

Ústav aplikovanej informatiky
Fakulta informatiky a informačných technológií
Slovenská technická univerzita v Bratislave

Kvantové počítanie

(predbežný učebný text k prednáške)

Vladimír Kvasnička



November 2011

Úvod

Tieto prednášky z kvantového počítania začali vznikať niekedy na prelome tisícročí, keď som začal prednášať poslucháčom inžinierskeho štúdia “fyzikálnej chémie” na Fakulte chemickej a potravinárskej technológie našej školy STU lineárnu algebru so zameraním na kvantovú mechaniku. Po vytvorení FIIT STU som prešiel pracovať na túto novú fakultu, kde spontánne vznikla neformálna skupina pedagógov a doktorandov so záujmom o kvantové počítanie. Začali sme sa stretávať na bývalej Katedre matematiky FChPT STU, kde som mal prednášky z kvantového počítania, tieto poznámky slúžili ako podklad k týmto poznámkam. Neskôr som s prekvapením zistil, že sa im dostalo tej cti a že boli milou kolegyňou a prodekanou Majou Bielikovou zaradené do zoznamu výberových prednášok pre doktorandov našej fakulty. Touto inštitucionalizáciou mojej neformálnej prednášky z kvantového počítania bol som „vyzvaný“ zosumarizovať poznámky k prednáške ako predbežný študijný materiál a vytvoril som tiež web stránku k prednáške na adrese

<http://www2.fiit.stuba.sk/~kvasnicka/QuantumComputing/index.html>

kde sú uvedené jednotlivé prednášky aj so študijnými materiálmi a organizačné pokyny k prednáške. Na tejto stránke je možné „downloadovať“ rôzne študijné materiály, ale súč poučený jednou bláznivou vysokoškolskou pedagogičkou z Českej republiky, zahesloval som tieto prístupy. Študenti – doktorandi sa môžu na mňa s dôverou obrátiť, obratom im poskytnem login a password.

V Bratislave, dňa 9. 11. 2011

Vlado Kvasnička

Obsah

1. prednáška

Lineárna algebra I - pole skalárov, lineárny priestor, lineárna závislosť, dimenzia, podpriestor, suma podpriestorov, izomorfizmus

2. prednáška

Lineárna algebra II – skalárny súčin, norma, metrika, ortogonálnosť, ortonormálnosť, ortogonálny doplnok, lineárne operátory, maticová reprezentácia, hodnosť a defekt operátorov

3. prednáška

Lineárna algebra III – *hermitovsky združený operátor, hermitovský operátor, unitárny operátor, vlastné vektory a vlastné hodnoty operátora, tenzorový súčin, projekčné operátory*

4. prednáška

Lineárna algebra IV – Diracov formalizmus lineárnej algebry, bra a ket vektory, diadický súčin a skalárny súčin, spektrálny rozvoj operátora, funkcia operátora

5. prednáška

Kvantová mechanika I – stavy kvantového systému, experimenty s polarizovanými fotónmi, pozorovateľnosť, úplnosť vlastného systému pozorovateľnej, princíp superpozície, meranie

6. prednáška

Kvantová mechanika II – časový vývoj kvantových systémov, entaglované kvantové stavy

7. prednáška

Kvantové počítanie I – reverzibilné brány, Toffoliho brána a Fredkinova brána

8. prednáška

Kvantové počítanie II – výpočty pomocou biliardových gúl, model celulárnych automatov

9. prednáška

Kvantové počítanie III – kvantové brány

10. prednáška

Feynmanov kvantový počítač

11. prednáška

Kvantové algoritmy I – Deutschov a Jozsov algoritmus a Simonov algoritmus

12. prednáška

Kvantové algoritmy II – Groverov algoritmus prehľadovania

13. prednáška

Kvantové algoritmy III – Shorov algoritmus

1. prednáška

Lineárna algebra I - pole skalárov, lineárny priestor, lineárna závislosť, dimenzia, podpriestor, suma podpriestorov, izomorfizmus

Matematickým základom kvantovej mechaniky je teória Hilbertových priestorov, ktorá však pre potreby kvantového počítania môže byť prezentovaná v zjednodušenej podobe konečnorozmerného lineárneho priestoru so skalárnym súčinom. V tejto prednáške naformulujeme základy teórie konečnorozmerných lineárnych priestorov nad komplexnými číslami.

1.1 Pole skalárov

Prv než pristúpime k formulácii pojmu lineárny priestor, musíme si presne špecifikovať pojem „skalár“ a „pole skalárov“. Pod skalárom budeme rozumieť ľubovoľné (1) racionálne číslo, (2) iracionálne číslo, alebo (3) komplexné číslo. Nech $\mathcal{C} = \{a, b, c, \dots\}$ je množina skalárov, ktoré vyhovujú trom sadám axiém:

A. Ku každej dvojici $a, b \in \mathcal{C}$ je priradený skalár $a + b \in \mathcal{C}$ nazývaný *súčet*, pričom

- (1) $a + b = b + a$ (komutatívny zákon),
- (2) $a + (b + c) = (a + b) + c$ (asociatívny zákon)
- (3) existuje $0 \in \mathcal{C}$ (nula), pričom $a + 0 = a$,
- (4) ku každému $a \in \mathcal{C}$ existuje skalár $(-a) \in \mathcal{C}$ taký, že $a + (-a) = 0$.

B. Ku každej dvojici $a, b \in \mathcal{C}$ je priradený skalár $a \cdot b \in \mathcal{C}$ nazývaný *súčin*, pričom

- (1) $a \cdot b = b \cdot a$ (komutatívny zákon),
- (2) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (asociatívny zákon),
- (3) existuje $1 \in \mathcal{C}$ (jednotka, pričom $a \cdot 1 = a$,
- (4) ku každému skaláru $a \neq 0$ existuje skalár $a^{-1} \in \mathcal{C}$ taký, že $a \cdot a^{-1} = 1$.

C. Súčin je distributívny vzhľadom k súčtu

- (1) $a \cdot (b + c) = a \cdot b + a \cdot c$

Definícia 1.1. Množinou skalárov $\mathcal{C}$ nazýva **pole skalárov** (alebo jednoducho len **pole**) vtedy a len vtedy, ak nad touto množinou sú definované dve binárne operácie súčtu a súčinu, pričom sú splnené sady axiém A – C.

Ďalšie vlastnosti skalárov z pola $\mathcal{C}$ a ilustračné príklady sú uvedené v príkladoch 1.2-4.

1.2 Lineárny priestor

Predpokladajme, že máme definované pole skalárov $\mathcal{C}$. Nech $H = \{\alpha, \beta, \dots, \varphi, \psi, \dots\}$ je množina vektorov. Nech elementy – vektory tejto množiny vyhovujú týmto trom sadám axiém:

A. Ku každej dvojici $\alpha, \beta \in H$ je priradený vektor $\alpha + \beta \in H$ nazývaný *súčet*, pričom

- (1) $\alpha + \beta = \beta + \alpha$ (komutatívny zákon),
- (2) $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ (asociatívny zákon)
- (3) existuje nulový vektor $o \in H$ (nula), pričom $\alpha + o = \alpha$,
- (5) ku každému $\alpha \in H$ existuje vektor $(-\alpha) \in H$ taký, že $\alpha + (-\alpha) = o$.

B. Ku každej dvojici $a \in \mathcal{C}$ a $\alpha \in H$ je priradený vektor $a\alpha \in H$, ktorý sa nazýva *súčin skalára a vektorom*, pričom

- (1) $a(b\alpha) = (ab)\alpha$ (asociatívny zákon),
- (2) $1\alpha = \alpha$, kde $1 \in \mathcal{C}$ je skalárna jednotka.

C. Distributívne zákony pre súčin skalár a vektor

- (1) $(a + b)\alpha = a\alpha + b\alpha$,
- (2) $a(\alpha + \beta) = a\alpha + a\beta$.

Definícia 1.2. Množinou vektorov H spolu s polom skalárov $\mathcal{C}$ sa nazýva **lineárny priestor nad polom skalárov** (alebo **vektorový priestor nad polom skalárov**) vtedy a len vtedy, ak nad množinou H a polom $\mathcal{C}$ sú definované dve binárne operácie súčtu a súčinu, pričom sú splnené sady axiém A – C.

Ďalšie vlastnosti vektorov z lineárneho priestoru H a ilustračný príklad jeho nožnej realizácie sú ukázané v príkladoch 1.5 a 1.6.

1.3 Lineárna závislosť

Nech množina $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ obsahuje n vektorov a množina $\mathcal{B} = \{b_1, b_2, \dots, b_n\} \subset \mathcal{C}$ obsahuje n skalárov, potom výraz

$$b_1\beta_1 + b_2\beta_2 + \dots + b_n\beta_n \quad (1.1)$$

sa nazýva **lineárna kombinácia** vektorov $\beta_1, \beta_2, \dots, \beta_n \in H$ s koeficientmi a $b_1, b_2, \dots, b_n \in \mathcal{C}$.

Definícia 1.3. Hovoríme, že množina vektorov $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ je **lineárne nezávislá** vtedy a len vtedy, ak jej lineárna kombinácia sa rovná nulovému vektoru

$$b_1\beta_1 + b_2\beta_2 + \dots + b_n\beta_n = o \quad (1.2)$$

len pre nulové koeficienty $b_1 = b_2 = \dots = b_n = o$.

Jednoduchou negáciou tejto definície dostaneme pojem **lineárnej závislosti**, potom lineárna kombinácia je nulová, $b_1\beta_1 + b_2\beta_2 + \dots + b_n\beta_n = o$, pre nenulové koeficienty. Pre jednoduchosť

predpokladajme, že týmto nenulovým koeficientom je $b_1 \neq 0$, potom z (1.2) dostaneme špecifikáciu vektora β_1 ako lineárnej kombinácie ostatných vektorov

$$\beta_1 = -\frac{b_2}{b_1}\beta_2 - \dots - \frac{b_n}{b_1}\beta_n \quad (1.3)$$

Veta 1.1. Nech $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ je množina lineárne nezávislých vektorov, potom vektor φ je určený *jednoznačne* pomocou lineárnej kombinácie vektorov z B

$$\varphi = b_1\beta_1 + b_2\beta_2 + \dots + b_n\beta_n$$

Dôkaz tejto vety je vykonaný v príklade 1.7.

Definícia 1.4.

(1) Hovoríme, že lineárny priestor H je ***n-rozmerný*** vtedy a len vtedy, ak v ňom existuje maximálne práve n lineárne nezávislých vektorov, čo zapisujeme $\dim(H) = n$.

(2) Hovoríme, že množina n vektorov $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ tvorí ***bázu*** n -rozmerného priestoru H vtedy a len vtedy, ak sú tieto vektory lineárne nezávislé, čo zapisujeme $\text{báza}(H) = \{\beta_1, \beta_2, \dots, \beta_n\}$.

Veta 1.2. V n -rozmernom priestore H s bázou $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$, každý vektor φ je určený *jednoznačne* ako lineárna kombinácia vektorov báze

$$\varphi = b_1\beta_1 + b_2\beta_2 + \dots + b_n\beta_n$$

Koeficienty $b_1, b_2, \dots, b_n$ nazývame ***súradnice*** vektora φ v báze B .

Dôkaz tejto vety je uskutočnený v príklade 1.8.

1.4 Podpriestor

Nech $H' \subseteq H$ je podmnožina lineárneho priestoru H nad polom skalárov $\mathcal{C}$.

Definícia 1.5. Hovoríme, že podmnožina $H' \subseteq H$ je ***lineárny podpriestor*** (vzhľadom k lineárnemu priestoru H) vtedy a len vtedy, ak H' je lineárny priestor nad polom skalárov $\mathcal{C}$, pričom binárne operácie súčtu a súčinu sú rovnaké ako v pôvodnom priestore H .

Dimenzia podpriestoru H' je určená vzťahom (dôkaz je uvedený v príklade 1.9)

$$\dim(H') \leq \dim(H) \quad (1.4)$$

rovnosť platí len vtedy, keď $H = H'$. To znamená, že dimenzia priestoru patrí medzi najdôležitejšie charakteristiky lineárnych priestorov. Táto skutočnosť bude ešte potvrdená v ďalšej časti tejto kapitoly (pozri kapitolu 1.X), keď budeme špecifikovať izomorfizmus (niečo ako rovnocennosť alebo podobnosť) medzi lineárnymi priestormi. Bude ukázané, že ak dva priestory majú rovnakú dimenziu, potom sú aj izomorfné.

Najjednoduchšia špecifikácia podpriestoru je pomocou množiny vektorov. Nech $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ je množina n vektorov (nepredpokladáme, že sú lineárne nezávislé, potom podpriestor $H' \subseteq H$ môže byť špecifikovaný tak, že obsahuje všetky možné lineárne kombinácie vektorov z B (dôkaz tohto tvrdenia je uvedený v príklade 1.10)

$$H' = \{b_1\beta_1 + b_2\beta_2 + \dots + b_n\beta_n; b_1, b_2, \dots, b_n \in \mathcal{C}\} \quad (1.5)$$

Hovoríme, že podpriestor H' je **lineárny obal** vektorov z $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$

$$H' = \text{span}(B) \quad (1.6)$$

Pre dimenziu podpriestora H' platí (dôkaz je uvedený v príklade 1.11)

$$\dim(H') \leq n \quad (1.7)$$

kde rovnosť platí vtedy a len vtedy, ak množina $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ obsahuje len lineárne nezávislé vektory.

Nech $H_1, H_2 \subseteq H$ sú dva podpriestory priestoru H , suma týchto podpriestorov, označená $H_1 + H_2$, je množina, ktorá obsahuje všetky lineárne kombinácie vektorov z H_1 a H_2

$$H_1 + H_2 = \{a\alpha + b\beta; a, b \in \mathcal{C}; \alpha \in H_1; \beta \in H_2\} \quad (1.8)$$

Veta 1.3. Množina $H_1 + H_2$ je lineárnym priestorom, t. j. podpriestorom H .

Dôkaz tejto vety je uskutočnený v príklade 1.12.

Nech podpriestory H_1, H_2 majú spoločný prienik tvorený len nulovým vektorom

$$H_1 \cap H_2 = \{o\} \quad (1.9a)$$

Potom suma týchto podpriestorov prechádza na **priamu sumu**

$$H_1 \oplus H_2 = H_1 + H_2 \quad (H_1 \cap H_2 = \{o\}) \quad (1.9b)$$

Veta 1.4. Každý vektor $z \in H_1 \oplus H_2$ je vyjadrený jednoznačne suma dvoch vektorov

$$z = x_1 + x_2$$

kde $x_1 \in H_1$ a $x_2 \in H_2$.

Dôkaz tejto vety je uskutočnený v príklade 1.12.

Veta 1.5. Dimenzia priamej sumy podpriestorov je určená sumou dimenzií jednotlivých podpriestorov

$$\dim(H_1 \oplus H_2) = \dim(H_1) + \dim(H_2)$$

Táto veta je dokázaná v príklade 1.13.

1.5 Izomorfizmus

Dva lineárne priestory H a G sú izomorfné vtedy, ak existuje také zobrazenie H na G , ktoré zachováva súčet a súčin vektorov. Dva izomorfné priestory sú „skoro identické“, ich matematické vlastnosti sú „skoro“ totožné, odlišujú sa len v realizácii vektorov.

Definícia 1.6. Lineárne priestory H a G sa nazývajú izomorfné ($H \sim G$) vtedy a len vtedy, ak existuje také 1-1 značné zobrazenie $f: H \rightarrow G$, ktoré zachováva lineárnu kombináciu vektorov

$$f(a_1\alpha_1 + a_2\alpha_2) = a_1f(\alpha_1) + a_2f(\alpha_2) \quad (1.10)$$

Veta 1.6. Lineárne priestory H a G sú izomorfné vtedy a len vtedy, ak majú rovnakú dimenziu
 $H \sim G \Leftrightarrow \dim(H) = \dim(G)$

Veta 1.6. je dokázaná v príklade 1.14.

Ako dôsledok tejto vlastnosti je, že každý lineárny n -rozmerný priestor definovaný nad polom skalárov $\mathcal{C}$, je izomorfný s priestorom $\mathcal{C}^n$, ktorý bol špecifikovaný v príklade 1.6. To znamená, že ilustračné príklady lineárnej algebry, ktoré sú založené na tomto vektorov priestore, nie sú obmedzím všeobecnosti ilustračných príkladov.

Pojem izomorfizmu medzi lineárnymi priestormi je veľmi dôležitý. Ukazuje, že nie je dôležité, akým spôsobom je priestor realizovaný, ale podstatným znakom je ich dimenzia. Všetky vlastnosti špeciálneho priestoru H automaticky platia aj pre ostatné lineárne priestory, ktoré majú rovnakú dimenziu ako H .

Riešenie príkladov

Príklad 1.1. Dokáže pomocou axiém poľa skalárov tieto vlastnosti:

- (1) $0 + a = a$
- (2) $x + a = b \Rightarrow x = b - a$
- (3) $(a + b = a + c) \Rightarrow (b = c)$
- (3) $a + (b - a) = b$
- (4) $a \cdot 0 = 0 \cdot a = 0$
- (5) $(-1)a = (-a)$
- (6) $(-a) \cdot (-b) = a \cdot b$
- (7) $(a \cdot b = 0) \Rightarrow (a = 0) \vee (b = 0)$
- (8) $xa = b \Rightarrow x = a^{-1}b$ (pre $a \neq 0$)
- (9) $ab = ac \Rightarrow b = c$ (pre $a \neq 0$)

Príklad 1.2. Nech $\mathcal{C} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ je množina celých čísel, pričom nad touto množinou sú definované obvyklým spôsobom operácie súčtu a súčinu. Je $\mathcal{C}$ pole skalárov?

Príklad 1.3. Nech $\mathcal{C} = \{p/q\}$ (množina racionálnych čísel, kde p a q sú celé a nesúdeliteľné čísla. Je $\mathcal{C}$ pole skalárov?

Príklad 1.4. Nech $\mathcal{C} = \{0, 1, 2, \dots, x, 1+x, \dots, 1+x+x^2, \dots\}$ je množina všetkých polynómov s celočíselnými koeficientmi, pričom nad polom $\mathcal{C}$ je definovaný súčet a súčin obvyklým spôsobom. Je $\mathcal{C}$ pole skalárov?

Príklad 1.5. Dokáže pomocou axiém lineárneho priestoru tieto vlastnosti:

- (1) $0 + \alpha = \alpha$,
- (2) $(-o) = o$,
- (3) $ao = o$,
- (4) $(-1)\alpha = (-\alpha)$,
- (5) $0\alpha = o$,
- (6) vektorová rovnica $\alpha + \beta = \gamma$, kde α je neznáma, má riešenie $\alpha = \gamma - \beta$,
- (7) $(\alpha + \beta = \alpha + \gamma) \Rightarrow (\beta = \gamma)$
- (7) $(a \cdot \alpha = o) \Rightarrow (a = 0) \vee (\alpha = o)$.

Príklad 1.6. Najznámejším príkladom lineárneho priestoru je množina usporiadaných n -tic komplexných čísel

$$H = \{(z_1, z_2, \dots, z_n); z_1, z_2, \dots, z_n \in \mathcal{C}\} = \underbrace{\mathcal{C} \times \mathcal{C} \times \dots \times \mathcal{C}}_{n\text{-krát}} = \mathcal{C}^n$$

kde $\mathcal{C}$ je pole komplexných čísel. Operácie súčtu a súčinu sú definované obvyklým spôsobom. Nech $\alpha = (a_1, a_2, \dots, a_n)$ a $\beta = (b_1, b_2, \dots, b_n)$, potom

$$\alpha + \beta = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

$$a\alpha = (aa_1, aa_2, \dots, aa_n)$$

$$(-\alpha) = (-a_1, -a_2, \dots, -a_n)$$

$$o = (0, 0, \dots, 0)$$

Dokážte, že takto špecifikovaná množina H vektorov a pole komplexných čísel $\mathcal{C}$ je lineárny priestor, t. j. axiomy lineárneho priestoru sú splnené.

Príklad 1.7. Dokážte vetu 1.1.

Príklad 1.8. Dokážte, že v n -rozmernom priestore H s bázou $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$, každý vektor φ je vyjadrený *jednoznačne* ako lineárna kombinácia vektorov báze

$$\varphi = b_1\beta_1 + b_2\beta_2 + \dots + b_n\beta_n$$

Príklad 1.9. Dokážte vzťah (1.4).

Príklad 1.10. Dokážte, že množina H' (1.5) je lineárnym priestorom.

Príklad 1.11. Dokážte reláciu (1.7).

Príklad 1.12. Dokáže pomocou (1.8a), že rozklad (1.8c) špecifikuje vektor z jednoznačne.

Príklad 1.13. Dokážte rovnosť (1.9).

Príklad 1.14. Dokážte nutnú podmienku (implikácia zľava do prava v (1.11)) izomorfizmu medzi vektormi H a G ,

2. prednáška

Lineárna algebra II – skalárny súčin, norma, metrika, ortogonálnosť, ortonormálnosť, ortogonálny doplnok, lineárne operátory, maticová reprezentácia, hodnosť a defekt operátorov

2.1 Skalárny súčin

Definícia 2.1. Binárna operácia, ktorá dvom vektorom $\alpha, \beta \in H$ priradí skalár $(\alpha, \beta) \in \mathbb{C}$ sa nazýva **skalárny súčin** vtedy a len vtedy, ak platia tieto 4 axiómy:

- (1) $(\alpha, \beta) = (\beta, \alpha)^*$,
- (2) $(\alpha, a\beta) = a(\alpha, \beta)$,
- (3) $(\alpha, \beta_1 + \beta_2) = (\alpha, \beta_1) + (\alpha, \beta_2)$,
- (4) $(\alpha, \alpha) \geq 0$ ($= 0$ len pre $\alpha = o$).

Z axióm 1 a 2 plynie

$$(a\alpha, \beta) = (\beta, a\alpha)^* = a^* (\beta, \alpha)^* = a^* (\alpha, \beta)$$

Podobne, z axióm 1 a 3 dostaneme

$$(\alpha_1 + \alpha_2, \beta) = (\beta, \alpha_1 + \alpha_2)^* = (\beta, \alpha_1)^* + (\beta, \alpha_2)^* = (\alpha_1, \beta) + (\alpha_2, \beta)$$

Skalárny súčin ľubovoľného vektora $\alpha \in H$ s nulovým vektorom o je nula

$$(\alpha, o) = (\alpha, 0\beta) = 0(\alpha, \beta) = 0$$

Ak v lineárnom priestore H je definovaný skalárny súčin, potom H sa nazýva **unitárny priestor**. V tomto bode sa dostávame do kontaktu aj s teóriou Hilbertových priestorov, Hilbertov priestor konečnej dimenzie je totožný s unitárnym priestorom. Prevažná väčšina našich úvah o kvantovom počítaní je založená na konečno-rozmernom Hilbertovom priestore, preto vystačíme s teóriou konečno-rozmerných unitárnych priestorov.

Veta 2.1. Nech H je lineárny priestor realizovaný $\mathbb{C}^n$, potom pre každý vektor $\alpha = (a_1, a_2, \dots, a_n)$, kde $a_i \in \mathbb{C}$. Binárna operácia pre vektory α a $\beta = (b_1, b_2, \dots, b_n)$

$$(\alpha, \beta) = \sum_{i=1}^n a_i^* b_i \quad (2.1)$$

vyhovuje axiómam skalárneho súčinu z definície 2.1.

Dôkaz vety 2.1 je uskutočnený v príklade 2.1.

Pre unitárne priestory je potrebné zovšeobecniť definíciu 1.6 izomorfizmu. Nech H a G sú dva unitárne priestory v ktorých sú definované skalárne súčiny $(\cdot, \cdot)_H$ resp. $(\cdot, \cdot)_G$.

Pôvodná definícia izomorfizmu 1.6 je pre unitárne priestory rozšírená pomocou nasledujúcej definície.

Definícia 2.2. Unitárne priestory H a G sa nazývajú izomorfné ($H \sim G$) vtedy a len vtedy, ak existuje také 1-1 značné zobrazenie $f: H \rightarrow G$, ktoré zachováva lineárnu kombináciu vektorov a skalárny súčin

$$f(a_1\alpha_1 + a_2\alpha_2) = a_1 f(\alpha_1) + a_2 f(\alpha_2) \quad (2.2a)$$

$$(\alpha, \beta)_H = (f(\alpha), f(\beta))_G \quad (2.2b)$$

Pomocou skalárneho súčinu môžeme definovať **normu (dĺžku)** vektora α takto

$$|\alpha| = \sqrt{(\alpha, \alpha)} \quad (2.3)$$

Veta 2.2. Pre normu platí Schwartzova nerovnosť

$$|(\alpha, \beta)| \leq |\alpha| |\beta| \quad (2.4)$$

Veta 2.2 je dokázaná v príklade 2.2. Pomocou normy môžeme definovať aj **vzdialenosť (metriku)** medzi dvoma vektormi α a β

$$d(\alpha, \beta) = |\alpha - \beta| \quad (2.5)$$

Niektoré základné vlastnosti normy a vzdialenosti sú dokázané v príklade 2.3 resp. 2.4.

Definícia 2.3. Vektor $\alpha \in H$ sa nazýva normalizovaný (normovaný) vtedy a len vtedy, ak

$$|\alpha| = 1$$

Definícia 2.4. Dva vektory $\alpha, \beta \in H$ sa nazývajú **ortogonálne** (čo zapisujeme $\alpha \perp \beta$) vtedy a len vtedy, ak ich skalárny súčin je nulový

$$(\alpha \perp \beta) \Leftrightarrow (\alpha, \beta) = 0$$

Relácia ortogonálnosti je symetrická ale nie je tranzitívna. Množina vektorov $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ sa nazýva **ortogonálna**, ak pre každú dvojicu rôznych vektorov z B platí

$$(\beta_i, \beta_j) = 0 \quad (\text{pre } i, j = 1, 2, \dots, n \text{ a } i \neq j) \quad (2.6)$$

Ak množina $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ obsahuje vektory, ktoré sú súčasne normalizované a aj ortogonálne, potom táto množina sa nazýva **ortonormálna**

$$(\beta_i, \beta_j) = \delta_{ij} = \begin{cases} 1 & (\text{ak } i = j) \\ 0 & (\text{ak } i \neq j) \end{cases} \quad (2.7)$$

Veta 2.3. Ak množina $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ obsahuje nenulové ortogonálne vektory, potom tieto vektory sú lineárne nezávislé.

Táto veta je dokázaná v príklade 2.6. Z vlastností dokazovanej v príklade 2.6 vyplýva, že ak priestor H je n -rozmerný, potom existuje maximálne n ortogonálnych nenulových vektorov. V lineárnej algebre existuje konštruktívny dôkaz (nazývaný Schmidtov ortogonalizačný

proces) skutočnosti, že v každom n -rozmernom lineárnom priestore H s definovaným skalárnym súčinom, existuje ortonormálna báza $B_{orthonorm} = \{\tilde{\beta}_1, \tilde{\beta}_2, \dots, \tilde{\beta}_n\} \subset H$.

Nech $B = \{\beta_1, \beta_2, \dots, \beta_n\} \subset H$ je báza n -rozmerného lineárneho priestoru H v ktorom je definovaný skalárny súčin. **Schmidtov ortogonalizačný proces** je špecifikovaný rekuretným spôsobom takto:

1. krok. $\tilde{\beta}_1 = \beta_1$.
2. krok. $\tilde{\beta}_2 = a_1 \tilde{\beta}_1 + \beta_2$, kde koeficient a_1 je určený podmienkou $\tilde{\beta}_1 \perp \tilde{\beta}_2$.
3. krok. $\tilde{\beta}_3 = a_1 \tilde{\beta}_1 + a_2 \tilde{\beta}_2 + \beta_3$, kde koeficienty a_1, a_2 sú určené podmienkami $\tilde{\beta}_3 \perp \tilde{\beta}_1$ a $\tilde{\beta}_3 \perp \tilde{\beta}_2$.

Tento postup opakujeme tak dlho až vyčerpáme všetky vektory z množiny B .

Nech $H_1 \subset H$ je lineárny podpriestor unitárneho priestoru H . Symbol $H_1^\perp$ reprezentuje takú množinu vektorov, nazývanú **ortogonálny doplnok** k podpriestoru H_1 , ktoré sú ortogonálne k vektorom z podpriestora H_1

$$H_1^\perp = \{\alpha \in H; \forall (\beta \in H_1)(\alpha, \beta) = 0\} \quad (2.8)$$

Veta 2.4.

- (1) Ak $H_1 \subset H$ je lineárny podpriestor, potom aj jeho ortogonálny doplnok $H_1^\perp \subset H$ je taktiež lineárny podpriestor.
- (2) Unitárny priestor je možné vyjadriť ako priamu sumu podpriestoru $H_1 \subset H$ a jeho ortogonálneho doplnku $H_1^\perp \subset H$

$$H = H_1 \oplus H_1^\perp \quad (2.9)$$

Pre ortogonálne doplnky unitárneho priestoru H platia tieto vzťahy:

- (1) Nech $H_1 \subset H$ je lineárny podpriestor, potom

$$(H_1^\perp)^\perp = H_1 \quad (2.10a)$$

- (2) Ortogonálny komplement unitárneho priestoru H je

$$H^\perp = \{0\}, \quad \{0\}^\perp = H \quad (2.10b)$$

2.2 Lineárne operátory

Pojem operátora patrí v matematickej teórii kvantovej mechaniky medzi centrálnymi pojmami, každá pozorovateľná (alebo merateľná) veličina je v kvantovej mechanike vyjadrená pomocou operátora – zobrazenia lineárneho priestoru na seba.

