázový posun	$\begin{pmatrix} -i\omega_1 \\ i\omega_0 \end{pmatrix}$
σ_z	fázový posun	$\begin{pmatrix} \omega_0 \\ -\omega_1 \end{pmatrix}$
$\boldsymbol{I}$	bez chyby	$\begin{pmatrix} \omega_0 \\ \omega_1 \end{pmatrix}$

Pro vícequbitové systémy vytváříme operátory složené direktním součinem dílčích operátorů. Například chybu σ_y na druhém qubitu ve 2-qubitovém systému vyjádříme jako $\boldsymbol{I} \otimes \sigma_y$.

Chyby, které při výpočtu vznikají si zákonitě vyžadují svoji korekci. Principy detekčních a opravných kódů u kvantových systémů vycházejí z poznatků zabezpečovacích metod v klasické teoretické informatice, které eliminují chyby způsobené nedokonalostmi technologií nebo rušivým vlivem (makroskopického) prostředí. Problémy u kvantového systému ovšem nastávají ve chvíli, kdy chceme chyby detekovat nebo je opravovat, protože měřením přirozeně stav porušíme.

Na první pohled vypadá problém s měřením nepřekonatelný. Jak je možné zjistit zda došlo k chybě, když vlastně nemůžeme chybu změřit? Nebo dokonce jak takovou chybu opravit? Odpověď na tyto otázky přinesly až důmyslné algoritmy, z nichž některé si nyní představíme.

7.2 Oprava symetrizací

Princip opravy symetrizací společně navrhli Andre Berthiaume, David Deutsch a Richard Jozsa a opírá se redundanci výpočtu na několika kvantových počítačích, které jsou určitým způsobem spjaty s pomocným kvantovým systémem, jehož měřením korigujeme chyby vzniklé v redundantních počítačích. Řekněme, že máme R replik kvantového počítače, které provádějí stejný výpočet. V mírně chybovém prostředí si každá replika udržuje trochu jiný stav, než by byl ideální $|\psi\rangle$, který souhrnně zapíšeme pomocí direktního součinu jako

$$|\Psi\rangle = |\psi_1\rangle \otimes \ldots \otimes |\psi_R\rangle.$$

Pokud je výpočet prováděn v nechybovém prostředí, pak jsou stavy na jednotlivých kopiích shodné a okupují pouze malou část celého Hilbertova prostoru. O této čísti říkáme, že je symetrická[14] a tvoří podprostor $\mathcal{S}$ složený z vektorů $\bigotimes_{i=1}^{R} |\psi\rangle$. Pokud provedeme měření, které je projekcí aktuálního stavu kopií do tohoto ideálního podprostoru, pak bezchybné stavy zůstanou zachovány, kdežto chybové se odstraní.

Stabilizace kvantového počítače symetrizací funguje dobře na menší odchylování od ideálního stavu. Velké chyby typu prohození bitu však vyžadují složitější opravné strategie.

7.3 Kvantové opravné kódy

Kvantové opravné kódy do jisté míry kopírují klasické opravné kódy. Snaží se jeden logický qubit nahradit kódovým slovem, které je navrženo tak, aby přes náhodné prohození některé jeho části bylo stále možné odhalit, že došlo k chybě, případně tuto chybu odstranit. To je možné tehdy pokud v sobě kódová slova obsahují mezi jednotlivými qubity vzájemné závislosti. První kvantový kód navrhl v roce 1995 Peter Shor. Ten zakódoval jeden logický qubit pomocí 9 fyzických propletených qubitů. Stavy $|0\rangle$ a $|1\rangle$ kóduje pomocí stavů $|0_E\rangle$ a $|1_E\rangle$, jejichž definice jsou shrnuty v tabulce.

qubit	Shorův kód – 9-qubitový
$\lvert 0_E\rangle$	$\frac{1}{2\sqrt{2}}(\lvert 000\rangle + \lvert 111\rangle)(\lvert 000\rangle + \lvert 111\rangle)(\lvert 000\rangle + \lvert 111\rangle)$
$\lvert 1_E\rangle$	$\frac{1}{2\sqrt{2}}(\lvert 000\rangle - \lvert 111\rangle)(\lvert 000\rangle - \lvert 111\rangle)(\lvert 000\rangle - \lvert 111\rangle)$

Novější metoda, kterou vymysleli vědci ze skupiny Raymonda Laflammeho proti tomu používá jen 5 qubitů.