Definícia 2.5. Hovoríme, že nad lineárnym priestorom H je definovaný **lineárny operátor**

$$A: H \rightarrow H$$

vtedy a len vtedy, ak pre každé $\alpha \in H$ existuje práve jeden vektor $\beta \in H$ taký, že $\beta = A\alpha$, pričom je splnená podmienka

$$A(a_1 \alpha_1 + a_2 \alpha_2) = a_1 A\alpha_1 + a_2 A\alpha_2$$

Nech v n -rozmernom lineárnom priestore H existuje ortonormálna báza $B = \{\beta_1, \beta_2, \dots, \beta_n\}$, pomocou ktorej zavedieme maticovú reprezentáciu operátora. Pretože $A\beta_i \in H$, potom vektor $A\beta_i$ môžeme vyjadriť pomocou lineárnej kombinácie vektorov ortonormálnej báze

$$A\beta_i = \sum_{j=1}^n A_{ji} \beta_j \quad (2.11a)$$

Ak vynásobíme skalárne túto rovnicu zľava vektorom β_k , po jednoduchých úpravách dostaneme

$$(\beta_k, A\beta_i) = A_{ki} \quad (2.11b)$$

Matica $A = (A_{ij})$ sa nazýva **maticová reprezentácia** operátora A v báze $B = \{\beta_1, \beta_2, \dots, \beta_n\}$, jej maticové elementy sú určené vzťahom (2.11b).

Môžeme si položiť otázku, ako sa zmení maticová reprezentácia operátora A pri prechode od ortonormálnej báze $B = \{\beta_1, \beta_2, \dots, \beta_n\}$ k inej ortonormálnej báze $B' = \{\beta'_1, \beta'_2, \dots, \beta'_n\}$. Pretože H je n -rozmerný unitárny priestor, každý vektor báze $B' = \{\beta'_1, \beta'_2, \dots, \beta'_n\}$ môže byť vyjadrený pomocou lineárnej kombinácie vektorov z pôvodnej bázy $B = \{\beta_1, \beta_2, \dots, \beta_n\}$

$$\beta'_i = \sum_{j=1}^n T_{ji} \beta_j \quad (2.12a)$$

Pretože matica $T = (T_{ij})$ popisuje prechod od pôvodnej ortonormálnej báze k novej ortonormálnej báze, musí byť regulárna, t. j. existuje inverzná matica T^{-1} , ktorá vyhovuje podmienkam $T^{-1}T = TT^{-1} = E$. Potom platí aj „inverzná“ formula k (1.23a)

$$\beta_i = \sum_{j=1}^n T_{ji}^{-1} \beta'_j \quad (2.12b)$$

Nech maticová reprezentácia operátora A v bázy $B' = \{\beta'_1, \beta'_2, \dots, \beta'_n\}$ má tvar

$$A\beta'_i = \sum_{j=1}^n B_{ji} \beta'_j \quad (2.13a)$$

kde maticové elementy reprezentácie sú určené formulou

$$(\beta'_k, A\beta'_i) = B_{ki} \quad (2.14b)$$

Jednoduchými úvahami je možné dokázať, že medzi týmito dvoma maticovými reprezentáciami operátora A existuje vzťah vyjadrení pomocou transformácie podobnosti

$$B_{ij} = \sum_{k,l=1}^n T_{ik}^{-1} A_{kl} T_{lj} \quad (2.15a)$$

alebo pomocou matic

$$B = T^{-1}AT \quad (2.15b)$$

Pomocou maticovej reprezentácie operátorov zavedieme definície stopy a determinantu operátora A . Pripomeňme, že tieto veličiny sú definované v algebre len pre štvorcové matice, ich maticová reprezentácia umožňuje ich definíciu aj pre operátory, aby táto definícia mala zmysel, musíme ukázať, že tak stopa, ako aj determinant sú nezávislé od ich maticovej reprezentácie.

Nech lineárny operátor A v báze $B = \{\beta_1, \beta_2, \dots, \beta_n\}$ je reprezentovaná maticou $A = (A_{ij})$, potom stopa operátora A je definovaná pomocou stopy matice A

$$\text{Tr}(A) = \text{Tr}(A) = \sum_{i=1}^n A_{ii} \quad (2.16)$$

Stopa súčinu dvoch štvorcových je nezávislá od ich poradia

$$\text{Tr}(AB) = \text{Tr}(BA) \quad (2.17)$$

Predpokladajme, že maticová reprezentácia operátora A pri prechode z pôvodnej báze $B = \{\beta_1, \beta_2, \dots, \beta_n\}$ do novej báze $B' = \{\beta'_1, \beta'_2, \dots, \beta'_n\}$ sa zmení podľa formuly transformácie podobnosti (2.15b), jej stopa je

$$\text{Tr}(B) = \text{Tr}(T^{-1}AT) = \text{Tr}\left(\underbrace{TT^{-1}}_E A\right) = \text{Tr}(A) \quad (2.18)$$

Týmto sme dokázali, že stopa maticovej reprezentácie operátora je nezávislá od zvolenej báze, pre každú bázu dostaneme rovnakú stopu maticovej reprezentácie daného operátora A .

Podobným spôsobom pomocou maticovej reprezentácie môžeme definovať aj determinant operátora A

$$\det(A) = \det(A) \quad (2.19)$$

Determinat súčinu dvoch matic sa rovná súčinu ich determinantov

$$\det(AB) = \det(A)\det(B) \quad (2.20)$$

Pomocou tejto vlastnosti determinantov taktiež dokážeme, že determinanty maticových reprezentácií toho istého operátora sú navzájom rovné

$$\det(B) = \det(T^{-1}AT) = \underbrace{\det(T^{-1})\det(T)}_1 \det(A) = \det(A) \quad (2.21)$$

V lineárnej algebre medzi dôležité špecifikácie matic patrí patria dve komplementárne celočíselné charakteristiky matic, hodnosť a defekt matice. Ich komplementárnosť spočíva v tom, že ich suma sa pre štvorcové matice rovná dimenzii matice (počtu riadkov/stĺpcov matice). Nech A je lineárny operátor definovaný nad n -rozmerným priestorom H , definujme si množinu jeho funkčných hodnôt

$$\text{im}(A) = \{\beta \in H; \exists(\alpha \in H) : \beta = A\alpha\} \subseteq H \quad (2.22)$$

Definícia 2.6. Prirodzené číslo $r(A)$ sa nazýva **hodnosť** operátora A vtedy a len vtedy, ak sa rovná dimenzii podpriestoru $\text{im}(A)$

$$r(A) = \dim(\text{im}(A)) .$$

Celočíselná veličina nazývaná defekt operátora A je definovaná pomocou jadra operátora

$$\ker(A) = \{\alpha \in H; A\alpha = 0\} \subseteq H \quad (2.23)$$

Táto množina vektorov obsahuje tie vektory z H , ktoré sú zobrazené na nulový vektor.

Definícia 2.7. Prirodzené číslo $d(A)$ sa nazýva **defekt** operátora A vtedy a len vtedy, ak sa rovná dimenzii podpriestoru $\ker(A)$

$$d(A) = \dim(\ker(A)) .$$

Podpriestory $\text{im}(A)$ a $\ker(A)$ nie sú nezávislé, ich komplementárny charakter spočíva v tom, že ich priama suma sa rovná priestoru H nad ktorým je definovaný operátor A

$$\text{im}(A) \oplus \ker(A) = H \quad (2.24a)$$

Potom taktiež aj hodnosť a defekt majú komplementárnych charakter

$$r(A) + d(A) = \dim(H) \quad (2.24b)$$

Pomocou defektu zobrazenia môžeme definovať jeho 1-1-značnosť takto: Nech A je lineárny operátor v priestore H , tento operátor A je 1-1 značný vtedy a len vtedy, ak sa jeho hodnosť rovná dimenzii H

$$r(A) = \dim(H) \quad (2.25)$$

V prvej časti tejto prednášky sme definovali maticovú reprezentáciu A lineárneho operátora A pomocou ortonormálnej bázy. Hodnosť operátora A sa rovná hodnosti jeho maticovej reprezentácie A v ľubovoľnej ortogonálnej báze B , čo formálne zapíšeme takto

$$\forall B : r(A) = r(A) \quad (2.26)$$

Príklady

Príklad 2.1. Vykonajte dôkaz vety 2.1.

Príklad 2.2. Dokážte Schwartzovu nerovnosť (2.4).

Príklad 2.3. Dokážte tieto vlastnosti normy:

- (1) $|\alpha| \geq 0$ ($= 0$ len pre $\alpha = 0$),
- (2) $|\alpha + \beta| \leq |\alpha| + |\beta|$ (trojuholníková nerovnosť, rovnosť platí len pre $\beta = a\alpha$),
- (3) $|a\alpha| = |a||\alpha|$

Návod: Trojuholníková nerovnosť sa dokáže pomocou Schwartzovej nerovnosti (2.4).

Príklad 2.4. Dokážte tieto vlastnosti vzdialenosti:

- (1) $d(\alpha, \beta) \geq 0$ ($= 0$ len pre $\alpha = \beta$),
- (2) $d(\alpha, \beta) = d(\beta, \alpha)$,
- (3) $d(\alpha, \beta) \leq d(\alpha, \gamma) + d(\gamma, \beta)$ (trojuholníková nerovnosť).

Návod: Trojuholníková nerovnosť pre vzdialenosť sa dokáže pomocou trojuholníkovej nerovnosti pre normu z príkladu 2.3.

Príklad 2.5. Nech $B = \{\beta_1, \beta_2, \dots\} \subset H$ je množina normovaných vektorov z n -rozmerného lineárneho priestoru a nech existuje také $\epsilon > 0$, že pre každé $\alpha, \beta \in B, \alpha \neq \beta$, platí $|\alpha - \beta| \geq \epsilon$.
Obsahuje množina B konečný počet vektorov?

Návod: Z trojuholníkovej nerovnosti (príklad 1.15) vyplýva, že ak pre dva normalizované vektory $\alpha, \beta \in B$ platí $|\alpha - \beta| \geq \epsilon$, potom sú lineárne nezávislé.

Príklad 2.6. Dokážte vetu 2.3.

Príklad 2.7. Nech $B = \{\beta_1 = (1, 0, 1), \beta_2 = (0, -1, 1), \beta_3 = (1, 2, -1)\} \subset H$ je báza v 3-rozmernom lineárnom priestore H , použitím Schmidtovho ortogonalizačného procesu zostrojte z tejto bázy ortonormálnu bázu $B_{\text{orthonorm}} = \{\tilde{\beta}_1, \tilde{\beta}_2, \tilde{\beta}_3\} \subset H$.

Príklad 2.8. Dokážte vetu 2.4.

Príklad 2.9. Dokáže formule (2.10).

Príklad 2.10. Dokážte rovnosť (2.17).

Príklad 2.11. Dokážte, že množina $\text{im}(A)$ je podpriestor lineárneho operátora H .

Príklad 2.12. Dokážte, že množina $\text{ker}(A)$ je podpriestor lineárneho operátora H .

Príklad 2.13. Dokážte (2.24a), priama suma podpriestoru funkčných hodnôt a jadra operátora sa rovná priestoru H .

Príklad 2.14. Dokážte, že formula (2.25) je nutnou a postačujúcou podmienkou k tomu, aby operátor A bol 1-1 značný.

3. prednáška

Lineárna algebra III – hermitovský združený operátor, hermitovský operátor, unitárny operátor, vlastné vektory a vlastné hodnoty operátora, tenzorový súčin, projekčné operátory

3.1 Hermitovský združený operátor

Nech A je lineárny operátor definovaný nad unitárnym priestorom H .

Definícia 3.1. Operátor A^+ sa nazýva *hermitovský združený* operátor k operátoru A vtedy a len vtedy, ak pre každé $\alpha, \beta \in H$ platí

$$(A\alpha, \beta) = (\alpha, A^+\beta)$$

Vlastnosti hermitovský združeného operátora sú súhrnne obsiahnuté v tejto vete

Veta 3.1.

- (1) Ak A je lineárny operátor, potom aj A^+ je lineárny operátor.
- (2) Keď operátor A je v ortonormálnej báze $B = \{\beta_1, \beta_2, \dots, \beta_n\}$ reprezentovaný maticou $A = (A_{ij} = (\beta_i, A\beta_j))$, potom hermitovský združený operátor A^+ je reprezentovaný maticou $A^+ = (A_{ij}^+ = (\beta_i, A^+\beta_j))$, pričom maticové elementy $A_{ij}^+ = A_{ji}^*$ (hovoríme, že matica A^+ je hermitovský združená k matici A).
- (3) $(AB)^+ = B^+A^+$.
- (4) $(A^+)^+ = A$.
- (5) $(A \pm B)^+ = A^+ \pm B^+$.
- (6) $(aA)^+ = a^*A^+$.

Táto veta je dokázaná v príklade 3.1.

Pomocou hermitovský združeného operátora sa môžu definovať dva druhy operátorov, ktoré majú centrálny význam v kvantovej teórii:

- (a) *Hermitovský operátor*, $A^+ = A$.
- (b) *Unitárny operátor*, $AA^+ = A^+A = E$, kde E je jednotkový operátor.

Unitárny operátor U zachováva vzťahy ortonormality pre množinu ortonormálnych vektorov $\mathcal{B} = \{\beta_1, \beta_2, \dots, \beta_n\}$, kde $(\beta_i, \beta_j) = \delta_{ij}$. Nech

$$\mathcal{B}' = U\mathcal{B} = \{U\beta_1, U\beta_2, \dots, U\beta_n\} = \{\beta'_i = U\beta_i; i = 1, 2, \dots, n\}$$

je množina vektorov, ktoré vznikla aplikáciou U na vektory množiny $\mathcal{B}$. Jednoducho dokážeme, že vektory $\mathcal{B}'$ tvoria taktiež ortonormálny systém

$$(e'_i, e'_j) = (Ue_i, Ue_j) = \left(e_i, \underbrace{U^+ U}_E e_j \right) = (e_i, e_j) = \delta_{ij}$$

Na základe tohto výsledku môžeme aplikáciu unitárneho operátora na systém vektorov interpretovať, ako rotáciu celého systému okolo jedného bodu.

Maticová reprezentácia A hermitovského operátora A vyhovuje podmienke $A = A^+$, alebo vyjadrené pomocou maticových elementov dostaneme

$$A_{ji}^* = A_{ij} \quad (3.1)$$

To znamená, že hermitovská matica A sa nemení ak ju transponujeme a komplexne združíme.

Ilustračný príklad hermitovsky združenej matice je uvedený v príklade 3.2.

Maticová reprezentácia unitárneho operátora vyhovuje podmienkam

$$AA^+ = A^+A = E$$

Ak prepíšeme tieto rovnice pomocou riadkov alebo stĺpcov matice tak dostaneme, že platí táto veta:

Veta 3.2. Matica U je unitárna vtedy a len vtedy, ak je riadky (stĺpce) tvoria ortonormálny systém.

Dôkaz tejto vety je uvedený v príklade 3.3.

Nech A je lineárny operátor nad unitárnym priestorom H . **Vlastný problém** pre operátor A má tvar

$$A\alpha = \lambda\alpha \quad (3.2)$$

kde nenulový vektor $\alpha \in H$ sa nazýva **vlastný vektor** a skalár $\lambda \in \mathbb{C}$ sa nazýva **vlastná hodnota**. Použitím Gaussovej fundamentálnej vety algebry je možné dokázať, že pre každý operátor A rovnica (3.2) má aspoň jedno riešenie (t. j. existuje aspoň jedna vlastná hodnota λ a k nej priradený vlastný vektor α taký, že platí rovnica $A\alpha = \lambda\alpha$).

V našich ďalších úvahách budeme predpokladať, že operátor A je hermitovský. Tento predpoklad umožňuje, aby vlastný problém (3.2) dve dôležité vlastnosti:

Veta 3.3.

- (1) Vlastné hodnoty hermitovského operátora sú reálne.
- (2) Vlastné vektory α_1 a α_2 patriace rôznym vlastným hodnotám $\lambda_1 \neq \lambda_2$ sú ortogonálne, $(\alpha_1, \alpha_2) = 0$. Slabšia verzia tejto vlastnosti (A nie je hermitovský operátor) je, že charakteristické vektory α_1 a α_2 patriace rôznym vlastným hodnotám $\lambda_1 \neq \lambda_2$ sú lineárne nezávislé.

Dôkaz tejto vety je vykonaný v príklade 3.4.

Veta 3.4.

- (1) Vlastné hodnoty λ_i unitárneho operátora U ležia na jednotkovej kružnici v komplexnej rovine, $|\lambda_i| = 1$.

(2) Vlastné vektory α_1 a α_2 patriace rôznym vlastným hodnotám $\lambda_1 \neq \lambda_2$ sú ortogonálne.

Dôkaz tejto vety je vykonaný v príklade 3.5.

Študujme *sekulárny determinant* priradený operátoru A

$$\det(A - \lambda E) = \det(A - \lambda E) \quad (3.3)$$

Podobne, ako v predchádzajúcich dvoch prípadoch stopy a determinantu, aj teraz ľahko dokážeme, že hodnota sekulárneho determinantu nezávisí od zmeny báze pri tvorbe maticovej reprezentácie

$$\det(B - \lambda E) = \det(T^{-1}AT - \lambda E) = \det[T^{-1}(A - \lambda E)T] = \det(A - \lambda E) \quad (3.4)$$

Výpočtom determinantu na pravej strane upravíme túto formulu do tvaru *sekulárnej rovnice* (niekedy aj *sekulárny polynóm*)

$$\det(A - \lambda E) = \det(A - \lambda E) = \lambda^n + c_1 \lambda^{n-1} + \dots + c_{n-1} \lambda + c_n \quad (3.5)$$

kde $c_1 = \text{Tr}(A)$ a $c_n = \text{Det}(A)$, ostatné koeficienty $c_2, \dots, c_{n-1}$ patria taktiež k invariantom operátora A . Podľa Gaussovej fundamentálnej vety algebry, každá algebraická rovnica má aspoň jeden koreň (komplexný), použitím tejto dôležitej vety, môžeme vlastný polynóm prepísať do tvaru

$$\det(A - \lambda E) = (\lambda - \lambda_1)^{k_1} (\lambda - \lambda_2)^{k_2} \dots (\lambda - \lambda_p)^{k_p} \quad (3.6)$$

kde $\lambda_1, \lambda_2, \dots, \lambda_p$ sú vlastné hodnoty operátora A , exponenty $k_1, k_2, \dots, k_p \geq 0$ špecifikujú násobnosť vlastných hodnôt, vyhovujú podmienke $k_1 + k_2 + \dots + k_p = n$. Ak pre λ_i platí $k_i = 1$ ($k_i > 1$), potom charakteristická hodnota sa nazýva *nedegenerovaná* (*degenerovaná*). Význam týchto exponentov spočíva v tom, že špecifikujú dimenziu charakteristického podpriestoru $H_i \subset H$ obsahujúceho vlastné vektory, ktoré sú priradené vlastnej hodnote λ_i

$$\dim(H_i) = k_i \quad (3.7)$$

$$\varphi \in H_i \Rightarrow A\varphi = \lambda_i \varphi \quad (3.8)$$

V dôsledku podmienky ortogonalnosti medzi vlastnými vektormi, ktoré sú priradené rôznym charakteristickým hodnotám, podpriestory $H_i \subset H$ sú navzájom ortogonálne. Priama suma týchto podpriestorov špecifikuje priestor H nad ktorým je definovaný operátor A

$$H = H_1 \oplus H_2 \oplus \dots \oplus H_n \quad (3.9)$$

Podpriestor H_i obsahuje vektory, ktoré sú riešením homogénneho systému

$$(A - \lambda_i E)\varphi = 0 \quad (3.10)$$

kde homogénny systém má nenulové (netriviálne) riešenie vtedy, ak $r(A - \lambda_i E) < n$, pričom $n - r(A - \lambda_i E) = k_i$, čiže homogénny systém má práve k_i lineárne nezávislých riešení. Pomocou Schmidtovho ortogonalizačného procesu v každom podpriestore H_i môžeme zostrojiť ortonormálnu bázu $\mathcal{B}_i = \{\varphi_1^{(i)}, \varphi_2^{(i)}, \dots, \varphi_{k_i}^{(i)}\}$, alebo $H_i = \text{span}(\varphi_1^{(i)}, \varphi_2^{(i)}, \dots, \varphi_{k_i}^{(i)})$. Potom priestor H vyjadrený ako priama suma (3.9) vlastných podpriestorov H_i má bázu, ktorá vznikne zjednotením báz týchto vlastných podpriestorov

$$\mathcal{B} = \{\psi_1, \psi_2, \dots, \psi_n\} = \bigcup_{i=1}^p \mathcal{B}_i \quad (3.11)$$

Veta 3.5. (Nazývaná *veta o úplnosti*) Nech A je hermitovský operátor definovaný nad

unitárnym priestorom H , potom ľubovoľný vektor $\varphi \in H$ môže byť vyjadrený ako lineárna kombinácia vektorov ortonormálnej báze $\mathcal{B}$

$$\varphi = a_1\psi_1 + a_2\psi_2 + \dots + a_n\psi_n \quad (3.12)$$

Veta je dokázaná v príklade 3.6.

Nech dva hermitovské operátory A a B definované nad unitárnym priestorom H , navzájom **komutujú**, $AB = BA$, čo sa alternatívne môže zapísať pomocou operácie komutátora, $[A, B] = 0$, kde $[A, B] = AB - BA$. Pre jednoduchosť predpokladajme, že vlastné hodnoty operátorov A a B sú nedegenerované, t. j. vlastné podpriestory $H_i^{(A)}$ a $H_i^{(B)}$ sú jednorozmerné. Nech $A\varphi_i = \lambda_i\varphi_i$, potom $BA\varphi_i = \lambda_i B\varphi_i$, ak využijeme vlastnosť komutácie operátorov A a B , potom taktiež musí platiť $A(B\varphi_i) = \lambda_i(B\varphi_i)$. Z tejto vlastnosti vyplýva, že tak φ_i , ako aj $B\varphi_i$ sú vlastné vektory operátora A , ktoré sú priradené vlastnej hodnote λ_i . Pretože sme postulovali 1-rozmernosť vlastných podpriestorov, potom vektory φ_i , ako aj $B\varphi_i$ sa „kolíneárne“, t. j. $B\varphi_i = \mu_i\varphi_i$, kde μ_i je reálne číslo, ktoré môžeme interpretovať ako vlastnú hodnotu operátora B .

Veta 3.6. Komutujúce operátory A a B majú spoločný systém vlastných vektorov.

3.2 Tenzorový súčin

Nech H a G sú unitárne priestory, **tenzorový súčin** je asociatívna binárna operácia, ktorá každej dvojici vektorov $\alpha \in H$ a $\beta \in G$ priradí usporiadanú dvojicu $\alpha \otimes \beta$, pričom platia tieto axiomy:

- (1) $(\alpha_1 + \alpha_2) \otimes \beta = \alpha_1 \otimes \beta + \alpha_2 \otimes \beta$,
- (2) $\alpha \otimes (\beta_1 + \beta_2) = \alpha \otimes \beta_1 + \alpha \otimes \beta_2$,
- (3) $a(\alpha \otimes \beta) = (a\alpha) \otimes \beta = \alpha \otimes (a\beta)$
- (4) $(\alpha_1 \otimes \beta_1, \alpha_2 \otimes \beta_2) = (\alpha_1 \otimes \beta_1)(\alpha_2 \otimes \beta_2)$

Prvé tri axiomy špecifikujú tenzorový súčin ako „lineárnu operáciu“, štvrtá operácia špecifikuje skalárny súčin pre vektory, ktoré vznikli pomocou tenzorového súčinu.

Ak priestory H a G majú báze $\mathcal{B}_1 = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ resp. $\mathcal{B}_2 = \{\beta_1, \beta_2, \dots, \beta_m\}$ tenzorový súčin týchto báz

$$\mathcal{B} = \mathcal{B}_1 \otimes \mathcal{B}_2 = \{\alpha_i \otimes \beta_j ; i = 1, 2, \dots, n, j = 1, 2, \dots, m\}$$

môže byť interpretovaný ako báza tenzorového súčinu $H \otimes G$, t. j.

$$F = H \otimes G = \text{span}(\mathcal{B}_1 \otimes \mathcal{B}_2)$$

Dimenzia priestoru F je špecifikovaná súčinom dimenzií priestorov H a G

$$\dim(H \otimes G) = \dim(H) \cdot \dim(G) \quad (3.13)$$

Veta 3.7. Nech $\mathcal{B}_1 = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ resp. $\mathcal{B}_2 = \{\beta_1, \beta_2, \dots, \beta_m\}$ sú báze priestorov H resp. G . Vektory tenzorového súčinu týchto báz sú lineárne nezávislé, t. j. tvoria bázu priestoru $H \otimes G = \text{span}(\mathcal{B}_1 \otimes \mathcal{B}_2)$.

Dôkaz tejto vety je uvedený v príklade 3.8.

Viacnásobný tenzorový súčin vektorov $\alpha_1, \alpha_2, \dots, \alpha_n$ môžeme alternatívne interpretovať ako usporiadanú n -ticu vektorov

$$\alpha_1 \otimes \alpha_2 \otimes \dots \otimes \alpha_n = \alpha_1 \alpha_2 \dots \alpha_n = (\alpha_1, \alpha_2, \dots, \alpha_n) \quad (3.14)$$

Nech operátory A a B , definovaný v unitárnom priestore H resp. H' , v ktorom sú zvolené bázy $\mathcal{B} = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ resp. $\mathcal{B}' = \{\alpha'_1, \alpha'_2, \dots, \alpha'_m\}$, majú maticové reprezentácie A resp. B . Potom tenzorový súčin operátorov $A \otimes B$, definovaný nad priestorom $H \otimes G = \text{span}(\mathcal{B}_1 \otimes \mathcal{B}_2)$ má maticovú reprezentáciu vyjadrenú pomocou tenzorového súčinu matic

$$A \otimes B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \dots & \dots & \dots & \dots \\ b_{m1} & b_{m2} & \dots & b_{mm} \end{pmatrix} = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \dots & \dots & \dots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix} \quad (3.15)$$

Tenzorový súčin matic je dokázaný v príklade 3.7. Jednoduchý ilustračný príklad tenzorového súčinu matic je uvedený v príklade 3.8.

3.3 Projekčné operátory

Nech unitárny priestor H sa rovná priamej sume dvoch podpriestorov H_1 a H_2 , $H = H_1 \oplus H_2$. To znamená, že každý vektor $\alpha \in H$ môže byť jednoznačne vyjadrený ako suma dvoch vektorov z H_1 resp. H_2 ,

$$\alpha = \alpha_1 + \alpha_2 \quad (3.16)$$

Definícia 3.2. Operátor P_1 sa nazýva **projekčný operátor** na podpriestor H_1 vtedy a len vtedy, ak pre každé $\alpha \in H$ platí $P_1 \alpha = \alpha_1$.

Podobným spôsobom sa môže definovať aj projektor P_2 na podpriestor H_2 , jednotlivé projekčné operátory vyhovujú podmienkam

$$P_1^2 = P_1, P_2^2 = P_2 \text{ a } P_1 P_2 = 0 \quad (3.17a)$$

$$P_1 + P_2 = 1 \quad (3.17b)$$

Dôkaz týchto vlastností je uvedený v príklade 3.9.

Definíciu projektoru na podpriestor môžeme zovšeobecniť pre všeobecnú priamu sumu podpriestorov

$$H = H_1 \oplus H_2 \oplus \dots \oplus H_n \quad (3.18)$$

Nech P_i je projektor na podpriestor H_i , potom (3.17) môžeme zovšeobecniť takto

$$P_i P_j = \delta_{ij} P_i \quad (3.18a)$$

$$\sum_{i=1}^n P_i = 1 \quad (3.18b)$$

Predpokladajme, že podpriestory z $H = H_1 \oplus H_2$ sú navzájom ortogonálne, to znamená, že

$$\forall (\alpha \in H_1) \forall (\beta \in H_2) : (\alpha, \beta) = 0$$

Projektory na tieto podpriestory sú nielen idempotentné ale aj hermitovské (dôkaz tejto vlastnosti je uvedený v príklade 3.10)

$$P_1^2 = P_1, P_2^2 = P_2 \text{ a } P_1 P_2 = 0 \quad (3.19a)$$

$$P_1 = P_1^+, P_2 = P_2^+ \quad (3.19b)$$

$$P_1 + P_2 = 1 \quad (3.19c)$$

Zostrojíme maticovú reprezentáciu projekčného operátora P v ortonormálnych bázach $\mathcal{B}_1 = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ resp. $\mathcal{B}_2 = \{\alpha'_1, \alpha'_2, \dots, \alpha'_m\}$, pričom P je projektor na $H_1 = \text{span}\{\mathcal{B}_1\}$, ortogonálny komplement k H_1 je označený $H_2 = \text{span}\{\mathcal{B}_2\}$, kde $H = H_1 \oplus H_2$. Pre maticové elementy projekčného operátora platí

$$\langle \alpha_i | P | \alpha_j \rangle = \delta_{ij} \quad (\text{pre } \forall \alpha_i, \alpha_j \in \mathcal{B}_1) \quad (3.20a)$$

$$\langle \alpha_i | P | \alpha'_j \rangle = 0 \quad (\text{pre } \forall (\alpha_i \in \mathcal{B}_1) \forall (\alpha'_j \in \mathcal{B}_2)) \quad (3.20b)$$

$$\langle \alpha'_i | P | \alpha'_j \rangle = 0 \quad (\text{pre } \forall \alpha'_i, \alpha'_j \in \mathcal{B}_2) \quad (3.20c)$$

Potom maticová reprezentácia projektora P v bázach $\mathcal{B}_1$ a $\mathcal{B}_2$ má tvar matice

$$P = \begin{pmatrix} E_1 & \theta_{12} \\ \theta_{12}^T & \theta_{22} \end{pmatrix} = \left(\begin{array}{ccc|ccc} 1 & \dots & 0 & 0 & 0 & 0 \\ 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & \dots & 1 & 0 & 0 & 0 \\ \hline 0 & \dots & 0 & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 0 \end{array} \right) \quad (3.21)$$

kde E_1 je jednotková matica typu (n,n) , θ_{12} je nulová matica typu (n,m) a θ_{22} je nulová matica typu (m,m) .

Veta 3.7. Stopa maticovej reprezentácie P sa rovná stope projektora P

$$\text{Tr}(P) = n = \dim(H_1) \quad (3.22)$$

Sekulárny determinant (3.6) môžeme prepísať do tvaru

$$\det(P - \lambda E) = (\lambda - 1)^n (\lambda)^m \quad (3.23)$$

To znamená, že projektor P má dve vlastné hodnoty: jednotkovú vlastnú hodnotu $\lambda_1 = 1$, ktorá je n -násobná a nulovú vlastnú hodnotu $\lambda_2 = 0$, ktorá je m -násobná.

Príklady

Príklad 3.1. Dokážte vlastnosti (1-6) hermitovsky združeného operátora, ktoré sú uvedené vo vete 3.1.

Príklad 3.2. Študujme maticu

$$A = \begin{pmatrix} 1 & 1+i \\ 1-i & -1 \end{pmatrix}$$

Potom hermitovsky združená matica má tvar

$$A^+ = \begin{pmatrix} 1 & (1-i)^* \\ (1+i)^* & -1 \end{pmatrix} = \begin{pmatrix} 1 & 1+i \\ 1-i & -1 \end{pmatrix} = A$$

To znamená, že táto matica je hermitovská.

Príklad 3.3. Dokážte vetu 3.2

Príklad 3.4. Dokážte vetu 3.3.

Príklad 3.5. Dokážte vetu 3.4.

Príklad 3.6. Dokážte vetu 3.5.

Príklad 3.7. Dokážte formulu (3.15), ktorá špecifikuje maticovú reprezentáciu tenzorového súčinu dvoch operátorov.

Príklad 3.8. Zostrojte tenzorový súčin matíc

$$A = \begin{pmatrix} 1 & 2 \\ 1 & -1 \end{pmatrix} \text{ a } B = \begin{pmatrix} 2 & 1 & -1 \\ 0 & 1 & 1 \\ -2 & 1 & 0 \end{pmatrix}.$$

Príklad 3.9. Dokážte vlastnosti (3.17a-b).

Príklad 3.10. Dokážte, že podpriestory H_1 a H_2 z rozkladu $H = H_1 \oplus H_2$ sú ortogonálne vtedy a len vtedy, keď projektory na tieto podpriestory sú hermitovské.

4. prednáška

Lineárna algebra IV – Diracov formalizmus lineárnej algebry, bra a ket vektory, diadický súčin a skalárny súčin, spektrálny rozvoj operátora, funkcia operátora

Paul A. M. Dirac, anglický fyzik a jeden zo spoluzakladateľov kvantovej mechaniky, vo svojej známej knižke *The Principles of Quantum Mechanics* z r. 1930, položil základy moderného formalizmu kvantovej mechaniky, ktorý bol založený na teórii lineárnych priestorov a operátorov. Táto knižka, už viac ako polstoročie patrí medzi nestarnúce knihy, v ktorej jasným, jednoduchým a súčasne presným spôsobom sú formulované základné princípy kvantovej mechaniky.

4.1 Diracov formalizmus

Definícia 4.1.

Nech H je n -rozmerný unitárny lineárny priestor. Definujme dva nové typy vektorov:¹ **ket vektor** $|\alpha\rangle$ a **bra vektor** $\langle\alpha|$. Nech existuje vzájomne 1-1-značné priradenie

$$\begin{cases} |\alpha\rangle \leftrightarrow \alpha \\ \langle\alpha| \leftrightarrow \alpha \end{cases} \quad \forall \alpha \in H \quad (4.1)$$

Pre tieto dva nové typy vektorov základné algebraické operácie sú definované takto:

(1) **Násobenie vektora** komplexným číslom

$$a|\alpha\rangle = |a\alpha\rangle \quad \text{a} \quad a^*\langle\alpha| = \langle a\alpha| \quad (4.2)$$

kde vektory $|a\alpha\rangle$ a $\langle a\alpha|$ sú realizované pomocou (1.37).

(2) **Súčet vektorov**

$$|\alpha\rangle + |\beta\rangle = |\alpha + \beta\rangle \quad \text{a} \quad \langle\alpha| + \langle\beta| = \langle\alpha + \beta| \quad (4.3)$$

kde vektory $|\alpha + \beta\rangle$ a $\langle\alpha + \beta|$ sú realizované pomocou priradenia (4.1).

(3) **Pôsobenie operátora**

$$A|\alpha\rangle = |A\alpha\rangle \quad \text{a} \quad \langle\alpha|A^+ = \langle A\alpha| \quad (4.4)$$

kde vektory $|A\alpha\rangle$ a $\langle A\alpha|$ sú realizované pomocou priradenia (4.1).

¹ Dirac zaviedol túto terminológiu tak, že rozdelil anglické slovo *bracket* - zátvorka, ľavá časť zátvorky je označená *bra* a pravá časť je označená *ket*. Dirac pri návrhu tejto terminológie prejavil aj určitú dávku vtipnosti, *bra* znamená po anglicky špeciálny typ podprsenky bez ramienok.

Pre názornosť poznamenajme, že bra- a ket vektory sú v rámci klasickej lineárnej algebry realizované pomocou riadkových resp. stĺpcových vektorov.

Ket-vektory a bra-vektory tvoria množinu vektorov

$$H_K = \{|\alpha\rangle; \alpha \in H\} \quad (4.5a)$$

$$H_B = \{\langle\alpha|; \alpha \in V\} \quad (4.5b)$$

Jednoduchým spôsobom možno dokázať, že množiny vektorov H_K a H_B tvoria lineárne priestory nad polom komplexných čísel, pričom priestory H_K , H_B a H sú navzájom izomorfné (pozri príklad 4.1).

Veta 4.1. Binárna operácia medzi bra- a ket-vektormi $H_K \times H_B \rightarrow \mathcal{C}$, ktorá dvojici vektorov priradí skalár (komplexné číslo) z $\mathcal{C}$ podľa predpisu

$$\langle\alpha|\beta\rangle = (\alpha, \beta) \quad (4.6)$$

je skalárny súčin, t. j. platia podmienky (1-4) z definície 2.1.

V príklade 4.2 je dokázané, že takto definovaná binárna operácia $\langle\alpha|\beta\rangle$ je skalárny súčin.

Maticový element operátora A medzi bra- a ket-vektormi je definovaný vzťahom

$$\langle\alpha|A|\beta\rangle = (\alpha, A\beta) \quad (4.7)$$

Substitúciou $A \rightarrow A^+$ a použitím základných vlastností skalárneho súčinu (x, y) dostaneme dôležitý výraz pre maticový element hermitovsky združeného operátora

$$\langle\alpha|A^+|\beta\rangle = (\alpha, A^+\beta) = (A\alpha, \beta) = (\beta, A\alpha)^* = \langle\beta|A|\alpha\rangle^* \quad (4.8)$$

Operátor A je lineárnym operátorom v priestoroch H_K a H_B

$$\begin{aligned} A(|\alpha\rangle + |\beta\rangle) &= A|\alpha + \beta\rangle = |A(\alpha + \beta)\rangle \\ &= |A\alpha + A\beta\rangle = |A\alpha\rangle + |A\beta\rangle = A|\alpha\rangle + A|\beta\rangle \end{aligned} \quad (4.9)$$

Definícia 4.2. Medzi bra- a ket-vektormi sa postulujú tieto jednoduché vzťahy

$$(A|\alpha\rangle)^+ = \langle\alpha|A^+ \quad (4.10a)$$

$$(|\alpha\rangle)^+ = \langle\alpha| \quad (4.10b)$$

Pri operácii hermitovského združenia môžeme bra- a ket-vektory chápať ako operátory.

Definujme operátor $\Omega_{\varphi\psi}$ pomocou maticových elementov

$$\langle\alpha|\Omega_{\varphi\psi}|\beta\rangle = \langle\alpha|\varphi\rangle\langle\psi|\beta\rangle \quad \forall \alpha \in H_B, \forall \beta \in H_K \quad (4.11)$$

Použitím (8) dostaneme

$$\begin{aligned} \langle\alpha|\Omega_{\varphi\psi}^+|\beta\rangle &= \langle\beta|\Omega_{\varphi\psi}|\alpha\rangle^* = \langle\beta|\varphi\rangle^*\langle\psi|\alpha\rangle^* = \\ &= \langle\alpha|\psi\rangle\langle\varphi|\beta\rangle \end{aligned} \quad (4.12)$$

Tieto dve vlastnosti operátora $\Omega_{\varphi\psi}$ môžeme formálne vyjadriť pomocou tzv. **dyadického súčinu**

$$\Omega_{\varphi\psi} = |\varphi\rangle\langle\psi| \quad \text{a} \quad \Omega_{\varphi\psi}^+ = |\psi\rangle\langle\varphi| \quad (4.13)$$

Aplikáciou dyadického súčinu na ket-vektor dostaneme ket-vektor (to znamená, že dyadický produkt svojim pôsobením na vektory je ekvivalentný operátoru)

$$\Omega_{\varphi\psi}|\alpha\rangle = |\varphi\rangle\langle\psi|\alpha \quad \text{a} \quad \langle\alpha|\Omega_{\varphi\psi} = \langle\alpha|\psi\rangle\langle\varphi| \quad (4.14)$$

Pomocou diadického súčinu definujeme operátor

$$P = |\tau\rangle\langle\tau| \quad (4.15)$$

kde $|\tau\rangle$ je normalizovaný ket-vektor, $\langle\tau|\tau\rangle = 1$. Operátor P vyhovuje nutnej a postačujúcej podmienke projekčného operátora

$$P^2 = P \quad (4.16a)$$

$$P^+ = P \quad (4.16b)$$

Veta 4.2. Operátor P je projektorom na podpriestor indukovaný vektorom $|\tau\rangle$, $H_\tau = \text{span}\{|\tau\rangle\}$. Podobne, operátor $1-P$ je projektor na ortogonálny doplnok $H_\tau^\perp$.

Definujeme v n -rozmernom unitárnom priestore V ortonormálny systém vektorov

$$\mathcal{B} = \{|\varepsilon_1\rangle, |\varepsilon_2\rangle, \dots, |\varepsilon_n\rangle\} \quad (4.17)$$

kde

$$\langle\varepsilon_i|\varepsilon_j\rangle = \delta_{ij} \quad (4.18)$$

Postulát **úplnosti** systému (4.17) znamená, že ľubovoľný vektor $|\varepsilon\rangle \in V$ môžeme vyjadriť ako lineárnu kombináciu jeho vektorov

$$|\psi\rangle = \sum_i a_i |\varepsilon_i\rangle \quad (4.19a)$$

$$a_i = \langle\varepsilon_i|\psi\rangle \quad (4.19b)$$

Použitím jazyka klasickej lineárnej algebry predpoklad úplnosti ortonormálneho systému (4.17) znamená, že počet prvkov tohto systému je totožný s dimenziou unitárneho priestoru V , alebo ináč, systém (4.17) tvorí bázu priestoru V .

Definujeme projektory

$$P_i = |\varepsilon_i\rangle\langle\varepsilon_i| \quad (\text{pre } i = 1, 2, 3, \dots) \quad (4.20a)$$

ktoré vyhovujú vzťahom

$$P_i^+ = P_i \quad (4.20b)$$

$$P_i P_j = \delta_{ij} P_i \quad (4.20c)$$

Veta 4.3. Podmienka úplnosti systému $\mathcal{B}$ (4.17) je ekvivalentná formule

$$\sum_i P_i = 1 \quad (4.21)$$

kde '1' je jednotkový operátor v priestore V_K .

Aplikovaním (21) na ľubovoľný ket-vektor dostaneme podmienku úplnosti (19)

$$1|\psi\rangle = \sum_i P_i |\psi\rangle = \sum_i |\varepsilon_i\rangle\langle\varepsilon_i|\psi\rangle = \sum_i a_i |\varepsilon_i\rangle \quad (4.22)$$

Definujeme operátor

$$P_o = \sum_{i \in M_o} P_i \quad (4.23)$$

kde množina M_o obsahuje d indexov, $M_o = \{i_1, i_2, \dots, i_d\}$. Takto definovaný operátor P_o je projektorom na podpriestor H_o generovaný vektormi $\{|\varepsilon_i\rangle; i \in M_o\}$, $H_o = \text{span}\{|\varepsilon_i\rangle; i \in M_o\}$.

Stopa operátora A v báze (4.17) je definovaná ako suma diagonálnych maticových elementov (pozri (2.16))

$$\text{Tr}(A) = \sum_i \langle \varepsilon_i | A | \varepsilon_i \rangle \quad (4.24)$$

Stopa operátora je invariantná vzhľadom k výberu systému vektorov (17), má nasledujúcu hodnotu

$$\begin{aligned} \text{Tr}(P_o) &= \sum_i \langle \varepsilon_i | P_o | \varepsilon_i \rangle = \sum_i \langle \varepsilon_i | \left(\sum_{j \in M_o} | \varepsilon_j \rangle \langle \varepsilon_j | \right) | \varepsilon_i \rangle = \\ &= \sum_i \sum_{j \in M_o} \langle \varepsilon_i | \varepsilon_j \rangle \langle \varepsilon_j | \varepsilon_i \rangle = \sum_i \sum_{j \in M_o} \delta_{ij} \delta_{ij} = d \end{aligned} \quad (4.25)$$

Veta 4.4. Stopa projekčného operátora sa rovná dimenzii podpriestoru, vzhľadom ku ktorému je projekčný operátor definovaný

$$\dim(V_o) = \text{Tr}(P_o) \quad (4.26)$$

Nech A je hermitovský operátor, $A^+ = A$, vlastný problém tohto operátora má tvar

$$A | \varepsilon_{i,a} \rangle = \lambda_i | \varepsilon_{i,a} \rangle \quad (a = 1, 2, \dots, d_i) \quad (4.27)$$

kde λ_i je i -tá vlastná hodnota a index $\alpha = 1, 2, \dots, d_i$ popisuje multiplicitu (degenerovanosť) charakteristickej hodnoty λ_i . Vlastné z (27) sú vybrané tak, že tvoria ortonormálny systém

$$\langle \alpha_{i,a} | \alpha_{j,b} \rangle = \delta_{ij} \delta_{ab} \quad (4.28)$$

Projekčný operátor na podpriestor indukovaný vlastnými vektormi s vlastnou hodnotou λ_i má tvar

$$P_i = \sum_{a=1}^{d_i} | \varepsilon_{i,a} \rangle \langle \varepsilon_{i,a} | \quad (4.29)$$

pričom $\text{Tr}(P_i) = d_i$, t.j. dimenzia podpriestoru definovaného projektorom P_i sa rovná multiplicitu vlastnej hodnoty λ_i . Projektor P_i sa nazýva **vlastný projektor** priradený i -tej vlastnej hodnote λ_i .

Pomocou projektorov (4.29) vlastný problém (4.27) môže byť prepísaný do tvaru

$$AP_i = P_i A = \lambda_i P_i \quad (4.30)$$

ktorý sa nazýva operátorový vlastný problém.

Predpokladajme, že systém vlastných vektorov $\{ | \varepsilon_{i,a} \rangle \}$ operátora A tvorí úplný systém, potom (pozri vetu 4.3)

$$\sum_i P_i = 1 \quad (4.31)$$

$$A = A1 = A \sum_i P_i = \sum_i AP_i = \sum_i \lambda_i P_i \quad (4.32)$$

Definícia 4.3. *Spektrálny rozvoj* hermitovského operátora A má tvar

$$A = \sum_i \lambda_i P_i \quad (4.33a)$$

alebo v zovšeobecnenom tvare

$$f(A) = \sum_i f(\lambda_i) P_i \quad (4.33b)$$

pričom sa predpokladá, že funkcia $f(z)$ je definovaná pre každú vlastnú hodnotu operátora A .

Predpokladajme, že funkcia $f(z)$ je analytická funkcia na nejakej oblasti, potom na tejto oblasti komplexných čísel môže sa vyjadriť pomocou rozvoja

$$f(z) = \sum_{n=0}^{\infty} c_n z^n \quad (4.34)$$

Alternatívna formula pre funkciu operátora $f(A)$ má tvar

$$f(A) = \sum_{n=0}^{\infty} c_n A^n \quad (4.35)$$

kde rozvojové koeficienty c_n sú rovnaké ako v (4.34). Ukážeme za akých podmienok môže byť funkcia $f(A)$ definovaná (4.34) ekvivalentná s definíciou (4.33). Pre mocniny operátora A^n zo spektrálneho rozvoja (4.32) dostaneme

$$A^n = \sum_i \lambda_i^n P_i \quad (4.36)$$

Dosadením tohoto vzťahu do (35) dostaneme

$$f(A) = \sum \left(\sum_{n=0}^{\infty} c_n \lambda_i^n \right) P_i \quad (1.37)$$

Tento výraz je totožný s (33) za predpokladu, že všetky charakteristické hodnoty operátora A ležia v oblasti analytičnosti funkcie $f(z)$. Táto skutočnosť má význam vtedy, ak rozvíjame funkciu operátora do mocninného radu. Tak napríklad, študujme funkciu operátora

$$f(A) = (1 - A)^{-1} \quad (4.38)$$

ktorá zodpovedá funkcii $f(z) = (1 - z)^{-1}$. Táto funkcia je analytická len pre $|z| < 1$, potom

$$f(A) = (1 - A)^{-1} = \sum_{n=0}^{\infty} A^n \quad (4.39)$$

platí len vtedy, ak vlastné hodnoty operátora A ležia vo vnútri jednotkovej kružnici, $|\lambda_i| < 1$.

Operátorový rozvoj exponenciály

$$e^A = \sum_{n=0}^{\infty} \frac{1}{n!} A^n \quad (4.40)$$

platí pre každý operátor, pretože funkcia $f(z) = e^z$ je analytická pre každé z .

Pomocou spektrálneho rozvoja (4.33b) môžeme pomocou hermitovského operátora H zostrojiť unitárny operátor U takto

$$U = e^{iH} = \sum_{k=1}^n e^{i\lambda_k} P_k \quad (4.41)$$

Z tejto formule bezprostredne vyplýva veta 3.4 pre unitárny operátor, t. j. vlastné hodnoty ležia na jednotkovej kružnici a vlastné vektory sú navzájom ortonormálne.

Veta 4.5. Pre každý unitárny operátor U existuje taký hermitovský operátor H , že $U = e^{iH}$.

Dôkaz vety 4.5 je vykonaný v príklade 4.3.

Príklady

Príklad 4.1. Dokážte, že množiny H_B a H_K (4.5a-b) sú lineárne priestory, pričom trojica H , H_B a H_K tvorí navzájom izomorfné priestory.

Príklad 4.2. Dokážte, že binárna operácia $\langle \alpha | \beta \rangle$ vyhovuje podmienkam skalárneho súčinu (1-4) z definície 2.1.

Príklad 4.3. Dokážte vetu 4.5.

5. prednáška

Kvantová mechanika I – stavy kvantového systému, experimenty s polarizovanými fotónmi, pozorovateľnosť, úplnosť vlastného systému pozorovateľnej, princíp superpozície, meranie

Kvantová mechanika je prezentovaná vo forme, ako bola rozvinutá Diracom prostredníctvom jeho formalizmu založená na konečno-rozmerných Hilbertových priestoroch, ktorých teória bola prezentovaná v predchádzajúcej 4. prednáške. Fyzikálne princípy kvantovej mechaniky sú vyjadrené v koncentrovanej podobe pomocou niekoľkých postulátov (axiém).

5.1 Kvantový systém a jeho stavy

Kvantový systém Q je špecifikovaný stavmi, ktoré sú reprezentované ket vektormi z n -rozmerného Hilbertovho priestoru H

$$|label\rangle \quad (5.1)$$

kde „*label*“ je obvykle reprezentovaný reťazcom symbolov, ktoré špecifikujú stav systému.

Definícia 5.1. Hovoríme, že dva vektory $|\alpha\rangle$ a $|\beta\rangle$ reprezentujú *rovnaký stav* kvantového systému Q vtedy a len vtedy, ak vektory sú lineárne závislé, t. j. existuje také komplexné číslo $a \in \mathbb{C}$

$$|\alpha\rangle = a|\beta\rangle \quad (5.2)$$

K tomu, aby sme odstránili nejednoznačnosť (5.2) s reprezentáciou stavov kvantových systémov, budeme požadovať, aby ket vektory, ktoré reprezentujú stavy, boli normalizované

$$\|\alpha\rangle = 1 \Leftrightarrow \langle\alpha|\alpha\rangle = 1 \quad (5.3)$$

5.1.1 Kvantovo-mechanická reprezentácia polarizovaných fotónov

Polarizovaný stav fotónu bude reprezentovaný vektorom vektorom z 2-rozmerného Hilbertového priestoru. V tomto priestore si môžeme zvoliť niekoľko alternatívnych ortonormálnych báz:

(1) Ľavo a pravotočivá cirkulárna polarizácia fotónov

$$\mathcal{B}_1 = \{|\circlearrowleft\rangle, |\circlearrowright\rangle\} \quad (5.4a)$$

(2) Vertikálna a horizontálna polarizácia fotónov

$$\mathcal{B}_2 = \{|\uparrow\rangle, |\rightarrow\rangle\} \quad (5.4b)$$

(3) Lineárne polarizované fotóny s uhlom polarizácie $\varphi=\pi/2$ resp. $\varphi=-\pi/2$

$$\mathcal{B}_3 = \{|\nearrow\rangle, |\searrow\rangle\} \quad (5.4c)$$

Prechody medzi týmito ortonormálnymi bázami sú realizované lineárnymi kombináciami

$$\left\{ \begin{array}{l} |\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle) \\ |\searrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - |\rightarrow\rangle) \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} |\uparrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle + |\searrow\rangle) \\ |\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\searrow\rangle) \end{array} \right. \quad (5.5a)$$

$$\left\{ \begin{array}{l} |\circ\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle - i|\rightarrow\rangle) \\ |\ominus\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + i|\rightarrow\rangle) \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} |\uparrow\rangle = \frac{1}{\sqrt{2}}(|\circ\rangle + |\ominus\rangle) \\ |\rightarrow\rangle = \frac{i}{\sqrt{2}}(|\circ\rangle - |\ominus\rangle) \end{array} \right. \quad (5.5a)$$

$$\left\{ \begin{array}{l} |\nearrow\rangle = \frac{1+i}{2}|\circ\rangle + \frac{1-i}{2}|\ominus\rangle \\ |\searrow\rangle = \frac{1-i}{2}|\circ\rangle - \frac{1+i}{2}|\ominus\rangle \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} |\circ\rangle = \frac{1-i}{2}|\nearrow\rangle + \frac{1+i}{2}|\searrow\rangle \\ |\ominus\rangle = \frac{1+i}{2}|\nearrow\rangle - \frac{1-i}{2}|\searrow\rangle \end{array} \right. \quad (5.5c)$$

Tieto vzťahy môžeme vyjadriť pomocou transformačných matic

	$ \uparrow\rangle$	$ \rightarrow\rangle$	$ \nearrow\rangle$	$ \searrow\rangle$	$ \circ\rangle$	$ \ominus\rangle$
$ \uparrow\rangle$	1	0	$1/\sqrt{2}$	$1/\sqrt{2}$	$1/\sqrt{2}$	$1/\sqrt{2}$
$ \rightarrow\rangle$	0	1	$1/\sqrt{2}$	$-1/\sqrt{2}$	$i/\sqrt{2}$	$-i/\sqrt{2}$
$ \nearrow\rangle$	$1/\sqrt{2}$	$1/\sqrt{2}$	1	0	$(1+i)/2$	$(1-i)/2$
$ \searrow\rangle$	$1/\sqrt{2}$	$-1/\sqrt{2}$	0	1	$(1-i)/2$	$(1+i)/2$
$ \circ\rangle$	$1/\sqrt{2}$	$-i/\sqrt{2}$	$(1-i)/2$	$(1+i)/2$	1	0
$ \ominus\rangle$	$1/\sqrt{2}$	$i/\sqrt{2}$	$(1+i)/2$	$(1-i)/2$	0	1

Pre názornosť vyjadríme ket vektory pomocou stĺpcových vektorov, potom bra vektory musia byť vyjadrené pomocou riadkových vektorov

$$\left\{ \begin{array}{l} |\uparrow\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ |\rightarrow\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} \langle\uparrow| = (1 \ 0) \\ \langle\rightarrow| = (0 \ 1) \end{array} \right. \quad (5.6a)$$

$$\left\{ \begin{array}{l} |\nearrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ |\searrow\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{array} \right\} \Leftrightarrow \left\{ \begin{array}{l} \langle\nearrow| = \frac{1}{\sqrt{2}} (1 \ 1) \\ \langle\searrow| = \frac{1}{\sqrt{2}} (1 \ -1) \end{array} \right. \quad (5.6b)$$

$$\begin{aligned} \left. \begin{aligned} |\circ\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \\ |\ominus\rangle &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} \end{aligned} \right\} \Leftrightarrow \left\{ \begin{aligned} \langle\circ| &= \frac{1}{\sqrt{2}} (1 \quad -i) \\ \langle\ominus| &= \frac{1}{\sqrt{2}} (1 \quad i) \end{aligned} \right. \end{aligned} \quad (5.6c)$$

V tejto reprezentácii tenzorový súčin $|\nearrow\circ\rangle$ je interpretovaný stĺpcovým vektorom

$$|\nearrow\circ\rangle = |\nearrow\rangle \otimes |\circ\rangle = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ -i \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 \\ -i \\ 1 \\ -i \end{pmatrix} \quad (5.7a)$$

$$|\circ\rangle\langle\circ| = \frac{1}{2} \begin{pmatrix} 1 \\ i \end{pmatrix} (1 \quad -i) = \frac{1}{2} \begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix} \quad (5.7b)$$

5.2 Pozorovateľná

Definícia 5.2. Nech stavy kvantového systému Q sú reprezentované vektormi z n -rozmerného Hilbertovho priestoru H . Hovoríme, že lineárny operátor O definovaný v H špecifikuje **pozorovateľnú** kvantového systému Q vtedy a len vtedy, keď je tento operátor hermitovský, $O^+ = O$.

Spektrálny rozvoj pozorovateľnej O má tvar (4.33)

$$O = \sum_{i=1}^p \lambda_i P_i \quad (5.8)$$

kde vlastná hodnota λ_i vyjadruje i -tú vlastnosť pozorovateľnej O , P_i je hermitovský projekčný operátor na podpriestor $H_i \subseteq H$ indukovaný vlastnými vektormi, ktoré sú prídružené vlastnej hodnote λ_i

$$|\phi\rangle \in H_i \Rightarrow O|\phi\rangle = \lambda_i |\phi\rangle.$$

Definícia 5.3. Hovoríme, že charakteristický systém pozorovateľnej O je **úplny** vtedy a len vtedy, ak

$$\sum_{k=1}^p P_k = 1 \quad (5.9)$$

Podmienka úplnosti charakteristického systému pozorovateľnej O umožňuje formulovať princíp superpozície.

Definícia 5.4. Hovoríme, že platí **princíp superpozície** vtedy a len vtedy, ak každý stav $|\psi\rangle$ systému Q môžeme vyjadriť ako lineárnu kombináciu charakteristických funkcií nejakej pozorovateľnej O

$$|\psi\rangle = 1 \cdot |\psi\rangle = \left(\sum_{i=1}^p P_i \right) |\psi\rangle = \sum_{j=1}^n a_j |\varphi_j\rangle \quad (5.10)$$

Pri definícii princípu superpozície sme využili podmienku úplnosti (5.9) charakteristického systému pozorovateľnej O , ktorú môžeme prepísať do ekvivalentného tvaru, ak každý projektor P_i vyjadríme pomocou dyadických produktov charakteristických vektorov pozorovateľnej O

$$P_i = \sum_{j=1}^{k_i} |\varphi_j^{(i)}\rangle \langle \varphi_j^{(i)}| \Rightarrow \sum_{i=1}^p P_i = \sum_{i=1}^p \sum_{j=1}^{k_i} |\varphi_j^{(i)}\rangle \langle \varphi_j^{(i)}| = \sum_{k=1}^n |\varphi_k\rangle \langle \varphi_k| = 1 \quad (5.11)$$

kde na pravej strane (5.11) sme vhodným preindexovaním použili ortonormálnu bázu funkcií, ktorá vznikla z charakteristických funkcií $|\varphi_j^{(i)}\rangle$.