[14] To znamená, že nezáleží na pořadí v jakém spojujeme pomocí tenzorového součinu jednotlivé stavy.

qubit	Laflammeho kód – 5-qubitový
$\|0_E\rangle$	$\frac{1}{2\sqrt{2}}(\|00000\rangle + \|00110\rangle + \|01001\rangle - \|01111\rangle +$ $\|10011\rangle + \|10101\rangle + \|11010\rangle - \|11100\rangle)$
$\|1_E\rangle$	$\frac{1}{2\sqrt{2}}(\|11111\rangle + \|11001\rangle + \|10110\rangle - \|10000\rangle +$ $\|01100\rangle - \|01010\rangle - \|00101\rangle - \|00011\rangle)$

Kvantová oprava chyb se skládá z několika kroků:
- procesu kódování stavů $|0\rangle \to |0_E\rangle, |1\rangle \to |1_E\rangle$,
- vzniku chyby ve stavu zakódovaných qubitů,
- dekódování chybového stavu,
- určení chybového syndromu (tj. chyby, která nastala),
- aplikace unitární transformace k opravě stavu.

Pro kódování a dekódování existují příslušné kvantové obvody. V případě Laflammeho kódu je obvod složen z bran $\boldsymbol{CNOT}$, Hadamardovy transformace $\boldsymbol{H}$ a podmíněné rotace o úhel π. Jeden qubit je v tomto obvodu informační, ostatní čtyři opravné. Laflammeho schéma přitom dokáže opravit jednu ze tří typů chyb. Jsou to chyby prohození bitu, znaménka nebo bitu i znaménka pro všechny bity kódového slova. Konkrétní chyba je detekována výpočtem chybového syndromu a odstraněna aplikací příslušné opravné transformace. V případě 5-qubitového kódu se výpočet syndromu provádí aplikací kódovacího obvodu v opačném směru. Například pokud pro syndrom $|0000\rangle$ (což odpovídá čtyřem opravným qubitům po opačné aplikaci kódovacího obvodu) nedošlo ve stavu $\omega_0|0\rangle + \omega_1|1\rangle$ k chybě, pak pro syndrom $|1000\rangle$ došlo k prohození druhého bitu kódového slova.

Kvantová oprava chyb je velmi důležitá oblast kvantové informatiky, protože podmiňuje samotnou realizaci kvantového počítače. O univerzálních kvantových počítačích odolných chybám a běžících nepřetržitě se však dá nyní pouze spekulovat. Není totiž jasné, zda lze dekoherenci zabránit na stálo, případně zda se během výpočtu nebudou muset předávat částečné výsledky vzniklé v čase koherence mezi více uzly kvantového počítače. Navíc je zřejmé, že u opravných kódů je problémem samotný proces de/kódování, o kterém nemůžeme přímo tvrdit, že je bezchybný. Také množina popsaných chyb, ke kterým v kvantových systémech dochází nemusí být nutně úplná.

8 Experimentální kvantové procesory

Kvantová informatika by zůstala jen teoretickou kuriozitou nebýt úsilí a důvtipu vědců, kteří se snaží na bázi dnešních technologií konstruovat první ovladatelné kvantové systémy, které by bylo možno alespoň vzdáleně považovat za předchůdce kvantových počítačů. První experimenty v této oblasti společně spadají do nedávné minulosti – na závěr 90.let. Provádět pomocí precizních zásahů do kvantových systémů operace odpovídající kvantovým bránám je přirozeně obtížné. V této kapitole se zaměříme na technologie, které vypadají nejnadějněji vzhledem ke konstrukci kvantových procesorů, a které zároveň jasně demonstrují problémy, jež tyto technologie provází. Je zřejmé, že při konstrukci budeme především chtít,

1. aby byl náš procesor dostatečně jednoduchý na ovládání

2. aby byl zároveň dostatečně (dlouho) izolovatelný od okolí

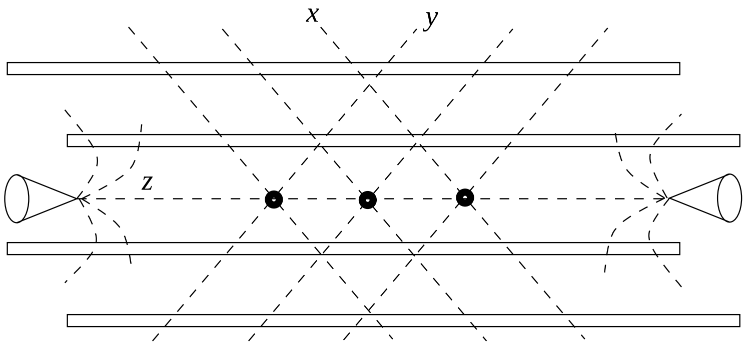
3. aby byl schopen pojmout dostatečný objem informací[15].