Ak kvantový systém Q je v stave popísanom normalizovaným vektorom $|\psi\rangle$, kde $\| |\psi\rangle \| = 1 \Rightarrow \langle \psi | \psi \rangle = 1$, potom stredná hodnota pozorovateľnej O je určená maticovým elementom $\langle O \rangle = \langle \psi | O | \psi \rangle$. Ak stav $|\psi\rangle$ je vyjadrený pomocou superpozície (5.10) charakteristických funkcií pozorovateľnej O , potom stredná hodnota $\langle O \rangle$ má tvar

$$\langle O \rangle = \sum_{i,j=1}^n a_i^* a_j \langle \varphi_i | O | \varphi_j \rangle = \sum_{i=1}^n |a_i|^2 \lambda_i \quad (5.12)$$

kde λ_i je charakteristická hodnota pozorovateľnej O . V prípade, že stav $|\psi\rangle = |\varphi_i\rangle$ (hovoríme, že je čistý, v opačnom prípade, ak stav $|\psi\rangle$ je určený lineárnou kombináciou viacerých stavov, hovoríme, že je zmiešaný).

5.2.1 Ilustračný príklad úplnosti a princípu superpozície

Nech unitárny priestor H obsahuje bázu 4 ortonormálnych vektorov

$$\mathcal{B} = \{ |0\rangle, |1\rangle, |2\rangle, |3\rangle \}$$

a nech v tejto báze pozorovateľná O je reprezentovaná maticou

$$O = \begin{pmatrix} 0 & 0 & -2i & 0 \\ 0 & 0 & 0 & 2i \\ 2i & 0 & 0 & 0 \\ 0 & -2i & 0 & 0 \end{pmatrix}$$

Charakteristické hodnoty pozorovateľnej O určíme pomocou sekulárnej rovnice

$$|O - \lambda E| = \begin{vmatrix} -\lambda & 0 & -2i & 0 \\ 0 & -\lambda & 0 & 2i \\ 2i & 0 & -\lambda & 0 \\ 0 & -2i & 0 & -\lambda \end{vmatrix} = 0 \Rightarrow (\lambda^2 - 4)^2 = 0$$

Táto algebraická rovnica má dva reálne korene

$$\lambda_1 = 2 \quad (k_1 = 2)$$

$$\lambda_1 = -2 \quad (k_2 = 2)$$

Charakterické vektory priradené týmto hodnotám sú určené riešením homogénneho systému rovníc

$$(\mathbf{O} - \lambda \mathbf{E})\mathbf{c} = 0$$

Ak $\lambda = \lambda_1$, potom tento homogénny systém má tvar

$$\begin{pmatrix} -2 & 0 & -2i & 0 \\ 0 & -2 & 0 & 2i \\ 2i & 0 & -2 & 0 \\ 0 & -2i & 0 & -2 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{pmatrix} = 0$$

Ak prepíšeme túto maticou rovnicu do zložkového tvaru a vynecháme lineárne závislé rovnice, potom dostaneme

$$c_1 + ic_3 = 0$$

$$c_2 - ic_4 = 0$$

Riešenie týchto rovníc dostaneme má tvar 2-parametrického systému

$$\mathbf{c} = \begin{pmatrix} -iu \\ iv \\ u \\ v \end{pmatrix} = u \begin{pmatrix} -i \\ 0 \\ 1 \\ 0 \end{pmatrix} + v \begin{pmatrix} 0 \\ i \\ 0 \\ 1 \end{pmatrix}$$

Pre $u = i, v = 0$ a $u = 0, v = -i$ dostaneme dva ortogonálne vektory

$$\mathbf{c}_1^{(1)} = \begin{pmatrix} 1 \\ 0 \\ i \\ 0 \end{pmatrix}, \mathbf{c}_2^{(1)} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ -i \end{pmatrix}$$

Podobným spôsobom získame aj charakteristické vektory priradené charakteristickej hodnote λ_2 , výsledky sú zhrnuté v tabuľke

charakteristické hodnoty	charakteristické vektory
$\lambda_1 = 2$	$ \varphi_1^{(1)}\rangle = \frac{1}{\sqrt{2}}(0\rangle + i 2\rangle) = \frac{1}{\sqrt{2}}(1, 0, i, 0)^T$ $ \varphi_1^{(2)}\rangle = \frac{1}{\sqrt{2}}(1\rangle - i 3\rangle) = \frac{1}{\sqrt{2}}(0, 1, 0, -i)^T$
$\lambda_2 = -2$	$ \varphi_2^{(1)}\rangle = \frac{1}{\sqrt{2}}(0\rangle - i 2\rangle) = \frac{1}{\sqrt{2}}(1, 0, -i, 0)^T$ $ \varphi_2^{(2)}\rangle = \frac{1}{\sqrt{2}}(1\rangle + i 3\rangle) = \frac{1}{\sqrt{2}}(0, 1, 0, i)^T$

Spektrálny rozvoj pozorovateľnej O má tvar

$$O = 2(|\varphi_1^{(1)}\rangle\langle\varphi_1^{(1)}| + |\varphi_2^{(1)}\rangle\langle\varphi_2^{(1)}|) + (-2)(|\varphi_1^{(2)}\rangle\langle\varphi_1^{(2)}| + |\varphi_2^{(2)}\rangle\langle\varphi_2^{(2)}|)$$

alebo v maticovej reprezentácii

$$\mathbf{O} = 2 \underbrace{\begin{pmatrix} 1/2 & 0 & -i/2 & 0 \\ 0 & 1/2 & 0 & i/2 \\ i/2 & 0 & 1/2 & 0 \\ 0 & -i/2 & 0 & 1/2 \end{pmatrix}}_{P_1} + (-2) \underbrace{\begin{pmatrix} 1/2 & 0 & i/2 & 0 \\ 0 & 1/2 & 0 & -i/2 \\ -i/2 & 0 & 1/2 & 0 \\ 0 & i/2 & 0 & 1/2 \end{pmatrix}}_{P_2}$$

Lahko sa presvedčíme, že suma týchto projekčných operátorov – matic je jednotková matica

$$P_1 + P_2 = E$$

5.2.2 Ilustračný príklad Pauliho spinových matic

Pauliho spinové matice majú tvar

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

sú príkladom pozorovateľných, ktoré sa často využívajú v kvantovom počítaní. Ich charakteristické systémy sú špecifikované v tabuľke

Pauliho matice	Charakteristické hodnoty/vektory	
$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	+1	$\frac{1}{\sqrt{2}}(0\rangle + 1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$
	-1	$\frac{1}{\sqrt{2}}(0\rangle - 1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$
$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$	+1	$\frac{1}{\sqrt{2}}(0\rangle + i 1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}$
	-1	$\frac{1}{\sqrt{2}}(0\rangle - i 1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}$
$\sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$	+1	$ 0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$
	-1	$ 1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Tak napríklad spektrálny rozklad matice σ_1 má tvar

$$\begin{aligned} \sigma_1 &= (+1) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0| + \langle 1|}{\sqrt{2}} \right) + (-1) \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \left(\frac{\langle 0| - \langle 1|}{\sqrt{2}} \right) \\ &= (+1)|1\rangle\langle 1| + (-1)|-1\rangle\langle -1| \end{aligned}$$

Podľa tejto definície, stav z predchádzajúceho príkladu $|\psi(1)\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$, systému Q, ktorý obsahuje ako podsystemy Q_1 a Q_2 , je entaglovaný; nemôžeme ho vyjadriť pomocou tenzorového súčinu dvoch stavov, ktoré špecifikujú 1-qubitové systémy Q_1 a Q_2 .

5.3 Heisenbergov princíp neurčitosti

Nech kvantový systém Q obsahuje dve pozorovateľné A a B , ktoré medzi sebou nekomutujú, $[A, B]_- \neq 0$, zavedieme dva nové operátory

$$\Delta A = A - \langle A \rangle, \quad \Delta B = B - \langle B \rangle$$

Veta 5.1. Pre pozorovateľné A a B , ktoré spolu nekomutujú, $AB - BA = [A, B] \neq 0$, neurčitosti

$\langle \Delta A \rangle = \sqrt{\langle \psi | (\Delta A)^2 | \psi \rangle}$ a $\langle \Delta B \rangle = \sqrt{\langle \psi | (\Delta B)^2 | \psi \rangle}$ spĺňajú nerovnosť

$$\langle \Delta A \rangle \langle \Delta B \rangle \geq \frac{1}{2} |\langle \psi | [A, B]_- | \psi \rangle| \quad (5.13)$$

Ako dôsledok tejto vety naformulujeme podmienky, kedy pozorovateľné A a B sú súčasne presne merateľné.

Veta 5.2. Pre pozorovateľné A a B môžeme súčasne presne merať pre $\langle \Delta A \rangle = \langle \Delta B \rangle = 0$ vtedy a len vtedy, ak pozorovateľné spolu komutujú, $AB - BA = [A, B] = 0$.

Dôkaz vety 5.1 je založený na Schwartzovej nerovnosti (2.4). Počítajme veličinu

$$\begin{aligned} \langle \Delta A \rangle^2 \langle \Delta B \rangle^2 &= \langle \psi | (\Delta A)^2 | \psi \rangle \langle \psi | (\Delta B)^2 | \psi \rangle \\ &= \langle \Delta A \psi | \Delta A \psi \rangle \langle \Delta B \psi | \Delta B \psi \rangle \\ &= |\Delta A \psi|^2 |\Delta B \psi|^2 \\ &\geq \langle \Delta A \psi | \Delta B \psi \rangle^2 \\ &= (\operatorname{re} \langle \Delta A \psi | \Delta B \psi \rangle)^2 + (\operatorname{im} \langle \Delta A \psi | \Delta B \psi \rangle)^2 \end{aligned} \quad (5.14)$$

kde nerovnosť sme dostali použitím Schwartzovej nerovnosti. Pre reálnu a imaginárnu časť maticového elementu $\langle \Delta A \psi | \Delta B \psi \rangle$ dostaneme

$$\operatorname{re} \langle \Delta A \psi | \Delta B \psi \rangle = \frac{1}{2} (\langle AB + BA \rangle - 2 \langle A \rangle \langle B \rangle)$$

$$\operatorname{im} \langle \Delta A \psi | \Delta B \psi \rangle = \frac{1}{2i} \langle [A, B] \rangle$$

Dosadením týchto výrazov do (5.14) získame heisenbergovu reláciu neurčitosti (5.13).

Dôkaz vety 5.2 pre nutnú a dostatočnú podmienku k súčasnej presnej merateľnosti pozorovateľných A a B je jednoduchý. Z podmienky $\langle \Delta A \rangle = \langle \Delta B \rangle = 0$ priamo plynie podmienka vzájomnej komutovateľnosti pozorovateľných A a B , $[A, B] = 0$. Predpokladajme teraz, že pozorovateľné A a B vzájomne komutujú, potom tieto pozorovateľné majú spoločné vlastné vektory. Nech $|\psi\rangle$ je vlastný vektor pozorovateľných, potom

$$\begin{aligned} \langle \Delta A \rangle &= \sqrt{\langle \psi | (\Delta A)^2 | \psi \rangle} = \sqrt{\langle (A - \langle A \rangle) \psi | (A - \langle A \rangle) \psi \rangle} \\ &= \sqrt{\langle (\lambda - \langle A \rangle) \psi | (\lambda - \langle A \rangle) \psi \rangle} = 0 \end{aligned}$$

kde $A|\psi\rangle = \lambda|\psi\rangle$. Podobným spôsobom dokážeme aj $\langle \Delta B \rangle = 0$, čím sme dokončili dôkaz vety 5.2.

5.4 Meranie

Nech kvantový systém Q s pozorovateľnou O sa nachádza v stave $|\psi\rangle$, ktorý pomocou predpokladu úplnosti charakteristického systému O a princípu superpozície môžeme vyjadriť ako lineárnu kombináciu

$$|\psi\rangle = \sum_{i=1}^n a_i |\phi_i\rangle \quad (2.15)$$

kde $O|\phi_i\rangle = \lambda_i |\phi_i\rangle$, pre $i=1,2,\dots,n$.

Definícia 5.5. Hovoríme, že **meranie** kvantového systému Q v stave $|\psi\rangle$ produkuje charakteristickú hodnotu λ_i s pravdepodobnosťou $|a_i|^2$ vtedy a len vtedy, ak

$$\frac{P_i |\psi\rangle}{\sqrt{\langle \psi | P_i | \psi \rangle}} = |\phi_i\rangle \quad (2.16)$$

Ak platí (2.13), potom pravdepodobnosť $|a_i|^2$ nameranie charakteristickej hodnoty λ_i môžeme alternatívne vyjadriť takto

$$|a_i|^2 = \langle \psi | P_i | \psi \rangle \quad (2.17)$$

Parafrázujúc Diraca [xx] môžeme povedať, že meranie vždy zapríčiňuje skok kvantového systému na charakteristický stav pozorovateľnej O , ktorá je meraná. Ak kvantový systém Q je v stave $|\psi\rangle$, potom meranie môže byť schematicky reprezentované takto

$$|\psi\rangle = \sum_{k=1}^n P_k |\psi\rangle \xrightarrow[\text{prob} = \langle \psi | P_i | \psi \rangle]{\text{prvé meranie}} \frac{P_i |\psi\rangle}{\sqrt{\langle \psi | P_i | \psi \rangle}} \xrightarrow[\text{prob} = 1]{\text{druhé meranie}} \frac{P_i |\psi\rangle}{\sqrt{\langle \psi | P_i | \psi \rangle}}$$

5.4.1 Ilustračný príklad merania

Použijeme pozorovateľnú O z kapitoly 2.2.1. Nech stav kvantového systému Q s pozorovateľnou O je špecifikovaný vektorom

$$|\psi\rangle = \frac{1}{3}(2|0\rangle + 2i|1\rangle - |3\rangle) = \frac{1}{3}(2, 2i, 0, -1)^T$$

Potom meranie vzhľadom ku kvantovému systému Q vzhľadom ku pozorovateľnej O je sumarizované v tejto tabuľke

j	$\text{prob} = \langle \psi P_j \psi \rangle$	charakteristická hodnota λ_j	výsledný stav $P_j \psi\rangle / \sqrt{\langle \psi P_j \psi \rangle}$
0	5/18	+2	$(1/\sqrt{10})(2 0\rangle + i 1\rangle + 2i 2\rangle + 3\rangle)$
1	13/18	-2	$(1/\sqrt{26})(2 0\rangle + 3i 1\rangle - 2i 2\rangle - 3 3\rangle)$

5.4.2 Ilustračný príklad merania

Nech unitárny priestor obsahuje ortonormálnu bázu

$$\mathcal{B} = \{|0\rangle, |1\rangle, \dots, |n-1\rangle\}$$

a nech pozorovateľná O je definovaná ako projektor

$$O = |0\rangle\langle 0|$$

Charakteristický systém tohto operátora je špecifikovaný tabuľkou

charakteristické hodnoty	ortonormálne charakteristické vektory
$\lambda_1 = 1$	$ 1\rangle = \varphi_1\rangle$
$\lambda_2 = 0$	$ 2,1\rangle = \varphi_2\rangle$ $ 2,2\rangle = \varphi_3\rangle$ $ 2,n-1\rangle = \varphi_n\rangle$

Potom ľubovoľný stav $|\psi\rangle$ môže byť vyjadrený takto

$$|\psi\rangle = \sum_{i=1}^n a_i |\varphi_i\rangle$$

kde

$$\sum_{i=1}^n |a_i|^2 = 1$$

Ak je kvantový systém Q meraný vzhľadom k pozorovateľnej O , potom výsledky merania sú uvedené v tabuľke

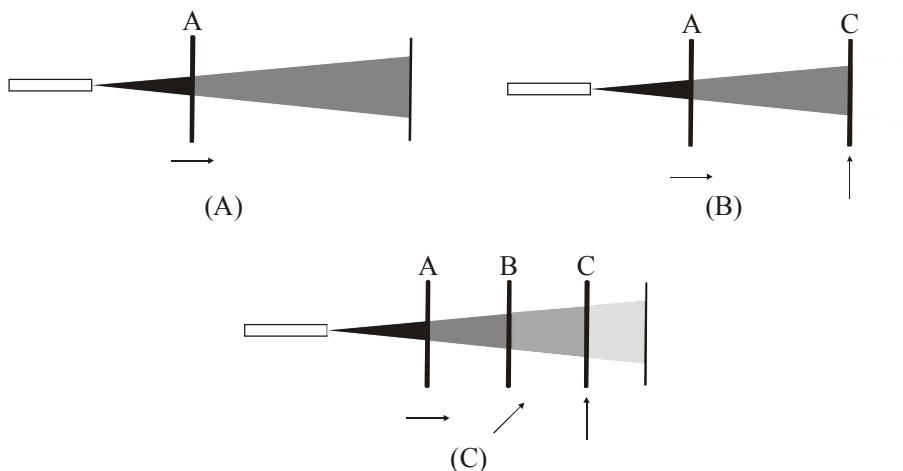
j	$prob = \langle \psi P_j \psi \rangle$	charakteristická hodnota λ_j	výsledný stav $P_j \psi\rangle / \sqrt{\langle \psi P_j \psi \rangle}$
1	$ a_1 ^2$	+1	$ \varphi_1\rangle$
2	$\sum_{i=2}^n a_i ^2$	0	$\sum_{i=2}^n a_i \varphi_i\rangle / \sqrt{\sum_{i=2}^n a_i ^2}$

5.4.3 Ilustračný príklad merania polarizovaných fotónov

Fotóny sú jediné elementárne častice, ktoré môžeme priamo pozorovať. Nasledujúce experimenty sú jednoducho uskutočniteľné pomocou optickej lavice, laserovho zdroja svetla a polarizačných filtrov. Pomocou týchto “fotónových” experimentov ukážeme základné kvantovo-mechanické vlastnosti, ktoré sú potrebné pre pochopenia základných princípov kvantového počítania.

Diagram (A) znázorňuje experiment v ktorom lúč svetla necháme prechádzať svetelným filtrom s horizontálnou polarizáciou. Predpokladáme, že svetlo je náhodne polarizované, výstupná intenzita svetla horizontálne polarizovaného je polovičná vzhľadom k intenzite dopadajúceho svetla. Funkcia filtru nemôže byť vysvetlená ako „sito“, ktoré prepúšťa len fotóny horizontálne polarizované. Prepúšťa ak fotóny, ktoré nie sú horizontálne polarizované, z týchto fotónov vytvára nové fotóny, ktoré už majú horizontálnu polarizáciu. Diagram (B) znázorňuje situáciu z predošlého diagramu, keď za filter A vložíme ešte ďalší filter C, ktorý má vertikálnu polarizáciu. V tomto prípade, žiadny horizontálne polarizovaný fotón už neprejde filtrom C, to znamená, že za týmto filtrom už máme nulovú intenzitu svetla.

V tomto prípade, už môžeme použiť analógiu so sitom, ktoré neprepúšťa horizontálne polarizované fotóny. Konečne, diagram (C) znázorňuje situáciu z predchádzajúceho diagramu, keď za filter B dáme ešte ďalší filter C s vertikálnou polarizáciou. V tomto prípade nastáva situácia, ktorá je v protiklade s našim intuitívnym očakávaním. Podľa našich „intuitívnych“ skúsenosti, vloženie ďalšieho filtra môže mať za dôsledok len zníženie intenzity prechádzajúceho svetla.



Obrázok 5.1. Na jednotlivých diagramoch je znázornený lúč svetla, ktorý je premietaný na projekčnú dosku. Polarizačné filtre A, B a C prepúšťajú svetlo polarizované horizontálne, 45° resp. vertikálne. Tieto filtre sú vkladané do dráhy svetelného lúča.

Diagram A môže byť prepísaný do tvaru merania, kde vstupný fotón má cirkulárnu polarizáciu, prechádza filtrom s horizontálnou polarizáciou s pravdepodobnosťou $\frac{1}{2}$. Túto skutočnosť interpretujeme ako proces merania vzhľadom k vektorom s horizontálnou polarizáciou. Musíme poznamenať, že po procese merania (po prechode polarizačným filtrom) výstupné fotóny s pravdepodobnosťou $\frac{1}{2}$ nemajú vertikálnu polarizáciu.

$$\alpha |\uparrow\rangle + \beta |\rightarrow\rangle \longrightarrow \begin{cases} \text{prob} = |\alpha|^2 \longrightarrow |\rightarrow\rangle \\ \text{prob} = |\beta|^2 \longrightarrow |\rightarrow\rangle \end{cases}$$

Diagram B vznikol z diagramu A tak, že na záver je pridaný ďalší filter s vertikálnou polarizáciou, to znamená, že vykonávame ďalšie meranie vzhľadom k charakteristickému stavu $|\uparrow\rangle$ fotónu s vertikálnou polarizáciou. Pretože predchádzajúce meranie vyprodukovalo fotón v čistom charakteristickom stave s horizontálnou polarizáciou, na záver druhého merania s jednotkovou pravdepodobnosťou nevzniká žiadny stav.

$$\alpha |\uparrow\rangle + \beta |\rightarrow\rangle \longrightarrow \begin{cases} \text{prob} = |\alpha|^2 \longrightarrow |\rightarrow\rangle \\ \text{prob} = |\beta|^2 \longrightarrow |\rightarrow\rangle \end{cases} \longrightarrow \begin{cases} \text{prob} = 1 \longrightarrow \text{žiadny fotón} \end{cases}$$

Konečne, diagram B je rozšírený o tretie meranie, ktoré je zaradené medzi prvé a druhé meranie, pre prehľadnosť uvedieme všetky tri merania:

1. meranie – náhodne vygenerovaný fotón je podrobený meraniu vzhľadom k charakteristickému stavu $|\rightarrow\rangle$ s horizontálnou polarizáciou,
2. meranie – fotón s horizontálnou polarizáciou $|\rightarrow\rangle$, vyprodukovaný prvým meraním, je podrobený meraniu vzhľadom k charakteristickému stavu $|\nearrow\rangle$,
3. meranie – fotón v stave $|\nearrow\rangle$ je podrobený meraniu vzhľadom k charakteristickému vektoru $|\uparrow\rangle$

$$\begin{aligned}
 \alpha |\uparrow\rangle + \beta |\rightarrow\rangle &\longrightarrow \text{detector} \xrightarrow{\text{prob} = |\alpha|^2} |\rightarrow\rangle = \frac{1}{\sqrt{2}} (|\nearrow\rangle + |\searrow\rangle) \longrightarrow \\
 &\longrightarrow \text{detector} \xrightarrow{\text{prob} = 1/2} |\nearrow\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle + |\rightarrow\rangle) \longrightarrow \text{detector} \xrightarrow{\text{prob} = 1/2} |\uparrow\rangle
 \end{aligned}$$

6. prednáška

Kvantová mechanika II – časový vývoj kvantových systémov, entaglované kvantové stavy

6.1 Časový vývoj kvantových systémov

Definícia 6.1. Hovoríme, že v čase t kvantový systém Q je popísaný stavom $|\psi(t)\rangle$ vtedy a len vtedy, ak jeho časový vývoj je popísaný **Schroedingerovou rovnicou**

$$i \frac{\partial}{\partial t} |\psi(t)\rangle = H |\psi(t)\rangle \quad (6.1)$$

operátor H je pozorovateľná nazývaná **hamiltonián** systému Q .

Pre jednoduchosť budeme predpokladať, že študovaný kvantový systém Q je **uzavretý**, t. j. hamiltonián H nezávisí explicitne na čase

$$\frac{\partial H}{\partial t} = 0 \quad (6.2)$$

Schroedingerovu rovnicu (6.1) môžeme pomocou unitárneho **vlnového operátora**

$$|\psi(t)\rangle = U(t) |\psi(0)\rangle \quad (6.3)$$

prepísať do integrálneho tvaru

$$U(t) = e^{-\frac{i}{\hbar} H t} \quad (6.4)$$

Lahko sa presvedčíme, že takto špecifikovaný vlnový operátor vyhovuje Schroedingerovej rovnici (6.1). Unitárnosť operátora (6.4) priamo plynie z predpokladu, že H je hermitovský operátor.

Nech $|\psi_1\rangle$ a $|\psi_2\rangle$ sú dva stavy kvantového systému Q , budeme požadovať, aby tieto stavy boli navzájom spriahnuté pomocou unitárneho operátora

$$|\psi_1\rangle = U |\psi_2\rangle, \text{ alebo } |\psi_2\rangle = U^\dagger |\psi_1\rangle \quad (6.5)$$

Tento predpoklad má zásadnú dôležitosť v teórii kvantového počítania, každá elementárna operácia pri implementácii kvantového počítania musí byť realizovaná pomocou unitárneho operátora. Pretože unitárny operátor musí byť 1-1-značný, tieto elementárne operácie sú vratné – mikoreverzibilné.

Budeme počítať časovú deriváciu strednej hodnoty $\langle O \rangle = \langle \psi | O | \psi \rangle$

$$\begin{aligned}
\frac{d}{dt}\langle O \rangle &= \frac{d}{dt}\langle \psi | O | \psi \rangle = \left\langle \frac{\partial}{\partial t} \psi \middle| O | \psi \right\rangle + \langle \psi | \frac{\partial}{\partial t} O | \psi \rangle + \left\langle \psi | O \middle| \frac{\partial}{\partial t} \psi \right\rangle \\
&= \left\langle -\frac{i}{\hbar} H \psi \middle| O | \psi \right\rangle + \langle \psi | \frac{\partial}{\partial t} O | \psi \rangle + \left\langle \psi | O \middle| -\frac{i}{\hbar} H \psi \right\rangle \\
&= \langle \psi | \underbrace{\left(\frac{i}{\hbar} (HO - OH) + \frac{\partial O}{\partial t} \right)}_{\frac{dO}{dt}} | \psi \rangle = \langle \psi | \frac{dO}{dt} | \psi \rangle
\end{aligned} \tag{6.6}$$

Tento výsledok môžeme formálne zapísať pomocou pojmu „**totálna derivácia pozorovateľnej**“

$$\frac{dO}{dt} = \frac{\partial O}{\partial t} + \frac{i}{\hbar} [H, O] \tag{6.7}$$

kde $[A, B] = AB - BA$ je **komutátor** operátorov A a B . Z tejto formuly vyplýva dôležitá vlastnosť, stredná pozorovateľnej O má nenulovú časovú deriváciu (t. j.) nie je konštantná v čase z dvoch dôvodov, buď explicitne závisí na čase (napr. prítomnosťou externého časovo premenného poľa), alebo, aj keď nezávisí explicitne na čase, nekomutuje s hamiltoniánom systému. Tento druhý dôvod je pre interpretáciu kvantovej mechaniky o mnoho zaujímavejší, k tomu, aby stredná hodnota pozorovateľnej bola konštantná v čase, nesmie samotná pozorovateľná O súčasne explicitne závisieť na čase a taktiež musí komutovať s hamiltoniánom systému.

6.2 Entaglované kvantové stavy

Nech Q_1 a Q_2 sú nezávislé kvantové systémy, ktoré boli pripravené v stavoch $|\psi_1\rangle \in H_1$ a $|\psi_2\rangle \in H_2$, ktoré sú spojené do jedného kvantového systému Q . Stav $|\psi\rangle \in H$ globálneho kvantového systému Q je špecifikovaný pomocou tenzorového súčinu stavov $|\psi_1\rangle \in H_1$ a $|\psi_2\rangle \in H_2$

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \in H = H_1 \otimes H_2$$

6.2.1 Tvorba entaglovaného kvantového stavu

Nech $Q_1, Q_2, \dots, Q_n$ sú nezávislé kvantové systémy, ktorých stavy sú popísané vektormi z unitárnych priestorov

$$H_1 = \text{span}\{|\uparrow_1\rangle, |\rightarrow_1\rangle\}$$

$$H_2 = \text{span}\{|\uparrow_2\rangle, |\rightarrow_2\rangle\}$$

$$\dots\dots\dots H_n = \text{span}\{|\uparrow_n\rangle, |\rightarrow_n\rangle\}$$

V každom tomto unitárnom priestore vytvoríme qubit

$$|\nearrow_1\rangle = \frac{1}{\sqrt{2}}(|\uparrow_1\rangle + |\rightarrow_1\rangle)$$

$$|\nearrow_2\rangle = \frac{1}{\sqrt{2}}(|\uparrow_2\rangle + |\rightarrow_2\rangle)$$

$$|\nearrow_n\rangle = \frac{1}{\sqrt{2}}(|\uparrow_n\rangle + |\rightarrow_n\rangle)$$

Nech Q je globálny kvantový systém, ktorého stav (nazývaný ***n-qubitový register***) je špecifikovaný pomocou tenzorového súčinu stavov z jednotlivých podsystémov

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|\uparrow_1\rangle + |\rightarrow_1\rangle) \otimes \frac{1}{\sqrt{2}}(|\uparrow_2\rangle + |\rightarrow_2\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|\uparrow_n\rangle + |\rightarrow_n\rangle) \\ &= \frac{1}{\sqrt{2^n}}(|\uparrow_1\uparrow_2\dots\uparrow_n\rangle + |\uparrow_1\uparrow_2\dots\rightarrow_n\rangle + \dots + |\rightarrow_1\rightarrow_2\dots\rightarrow_n\rangle) \end{aligned}$$

ktorý patrí do unitárneho priestoru $H = H_1 \otimes H_2 \otimes \dots \otimes H_n$. V teórii kvantového počítania sa tento výsledok často prepisuje pomocou binárnych premenných 0 a 1

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2}}(|0_1\rangle + |1_1\rangle) \otimes \frac{1}{\sqrt{2}}(|0_2\rangle + |1_2\rangle) \otimes \dots \otimes \frac{1}{\sqrt{2}}(|0_n\rangle + |1_n\rangle) \\ &= \frac{1}{\sqrt{2^n}}(|0_10_2\dots0_n\rangle + |0_10_2\dots1_n\rangle + \dots + |1_11_2\dots1_n\rangle) \\ &= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \end{aligned}$$

kde celočíselná premenná x je určená interpretáciu binárneho reťazca $(b_1b_2\dots b_n)$

$$x = b_n + 2b_{n-1} + 2^2b_{n-2} + \dots + 2^{n-1}b_1$$

To znamená, že n -qubitový register **obsahuje superpozíciu všetkých celých čísel** od 0 do 2^n-1 , toto je príklad kvantového masívneho paralelizmu. Táto vlastnosť má však aj jednu nepríjemnú vlastnosť, ak nad n -qubitovým registrom vykonáme meranie, potom tento paralelizmus zmizne a zostane len jeden stav z množiny $\{0,1,2,\dots,2^n-1\}$. Pravdepodobnosť pozorovania jedného stavu je $(1/2)^n$. Výber celého čísla, ktoré je pozorované nie je robený pozorovateľom, ale kvantovým systémom, čo podstatne komplikuje implementáciu algoritmov kvantového počítania.