Kvantových systémů splňujících co nejpřesněji tyto podmínky však není známo mnoho. Jedny z nejvíce experimentálně prověřených se zdají být systémy tzv. *iontových pastí (trapped ions).*

8.1 Iontová past

Myšlenka stojící za iontovou pastí spočívá v uvěznění iontů v prostoru tak, aby co nejméně vzájemně působily s okolím, a tím prodloužily dobu koherence systému. Experiment vypadá následovně: Ve vakuu se destička s čistým vápníkem (stříbrný kov) nejprve zahřeje na asi 800 °C. Při této teplotě se začnou z povrchu destičky „odpařovat“ jednotlivé atomy vápníku. Tyto atomy se posléze bombardují urychlenými elektrony, které odstraní elektrony z atomů vápníku za vzniku iontů Ca^+. Poblíž iontů se nachází speciální čtveřice elektrod, (asi 1mm široké a několik cm dlouhé) které v těchto místech vytváří proměnné elektrické pole. Pokud definujeme osu pasti jako z (podél elektrod), pak se v rovině xy vytváří potenciálové prohlubně, které zamezují pohyb iontů ve směru x. Změnou potenciálu následně omezujeme pohyb ve směru y. Rychlým přepínáním mezi potenciály (v řádech MHz) v obou směrech se nemohou ionty volně pohybovat, ale spíše vibrují s nenulovou kinetickou energií. S nejmenší kinetickou energií oscilují ionty uprostřed pasti, tj. ve směru osy z. Aby ionty neunikaly mimo past podél osy z, jsou na koncích osy aplikovány zakončovací elektrody vytvářející elektrostatický potenciál. Ionty jsou v takové konfiguraci uvězněny a vytváří podél osy z malý řetízek. Po takovém zařízení však musíme požadovat, aby nebyly změny kinetické energie způsobené tepelnými fluktuacemi větší, než ty, které vzniknou prováděnými operacemi s ionty. Operace se uskutečňují za použití laseru o vlnové délce $\lambda = 397$ nm. Při emisi nebo absorpci fotonu iont získá nebo ztratí část své hybnosti a jakoby uskočí do určitého směru. Změněná

[15] Což může být v částečném rozporu s bodem 1. Pokud budeme chtít například faktorizovat dlouhé celé číslo nebo hledat v nesetříděném seznamu, pak je zapotřebí tyto data (nebo alespoň část z nich) načíst do „paměti“, aby bylo možné využívat efektů superpozice a interference.



Obrázek 11: **Iontová past:** Aparatura se skládá ze čtyř podélných elektrod uvězňujících ionty ve směrech x a y a dvou menších, které znemožňují iontům pohyb mimo aparaturu v ose z.

energie se proto označuje jako *energie zpětného rázu (recoil energy)*. Tato energie je rovna jen asi $2 \cdot 10^{-29}$ J, a proto je nutné zachovat tepelnou energii na nižších hodnotách v dostatečném relativním odstupu. Toho je možné dosáhnout tak, že systém laserově ochladíme až na pouhých 10^{-3} K. Chlazení laserem se může jevit poněkud paradoxně: když chceme systému energii odebrat, přece jej nebudeme ostřelovat laserem. Musíme si ale uvědomit, že energie není všechno, co se počítá. Rozhodující faktor při chlazení představuje hybnost. Jde o to, že pokud fotony zasáhnou ionty proti jejich směru pohybu, je výsledek srážky zpomalení pohybu iontů. V takovém případě přichází na řadu efekty rezonance (kde se mísí frekvence laseru s frekvencí oscilací elektronového oblaku v atomu) a Dopplerova posunu (který způsobuje posun frekvence ve chvíli, kdy se k nám iont přibližuje). Proto je zapotřebí důkladně nastavit vlnovou délku laseru, aby byl proces chlazení účinný. Ionty pak ještě musí být druhou fází ochlazeny (Ramanovo chlazení) na nejnižší energetickou úroveň oscilací, aby se tak ocitly v základním oscilačním módu odpovídajícím stavu $|0\rangle$.

Nyní máme několik iontů připraveno k provádění operací. Pro jednoduchost uvažujme, že počet uvězněných iontů odpovídá šířce kvantového registru (jeden iont = jeden qubit). Uvězněných iontů mohou být maximálně desítky (dnes se hovoří o tom, že budoucí vylepšení mohou uvěznit kolem stovky iontů). Protože jsou od sebe ionty vzdáleny asi 20 μm (vzdálenost je určena frekvencí slabě oscilujících ($f \approx 200$ MHz) uvězněných iontů podél osy z), lze je světlem kolem 1 mikronu zaměřit. Za cíl si můžeme klást, že chceme jednak ovlivňovat jednotlivé qubity a jednak provést operaci ***CNOT*** mezi libovolnými dvěma qubity. Operace se provádí zaměřením laseru na iont, který koherentně změní stav iontu. Pro změnu stavu na jednom qubitu se používají tzv. *V-pulzy*; pro změnu stavu qubitu a oscilačního módu iontů se používá *U-pulz*. Pro oba typy pulzů existují příslušné Hamiltoniány:

$$\boldsymbol{H}_V = \frac{\hbar\Omega}{2}(e^{-i\phi}|1\rangle\langle 0| + e^{i\phi}|0\rangle\langle 1|), \qquad \boldsymbol{H}_U = \frac{\hbar\eta\Omega}{2\sqrt{L}}(e^{-i\phi}|1\rangle\langle 0|\boldsymbol{a} + e^{i\phi}|0\rangle\langle 1|\boldsymbol{a}^\dagger),$$

kde Ω je Rabiho frekvence (související s intenzitou laseru), ϕ fáze laserového světla, η je Lamb-Dickeův parametr určující míru interakcí mezi laserem a oscilacemi iontů), L je počet iontů a $\boldsymbol{a}$ je anihilační operátor, pro který platí, že $\boldsymbol{a}|g\rangle = 0$, $\boldsymbol{a}^\dagger|g\rangle = |e\rangle$, kde $|g\rangle$ a $|e\rangle$ jsou základní respektive první excitovaný vibrační mód iontů uvězněných v pasti. Tyto stavy oscilátoru vlastně tvoří speciální qubit sloužící k provádění logických operací nad zvolenými qubity. Aby bylo možné operaci provést, musíme být schopni provádět s ionty podmíněné operace (které jsou zapotřebí například u operace $\boldsymbol{CNOT}$). To lze udělat tak, že pro určité vlnové délky laseru iont foton nevyzáří a pro jiné ano. Za druhé je zapotřebí ovládat vibrační módy $|g\rangle$ a $|e\rangle$ řetězce uvězněných iontů a ovlivňovat tak stavy i na větší vzdálenost.

Unitární operace pro m-tý qubit plynoucí ze zmíněných Hamiltoniánů jsou tyto:

$$\begin{aligned}
\boldsymbol{V}_m(\theta,\phi):\quad & |0\rangle_m \to \cos\theta/2\ |0\rangle_m - e^{i\phi}\ \sin\theta/2\ |1\rangle_m \\
& |1\rangle_m \to \cos\theta/2\ |1\rangle_m - e^{-i\phi}\sin\theta/2\ |0\rangle_m \\[1em]
\boldsymbol{U}_m(\theta,\phi):\quad & |0\rangle_m|e\rangle \to \cos\theta/2\ |0\rangle_m|e\rangle - e^{i\phi}\ \sin\theta/2\ |1\rangle_m|g\rangle \\
& |1\rangle_m|g\rangle \to \cos\theta/2\ |1\rangle_m|g\rangle - e^{-i\phi}\sin\theta/2\ |0\rangle_m|e\rangle,
\end{aligned}$$