6.2.2 Dynamika 2-qubitového registra

Podľa postupu z predchádzajúcej kapitoly 2.5.1 vytvoríme 4 stavy 2-qubitového registra

$$\begin{aligned} |0\rangle &= |00\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad |1\rangle = |01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \\ |2\rangle &= |10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \quad |3\rangle = |11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned}$$

Predpokladajme, že počiatočný stav $|\psi\rangle_{t=0}$ nášho 2-qubitového registra má tvar

$$|\psi\rangle_{t=0} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) = \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix}$$

Taktiež predpokladajme, že kvantový systém je popísaný hamiltoniánom, ktorý v báze $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\} = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\}$ má maticovú reprezentáciu

$$\frac{\pi\hbar}{2} \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & 1 \end{pmatrix}$$

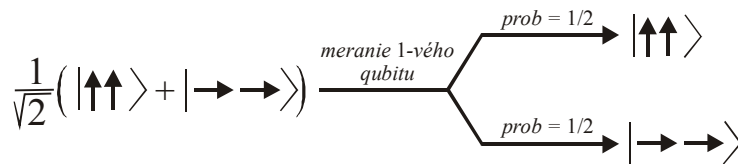
Potom unitárny vlnový operátor má tvar

$$U_{CNOT}(1,0) = e^{-\frac{i}{\hbar}H} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = |0\rangle\langle 0| + |1\rangle\langle 1| + |2\rangle\langle 2| + |3\rangle\langle 3|$$

Potom

$$|\psi(1)\rangle = U(1,0)|\psi(0)\rangle = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ -1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

To znamená, že z počiatočného stavu $|\psi\rangle_{t=0} = 1/\sqrt{2}(|0\rangle - |1\rangle) \otimes |0\rangle = 1/\sqrt{2}(|00\rangle - |10\rangle)$, ktorý bol špecifikovaný pomocou tenzorového súčinu dvoch 1-qubitových stavov, sme aplikovaním unitárneho evolučného operátora dostali nový stav $|\psi(1)\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$, ktorý sa nedá špecifikovať pomocou tenzorového súčinu dvoch elementárnych stavov. Táto skutočnosť môže byť alternatívne vyjadrená tak, že časovou evolúciou pôvodne separované dva qubity stratili svoju identitu, meranie jedného qubitu ovplyvňuje identitu druhého qubitu



Táto skutočnosť je neobvyčajného charakteru a nemá obdobu v našom „klasickom svete“.

6.2.3 Definícia entaglovaných stavov

Definícia 6.2. Nech $Q_1, Q_2, \dots, Q_n$ sú kvantové systémy, ktorých stavy sú charakterizované vektormi z unitárnych priestorov $H_1, H_2, \dots, H_n$. Globálny kvantový systém Q , ktorý obsahuje ako podsystemy $Q_1, Q_2, \dots, Q_n$ sa nazýva **entaglovaný** vtedy a len vtedy, ak jeho stav $|\psi\rangle \in H = \bigotimes_{i=1}^n H_i$ nemôže byť písaný v tvare

$$|\psi\rangle = \bigotimes_{i=1}^n |\psi_i\rangle \quad (6.8)$$

kde $\forall i (|\psi_i\rangle \in H_i)$. Taktiež môžeme povedať, že stav $|\psi\rangle$ je **entanglovaný**.

Podľa tejto definície, stav z predchádzajúceho príkladu $|\psi(1)\rangle = 1/\sqrt{2}(|00\rangle - |11\rangle)$, systému Q , ktorý obsahuje ako podsystemy Q_1 a Q_2 , je entaglovaný; nemôžeme ho vyjadriť pomocou tenzorového súčinu dvoch stavov, ktoré špecifikujú 1-qubitové systémy Q_1 a Q_2 .

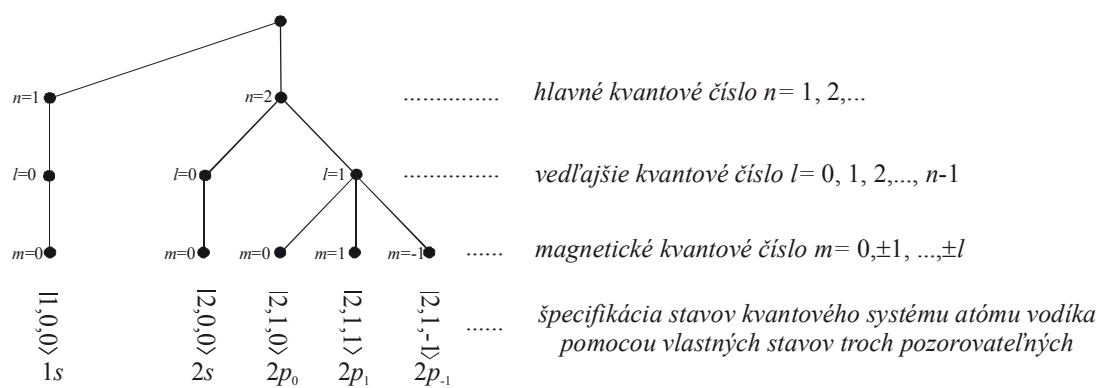
6.3 Úplný súbor komutujúcich pozorovateľných

Určitý formálny problém pri meraní môže vzniknúť s vhodnou interpretáciou takých stavov kvantového systému, ktoré sú degenerované, t. j. sú priradené viacnásobnej vlastnej hodnote. Predpokladajme, že v kvantovom systéme Q máme p pozorovateľných $\mathcal{O} = \{O_1, O_2, \dots, O_p\}$, ktoré sú po dvojiciach komutujúce, $O_i O_j = O_j O_i$, pre $i \neq j$. Systém vlastných hodnôt pozorovateľnej O_i nech je označený $\{\lambda_1^{(i)} < \lambda_2^{(i)} < \dots < \lambda_{n_i}^{(i)}\}$, kde každá vlastná hodnota je uvedená práve raz. Potom každý stav kvantového systému Q môže byť popísaný pomocou vlastných hodnôt množiny pozorovateľných $\mathcal{O}$, $|\lambda_{i_1}^{(1)}, \lambda_{i_2}^{(2)}, \dots, \lambda_{i_p}^{(p)}\rangle$, alebo pre jednoduchosť uvedieme len poradie príslušnej vlastnej hodnoty, $|i_1, i_2, \dots, i_p\rangle = |\mathbf{i}\rangle$, kde $\mathbf{i} = (i_1, i_2, \dots, i_p)$ je p -tica celých čísel. Hovoríme, že množina pozorovateľných $\mathcal{O} = \{O_1, O_2, \dots, O_p\}$ tvorí **úplný systém** vtedy a len vtedy, ak každý kvantový stav systému Q je jednoznačne špecifikovaný vlastnými hodnotami systému $\mathcal{O}$, t. j. nevyskytujú sa také dva rôzne stavy systému, ktoré by boli špecifikované rovnakou p -ticou indexov $\mathbf{i} = (i_1, i_2, \dots, i_p)$.

Definícia 6.3. V každom kvantovom systéme Q existuje **úplný súbor navzájom komutujúcich pozorovateľných** $\mathcal{O} = \{O_1, O_2, \dots, O_p\}$, ktorých vlastné stavy jednoznačne špecifikujú stavy systému Q .

Z tejto definície vyplýva, že ak nejaké dva stavy sú degenerované, potom tieto stavy môžu byť rozlíšené pomocou vlastných hodnôt existujúceho úplného súboru pozorovateľných.

Pre ilustráciu pojmu úplného systému pozorovateľných a jeho použitia pre jednoznačnú špecifikáciu stavov systému, uvažujme atóm vodíka, ktorého stavy sú jednoducho plne špecifikované pomocou trojice operátorov, ktoré pochádzajú z hamiltoniánu systému separovaného vo sférických súradniciach na (1) radiálna časť, (2) angulárna časť a (3) xxxx časť. Z teórie riešenia Schroedingerovej rovnice vyplýva, že stavy systémov sú plne špecifikované ako $|n, l, m\rangle$, kde $n \geq 1$ je hlavné kvantové číslo, $l = 0, 1, \dots, n-1$ je vedľajšie kvantové číslo, a $m = 0, \pm 1, \dots, \pm l$ je magnetické kvantové číslo. Klasifikácia prvých dvoch stavov (degenerovaných s $n = 1$ a $n = 2$) je ukázaná na obrázku.



7. prednáška

Kvantové počítanie I – reverzibilné brány, Toffoliho brána a Fredkinova brány,

Budeme študovať elementárne zariadenia na kvantové počítanie, ktoré sú založené na predpoklade, že uskutočňuje unitárnu transformáciu U , ktorá sa rovná súčinu elementárnych unitárnych transformácií

$$U = U_n U_{n-1} \dots U_2 U_1$$

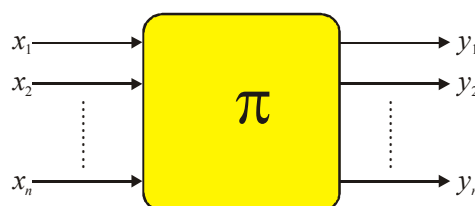
Každá elementárna transformácia U_i je priradená nejakému kroku elementárneho zariadenia na kvantové počítanie. To znamená, že toto klasické výpočtové zariadenia sa budeme snažiť naformulovať pomocou unitárnych transformácií. Pretože unitárne transformácie sú invertibilné (pre unitárnu transformáciu platí $U^+ = U^{-1}$), potom môžeme povedať, že len také klasické výpočtové zariadenia môžu byť formálne diskutované ako kvantové výpočtové zariadenia, ktoré sú reverzibilné. Ak nejaké klasické výpočtové zariadenia je a-priori ireverzibilné, potom nemôže byť interpretované ako nejaká forma kvantového výpočtového zariadenia. Len reverzibilné klasické výpočtové zariadenia má šancu byť implementované na kvantovej úrovni. V nasledujúcej časti tejto kapitoly budeme postupne študovať klasické výpočtové zariadenia, ktoré sú implementované pomocou Boolových funkcií (ich konkrétna realizácia ako výpočtových brán môžete byť uskutočnená pomocou niekoľkých elementárnych brán pre logické spojky AND, OR a NOT), v nasledujúcej časti budeme diskutovať reverzibilné verzie týchto klasických zariadení. V konečnej tretej časti kapitoly budeme diskutovať kvantové brány, ktoré sú implementované pomocou unitárnych operátorov a pôsobia na stavové vektory kvantového systému.

7.1 Klasické výpočtové zariadenie

Uvažujeme klasické výpočtové zariadenie, ktoré je formálne interpretované ako zobrazenie

$$\pi : \{0,1\}^n \rightarrow \{0,1\}^m \quad (7.1)$$

ktoré zobrazuje binárny reťazec $x \in \{0,1\}^n$ dĺžky n na binárny reťazec $y \in \{0,1\}^m$ dĺžky m , pozri obr. 7.1



Obrázok 7.1. Grafická interpretácia klasického výpočtového zariadenia, ktoré chápeme ako Boolovu funkciu (3.1), ktorá priradí n binárnym premenným $x_1, x_2, \dots, x_n$ n binárných argumentov $y_1, y_2, \dots, y_m$.

Boolova algebra poskytuje formálne prostriedky k simulácii ľubovoľnej Boolovej funkcie typu (3.1) pomocou DNF tvaru

$$f(x_1, x_2, \dots, x_n) = \bigvee_{e \in \{0,1\}^n} f(e_1, e_2, \dots, e_n) \wedge x_1^{e_1} \wedge x_2^{e_2} \wedge \dots \wedge x_n^{e_n} \quad (7.2a)$$

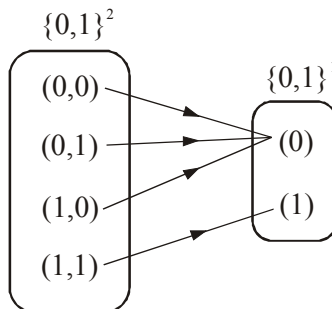
kde

$$x_i^{e_i} = \begin{cases} x_i & (e_i = 1) \\ \bar{x}_i & (e_i = 0) \end{cases} \quad (7.2b)$$

$x_i^{e_i}$ je literál i -tej premennej x_i . Na pravej strane (3.2a) sú aktívne len jednotkové funkčné hodnoty $f(e_1, e_2, \dots, e_n) = 1$, členy s nulovými funkčnými hodnotami, $f(e_1, e_2, \dots, e_n) = 0$, môžu byť ignorované ako nepodstatné. To znamená, že pri konštrukcii Boolovej funkcie pomocou (7.2a) z príslušnej tabuľky funkčných hodnôt berieme používame len riadky s jednotkovou funkčnou hodnotou (čo môže byť výhodné vtedy, ak daná Boolova funkcia obsahuje len niekoľko jednotkových funkčných hodnôt, vo väčšine prípadov má nulové funkčné hodnoty).

7.2 Reverzibilné klasické výpočty

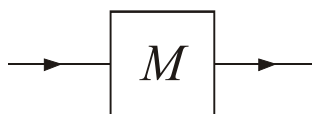
Hlavným nedostatkom Boolovej funkcie zostrojenej v predchádzajúcej kapitole 3.1 je, že nie je reverzibilná, t. j. z jej funkčných hodnôt nie sme schopný jednoznačne priradiť argumenty, pozri obr. 7.2. Podmienka reverzibilita danej funkcie je veľmi dôležitá pre jej implementáciu v prostredí kvantovej teórie, ktorá požaduje, aby daná funkcia bola realizovaná pomocou unitárneho operátora, ktorý je automaticky invertibilný. Tento pomerne tvrdú požiadavku zoslabíme tak, že každá funkcia, ktorá sa použije vo výpočte je invertibilná.



Obrázok 7.2. Znáznornenie Boolovej funkcie AND ako zobrazenia $f: \{0,1\}^2 \rightarrow \{0,1\}^1$, k tomuto zobrazeniu neexistuje inverzné zobrazenie, t. j. funkcia AND nie je reverzibilná.

7.2.1 Reverzibilné 1-bitové brány

Tieto najjednoduchšie brány sú určené transformáciou $\pi: \{0,1\} \rightarrow \{0,1\}$, pozri obr. 7.3.



Obrázok 7.3. Grafická reprezentácia 1-bitovej reverzibilnej brány.

Existujú dve reverzibilné 1-bitové brány, brána identity I a brána negácie N , ktoré sú znázornené pomocou tabuľky

x	Identita (I)	Negácia (N)
0	0	1
1	1	0

7.2.2 Reverzibilné 2-bitové brány

Tieto brány sú určené transformáciou $\pi: \{0,1\}^2 \rightarrow \{0,1\}^2$, pozri obr. 7.4.



Obrázok 7.4.

2-bitovú bránu môžeme špecifikovať pomocou tabuľky

#	argumenty		M_1		M_2		M_{24}	
1	0	0	0	0	0	0	1	1
2	0	1	0	1	1	0	1	0
3	1	0	1	0	0	1	0	1
4	1	1	1	1	1	1	0	0
			$P=I$		$P=(1,2)$		$P=(1,4)(2,3)$	

Z tejto tabuľky vyplýva, že existuje $4!=24$ rôznych 2-bitových reverzibilných brán, ktoré sú jednoznačne určené permutáciou 4 objektov špecifikujúcich dvojicu funkčných hodnôt danej brány.

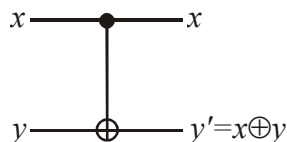
Z binárnych Boolových funkcií môžeme vyjadriť pomocou reverzibilných brán logickú spojku XOR

$$M_{XOR} : (x, y) \rightarrow (x, x \oplus y) \quad (7.3)$$

V tabuľke sú uvedené jednoduché ilustračné príklady 2-bitových brán, ktoré sú priradené logickým spojkám AND, OR a IMP

#	(x,y)	$(x, f_{XOR}(x,y))$
1	(0,0)	(0,0)
2	(0,1)	(0,1)
3	(1,0)	(1,1)
4	(1,1)	(1,0)

Grafická interpretácia tohto reverzibilného obvodu je znázornená na obr. 7.5. Alternatívny názor tohto 2-bitovej brány je brána riadenej negácie (C_{NOT}), hodnota prvej premennej x špecifikuje, či druhá premenná y bude negovaná (pre $x = 1$) alebo nebude negovaná (pre $x = 0$).



Obrázok 7.5.

Každá reverzibilná 2-bitová brána môže byť kompletne popísaná pomocou permutácie vstupných binárnych dvojíc na výstupné binárne dvojice. Tak napríklad, 2-bitová brána C_{NOT} je charakterizovaná permutáciou (pozri vyššie uvedenú tabuľku) $P = (3,4)$. Pre ilustráciu tohto prístupu uvažujme permutácie $P = (1,2)(3,4)$, tabuľka vstupných a výstupných binárnych dvojíc pre túto permutáciu má tvar

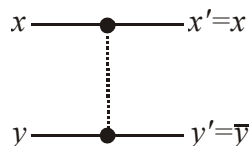
#	(x,y)	(x',y')
1	(0,0)	(0,1)
2	(0,1)	(0,0)
3	(1,0)	(1,1)
4	(1,1)	(1,0)

kde tretí stĺpec sme zostrojili z druhého stĺpca tak, že sme prehodili prvý - druhý a tretí - štvrtý riadky. Výstupné premenné sú ohodnotené Boolovými funkciami, ktoré sú zostrojené štandardným postupom

$$x' = x\bar{y} + xy = x$$

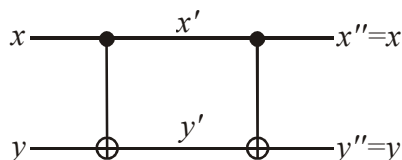
$$y' = \bar{x}\bar{y} + x\bar{y} = \bar{y}$$

To znamená, že táto reverzibilná 2-bitová brána na prvom výstupe má vstupnú premennú x a na druhom výstupe negovanú premennú $\bar{y}$, pozri obr. 7.6.

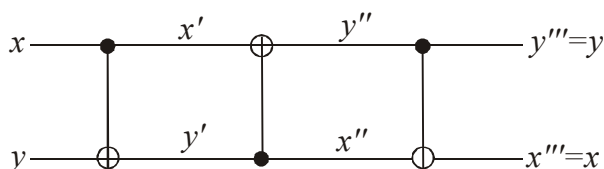


Obrázok 7.6.

Bránu C_{NOT} môžeme medzi sebou kombinovať rôznymi spôsobmi. Napríklad opakované prepojenie tejto brány dáva identitu, pozri obr. 7.7.



Obrázok 7.7. Medzi výsledok je špecifikovaný $x' = x, y' = x \oplus y$, potom pre konečné výsledky platí $x'' = x, y'' = x \oplus (x \oplus y)$. Pretože operácia XOR je asociatívna, formulu pre y'' môžeme zjednodušiť, $y'' = x \oplus (x \oplus y) = \underbrace{(x \oplus x)}_0 \oplus y = y$.



Obrázok 7.8. Trojnásobné použitie brány C_{NOT} , ktoré vedie k „transpozícii“ binárneho výstupu.

Trojnásobné použitie brány C_{NOT} znázornené na obr. 7.8 vedie k transpozícii vstupných binárnych argumentov ako výstupných binárnych premenných. Dôkaz tejto vlastnosti je pomerne jednoduchý, postupne (pomocou troch krokov) budeme počítať binárne veličiny (x', y') , (x'', y'') a (x''', y''') :

1. krok: $x' = x, y' = x \oplus y$
2. krok: $x'' = y' = x \oplus y, y'' = y' \oplus x' = (x \oplus y) \oplus x = y$
3. krok: $x''' = y'' \oplus x'' = y \oplus (x \oplus y) = x, y''' = y'' = y$

7.2.3 Reverzibilné 3-bitové brány

Konštrukcia 3-bitových reverzibilných brán $\pi: \{0,1\}^3 \rightarrow \{0,1\}^3$, bola navrhnutá Toffolim a Fredkinom. Ich postup vysvetlíme pomocou jednoduchého ilustračného príkladu funkcie AND, ktorá je špecifikovaná na obr. 7.1. Táto funkcia $f_{AND}: \{0,1\}^2 \rightarrow \{0,1\}$ je v explicitnom tvare určená formulou $f_{AND}(x_1, x_2) = y$, kde x_1, x_2 sú binárne argumenty – premenné a y je funkčná hodnota. Definujme funkciu $\tilde{f}_{AND}: \{0,1\}^3 \rightarrow \{0,1\}^3$, ako rozšíreniu pôvodnej funkcie f_{AND} takto

$$\tilde{f}(x_1, x_2, z) = (x_1, x_2, z \oplus f(x_1, x_2)) \quad (3.3)$$

kde symbol $\oplus$ reprezentuje binárnu operáciu XOR (eXclusive OR). Tento prístup môžeme pomocou dvoch tabuliek vyjadriť takto

x_1	x_2	z	#
0	0	0	0
0	1	0	2
1	0	0	4
1	1	0	6
0	0	1	1
0	1	1	3
1	0	1	5
1	1	1	7

x_1	x_2	$z \oplus f_{AND}(x_1, x_2)$	#
0	0	0	0
0	1	0	2
1	0	0	4
1	1	1	7
0	0	1	1
0	1	1	3
1	0	1	5
1	1	0	6

Ľavá tabuľka rozšírenie dvoch argumentov x_1 a x_2 o ďalší tretí pomocný argument z , ktorý „riadi“ výsledky uvedené v pravej tabuľke pomocou binárnej operácie XOR. Ak pomocný argument $z = 0$ ($z = 1$), potom v treťom stĺpci pravej tabuľky sú uvedené výsledky binárnej operácie AND (Negácie AND, ktorá sa preto občas nazýva NAND, alebo v klasickej logike sa nazýva Shefferov symbol). Pravá a aj ľavá tabuľka v poslednom stĺpci (označenom symbolom #) obsahujú celočíselnú interpretáciu prvých troch binárnych čísel, potom symbol (3.3) môžeme interpretovať pomocou súčiny transpozícií jednotlivých riadkov v tabuľke, napríklad v tomto prípade tabuľka je jednoznačne špecifikovaná permutáciou symbolom

$$P = (6,7) \quad (7.4)$$

To znamená, že tabuľku môžeme zostrojiť tak, že vedľa seba napíšeme všetkých 8 binárnych trojíc (argumentov resp. funkčných hodnôt) a prehodíme medzi sebou dva riadky, ktoré majú celočíselnú interpretáciu 6 a 7.

Na rozdiel od 2-bitových reverzibilných brán, Toffoliho brána je univerzálna pre výrokovú logiku. Pre zjednodušenie formulácie tejto skutočnosti definujeme funkciu T , ktorá má tri argumenty

$$T(x_1, x_2, y) = (x_1, x_2, y \oplus x_1 x_2)$$

kde súčin $x_1 x_2$ reprezentuje konjunkciu daných binárnych premenných (výrokov). Ľahko sa presvedčíme, že Toffoliho brána má iniverzálny charakter, pomocou nej môžeme zostrojiť základné logické spojky:

spojka NOT

$$T(1, 1, y) = (1, 1, \overline{y})$$

spojka AND

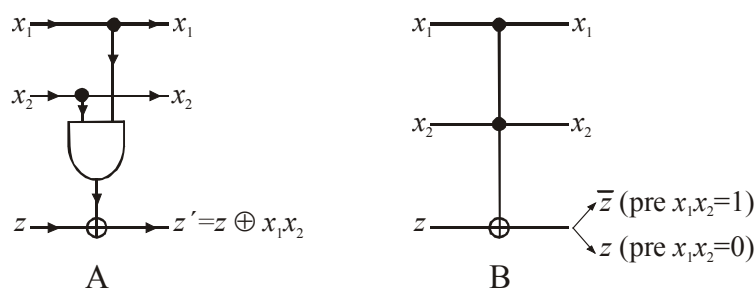
$$T(x_1, x_2, 0) = (x_1, x_2, \boxed{x_1 x_2})$$

spojka OR (dvojkroková konštrukcia)

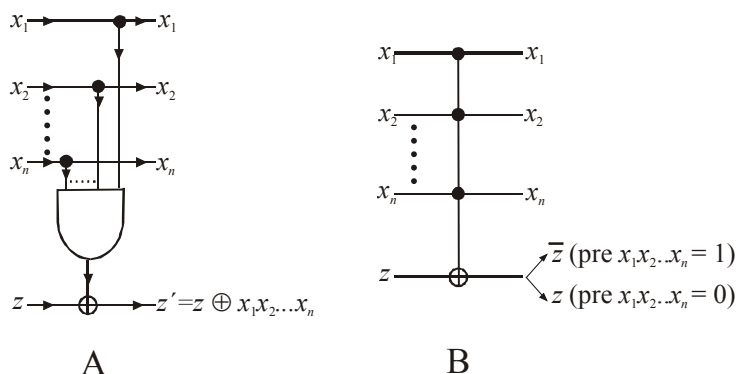
$$T(\overline{x}, \overline{y}, 0) = (\overline{x}, \overline{y}, \boxed{\overline{x} \overline{y}}) \Rightarrow T(1, 1, \overline{x} \overline{y}) = (1, 1, \boxed{x + y})$$

Týmto sme dokázali, že pomocou Toffoliho 3-bitovej reverzibilnej brány sme schopný simulovať ľubovoľnú Boolovu funkciu.

Diagramatické znázornenie Toffoliho brány je na obr. 7.9.

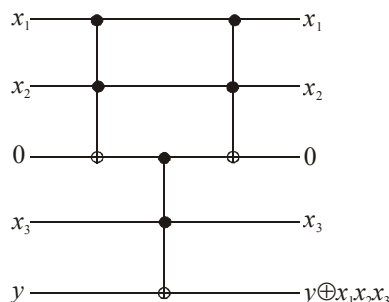


Obrázok 7.9. Znázornenie Toffoliho brány (taktiež často nazývaná CC_{NOT} brána, dvakrát kontrolované NOT). Diagram (A) znázorňuje „klasickú“ realizáciu Toffoliho brány, ktorá je založená na použití brány konjunkcie (dobré známej z teórie logických obvodov). Diagram (B) je zjednodušenie diagramu (A).



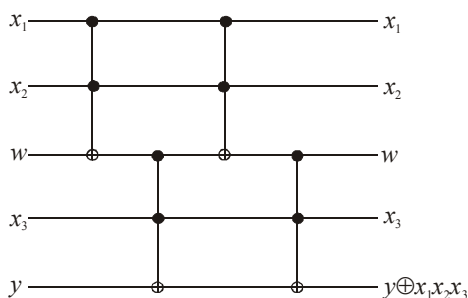
Obrázok 7.10. Zovšeobecnená Toffoliho reverzibilná brána obsahujúca $(n+1)$ vstupných binárnych premenných, posledná vstupná premenná z je negovaná vtedy a len vtedy, ak konjunkcia prvých n vstupných premenných sa rovná 1.

Univerzálnosť Toffoliho brány môže byť chápaná nielen ako možnosť vyjadrenia pomocou nej základných logických spojok, ale taktiež aj možnosť vyjadriť každú reverzibilnú n -bitovú funkciu pomocou kombinácie Toffoliho 3-bitových brán. K tomu, aby sme demonštrovali túto skutočnosť, vykonáme formuláciu zovšeobecnených n -bitových Toffoliho brán. Táto univerzálnosť spočíva v tom, že pomocou tejto „elementárnej“ bráni sme schopný zostrojiť n -bitovú Toffoliho bránu (kde $n > 3$), pozri obr. 7.11.