kde θ je parametr doby působení laseru a ϕ je jeho fáze. Aby bylo možné uskutečnit nějakou logickou operaci, je zapotřebí definovat ještě jednu pomocnou hladinu (kromě $|0\rangle$ a $|1\rangle$) ve stavech qubitů $|pom\rangle$ a vytvořit tak ještě jeden typ U-pulzu. Nový Hamiltonián se pak podobá $\boldsymbol{H}_U$, kromě náhrady $|pom\rangle$ za $|1\rangle$. Unitární operaci $\boldsymbol{U}^{pom}(\theta,\phi)$ Hamiltoniánu $\boldsymbol{H}_U^{pom}$ použijeme k definici operace kontrolovaného prohození znaménka (controlled-sign-flip – CSF). $\boldsymbol{CSF}$ zachovává pro dvojici qubitů stejná znaménka kromě případu $|1\rangle_c|1\rangle_t \to -|1\rangle_c|1\rangle_t$, kde c a t jsou indexy dvou qubitů. Jestliže

$$\boldsymbol{CSF}_{ct} = \boldsymbol{U}_c(\pi,0)\,\boldsymbol{U}_t^{pom}(2\pi,0)\,\boldsymbol{U}_c(\pi,0),$$

pak lze definovat i operaci

$$\boldsymbol{CNOT}_{ct} = \boldsymbol{V}_t(\pi/2,\pi/2)\,\boldsymbol{CSF}_{ct}\,\boldsymbol{V}_t(\pi/2,\pi/2).$$

Pokud se operace zdaří, je zapotřebí výsledný qubit přečíst. To se provádí tak, že mu laserem dodáme energii, která způsobí přechod mezi $|0\rangle$ stavem a vyšším vybuzeným stavem, který není stabilní a rychle se vrací na $|0\rangle$. Pokud byla hodnota qubitu právě $|0\rangle$, pak iont vyzáří příslušný foton, kdežto qubit ve stavu $|1\rangle$ zůstane temný.

Je zřejmé, že technologie iontových pastí má i své slabiny a limity:
- počet iontů je omezen asi na stovce,
- technika pokusu je velmi náročná (vakuum, chlazení, ovládání laserem),
- dekoherující ionty nelze vracet do koherentního stavu.

8.2 NMR

Zcela jiným přístupem k problematice konstrukce kvantového procesoru je technologie, která používá nukleární magnetickou rezonanci – NMR. U uvězněných iontů jsme ovlivňovali pokaždé jen jeden qubit a měřili jeho vlastní stav. NMR místo toho využívá velkého počtu jedno-molekulových kvantových počítačů, jejichž měřením obdržíme střední hodnotu výsledku. Tyto molekuly tvoří kapalinu, která je uzavřena v nádobě obsahující asi 10^{22} molekul. U systémů podobných uvězněným iontům jsou tradiční problémy s dobou dekoherence. Naproti tomu u NMR je dekoherenční čas velký. To proto, že NMR používá ke kódování qubitů spinové stavy jader atomů, které jsou elektronovým mrakem dobře od okolí izolovány a samotné jádro zabírá v porovnání s celým atomem minimální objem. Každé jádro navíc tvoří určitý magnetický dipól a chová se tak jako malý magnet. Pokud na kapalinu aplikujeme vnější magnetické pole, nastaví se spiny ve dvou možných směrech: paralelním nebo anti-paralelním vzhledem k orientaci pole. To odpovídá hodnotám qubitu $|0\rangle$ a $|1\rangle$. Paralelní spin má přitom nižší energii než spin anti-paralelní o hodnotu, která je úměrná síle magnetického pole. V běžné kapalině jsou oba typy spinů zastoupeny stejně; pod vlivem magnetického pole jsou upřednostněny paralelní směry s nižší energií. Pokud k vnějšímu poli přidáme působení pomocí elektromagnetického pole s radiovými frekvencemi, pak je možné stavy spinů jemně upravovat a vytvářet tak superpozice stavů. Pokud například vystavíme proton externímu poli kolem 10 Tesla, pak oscilacemi 400 MHz můžeme podle délky pulzu buď vytvořit superpozici nebo úplně otočit směr spinu qubitu. Jakmile je částice v elektromagnetickém poli, podléhá směr spinu precesi a osciluje s charakteristickou frekvencí. Přitom vysílá rádiové vlny, které aparatura NMR detekuje.