Obrázok 7.11. Znázornenie rekonštrukcie zovšeobecnenej Toffoliho brány pre $n = 3$, pričom brána obsahuje prostredný spoj s nulovou premennou. Cieľom tretej Toffoliho brány je vynulovanie premennej späť do jej nulovej hodnoty.

Ak túto schému z obr. 7.11 rozšírime o štvrtú Toffoliho bránu, potom výsledky celkovej siete nebudú závislé od skutočnosti, či počiatočná hodnota prostredného bitu je nulová alebo nie, pozri obr. 7.12.



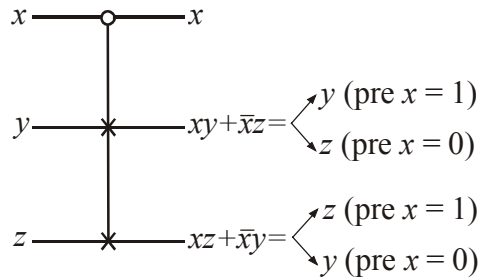
Obrázok 7.12. Modifikovaná rekonštrukcia z obr. 7.11, ktorá má navyše štvrtú Toffoliho bránu, potom výsledok celkovej brány už nie je závislý od hodnoty binárnej premennej w .

Pre úplnosť budeme študovať ešte Fredkinovu 3-bitovú reverzibilnú bránu, ktorá má použitie v ilustrácii reverzibilných brán pomocou biliardových gúľ (pozri nasledujúcu kapitolu). **Fredkinova brána** je špecifikovaná tabuľkou

x	y	z	x'	y'	z'
0	0	0	0	0	0
0	0	1	0	1	0
0	1	0	0	0	1
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	0
1	1	1	1	1	1

Prvá vstupná premenná x je riadiaca, podľa jej hodnoty (ak $x = 1$) dochádza na výstupe k transpozícii premenných y a z , t. j. $z' = y, y' = z$, pozri obr. 7.13. Pomocou výrokových formúl môžeme Fredkinovu bránu vyjadriť takto:

$$\begin{aligned} F(x, y, z) &= (x, \bar{x}z + xy, \bar{x}y + xz) \\ x' &= x, \\ y' &= \bar{x}\bar{y}z + \bar{x}yz + xy\bar{z} + xyz = \bar{x}(\bar{y} + y)z + xy(z + \bar{z}) = \bar{x}z + xy \\ z' &= \bar{x}y\bar{z} + \bar{x}yz + x\bar{y}z + xyz = \bar{x}y(\bar{z} + z) + x(\bar{y} + y)z = \bar{x}y + xz \end{aligned}$$



Obrázok 7.13. Diagramatická špecifikácia Fredkinovej brány, ktorá pôsobí ako podmienený prepínač, ak vstupná premenná $x = 0$ ($x = 1$), potom na výstupe druhá a tretia premenná sú prehodené. $y \rightarrow z, z \rightarrow y$, (zostávajú zachované, $y \rightarrow y, z \rightarrow z$).

Podobne ako Toffoliho brána, aj Fredkinova brána má univerzálny charakter, pomocou tejto brány môžeme generovať základne logické spojky:

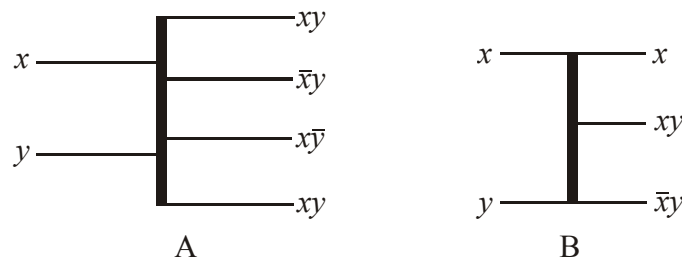
spojka OR: $F(x, 1, z) = (x, \boxed{x+z}, \bar{x} + z),$

spojka AND $F(x, y, 0) = (x, \boxed{xy}, \bar{x}y),$

spojka NOT $F(x, 1, 0) = (x, x, \boxed{\bar{x}}).$

Výstupné argumenty Fredkinovej brány, ktoré sú zarámované obdĺžnikom, sú interpretované ako výsledok brány, ostatne výstupné argumenty sú interpretované ako „odpad“.

Fredkinova brána sa obvykle interpretuje pomocou dvoch jednoduchších reverzibilných brán, ktoré sa nazývajú interakčná brána a prepínaná brána, pozri obr. 3.13.



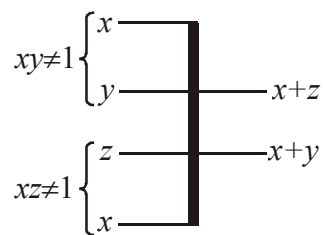
Obrázok 7.14. Reverzibilná (A) interakčná brána a (B) prepínaná brána.

Je potrebné zdôrazniť, že obe tieto brány, aj keď majú rozdielny počet vstupov a výstupov, sú reverzibilné, čo sa jednoducho overí z ich tabuľkových špecifikácií.

argumenty			interakčná brána				prepínaná brána		
#	x	y	xy	$\bar{x}y$	$x\bar{y}$	$\bar{x}\bar{y}$	x	xy	$\bar{x}y$
1	0	0	0	0	0	0	0	0	0
2	0	1	0	1	0	0	0	0	1
3	1	0	0	0	1	0	1	0	0
4	1	1	1	0	0	1	1	1	0

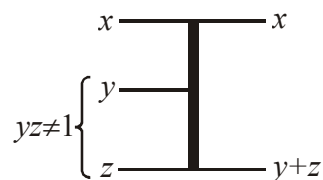
Z tejto tabuľky vyplýva, že vzťah medzi argumentmi a funkčnými hodnotami je 1-1-značný, čiže obe tieto brány sú reverzibilné.

Inverzná interakčná brána je znázornená na obr. 7.15.



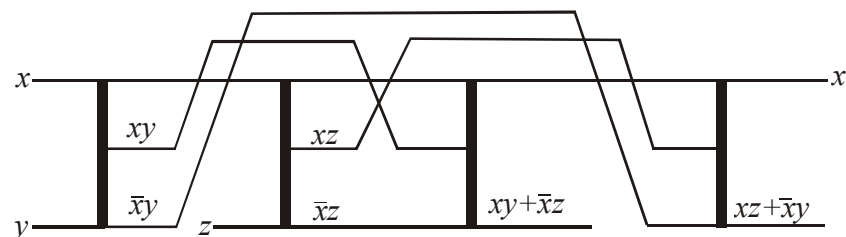
Obrázok 7.15. Inverzná interakčná brána vytvára súčet prvého a tretieho resp. prvého a druhého argumentu, vstupné argumenty sú ohraničené podmienkami $xy \neq 1$ a $xz \neq 1$.

Podobným spôsobom môžeme zostrojiť aj inverznú prepínanú bránu, ktorá taktiež môže slúžiť pre tvorbu súčtu druhého a tretieho argumentu, $y + z$, za predpokladu, že ich súčin sa nerovná jednej, $yz \neq 1$, pozri obr. 7.16.



Obrázok 7.16. Inverzná prepínaná brána slúži pre tvorbu súčtu druhého a tretieho argumentu, pričom ich súčin sa nerovná 1.

Pomocou štyroch prepínaných brán môžeme vytvoriť Fredkinovu bránu tak, že najprv použijeme dve „priame“ prepínané brány pre tvorbu súčinov argumentov a ich negácií, potom použijeme dve inverzné prepínané brány pre tvorbu súčtov, ktoré boli vytvorené predtým, pozri obr. 7.17. Ľahko sa presvedčíme, že podmienka nerovnosti súčinu druhého a tretieho argumentu jednej je v tomto prípade splnená. Podobným spôsobom môžeme zostrojiť aj Fredkinovu bránu pomocou štyroch (dvoch priamych a dvoch inverzných) inverzných brán.



Obrázok 7.17. Konštrukcia Fredkinovej brány pomocou štyroch prepínaných brán.

8. prednáška

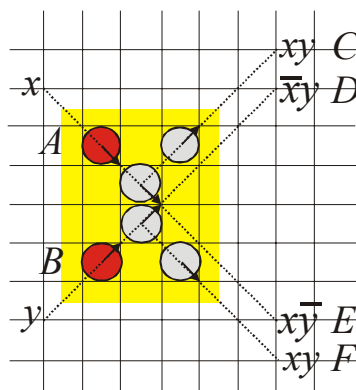
Kvantové počítanie II – výpočty pomocou biliardových gúl, model celulárnych automatov

8.1 Klasický model reverzibilného výpočtu pomocou biliardových gúl

Ilustračný model výpočtu pomocou biliardových gúl, ktorý bol navrhnutý Fredkinom a Toffolim, je názorným príkladom „gedanken“ experimentu, ktorý vo vede zohral a zohráva dôležitú úlohu. V súvislosti s kvantovým počítaním pripomeňme slávnu publikáciu Alberta Eisteina, Borisa Podolského a Nathana Rosena z r. 1935, ktorá sa zaoberala „gedanken“ experimentu s *entaglovanými* časticami a ktorá zohrala veľkú úlohu pri precizovaní pojmového aparátu kvantovej mechaniky a jej interpretácie pre potreby kvantového počítania.

Model počítania pomocou biliardových gúl je založený na fyzikálnych zákonoch pružného rázu. Predpokladá sa, že pre vhodnú počiatočnú konfiguráciu gúl, ktorých poloha evoluje v čase podľa známych fyzikálnych zákonitostí dokonalého rázu, uskutočňuje sa špecifický výpočet (prinajmenšom môžeme povedať, že systém počíta svoje budúce stavy).

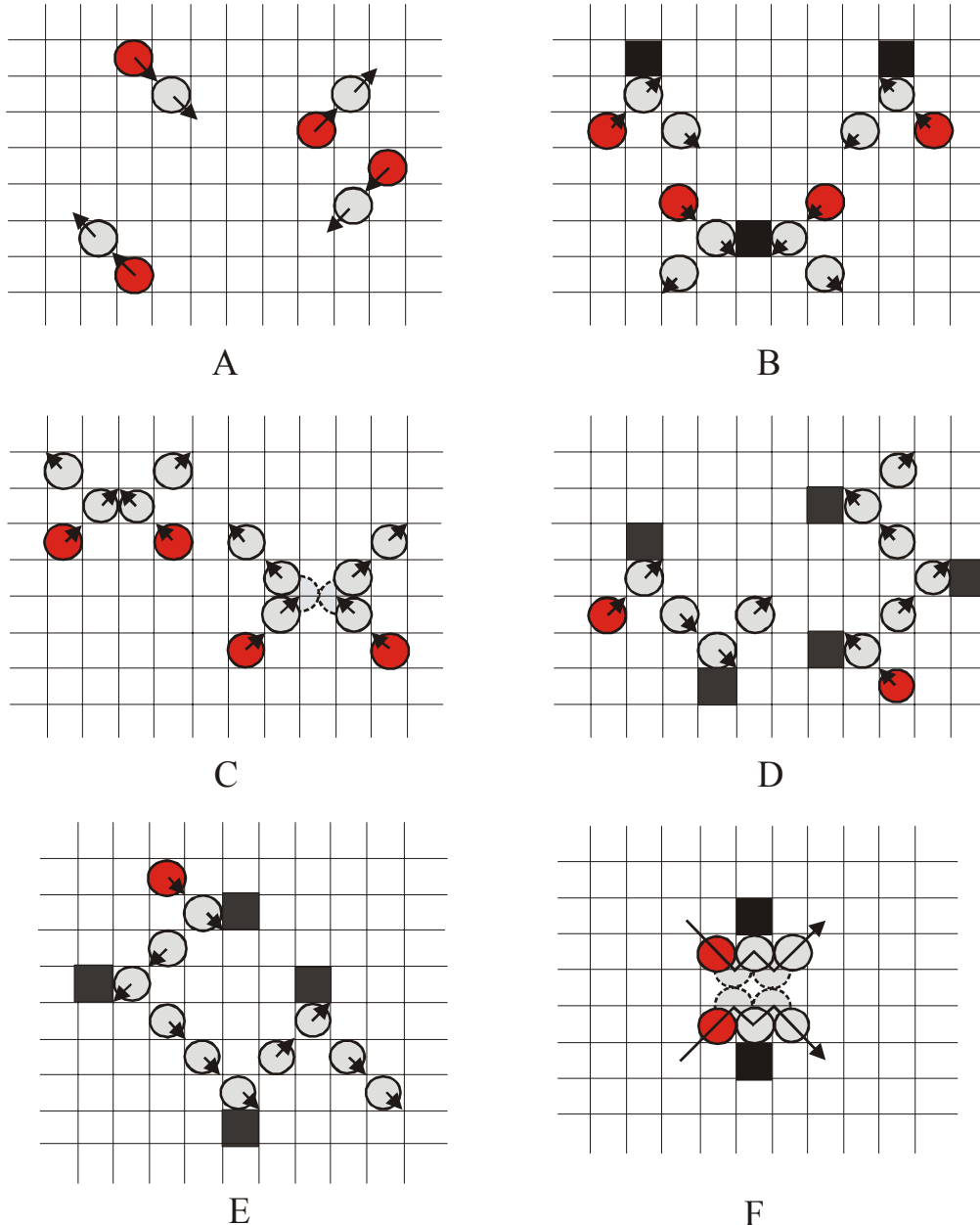
Interakčná brána (obr. 7.14 je v tomto prístupe modelovaná pomocou elementárneho aktu interakcie-zrážky dvoch biliardových gúl, pozri obr. 8.1. Tento experiment môže byť jednoducho špecifikovaný pomocou dvojice Boolových premenných x a y , ich pravdivostná hodnota určuje či vo východiskovom postavení v pozíciách existujú červené biliardové gule s vhodnými hybnosťami v polohách A resp. B. Ak sú obe premenné pravdivé, potom na výstupe obe gule sa v určitom následnom čase $t = 3$ nachádzajú v polohách C a F. Ak $x = 1$ a $y = 0$ v čase $t = 1$ (guľa B neexistuje), potom výsledná pozícia v čase $t = 3$ je E (t. j. guľa z A sa pohybuje priamočiaro, nezúčastnila sa aktu pružnej zrážky s druhou guľou).



Obrázok 8.1. Dokonalá elastická zrážka dvoch biliardových gúl simuluje interakčnú bránu znázornenú na obr. 7.14. Binárne premenné x a y špecifikujú, či v čase $t = 1$ sa v daných východiskových polohách nachádza prvá resp. druhá guľa. K elementárnemu aktu zrážky dochádza v čase $t = 2$. Výsledné polohy v čase $t = 3$ sú špecifikované súčinnami binárnych premenných $xy, \bar{x}y, x\bar{y}, xz$.

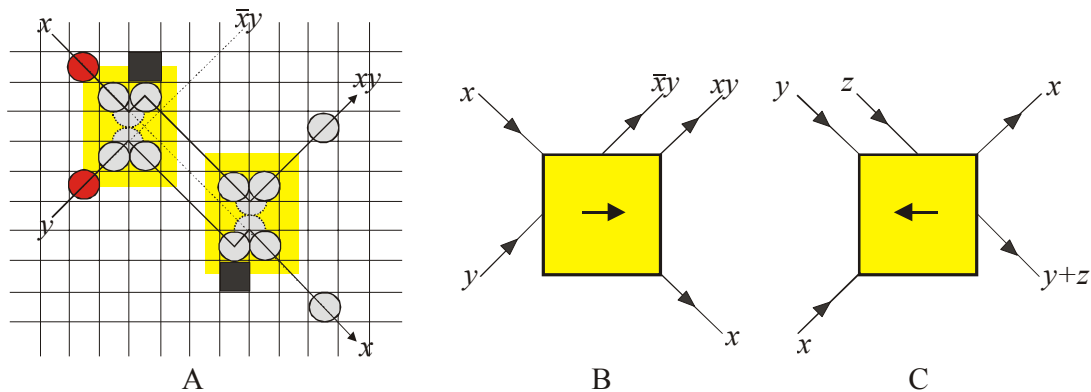
Jednotlivé elementárne situácie, ktoré sa môžu vyskytovať pri modelovaní výpočtu pomocou biliardových gúl sú znázornené na obr. 8.2. Vhodnou kombináciou týchto

elementárnych situácií môžeme vytvárať zložité výpočtové zariadenia, ktoré simulujú Boolové funkcie. Pretože dá sa ukázať, že Fredkinova brána je univerzálne výpočtové zariadenie, ktoré je, ako bude ukázané neskoršie, simulovateľné pomocou biliardových gúl, môžeme konštatovať, že tento prístup k výpočtom je ekvivalentný s Turingovým strojom.



Obrázok 8.2. Prostredie v ktorom sa pohybujú biliardové gule je reprezentované ortogonálnou mriežkou, gule sa môžu pohybovať len po diagonálach ortogonálnej oblasti. Čase t sa guľa nachádza v danej štvorcovej oblasti, prechod gule pri zmene času $t \rightarrow t+1$ sa deje tak, že obsadí voľné štvorcové mieste, ktoré je susedné po „diagonále“ s pôvodným miestom. Gule vo východnej pozícii sú označené červenou farbou. Niektoré oblasti prostredia sú permanentne obsadené „prekážkami“, ktoré sú reprezentované čiernou farbou a ktoré slúžia ako „reflektor“ pre odraz. Počiatočná poloha gule je znázornená červenou farbou, smer pohybu gule je špecifikovaný malou šipkou, zmena pohybu gule (pri odraze) je reprezentovaná zmenou orientácie šipky. Šesť základných foriem pohybu biliardových gúl: (A) priamočiary pohyb, guľa neinteraguje so svojim okolím, (B) odraz od reflektora (prekážky), guľa v dôsledku odrazu mení smer svojej dráhy, (C) pružný náraz dvoch gúl, (D) posun dráhy gule o dve jednotky v dôsledku dvojnásobného odrazu od reflektora, (E) pozdržanie gule v dôsledku štyroch odrazov od reflektorov a (F) kríženie dvoch dráh v dôsledku dvoch pružných zrážok a dvoch odrazov od reflektorov (efektívne pôsobí ako vzájomná výmena gúl).

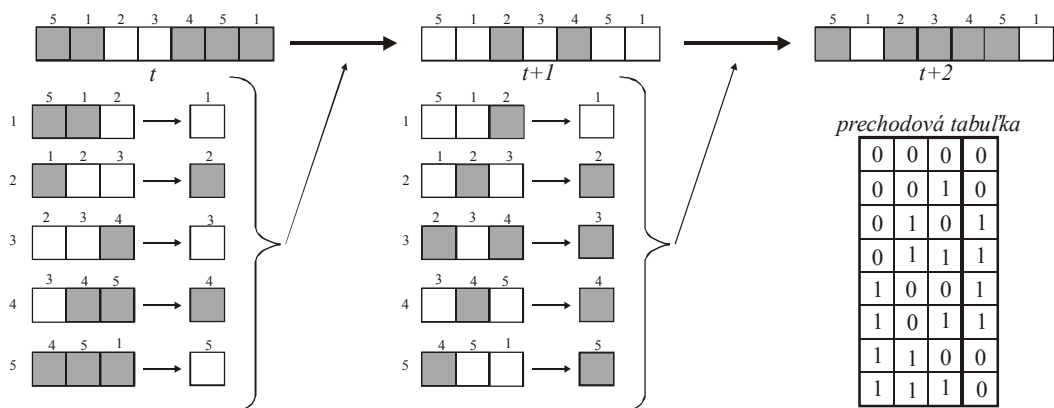
Implementácia elementárnej prepínanej brány pomocou biliardových gúľ je znázornená na obr. 8.3. Táto elementárna brána môže slúžiť ako „stavebný element“ pre konštrukciu Fredkinovej brány (pozri obr. 7.16). Pretože Fredkinova brána má univerzálny charakter (pomocou nej môžu byť definované elementárne binárne operácie Boolovej algebry), potom môžeme konštatovať, že ľubovoľná Boolova funkcia je vypočítateľná pomocou implementácie založenej na biliardových guliach, čím sa dostávame k náznaku dôkazu ekvivalentnosti s Turingovým strojom.



Obrázok 8.3. Diagram A znázorňuje prepínanú bránu implementovanú pomocou výpočtového modelu biliardových gúľ, vľavo sú umiestnené dve gule v počiatočnej polohe, ktoré sú špecifikované Boolovými premennými x a y . Vpravo na priamkach modelu sú umiestnené výstupné biliardové gule, ktoré reprezentujú výsledok výpočtu tejto elementárnej brány. Pretože prepínaná brána je reverzibilná, jednoduchou reorientáciou dráh dostaneme inverznú bránu znázornenú na diagrame B.

8.2. Celulárne automaty

Svet celulárneho automatu je realizovaný pomocou ortogonálnej štvorcovej mriežky obsahujúcej malé a pravidelne sa opakujúce oblasti - bunky. Každá bunka je v jednom z dvoch stavov $\{0,1\}$; ak je v nulovom (jednotkovom) stave, potom táto oblasť je vyfarbená bielou (čiernou) farbou, pozri obr. 8.4.



Obrázok 8.4. Jednoduchý 1-rozmerný celulárny automat obsahujúci 5 buniek vedľa seba, ktoré sú usporiadané do kružnice tak, že prvá a piata bunka sú susedné. Zmeny stavov sú špecifikované prechodovou tabuľkou, ktorá obsahuje 2^3 riadkov. Každý riadok tejto tabuľky popisuje zmenu vybranej bunky, ktorej stav (binárne hodnoty ľavej bunky, strednej – t. j. danej bunky, pravej bunky) tvorí argument prechodovej funkcie, výsledná binárna hodnota popisuje špecifikuje výsledný stav danej bunky. Tento proces je znázornený v prvom riadku obrázku, kde celulárny automat v čase t je zmenený na stav v čase $t+1$, ktorý je ďalšom kroku zmenený na stav v čase $t+2$.

Nech $x_i^{(t)} \in \{0,1\}$ reprezentuje stav i -tej bunky v čase t , potom jej stav v nasledujúcom čase je určený pomocou prechodovej funkcie $f: \{0,1\}^k \rightarrow \{0,1\}$, ktorá okoliu i -tej bunke a jej najbližšiemu okoliu priradí nový stav

$$x_i^{(t+1)} = f(\Gamma_i^{(t)})$$

Pre 1-rozmerný celulárny automat z obr. 8.4 prvých niekoľko aplikácií tejto formuly má tvar

$$\begin{aligned} x_1^{(t+1)} &= f\left(\underbrace{x_5^{(t)}, x_1^{(t)}, x_2^{(t)}}_{\Gamma_1^{(t)}}\right) = f(1,1,0) \\ x_2^{(t+1)} &= f\left(\underbrace{x_1^{(t)}, x_2^{(t)}, x_3^{(t)}}_{\Gamma_2^{(t)}}\right) = f(1,0,0) \\ &\dots\dots\dots \\ x_5^{(t+1)} &= f\left(\underbrace{x_4^{(t)}, x_5^{(t)}, x_1^{(t)}}_{\Gamma_5^{(t)}}\right) = f(1,1,1) \end{aligned}$$

Takto formulovaný celulárny automat môže byť jednoducho zovšeobecnený na viacrozmenný celulárny automat, kde bunky majú svojich susedov v 2- alebo viac-rozmernom priestore. Najznámejšie celulárne automaty sú 2-rozmerné, ktoré sa stali v informatike populárnymi vďaka hre „Život“. V tejto hre pre každú bunku platia tieto jednoduché pravidlá:

- (1) ak čierna bunka má dvoch alebo troch čiernych susedov, potom zostáva čierna,
- (2) ak biela bunka má troch čiernych susedov, potom sa zmení na čiernu bunku a
- (3) ak čierna bunka má jedného alebo štyroch čiernych susedov, potom sa zmení na bielu bunku,
- (4) ak biela bunka má jedného, dvoch alebo štyroch, potom si zachováva bielu farbu.

Aj napriek skutočnosti, že tieto pravidlá pre obnovu buniek v hre „Život“ sú extrémne jednoduché, v priebehu hry vzniká obrovská rôznorodosť, ktorá sa pohybuje na hrane medzi náhodnosťou a poriadkom. Jedna z najzaujímavejších čŕt tejto hry je výskyt „klzákov“, čo sú špeciálne obrazce čiernych buniek, ktoré sa dokážu pohybovať po diagonálach mriežky celulárneho automatu. Celulárny automat je možné usporiadať tak, že pomocou vzájomnej interakcie medzi klzákmi dochádza k výpočtom. Táto skutočnosť viedla k formulácii dôležitej vlastnosti hry „Život“, že môže emulovať univerzálny Turingov počítač.

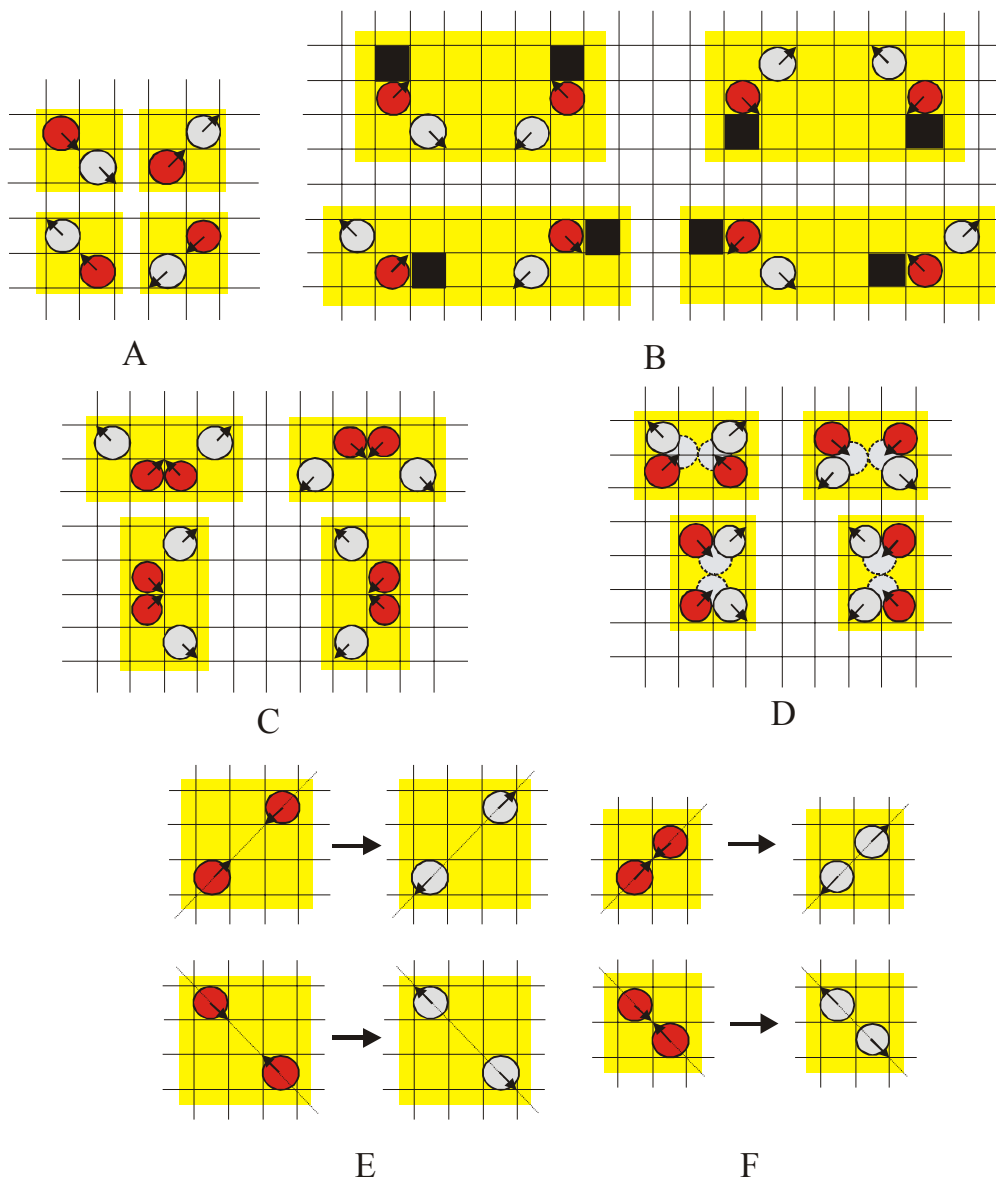
8.2.1 Biliardové gule a celulárne automaty

Svet celulárneho automatu biliardových guľ je realizovaný pomocou 2-rozmernej ortogonálnej mriežky pravidelných štvorcových buniek. Stav buniek je v tomto prípade o trochu zložitejší ako v štandardných celulárnych automatoch, kde sa obvykle rozlišujú len dva stavy (biely a čierny):

1. stav – bunka je neobsadená,
2. stav – bunka je obsadená guľou, pričom pohyb gule je určený jedným zo štyroch možných smerov (smer severozápadný ↖, severovýchodný ↗, juhozápadný ↙ a juhovýchodný ↘)

3. stav – bunka je obsadená pevnou čiernou kockou, ktorá je fixná pre celú evolúciu automatu a ktorá slúži ako „reflektor“ pre pohyb gúľ.

Stav celulárneho automatu v čase t je daný polohou a smerom pohybu gúľ a polohou prekážok – reflektorov. Pomocou aktuálneho stavu v čase t môžeme zostrojiť pomocou elementárnych pravidiel z obr. 8.5 stav automatu v nasledujúcom časovom okamžiku $t+1$. Tak napr. na obr. 8.3 je znázornený biliardový celulárny automat, ktorý v čase t obsahuje dve gule (červenej farby), ktoré použitím elementárnych pravidiel z obrázku 8.5 sa pretransformujú (evoluujú) do koncového stavu reprezentovaného dvoma tmavými guľami umiestnenými na obrázku vpravo.