Aby bylo možné qubity vhodně ovlivňovat, je však nejprve zapotřebí zjistit složení vzorku kapaliny. K tomu se používá efektu zvaného *chemický posun*, který u NMR jemně posouvá rezonanční frekvence v závislosti na konkrétním složení vzorku kapaliny v důsledku interakcí lokálních elektronových a externích magnetických polí. Protože nikdo není schopen ovlivňovat ani měřit stavy jednotlivých jader, je zapotřebí měřit průměrný spinový stav v celém objemu kapaliny. Do tohoto průměrného stavu vlastně kódujeme jednotlivé qubity, jejichž stavy ovládáme externími poli na makroskopických rozměrech nádoby s kapalinou. Různé spinové stavy vyvolávají po odečtu pomocí NMR různá NMR-spektra, která prozrazují stav qubitů. Abychom mohli provádět logické operace zahrnující více qubitů, je zapotřebí měnit energie atomů tak, aby v molekulách docházelo k tzv. *spinovým vazbám (spin-spin coupling)*, které umožňují ovlivňovat sousední atomy a tím implementovat například operaci ***CNOT***. Relativně snazší realizace technologie NMR je vykoupena několika značnými omezeními:
- velikost použitelných molekul a tím i složitost možných operací je technologicky omezena,
- technologie je velmi špatně škálovatelná – objem kapaliny roste exponenciálně s větším počtem qubitů (několik desítek qubitů je zřejmě maximum),
- obtížná příprava počátečního stavu

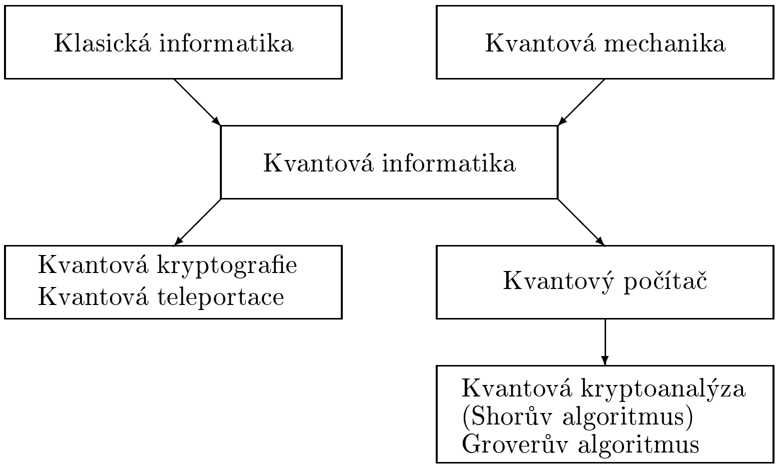
Technologii NMR předvedla skupina Isaaca Chuanga v roce 1996. Ti použili molekuly chloroformu $CHCl_3$. Jejich 2-qubitovému počítači se podařilo provést Groverův vyhledávací algoritmus[16] k nalezení jednoho označeného prvku ze čtyř.

[16] Groverův kvantový algoritmus vyhledává s využitím superpozice v nesetříděném seznamu v čase kolem $\mathcal{O}(\sqrt{n})$. Právě tolik kroků potřebuje algoritmus k tomu, aby se amplitudy pravděpodobností nad superpozicí všech prvků upravily tak, že hledaný prvek má amplitudu pravděpodobnosti blízkou 1 (to znamená, že bude změřen právě tento prvek). Klasicky trvá prohledání seznamu n prvků v průměru $n/2$ kroků, tj. $\mathcal{O}(n)$.

9 Budoucnost kvantových počítačů

V předchozích kapitolách jsme si představili základní elementy, ze kterých by měl být budoucí kvantový počítač sestaven a principy, na nichž by měl být takový počítač založen. Přestože se zdá, že současné technologické problémy zatím nedovolují plně rozvinout potenciál kvantové informatiky, je možné s nadějí prohlásit, že budoucnost kvantových počítačů vypadá slibně. Je vhodné se zde zmínit o konferenci Hot Chips konané v Palo Altu v polovině roku 2000 věnované vývoji v oblasti procesorů. IBM tady představila práci Isaaca Chuanga a jeho skupiny, která od 80.let pracuje v oblasti kvantové informatiky. Na konferenci uvedla jejich 5-qubitový počítač, který pracoval na frekvenci 215 Hz a byl použit pro hledání periody funkce z nám známého Shorova algoritmu. Můžeme se jen domýšlet, jaké principy budou u budoucích kvantových počítačů využity. Nadějně v tomto směru vzhlíží nedávno (2000) objevený efekt tzv. *kvantového přízraku (quantum mirage)*, při němž je na měděné destičce umístěno ve tvaru elipsy 36 atomů kobaltu tvořících tzv. *kvantovou hradbu (quantum corral)*. Tato hradba působí na elektronová mračna v destičce mědi uvnitř elipsy atomů kobaltu. Když byl do jednoho ohniska elipsy umístěn další atom kobaltu, začal interagovat s vlnami elektronů v destičce. Stejně ale elektrony působily na okolí v druhém ohnisku elipsy a vytvářely tam jakousi kopii (přízrak) atomu kobaltu o třetinové intenzitě, přestože tam žádný nebyl předtím umístěn. Není si obtížné přestavit, že tento efekt může mít v principu vliv na přenos informace mezi dvěma místy (například v kvantovém procesoru).

Kvantová informatika však pro některé její aplikace nutně nevyžaduje existenci kvantového počítače. Oblasti kvantové teleportace nebo kvantové kryptografie jsou oddělenými částmi kvantové informatiky, které nejsou přímo závislé na existenci kvantového počítače a které lze realizovat současnými technologiemi. Proto se s některými jejich praktickými realizacemi můžeme setkat již dnes. Tento fakt dokládá i následující schéma, které ukazuje, jakým způsobem jsou jednotlivé teoretické oblasti vzájemně provázány.



Je zřejmé, že uskutečnění vize o prakticky použitelném kvantovém algoritmu je svázáno s existencí kvantového počítače. Jeho konstrukce je zatím za hranicí současného technického rozvoje. Je téměř jisté, že první použitelné kvantové počítače budou úzce zaměřeny pouze na jednu konkrétní aplikaci. Sen o univerzálním kvantovém počítači pracujícím neomezeně dlouho se zdá být v tuto chvíli utopií. Hlavním hlediskem stojícím proti univerzálnosti je jev dekoherence, která časově omezuje použitelnost kvantového počítače při výpočtu. V nejistotě se rovněž nacházíme při pokusu o odhad časového horizontu příchodu aplikace, která by rozhodujícím způsobem ohrozila z dnešního pohledu bezpečná kryptoschémata. Pokud ale vezmeme v úvahu, jakého pokroku dosáhla kvantová informatika za posledních několik let (viz tabulka), vypadá budoucnost poměrně optimisticky.

1982: Richard Feynman – navrhl použití kvantových systémů k výpočtům
1984: Charles Bennett a Gilles Brassard – komunikační protokol BB84
1985: David Deutsch – kvantový Turingův stroj
1994: Peter Shor – faktorizační algoritmus
1995: poslána zpráva kvantovým kanálem
1996: Lov Grover – vyhledávací algoritmus
1996: Peter Shor a Andrew Steane – kvantová oprava chyb možná
1997: uskutečněna kvantová teleportace
1999: Richard Huges – iontové pasti s desítkami qubitů
2000: v Los Alamos byl vytvořen 7-qubitový NMR počítač
2000: společnost IBM ohlásila vytvoření 5-qubitového NMR počítače

Vidíme, že v poslední době se zájem ubírá k implementaci kvantových systémů pomocí metody NMR, která se zdá být z technologického hlediska schůdnější než jiné techniky. V tomto smyslu se nedávají velké naděje implementaci pomocí iontových pastí.

V kvantové informatice se dnes také setkáváme s různými kombinacemi a vylepšeními základních návrhů, o nichž byla řeč. Například klasická kryptografie veřejného klíče je existencí Shorova faktorizačního algoritmu jistě ohrožena. Již dnes se ale v rámci kvantové kryptografie veřejného klíče hledají vhodní kandidáti pro kvantově-jednosměrné funkce se zadními vrátky (které jsou jedním směrem klasicky schůdné, kdežto opačným nikoliv), které by nebyly silou kvantových počítačů napadnutelné. Je zřejmé, že problém nalezení takové funkce (a ověření, že se opravdu jedná o požadovanou funkci) je sám o sobě obtížný. Vylepšení se rovněž dočkal komunikační protokol BB84 v podobě verze B92 a později L99 (který vymyslel Hoi-Kwong Lo), z nichž druhý však vyžaduje, aby měly obě komunikační strany kvantový počítač.

Zajímavou oblastí ke studiu je také otázka využití kvantových počítačů k simulaci kvantových systémů, případně k ověřování fyzikálních teorií. Například simulace současných teorií sjednocujících fyzikální interakce by mohla vést k pozoruhodným závěrům. V případě platnosti teorie a její neefektivní simulace kvantovým počítačem by se jako závěr nabízela otázka, zda je kvantový počítač opravdovou hranicí výpočetních možností v přírodě nebo ne. Zatím na tyto a podobné otázky nedovedeme s jistotou odpovědět, ale máme dnes jistě dobrou naději, že se tak v budoucnu, s existencí kvantových počítačů a trochou štěstí, stane.