Obrázok 8.5. Rôzne elementárne možnosti pohybu gúľ v celulárnom automате simulujúcom pohyb biliardových gúľ. (A) Diagram znázorňuje najjednoduchšie štyri možnosti pohybu gúľ, ktoré neinteragujú s prostredím a ktorých smer pohybu je určený počiatočným stavom. V prípade, že v priebehu mnohých časových krokov guľa neinteraguje, potom sa pohybuje po diagonálach automatu a nemení svoj smer. (B) Osem rôznych prípadov, keď guľa narazí na fixnú prekážku, potom v nasledujúcom časovom okamžiku, okrem toho, že zmení polohu, zmení aj smer pohybu. (C a D) Interakcia dvoch gúľ pomocou „bočnej“ zrážky. (E a F) Interakcia dvoch gúľ pomocou čelnej zrážky. Poznamenajme, že všetky elementárne pravidlá sú reverzibilné.

Na obrázkoch 8.1 a 8.3 sú znázornené „biliardové“ implementácie interakčnej brány resp. prepínanej brány. Na obr. 7.17 je znázornená konštrukcia Fredkinovej bráni pomocou dvoch priamych prepínaných brán a dvoch inverzných brán (pozri taktiež diagramy B a C obr. 8.3).

9. prednáška

Kvantové počítanie III – kvantové brány,

9.1 Kvantové brány

9.1.1 1-qubitové brány

Budeme študovať päť jednoduchých 1-qubitových brán, ktoré sú reprezentované unitárnymi maticami $\{I, X, Y, Z, H\}$ v ortonormálnej báze $\{|0\rangle, |1\rangle\}$.

(1) Operátor identity

$$\begin{aligned}I|0\rangle &= |0\rangle \\ I|1\rangle &= |1\rangle\end{aligned}$$

Maticová reprezentácia operátora I má tvar

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad (9.1)$$

(2) Operátor negácie

$$\begin{aligned}X|0\rangle &= |1\rangle \\ X|1\rangle &= |0\rangle\end{aligned}$$

Maticová reprezentácia operátora negácie je

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (9.2)$$

(3) Operátor fázového posunu

$$\begin{aligned}Y|0\rangle &= -|1\rangle \\ Y|1\rangle &= |0\rangle\end{aligned}$$

Maticová reprezentácia operátora Y je

$$Y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad (9.3)$$

(4) Operátor zmeny znamienka

$$\begin{aligned}Z|0\rangle &= |0\rangle \\ Z|1\rangle &= -|1\rangle\end{aligned}$$

Maticová reprezentácia operátora Z je

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (9.4)$$

Túto transformáciu môžeme vyjadriť ako súčin $Z = XY$.

(5) *Hadamardov operátor*

$$H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

$$H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

Jeho maticová reprezentácia je

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (9.5)$$

Tento 1-qubitový operátor pomocou tenzorového súčinu môžeme aplikovať na stav $|000\dots 0\rangle = |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle$, potom

$$\begin{aligned} |\psi\rangle &= (H|0\rangle) \otimes (H|0\rangle) \otimes \dots \otimes (H|0\rangle) = (H \otimes H \otimes \dots \otimes H) |00\dots 0\rangle \\ &= \frac{1}{\sqrt{2^n}} (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \end{aligned} \quad (9.6)$$

kde x je celé číslo priradené bitovému reťazcu dĺžky n .

 9.1.2 *Brána 2-qubitová riadenej negácie*

Táto brána v klasickej reverzibilnej forme bola študovaná v kapitole 7.2.2. V kvantovej podobe je reprezentovaná unitárnym operátorom C_{not} , ktorý pôsobí na 2-qubitové stavové vektory

$$C_{not}|xy\rangle = \begin{cases} |x\bar{y}\rangle & (\text{pre } x=1) \\ |xy\rangle & (\text{pre } x=0) \end{cases} \quad (9.7a)$$

alternatívne

$$C_{not}|xy\rangle = |x, (x \wedge \bar{y}) \vee (\bar{x} \wedge y)\rangle = |x, x \oplus y\rangle \quad (9.7b)$$

alebo v rozpísanom tvare

$$\begin{aligned} C_{not}|00\rangle &= |00\rangle, C_{not}|01\rangle = |01\rangle \\ C_{not}|10\rangle &= |11\rangle, C_{not}|11\rangle = |10\rangle \end{aligned} \quad (9.8)$$

Pomocou dyadických súčinov môžeme operátor C_{not} vyjadriť takto

$$\begin{aligned} C_{not} &= |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10| \\ &= |0\rangle\langle 0| \otimes \underbrace{(|0\rangle\langle 0| + |1\rangle\langle 1|)}_I + |1\rangle\langle 1| \otimes \underbrace{(|0\rangle\langle 1| + |1\rangle\langle 0|)}_X \\ &= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X \end{aligned} \quad (9.9)$$

kde operátory I a X majú maticovú reprezentáciu v báze $\tilde{\mathcal{B}} = \{|0\rangle, |1\rangle\}$ (9.1) a (9.2). Pravú stranu (9.9) môžeme zovšeobecniť do tvaru

$$A = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U \quad (9.10)$$

kde U je 1-qubitový unitárny operátor, ktorý je interpretovaný ako nejaké „výpočtová transformácia“. Tento operátor A môžeme formálne interpretovať ako riadená aplikácia operátora U

$$A|00\rangle = |00\rangle \quad (9.11a)$$

$$A|01\rangle = |01\rangle \quad (9.11b)$$

$$A|10\rangle = |1\rangle \otimes U|0\rangle \quad (9.11c)$$

$$A|11\rangle = |1\rangle \otimes U|1\rangle \quad (9.11d)$$

Maticová reprezentácia tohto operátora v báze $\mathcal{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ má tvar unitárnej matice

$$\mathbf{A} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \langle 0|U|0\rangle & \langle 0|U|1\rangle \\ 0 & 0 & \langle 1|U|0\rangle & \langle 1|U|1\rangle \end{pmatrix} \quad (9.12)$$

Diagramatická interpretácia operátora C_{not} je identická s reprezentáciou na obr. 7.5.

Maticová reprezentácia operátora C_{not} v báze $\mathcal{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ má tvar unitárnej matice (pozri (9.12))

$$C_{not} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (9.13)$$

9.1.3 Toffoliho 3-qubitová brána

Klasická reverzibilná verzia tohto operátora bola študovaná v kapitole 7.2.3. Toffoliho brána je trojbitový operátor, ktorý je špecifikovaný takto

$$T|xyz\rangle = \begin{cases} |xy\bar{z}\rangle & (\text{pre } x \wedge y = 1) \\ |xyz\rangle & (\text{pre } x \wedge y = 0) \end{cases} \quad (9.14)$$

To znamená, že tretí bit je negovaný vtedy ak prvé dva bity sú jednotkové (ich konjunkcia je jednotková). Maticová reprezentácia Toffoliho operátora v báze

$$\mathcal{B} = \{|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle\}$$

má tvar

$$\mathbf{T} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Toffoliho operátor môže byť vyjadrený v tvare (3.5), podobne ako brána riadenej negácie

$$\begin{aligned}
 T &= |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| \\
 &\quad + |100\rangle\langle 100| + |101\rangle\langle 101| + |110\rangle\langle 111| + |111\rangle\langle 110| \\
 &= |0\rangle\langle 0| \otimes \underbrace{(|0\rangle\langle 0| + |1\rangle\langle 1|)}_I \otimes \underbrace{(|0\rangle\langle 0| + |1\rangle\langle 1|)}_I + |1\rangle\langle 1| \otimes C_{not} \\
 &= |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{not}
 \end{aligned} \tag{9.15}$$

Diagramatická interpretácia tejto brány je uvedená na obr. 7.9.

Toffoliho brána môže byť použitá ku konštrukcii úplného súboru logických spojok, táto možnosť je založená na jej vlastnostiach

$$T|1,1,x\rangle = |1,1,\bar{x}\rangle, T|x,y,0\rangle = |x,y,x \wedge y\rangle \tag{9.16a}$$

Spojka disjunkcie je vyjadrená takto

$$T|\bar{x},\bar{y},0\rangle = |\bar{x},\bar{y},\bar{x} \wedge \bar{y}\rangle, T|1,1,\bar{x} \wedge \bar{y}\rangle = |1,1,x \vee y\rangle \tag{9.16b}$$

9.1.4 Fredkinova 3-qubitová brána

Táto brána v klasickej reverzibilnej verzii bopla študovaná v kapitoly 3.2.3 spolu s Toffoliho reverzibilnou bránou. Jej tabuľka a špecifikácia pomocou Boolovych formúl bola taktiež uvedená v tejto kapitole. Použitím týchto vzťahov, Fredkinov operátor môžeme definovať takto

$$F|x,y,z\rangle = |x,\bar{x}y + xz,\bar{x}z + xy\rangle \tag{9.17a}$$

alebo

$$F|0,y,z\rangle = |0,y,z\rangle, F|1,y,z\rangle = |0,z,y\rangle \tag{9.17b}$$

V dyadickej forme Fredkinova brána má tvar

$$\begin{aligned}
 F &= |000\rangle\langle 000| + |001\rangle\langle 001| + |010\rangle\langle 010| + |011\rangle\langle 011| \\
 &\quad + |100\rangle\langle 100| + |101\rangle\langle 110| + |110\rangle\langle 101| + |111\rangle\langle 111| \\
 &= |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes S
 \end{aligned} \tag{9.18}$$

kde S je výmenný (swap) operátor $S = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$, ktorého maticová reprezentácia v báze $\mathcal{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ má tvar

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

Maticová reprezentácia operátora F má tvar

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

Na záver budeme študovať unitárny operátor U_f , ktorý vytvára ľubovoľnú Boolovu funkciu $f: \{0,1\}^n \rightarrow \{0,1\}$. Ako ilustračný príklad uvažujme funkciu AND , ktorá je špecifikovaná pomocou postupnosti troch tabuliek.

tabuľka 1			tabuľka 2				tabuľka 3					
x	y	AND	x	y	x'	AND	x	y	z	x	y	AND
0	0	0	0	0	0	0	0	0	0	0	0	0
0	1	0	0	1	0	0	0	1	0	0	1	0
1	0	0	1	0	0	0	0	0	0	1	0	0
1	1	1	1	1	0	1	1	1	0	1	1	1

Tabuľka 1 obsahuje funkciu AND v štandardnom tvare, prvé dva stĺpce obsahujú argumenty x a y , tretí stĺpec obsahuje argument. Pretože funkcia AND nie je 1-1-značná, potom transformácia prvých dvoch stĺpcov na tretí stĺpec nie je jednoznačná. Tabuľka 2 obsahuje pokus odstránenia tejto nejednoznačnosti tak, že sme zaviedli tretí stĺpec, ktorý obsahuje nový binárny argument, ani tento pokus nevedie k odstráneniu nejednoznačnosti. Tabuľka 3 už vyjadruje možný spôsob zavedenia jednoznačnosti do špecifikácie funkcie AND , argumentu boli rozšírené o tretí stĺpec, ktorý pre jednoduchosť obsahuje len nulové hodnoty. Ďalšie tri stĺpce sú funkčné, špecifikujú jednoznačným spôsobom funkciu AND , potom unitárny operátor U_{AND} môžeme špecifikovať takto

$$U_{AND}|000\rangle = |000\rangle, U_{AND}|010\rangle = |010\rangle, U_{AND}|100\rangle = |100\rangle, U_{AND}|110\rangle = |111\rangle$$

alebo

$$U_{AND} = |000\rangle\langle 000| + |010\rangle\langle 010| + |100\rangle\langle 100| + |110\rangle\langle 111|$$

Tento prístup ku konštrukcii unitárnej transformácie pre funkciu Boolovej s n argumentmi vyjadríme takto

$$\begin{aligned} U_f |x_1, x_2, \dots, x_n, 0\rangle &= U_f |x_1, x_2, \dots, x_n\rangle \otimes |0\rangle = |x_1, x_2, \dots, x_n\rangle \otimes |f(x_1, x_2, \dots, x_n)\rangle \\ &= |x_1, x_2, \dots, x_n, f(x_1, x_2, \dots, x_n)\rangle \end{aligned} \quad (9.19)$$

kde U_f je unitárny operátor špecifikovaný

$$U_f = \sum_{x_1, \dots, x_n \in \{0,1\}^n} |x_1, \dots, x_n, 0\rangle\langle x_1, \dots, x_n, f(x_1, \dots, x_n)|$$

Boolova funkcia f môže byť alternatívne špecifikovaná pomocou n -qubitovej funkcie $|\psi\rangle$ určenej (9.6), jej jednoduchou modifikáciou dostaneme

$$|\psi\rangle \otimes |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |0\rangle$$

Použitím (9.18) dostaneme

$$U_f |\psi\rangle \otimes |0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \otimes |f(x)\rangle \quad (9.20)$$

Týmto spôsobom sme dostali špecifikáciu ľubovoľnej Boolovej funkcie $f: \{0,1\}^n \rightarrow \{0,1\}$ pomocou unitárneho operátora. Formulu (9.20) môžeme interpretovať ako tabuľku funkcie f , ktorá pre každý argument špecifikuje jej funkčnú hodnotu.

9.2 Kvantový replikátor a nemožnosť klonovania

Nech H je unitárny priestor H pre ktorý platí $\dim(H) \geq 2$, unitárna transformácia U sa nazýva **kvantový replikátor** vtedy a len vtedy, ak vyhovuje podmienke

$$U|\alpha, 0\rangle = |\alpha, \alpha\rangle \quad (9.21)$$

kde $|\alpha, 0\rangle = |\alpha\rangle \otimes |0\rangle$, $|\alpha, \alpha\rangle = |\alpha\rangle \otimes |\alpha\rangle \in H \otimes H$ a stav $|0\rangle \in H$ sa nazýva **prázdny**. V ďalšej časti tejto kapitoly dokážeme, že kvantový replikátor nemôže existovať.

Predpokladajme, že existuje taký unitárny operátor U , že pre dva lineárne nezávislé 1-qubitové stavy $|\alpha\rangle$ a $|\beta\rangle$ platí

$$U|\alpha, 0\rangle = |\alpha, \alpha\rangle \quad \text{a} \quad U|\beta, 0\rangle = |\beta, \alpha\rangle$$

Zavedieme nový stavový vektor $|\gamma\rangle = (1/2)(|\alpha\rangle + |\beta\rangle)$, potom musí taktiež platiť

$$U|\gamma, 0\rangle = (1/2)(|\alpha, \alpha\rangle + |\beta, \beta\rangle) \quad (9.22a)$$

Potom taktiež musí platiť

$$U|\gamma, 0\rangle = |\gamma, \gamma\rangle = (1/4)(|\alpha\rangle + |\beta\rangle) \otimes (|\alpha\rangle + |\beta\rangle) = (1/4)(|\alpha, \alpha\rangle + |\alpha, \beta\rangle + |\beta, \alpha\rangle + |\beta, \beta\rangle) \quad (9.22b)$$

Porovnaním (9.22a) a (9.22b) dostaneme, že tieto dve aplikácie unitárneho operátora na stav $|\gamma, 0\rangle$ poskytuje dva diametrálne odlišné vektory. Z tejto skutočnosti vypláva, že nemôže existovať taký unitárny operátor U , ktorý by bol kvantový replikátor, jeho existencia vedie ku kontradikcii.

Nemožnosť klonovania je veľmi dôležitá vlastnosť, ktorá má zásadný význam pre kvantové počítanie. Ako bolo ukázané možnosť klonovanie vedie k paradoxom. Tak napríklad, kombinácia klonovania s teleportáciou môže viesť k procesom, ktoré sa šíria rýchlejšie ako svetlo.

Poznamenajme, že dôkazy vety o nemožnosti klonovania sme využili len vlastnosť lineárnosti operátora U , predpoklad o jeho unitárnosti nebol použitý. Dôkaz je potrebné interpretovať tak, že predpoklad unitárnosti transformácie je implicitný, vyplýva zo skutočnosti, že každá transformácia stavov v kvantovej mechanike musí byť unitárna. „Pikantné“ na dôkaze je to, že z neho vyplýva neexistencia lineárneho operátora U , ktorý by realizoval transformáciu (3.23), bez ohľadu na to, či je unitárny alebo nie je.

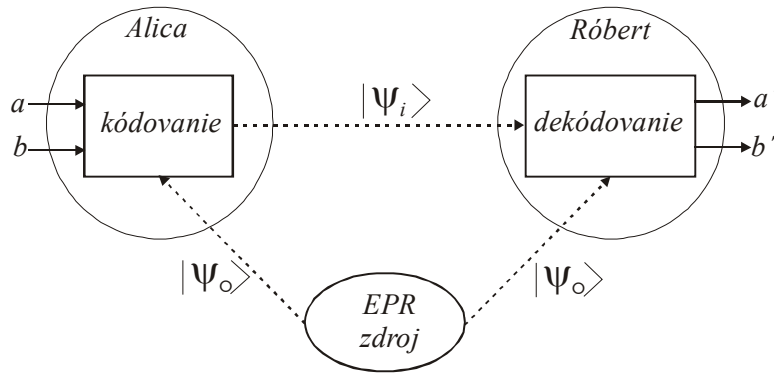
9.3 Ilustračné príklady

Použitie jednoduchých kvantových brán budeme demonštrovať na nasledujúcich dvoch jednoduchých príkladoch. Prvý príklad sa bude zaoberať s tzv. *hustým kódovaním* v ktorom sa používa jeden kvantový bit spolu s EPR dvojicou na zakódovanie a prenos dvoch klasických bitov. To znamená, že jedna častica (qubit) môže preniesť informáciu 2 bitov; tento výsledok je prekvapujúci, pretože v 3. kapitole bolo ukázané, že z jedného qubitového stavu môžeme extrahovať len jedno-bitovú informáciu. Druhý príklad sa bude zaoberať tzv. *teleportáciou*, čo je jav opačný k hustému kódovaniu v tom zmysle, že používa dva klasické bity na prenos jedného qubitového stavu. Teleportácia je prekvapujúcim javom z pohľadu nemožnosti klonovania neznámych kvantových stavov, pretože pomocou nej vlastne prenášame neznámy kvantový stav.

Základný proces v oboch ilustračných príkladoch hustého kódovania a teleportácie je použitie entaglovaného 2-časticového stavu

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

ktorý majú rovnaký oba zúčastnení (Alica a Róbert) v komunikačnom procese.



Obrázok 9.1. Kvantového hustého kódovania.

9.3.1 Husté kódovanie.

Alica. Prijala dva bity a a b klasickej informácie a taktiež qubit reprezentovaný neseparovateľnou časticou $|\psi_0\rangle$ (pozri obr. 9.1). Alica v závislosti na celom čísle $i = 2a + b$, vykoná transformáciu qubit $|\psi_0\rangle$ pomocou elementárnych transformácií I , X , Y a Z na nový qubit podľa tejto tabuľky

(a,b)	i	transformácia	nový stav
00	0	$ \psi_0\rangle = (I \otimes I) \psi_0\rangle$	$ \psi_0\rangle = 1/\sqrt{2}(00\rangle + 11\rangle)$
01	1	$ \psi_1\rangle = (X \otimes I) \psi_0\rangle$	$ \psi_1\rangle = 1/\sqrt{2}(10\rangle + 01\rangle)$
10	2	$ \psi_2\rangle = (Y \otimes I) \psi_0\rangle$	$ \psi_2\rangle = 1/\sqrt{2}(- 10\rangle + 01\rangle)$
11	3	$ \psi_3\rangle = (Z \otimes I) \psi_0\rangle$	$ \psi_3\rangle = 1/\sqrt{2}(00\rangle - 11\rangle)$

Alica pošle nový stav Róbertovi.

Róbert. Aplikuje riadenú negáciu C_{not} na prijatý qubit $|\psi_i\rangle, |\psi'_i\rangle = C_{not}|\psi_i\rangle$ výsledky sú uvedené v tabuľke

prijatý stav	nový stav	prvý bit	druhý bit (b)
$ \psi_0\rangle = 1/\sqrt{2}(00\rangle + 11\rangle)$	$ \psi'_0\rangle = 1/\sqrt{2}(00\rangle + 10\rangle)$	$1/\sqrt{2}(0\rangle + 1\rangle)$	$ 0\rangle$
$ \psi_1\rangle = 1/\sqrt{2}(10\rangle + 01\rangle)$	$ \psi'_1\rangle = 1/\sqrt{2}(11\rangle + 01\rangle)$	$1/\sqrt{2}(1\rangle + 0\rangle)$	$ 1\rangle$
$ \psi_2\rangle = 1/\sqrt{2}(- 10\rangle + 01\rangle)$	$ \psi'_2\rangle = 1/\sqrt{2}(- 11\rangle + 01\rangle)$	$1/\sqrt{2}(- 1\rangle + 0\rangle)$	$ 1\rangle$
$ \psi_3\rangle = 1/\sqrt{2}(00\rangle - 11\rangle)$	$ \psi'_3\rangle = 1/\sqrt{2}(00\rangle - 10\rangle)$	$1/\sqrt{2}(0\rangle - 1\rangle)$	$ 0\rangle$

Róbert môže získať pôvodný prvý bit a použitím Hadamardovej transformácie H , výsledky sú uvedené v tabuľke

<i>prijatý stav</i>	<i>prvý bit</i>	<i>H (prvý bit) (a)</i>
$ \psi_0\rangle = 1/\sqrt{2}(00\rangle + 11\rangle)$	$1/\sqrt{2}(0\rangle + 1\rangle)$	$1/\sqrt{2}(H 0\rangle + H 1\rangle) = 0\rangle$
$ \psi_1\rangle = 1/\sqrt{2}(10\rangle + 01\rangle)$	$1/\sqrt{2}(1\rangle + 0\rangle)$	$1/\sqrt{2}(H 1\rangle + H 0\rangle) = 0\rangle$
$ \psi_2\rangle = 1/\sqrt{2}(- 10\rangle + 01\rangle)$	$1/\sqrt{2}(- 1\rangle + 0\rangle)$	$1/\sqrt{2}(-H 1\rangle + H 0\rangle) = 1\rangle$
$ \psi_3\rangle = 1/\sqrt{2}(00\rangle - 11\rangle)$	$1/\sqrt{2}(0\rangle - 1\rangle)$	$1/\sqrt{2}(H 0\rangle - H 1\rangle) = 1\rangle$

Týmto sme ukázali, že Alica môže prijaté bity (a,b) jednoznačne zakódovať pomocou svojho qubitu, ktorý keď pošle Róbertovi, ten môže prijatý qubit dekodovať tak, že určí pôvodné bity (a,b) .

9.3.2 Kvantová teleportácia

Proces inverzný k hustému kódovaniu sa nazýva teleportácia, ktorá spočíva v tom, že štruktúra qubitu (ktorý nie je klonovateľný) sa pošle pomocou klasického kanála prostredníctvom bytov, pričom príjemca je ho schopný zrekonštruovať (pozri obr. 9.2). Kvantovú teleportáciu (podľa sci-fi) románov môžeme charakterizovať takto:

- (1) Objekt, ktorý má byť teleportovaný je najprv skanovaný, aby sme získali potrebnú informáciu o jeho zložení. Pri skanovaní pôvodný objekt zaniká, takže vlastnosť o nemožnosti klonovania nie je porušená.
- (2) Takto získaná informácia je zaslaná klasickými kanálmi na cieľové miesto teleportácie.
- (3) Rekonštrukcia presnej repliky objektu na cieľovom mieste pomocou prijatej informácie bez použitia lokálne dostupného materiálu

Alica. Alica má qubit (ktorého štruktúru nepozná)

$$|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$$

chce poslať špecifikáciu jeho stav pomocou klasického kanálu. Podobne, ako pri hustom kódovaní, Alica a Róbert vlastnia rovnaký qubit realizovaný entaglovanou časticou

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Alica aplikuje metódu použitú pre dekódovanie v hustom kódovaní. V prvom kroku sa uskutoční tenzorový súčin stavov $|\varphi\rangle$ a $|\psi_0\rangle$

$$|\varphi\rangle \otimes |\psi_0\rangle = \frac{1}{\sqrt{2}}(\alpha|0\rangle + \beta|1\rangle) \otimes (|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \beta|100\rangle + \alpha|011\rangle + \beta|111\rangle) \quad (3.25)$$

ktorý Alica ešte upraví pomocou unitárnych transformácií $H \otimes I \otimes I$ a $C_{not} \otimes I$

$$\begin{aligned} & (H \otimes I \otimes I)(C_{not} \otimes I)(|\varphi\rangle \otimes |\psi_0\rangle) \\ &= \frac{1}{\sqrt{2}}(H \otimes I \otimes I)(\alpha|000\rangle + \beta|110\rangle + \alpha|011\rangle + \beta|101\rangle) \\ &= \frac{1}{2}(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)) \end{aligned}$$

Alica meria vlastnosti tohto kvantového stavu vzhľadom k báze $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, vždy dostane s rovnakou pravdepodobnosťou jeden zo štyroch 1-časticových stavov

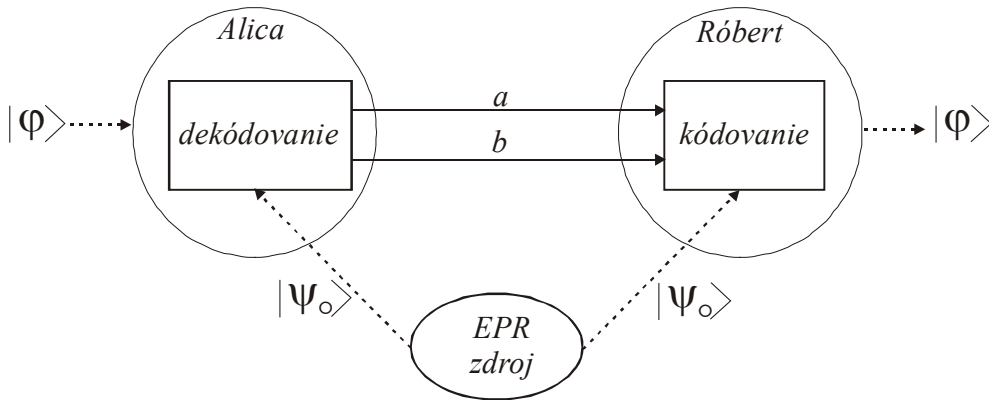
$$|\varphi_0\rangle = (\alpha|0\rangle + \beta|1\rangle) \quad (\text{pre } a=0, b=0)$$

$$|\varphi_1\rangle = (\alpha|1\rangle + \beta|0\rangle) \quad (\text{pre } a=0, b=1)$$

$$|\varphi_2\rangle = (\alpha|0\rangle - \beta|1\rangle) \quad (\text{pre } a=1, b=0)$$

$$|\varphi_3\rangle = (\alpha|1\rangle - \beta|0\rangle) \quad (\text{pre } a=1, b=1)$$

kde index vektorov $|\varphi_i\rangle$ je určený $i=2a+b$. Alice pošle pomocou klasického kanála Róbertovi bitovú informáciu (a,b) . Poznamenajme, že Alice meraním svojej časti (prvé dva qubity nevratne zmení stav zloženého stavu $|\varphi\rangle \otimes |\psi_0\rangle$, čo sa musí prejaviť aj Róbertovi.



Obrázok 9.2. Proces kvantovej teleportácie.

Róbert. Ak Róbert prijme klasické bity od Alici, potom vie ako transformovať stav svojej časti zloženého qubitu tak, aby zrekonštruoval pôvodný stav Alicinho qubitu $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$

a	b	i	transformácia $ \varphi_i\rangle$
0	0	0	$ \varphi\rangle = I \varphi_0\rangle = I(\alpha 0\rangle + \beta 1\rangle) = \alpha 0\rangle + \beta 1\rangle$
0	1	1	$ \varphi\rangle = X \varphi_1\rangle = X(\alpha 1\rangle + \beta 0\rangle) = \alpha 0\rangle + \beta 1\rangle$
1	0	2	$ \varphi\rangle = Y \varphi_2\rangle = Y(-\alpha 1\rangle + \beta 0\rangle) = \alpha 0\rangle + \beta 1\rangle$
1	1	3	$ \varphi\rangle = Z \varphi_3\rangle = Z(\alpha 0\rangle - \beta 1\rangle) = \alpha 0\rangle + \beta 1\rangle$

Poznamenajme, že táto transformácia korešponduje s krokom kódovania v hustom kódovaní.

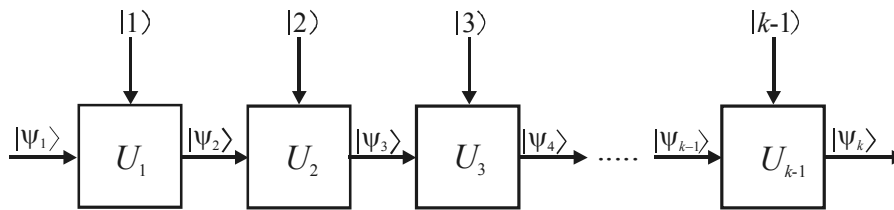
10. prednáška

Feynmanov kvantový počítač

V tejto kapitole budeme študovať ilustračný príklad mnoho-qubitového systému, ktorý je popísaný špecifickým hamiltoniánom, pričom riešením Schrödingerovej rovnice získame popis časovej evolúcie tohto systému.