10 Reference

V současné době vychází k problematice poměrně mnoho knih a toto odvětví zažívá značný rozmach. Jako nejpohotovější zdroj informací je bezpochyby elektronické nakladatelství (e-print) v Los Alamos National Laboratory na adrese `http://xxx.lanl.gov/archive/quant-ph` označované jako `arXiv`.

- Aharonov, Dorit. Quantum Computation, 1998.
  → `arXiv:quant-ph/9812038`
- Barenco, Adriano. A Universal Two-Bit Gate for Quantum Computation, 1995.
  → `arXiv:quant-ph/9505016`
- Barenco, Adriano a kol. Elementary Gates For Quantum Computation, Physical Review Letters, 1995.
- Bennett, Charles a kol. Teleporting an Unknown Quantum State via Dual Classical and EPR Channels, Physical Review Letters, 1992.
- Breinigm, Marianne. Quantum Mechanics, 2000.
  → `http://electron6.phys.utk.edu/qm1`
- Bužek, Vladimír. Quantum Information And Computation.
  → `http://quantum.savba.sk/buzek/qo1.html`
- Carter, John. A Brief Overview of Quantum Computing, 1999.
- Cohen, W. David. An introduction to Hilbert space and quantum logic, Springer-Verlag, 1989.
- DiVincenzo, David a Shor, Peter. Fault-Tolerant Error Correction with Efficient Quantum Codes, 1996.
- D'helon, Cassius. Quantum-Limited Measurement On Trapped Laser-Cooled Ions, 1997.
  → `http://www51.gu.edu.au/staff/dhelon/thesis/thesis.html`
- Gruska, Josef. Quantum Computing, McGraw-Hill Publishing Company, 1999.
- Hirvensalo, Mika. Quantum Error Correction, Turku Centre for CS, 1998.
- Hughes, Richard. Cryptography, Quantum Computation and Trapped Ions, Los Alamos National Lab, 1997.
- Chuang, Isaac a kol. Quantum Computers, Factoring and Decoherence, 1995.
- IBM, Almaden Research Center, News Releases.
  → `http://www.almaden.ibm.com`
- IEEE, Computer 9/1997, Volume 30, Number 9.
- Jozsa, Richard a kol. Quantum Algorithms and the Fourier Transform, 1997.
  → `arXiv:quant-ph/9707033`
- Klíma, Vlastimil a Rosa, Tomáš. Testy a zdroje neurčitosti v počítači: Rukavice hozená hackerům, CHIP 5/2000 (str. 50–53), 2000.
  → `http://www.decros.cz/security_division/crypto_research/archiv.htm`
- Menezes, J. Alfred a kol. Handbook of Applied Cryptography, 1999.
  → `http://cacr.math.uwaterloo.ca/hac`
- Meglicki, Zdzisław. Introduction to Quantum Computing, 2000
  → `http://ovpit.ucs.indiana.edu/gustav/B679/B679.html`

- Ömer, Bernhard. Quantum Programming in QCL, 2000.
  → http://tph.tuwien.ac.at/~oemer/doc/quprog/quprog.html
- Preskill, John. Quantum information and quantum computation, Caltech, 1996.
- Preskill, John. Courses of Quantum Informatics, Caltech.
  → http://www.theory.caltech.edu/people/preskill/ph229
- Rosa, Tomáš. Faktorizace velkých čísel pomocí Twinkle: Na to vezmi LED!, CHIP 8/1999 (str. 40–43), 1999.
  → http://www.decros.cz/security_division/crypto_research/archiv.htm
- Shor, Peter. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, 1995.
  → arXiv:quant-ph/9508027.
- Spencer, J. William a Seitz, L. Charles. Engines of Progress: Semiconductor Technology Trends and Issues, 1996.
  → http://www.nap.edu/readingroom/books/decade/ch4.html
- Steane, Andrew. Quantum Computing, 1997.
  → arXiv:quant-ph/9708022
- Toffoli, Tom. Quantum Computation Archive.
  → http://pks.bu.edu/qcl.
- Williams, Colin a Clearwater, Scott. Explorations in Quantum Computing, Springer-Verlag New York, 1998.