Koncepcia Feynmanovho kvantového počítača je založená na predstave deterministického počítača, ktorý obsahuje $k-1$ brán zapojených sériovým spôsobom, pozri obr. 10.1. Vstupný (počiatočný) stav $|\psi_1\rangle$ je unitárnym vlnovým operátorom U_0 pretransformovaný na nasledujúci stav $|\psi_2\rangle$, tento proces sa opakuje až po dosiahnutie konečného (výstupného) stavu $|\psi_k\rangle$

$$|\psi_{i+1}\rangle = U_i |\psi_i\rangle \quad (i = 1, \dots, k-1) \quad (10.1)$$



Obrázok 10.1. Feynmanov kvantový počítač obsahujúci $k-1$ brán, ktoré sú reprezentované unitárnymi transformáciami $U_1, U_2, \dots, U_{k-1}$, ktoré sú postupne aplikované na stavy $|\psi_1\rangle, |\psi_2\rangle, \dots, |\psi_k\rangle, |\psi_{k+1}\rangle$. Každá aplikácia brány U_i na stav $|\psi_i\rangle$ sa uskutočňuje v diskretnom čase i . Stav „počítača“ je potom reprezentovaný tenzorovým súčinom $|\Psi_i\rangle = |\psi_i\rangle \otimes |i\rangle$.

Ako ukážeme neskôr, postulovaný kvantový počítač je špecifikovaný pomocou vhodného hamiltoniánu H , ktorý nezávisí explicitne na čase. Tento postulát interpretujeme ako analógiu hardwaru v klasických počítačoch. Evolúcia kvantového počítača je špecifikovaná unitárnym vlnovým operátorom $U(t) = e^{-iHt}$, ktorý transformuje počiatočný stav (vstup do kvantového počítača) $|\Psi(0)\rangle$ na koncový stav (výstup z kvantového počítača) $|\Psi(t)\rangle$, ktorý je superpozíciou stavov jednotlivých qubitov a ktorý formálne interpretujeme ako analógiu software v klasických počítačoch. Hodnoty jednotlivých qubitov v tomto koncovom stave zistíme operáciou merania, ktoré nám zafixuje vybraný stav, vzhľadom ku ktorému sa meranie uskutočnilo. Od tohto okamžiku môžeme naštartovať novú evolúciu systému pomocou vlnového operátora, ktorá je formálne ekvivalentná s prvou evolúciou, pričom pôvodný počiatočný stav je nahradený vybraným stavom, vzhľadom ku ktorému sa uskutočnilo meranie.

Metóda explicitného zahrnutia času prostredníctvom pomocných časových stavov $|i\rangle$ odstraňuje závažný nedostatok pôvodných konštrukcií kvantových počítačov, v ktorých

unitárny vlnový operátor transformujúci stavy počítača nebol univerzálnym operátor, pretože hamiltonián systému nie je časovo invariantný. Feynmanov kvantový počítač je založený na rozšírenom predpoklade, podľa ktorého, stav systému nie je popísaný len čistým stavovým vektorom $|\psi_i\rangle$, ale je popísaný tenzorovým súčinom $|\Psi_i\rangle = |\psi_i\rangle \otimes |i\rangle$, kde druhá zložka „časový stav“ $|i\rangle$ špecifikuje „časový okamžik“ v ktorom bola transformácia vykonaná

$$|\Psi_{i+1}\rangle = G_i |\Psi_i\rangle \quad (10.2a)$$

$$G_i = U_i \otimes |i+1\rangle\langle i| \quad (10.2b)$$

Unitárny operátor U_i môžeme formálne vyjadriť ako dyadický súčin $U_i = |\psi_{i+1}\rangle\langle\psi_i|$, potom operátor G_i má tento formálny tvar

$$G_i = |\psi_{i+1}\rangle\langle\psi_i| \otimes |i+1\rangle\langle i| \quad (10.3)$$

Budeme predpokladať, že „časové“ stavové vektory $\{|1\rangle, |2\rangle, \dots\}$ tvoria ortonormálnu množinu vektorov, $\langle i|j\rangle = \delta_{ij}$. Pomocou reprezentácie (10.3) môžeme zostrojiť analógie formúl (10.2a-b) v ktorých vystupuje hermitovsky združený operátor G_i^+

$$|\Psi_{i-1}\rangle = G_i^+ |\Psi_i\rangle \quad (10.4a)$$

$$G_i^+ = |\psi_i\rangle\langle\psi_{i+1}| \otimes |i\rangle\langle i+1| \quad (10.4b)$$

Potom platí

$$G_i G_i^+ = (|\psi_{i+1}\rangle\langle\psi_i| \otimes |i+1\rangle\langle i|)(|\psi_i\rangle\langle\psi_{i+1}| \otimes |i\rangle\langle i+1|) = |\psi_{i+1}\rangle\langle\psi_{i+1}| \otimes |i+1\rangle\langle i+1| = I_{i+1} \quad (10.5a)$$

$$G_i^+ G_i = (|\psi_i\rangle\langle\psi_{i+1}| \otimes |i\rangle\langle i+1|)(|\psi_{i+1}\rangle\langle\psi_i| \otimes |i+1\rangle\langle i|) = |\psi_i\rangle\langle\psi_i| \otimes |i\rangle\langle i| = I_i \quad (10.5b)$$

Tieto dva výsledky môžeme interpretovať tak, že operátor G_i je unitárny. Definujme operátor G ako sumu operátorov $G_1, G_2, \dots$

$$G = \sum_{i=1}^{k-1} G_i \quad (10.6a)$$

Ak použijeme (10.2b), potom tento operátor môžeme písať v tvare

$$G = U_1 \otimes |2\rangle\langle 1| + U_2 \otimes |3\rangle\langle 2| + \dots + U_{k-1} \otimes |k\rangle\langle k-1| \quad (10.6b)$$

Nech operátory $U_1, U_2, \dots, U_{k-1}$, sú definované v lineárnom priestore s ortonormálnou bázou $\mathcal{B}_1 = \{\chi_1, \chi_2, \dots, \chi_p\}$, potom operátor G je definovaný v lineárnom priestore s bázou vyjadrenou ako tenzorový súčin tejto báze s bázou $\mathcal{B}_2 = \{|1\rangle, |2\rangle, \dots, |k\rangle\}$

$$\mathcal{B} = \{\chi_1, \chi_2, \dots, \chi_p\} \otimes \{|1\rangle, |2\rangle, \dots, |k\rangle\} = \{\chi_\alpha, j; \alpha = 1, 2, \dots, p; j = 1, 2, \dots, k\} \quad (10.7)$$

Maticová reprezentácia operátora G v tejto báze $\mathcal{B}$ má tvar

$$\langle\chi_\alpha, i|G|\chi_\beta, j\rangle = \langle\chi_\alpha|U_j|\chi_\beta\rangle \delta_{i,j+1} \quad (10.8)$$

alebo ako matica typu $(kp \times kp)$

$$G = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} \\ U_1 & \mathbf{0} & \dots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & U_2 & \dots & \mathbf{0} & \mathbf{0} \\ \dots & \dots & \ddots & \dots & \dots \\ \mathbf{0} & \mathbf{0} & \dots & U_{k-1} & \mathbf{0} \end{pmatrix} \quad (10.9)$$

kde U_i a $\mathbf{0}$ sú matice typu $(p \times p)$, ktoré reprezentujú operátor U_i resp. nulovú maticu.

Definujme hermitovský operátor – **hamiltonián**, ktorý reprezentuje „hardware“ hypotetického kvantového systému nazývaného „**kvantový počítač**“

$$H = G + G^+ \quad (10.10a)$$

Tento operátor už explicitne nezávisí od jednotlivých kvantových stavov na ktoré je aplikovaný, môžeme povedať, že nezávisí explicitne na čase, pričom čas je reprezentovaný pomocou diskkrétnej premennej – „indexu“ i . Tento operátor formálne interpretujeme ako **hamiltonián** kvantového systému, ktorý realizuje k postupných unitárnych transformácií (10.1). Maticová reprezentácia hamiltoniánu má tvar

$$\mathbf{H} = \begin{pmatrix} \mathbf{0} & U_1^+ & \mathbf{0} & \dots & \mathbf{0} \\ U_1 & \mathbf{0} & U_2^+ & \dots & \mathbf{0} \\ \mathbf{0} & U_2 & \mathbf{0} & \dots & \mathbf{0} \\ \dots & \dots & \dots & \ddots & \dots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \dots & \mathbf{0} \end{pmatrix} \quad (10.10b)$$

Elementy tejto matice sú potom špecifikované takto (pozri (10.8))

$$\begin{aligned} \langle \chi_\alpha, i | H | \chi_\beta, j \rangle &= \langle \chi_\alpha, i | G | \chi_\beta, j \rangle + \langle \chi_\beta, j | G | \chi_\alpha, i \rangle^* \\ &= G_{\alpha\beta} \delta_{i,j+1} + G_{\beta\alpha}^* \delta_{j,i+1} \end{aligned} \quad (10.10b)$$

Schrödingerova rovnica tohto hypotetického systému „kvantového počítača“ má tvar

$$i \frac{\partial}{\partial t} |\Psi(t)\rangle = H |\Psi(t)\rangle \quad (10.11a)$$

jej alternatívny integrálny tvar vyjadrený pomocou evolučného operátora U je

$$|\Psi(t)\rangle = U(t) |\Psi(0)\rangle = e^{-iHt} |\Psi(0)\rangle \quad (10.11b)$$

kde $|\Psi(0)\rangle$ je počiatočný stav špecifikujúci riešenie Schrödingerovej rovnice (10.11a).

Z definície (10.10a) hamiltoniánu H vyplýva, že tento operátor je špecifikovaný v konečno-rozmernom lineárnom priestore, ktorého ortonormálnu bázu je určená (10.7). Nech hamiltonián H kvantového počítača má systém vlastných vektorov $\{|\varphi_1\rangle, |\varphi_2\rangle, \dots, |\varphi_p\rangle\}$ a vlastných hodnôt $\{\lambda_1, \lambda_2, \dots, \lambda_p\}$, kde $H|\varphi_i\rangle = \lambda_i|\varphi_i\rangle$. Použitím spektrálneho rozvoja pre funkciu hamiltoniána H zostrojíme explicitný tvar vlnového operátora

$$U(t) = e^{-iHt} = \sum_{j=1}^p e^{-i\lambda_j t} |\varphi_j\rangle \langle \varphi_j| \quad (10.12)$$

Potom stavový vektor $|\Psi(t)\rangle$ kvantového počítača má tvar

$$|\Psi(t)\rangle = U(t) |\Psi(0)\rangle = e^{-iHt} |\Psi(0)\rangle = \sum_{j=1}^p e^{-i\lambda_j t} \langle \varphi_j | \Psi(0) \rangle |\varphi_j\rangle \quad (10.13)$$

Ak vlastné vektory hamiltoniánu H vyjadríme pomocou vektorov ortonormálnej báze $\mathcal{B}$ určenej (10.7)

$$|\varphi_j\rangle = \sum_{\alpha=1}^p \sum_{l=1}^k \langle \chi_\alpha, l | \varphi_j \rangle |\chi_\alpha, l\rangle \quad (10.14)$$

potom ak v (10.9) položíme $|\Psi(0)\rangle = |\chi_a, n\rangle = |\chi_a\rangle \otimes |n\rangle$, kde $a \in \{1, 2, \dots, p\}$ a $n \in \{1, 2, \dots, k\}$.

Dosadením (10.14) do (10.13) dostaneme

$$|\Psi(t)\rangle = \sum_{\alpha=1}^p \sum_{l=1}^k \left(\sum_{j=1}^{k \cdot p} e^{-i\lambda_j t} \langle \varphi_j | \chi_{\alpha}, n \rangle \langle \chi_{\alpha}, l | \varphi_j \rangle \right) |\chi_{\alpha}, l\rangle \quad (10.15)$$

Lahko sa presvedčíme, že takto špecifikovaná vlnová funkcia kvantového systému s hamiltoniánom (10.6) vyhovuje počiatočnej podmienke $|\Psi(0)\rangle = |\chi_{\alpha}, n\rangle$.

Niekoľko poznámok k evolúcii kvantového počítača pomocou exponenciálneho vlnového operátora $U(t) = e^{-iHt}$. Rozvoj tohto operátora má tvar

$$e^{-iHt} = 1 + \frac{(-it)}{1!} H + \frac{(-it)^2}{2!} HH + \frac{(-it)^3}{3!} HHH + \dots \quad (10.16)$$

Uvažujme štvrtý člen, ktorý obsahuje tretiu mocninu hamiltoniánu H , pre jednoduchosť našich úvah postulujeme, že hamiltonián má tvar (10.10a), kde $G = U_1|2\rangle\langle 1| + U_2|3\rangle\langle 2|$. Potom napr. tretia mocnina hamiltoniánu v rozvoji (10.16) má tvar

$$\begin{aligned} HHH &= (U_1 \otimes |2\rangle\langle 1| + U_2 \otimes |3\rangle\langle 2|)(2 + U_1^+ \otimes |1\rangle\langle 2| + U_2^+ \otimes |2\rangle\langle 3|)(3) \\ &= U_1 U_2 U_1^* \underbrace{|2\rangle\langle 1| |3\rangle\langle 2| |2\rangle\langle 1|}_{0} + U_1 U_1^+ U_2^+ \underbrace{|2\rangle\langle 1| |2\rangle\langle 3| |3\rangle\langle 2|}_{|2\rangle\langle 3|} + \dots \end{aligned} \quad (10.17)$$

Prvý člen na pravej strane reprezentuje nedovolenú postupnosť aplikácie 1-qubitových brán, ich výsledok je pomocou „časovej“ časti nulový. Druhý člen je „povolený“, „časová“ časť produkuje člen $|2\rangle\langle 3|$, t. j. postupnosť U operátorov bola aplikovaná na stav v „čase“ 3, výsledný „čas“ je 2. Môžeme teda konštatovať, že formálna štruktúra hamiltoniánu má také výhodné vlastnosti, ktoré odstraňujú a-priori nefyzikálne „nevýpočtové“ stavy kvantového zariadenia.

10.1 Jednoduchá implementácia Feynmanovho počítača pomocou 1-qubitovej brány negácie X

Kvantová brána negácie je určená maticou

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad (10.16)$$

Jej druhú odmocninu zostrojíme pomocou spektrálneho rozvoja funkcie matice

$$X = U^T A U \Rightarrow \sqrt{X} = U^T \sqrt{A} U \quad (10.17)$$

kde U je unitárna, ktorá diagonalizuje maticu negácie X , $A = U X U^+$. K tomu, aby sme zostrojili túto maticu, musíme nájsť vlastné hodnoty matice X pomocou sekulárneho determinantu

$$\begin{vmatrix} -\lambda & 1 \\ 1 & -\lambda \end{vmatrix} = 0 \Rightarrow \lambda^2 - 1 = 0 \Rightarrow \lambda_{1,2} = \pm 1$$

Vlastné vektory, ktoré sú určené týmito vlastnými hodnotami získame riešením dvoch homogénnych problémov

$$\begin{aligned} (X - \lambda_1 E) c_1 &= 0 \Rightarrow \begin{pmatrix} -1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = 0 \Rightarrow a = b = 1 \Rightarrow c_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ (X - \lambda_2 E) c_2 &= 0 \Rightarrow \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = 0 \Rightarrow a = -b = 1 \Rightarrow c_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \end{aligned}$$

Tieto dva vlastné vektory môžu byť chápané ako stĺpcové vektory unitárnej matice V , ktorá transformuje maticu X na diagonálny tvar

$$V = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (10.18)$$

Potom matica $\sqrt{X}$ má tvar

$$\sqrt{X} = V^T \sqrt{A} V = \frac{1}{2} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix} \quad (10.19)$$

Ľahko sa presvedčíme, že takto zostrojená matica je unitárna a že jej kvadrát sa rovná matici negácie X . Aplikácia matice $\sqrt{X}$ na vektory $|0\rangle$ a $|1\rangle$ je určená takto

$$\sqrt{X}|0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} (e^{i\pi/4}|0\rangle + e^{-i\pi/4}|1\rangle) \quad (10.20a)$$

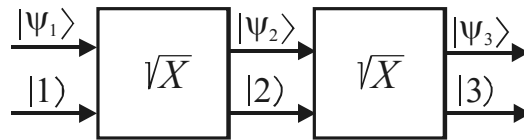
$$\sqrt{X}|1\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} e^{i\pi/4} & e^{-i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}} (e^{-i\pi/4}|0\rangle + e^{i\pi/4}|1\rangle) \quad (10.20b)$$

Operátor G (10.6b) obsahujúci operátor $\sqrt{X}$ má tvar (pozri obr. 11.2)

$$G = \sqrt{X} \otimes |2\rangle\langle 1| + \sqrt{X} \otimes |3\rangle\langle 2| \quad (10.21a)$$

Maticová reprezentácia tohto operátora má tvar

$$G = \begin{pmatrix} 0 & 0 & 0 \\ \sqrt{X} & 0 & 0 \\ 0 & \sqrt{X} & 0 \end{pmatrix} \quad (10.21b)$$



Obrázok 10.2. Kvantový počítač obsahujúci dve odmocniny 1-qubitovej negácie

Hamiltonián kvantového počítača má tvar

$$H = G + G^+ \quad (10.22a)$$

Maticová reprezentácia tohto operátora je

$$H = \begin{pmatrix} 0 & \sqrt{X}^* & 0 \\ \sqrt{X} & 0 & \sqrt{X}^* \\ 0 & \sqrt{X} & 0 \end{pmatrix} \quad (10.22b)$$

Tento operátor už explicitne nezávisí od jednotlivých kvantových stavov na ktoré je aplikovaný, môžeme povedať, že nezávisí explicitne na čase, pričom čas chápeme reprezentovaný pomocou diskkrétnej premennej „indexu“ i . Tento operátor formálne interpretujeme ako **hamiltonián** kvantového systému, ktorý realizuje 2 postupné unitárne transformácie (10.1). Maticová reprezentácia hamiltoniánu má tvar

$$\begin{aligned}
 \mathbf{H} &= \frac{1}{\sqrt{2}} \begin{pmatrix} 0 & 0 & e^{-i\pi/4} & e^{i\pi/4} & 0 & 0 \\ 0 & 0 & e^{i\pi/4} & e^{-i\pi/4} & 0 & 0 \\ e^{i\pi/4} & e^{-i\pi/4} & 0 & 0 & e^{-i\pi/4} & e^{i\pi/4} \\ e^{-i\pi/4} & e^{i\pi/4} & 0 & 0 & e^{i\pi/4} & e^{-i\pi/4} \\ 0 & 0 & e^{i\pi/4} & e^{-i\pi/4} & 0 & 0 \\ 0 & 0 & e^{-i\pi/4} & e^{i\pi/4} & 0 & 0 \end{pmatrix} \\
 &= \underbrace{\begin{pmatrix} 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 1/2 & 1/2 & 0 & 0 & 1/2 & 1/2 \\ 1/2 & 1/2 & 0 & 0 & 1/2 & 1/2 \\ 0 & 0 & 1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & 1/2 & 0 & 0 \end{pmatrix}}_{\mathbf{A}} + i \underbrace{\begin{pmatrix} 0 & 0 & -1/2 & 1/2 & 0 & 0 \\ 0 & 0 & 1/2 & -1/2 & 0 & 0 \\ 1/2 & -1/2 & 0 & 0 & -1/2 & 1/2 \\ -1/2 & 1/2 & 0 & 0 & 1/2 & -1/2 \\ 0 & 0 & 1/2 & -1/2 & 0 & 0 \\ 0 & 0 & -1/2 & 1/2 & 0 & 0 \end{pmatrix}}_{\mathbf{B}} \quad (10.22b) \\
 &= \mathbf{A} + i\mathbf{B}
 \end{aligned}$$

Zostrojená maticová reprezentácia hamiltoniánu (10.22b) má komplexné elementy, preto ju vyjadríme ako súčet reálnej a imaginárnej časti, $\mathbf{H} = \mathbf{A} + i\mathbf{B}$, kde matica $\mathbf{A}$ je symetrická a matica $\mathbf{B}$ je antisymetrická, $\mathbf{A}^T = \mathbf{A}$ resp. $\mathbf{B}^T = -\mathbf{B}$. Podobným spôsobom môžeme separovať aj vlastný vektor tejto matice $\mathbf{x} = \mathbf{u} + i\mathbf{v}$, kde $\mathbf{u}$ a $\mathbf{v}$ sú reálne vektory. Vlastný problém $\mathbf{H}\mathbf{x} = \lambda\mathbf{x}$ použitím týchto separácií prepíšeme do tvaru $(\mathbf{A} + i\mathbf{B})(\mathbf{u} + i\mathbf{v}) = \lambda(\mathbf{u} + i\mathbf{v})$, porovnaním reálnych a imaginárnych častí na oboch stranách rovnice dostaneme dve rovnice pre reálnu a imaginárnu zložku vlastného vektora $\mathbf{x}$

$$\mathbf{A}\mathbf{u} - \mathbf{B}\mathbf{v} = \lambda\mathbf{u} \quad (10.23a)$$

$$\mathbf{A}\mathbf{v} + \mathbf{B}\mathbf{u} = \lambda\mathbf{v} \quad (10.23b)$$

alebo v maticovom tvare

$$\underbrace{\begin{pmatrix} \mathbf{A} & -\mathbf{B} \\ \mathbf{B} & \mathbf{A} \end{pmatrix}}_{\tilde{\mathbf{H}}} \underbrace{\begin{pmatrix} \mathbf{u} \\ \mathbf{v} \end{pmatrix}}_{\tilde{\mathbf{x}}} = \lambda \begin{pmatrix} \mathbf{u} \\ \mathbf{v} \end{pmatrix} \quad (10.23c)$$

kde symetrická **rozšírená matica** $\tilde{\mathbf{H}}$ s reálnymi koeficientmi má dvojnásobnú dimenziu vzhľadom k pôvodnej matici $\mathbf{H}$. Týmto sme ukázali, že reálna a imaginárna časť vlastného vektora $\mathbf{x}$ je v pomoci nových vlastných vektorov reálnej symetrickej matice $\tilde{\mathbf{H}}$. Poznamenajme, že každá vlastná hodnota λ problému (10.23c) je aspoň dvakrát degenerovaná. Táto vlastnosť môže byť jednoducho verifikovaná tak, že ak stĺpcový vektor

$$\tilde{\mathbf{x}} = \begin{pmatrix} \mathbf{u} \\ \mathbf{v} \end{pmatrix} \quad (10.24a)$$

je vlastný vektor s vlastnou hodnotou λ , potom aj stĺpcový vektor

$$\tilde{\mathbf{x}}' = \begin{pmatrix} -\mathbf{v} \\ \mathbf{u} \end{pmatrix} \quad (10.24b)$$

je taktiež vlastný vektor s tou istou vlastnou hodnotou λ . O tejto skutočnosti sa môžeme ľahko presvedčiť nahradením pôvodného stĺpcového vektora $\tilde{\mathbf{x}}$ v (10.23c) vektorom (10.24b), dostaneme dve maticové rovnice, ktoré sú ekvivalentné s (10.23a-b). Táto vlastnosť je

dôsledkom jednoduchej vlastnosti: ak $\mathbf{x} = \mathbf{u} + i\mathbf{v}$ je vlastný vektor matice, potom aj vektor $i\mathbf{x} = i\mathbf{u} - \mathbf{v}$ je tiež vlastný vektor s tou istou vlastnou hodnotou λ . To znamená, že rozšírená matica z (10.23c) má všetky vlastné hodnoty párny-počet-krát degenerované.

Spektrálny rozvoj matice $\mathbf{H}$ má tvar

$$\mathbf{H} = \sum_{j=1}^n \lambda_j \mathbf{x}_j \mathbf{x}_j^+ \Rightarrow \mathbf{U}(t) = e^{-i\mathbf{H}t} = \sum_{j=1}^n e^{-i\lambda_j t} \mathbf{x}_j \mathbf{x}_j^+ \quad (10.25)$$

Ak vlastný vektor $\mathbf{x}_i$ vyjadríme v tvare v ktorom je reálna zložka separovaná od imaginárnej zložky, $\mathbf{x}_j = \mathbf{u}_j + i\mathbf{v}_j$, potom pravú stranu vlnového operátora (10.25) môžeme prepísať do tvaru

$$\begin{aligned} \mathbf{U}(t) = e^{-i\mathbf{H}t} &= \sum_{k=1}^n e^{-i\lambda_k t} \left[(\mathbf{u}_k \mathbf{u}_k^T + \mathbf{v}_k \mathbf{v}_k^T) + i(\mathbf{v}_k \mathbf{u}_k^T - \mathbf{u}_k \mathbf{v}_k^T) \right] \\ &= \sum_{k=1}^n \underbrace{\left[\cos \lambda_k t \cdot (\mathbf{u}_k \mathbf{u}_k^T + \mathbf{v}_k \mathbf{v}_k^T) + \sin \lambda_k t \cdot (\mathbf{v}_k \mathbf{u}_k^T - \mathbf{u}_k \mathbf{v}_k^T) \right]}_{\mathbf{U}_R(t)} \\ &\quad + i \sum_{k=1}^n \underbrace{\left[\cos \lambda_k t \cdot (\mathbf{v}_k \mathbf{u}_k^T - \mathbf{u}_k \mathbf{v}_k^T) - \sin \lambda_k t \cdot (\mathbf{u}_k \mathbf{u}_k^T + \mathbf{v}_k \mathbf{v}_k^T) \right]}_{\mathbf{U}_I(t)} \end{aligned} \quad (10.28)$$

Týmto sme zostrojili vlnovú maticu kvantového systému s hamiltonovou maticou $\mathbf{H}$, ktorá je v separovanom tvare, kde reálna časť je oddelená od imaginárnej časti.

Použitím tejto formule môžeme jednoducho zostrojiť stav kvantového počítača v čase t aplikáciou vlnovej matice (10.28) na počiatočný stav $|\Psi(0)\rangle = |\chi_1, 1\rangle$

$$\begin{aligned} |\Psi(t)\rangle &= \mathbf{U}(t) |\Psi(0)\rangle = e^{-i\mathbf{H}t} |\Psi(0)\rangle = e^{-i\mathbf{H}t} |\chi_1, 1\rangle \\ &= \sum_{k=1}^n \left[\cos \lambda_k t \cdot (\mathbf{u}_k \mathbf{u}_k^T + \mathbf{v}_k \mathbf{v}_k^T) + \sin \lambda_k t \cdot (\mathbf{v}_k \mathbf{u}_k^T - \mathbf{u}_k \mathbf{v}_k^T) \right] |\chi_1, 1\rangle \\ &\quad + i \sum_{k=1}^n \left[\cos \lambda_k t \cdot (\mathbf{v}_k \mathbf{u}_k^T - \mathbf{u}_k \mathbf{v}_k^T) - \sin \lambda_k t \cdot (\mathbf{u}_k \mathbf{u}_k^T + \mathbf{v}_k \mathbf{v}_k^T) \right] |\chi_1, 1\rangle \\ &= \mathbf{U}_R(t) |\chi_1, 1\rangle + i \mathbf{U}_I(t) |\chi_1, 1\rangle \end{aligned} \quad (10.29)$$

Počiatočný stav $|\Psi(0)\rangle = |\chi_1, 1\rangle = |\chi_1\rangle \otimes |1\rangle$ je zložený z dvoch zložiek, prvá reprezentuje binárny 1-qubitový stav, zatiaľ čo druhá prvý stavový vektor časového okamžiku. Poznamenajme, že v danej maticovej reprezentácii tento stav je vyjadrený 6-rozmerným stĺpcovým vektorom, ktorý obsahuje v prvej polohe jednotkový element a vo všetkých ostatných polohách nulový element

$$|\chi_1, 1\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, |\chi_1, 2\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \dots, |\chi_2, 3\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad (10.31)$$

Rezultujúci stavový vektor $|\Psi(t)\rangle$ je potom reprezentovaný 6-rozmerným komplexným vektorom

$$\begin{aligned}
 |\Psi(t)\rangle &= U(t)|\Psi(0)\rangle = (U_R(t) + iU_I(t))|\chi_1,1\rangle \\
 &= (U_R(t) + iU_I(t))(1,0,0,0,0,0)^T \\
 &= (\alpha_1 + i\beta_1, \alpha_2 + i\beta_2, \alpha_3 + i\beta_3, \alpha_4 + i\beta_4, \alpha_5 + i\beta_5, \alpha_6 + i\beta_6)^T
 \end{aligned} \tag{10.32}$$

kde z j -teho koeficienta $\alpha_j + i\beta_j$ môžeme jednoducho zostrojiť pravdepodobnosť toho, že v čase t sa kvantový počítač nachádza v j -tom stave

$$prob(j, k; 1, 1) = \alpha_j^2 + \beta_j^2 \tag{10.33}$$

Na obr. 10.2 je znázornený priebeh pravdepodobností (10.33). V čase $t = 0$ vlnová funkcia má tvar

$$|\Psi(0)\rangle = |\chi_1,1\rangle = (1,0,0,0,0,0)^T \tag{10.43a}$$

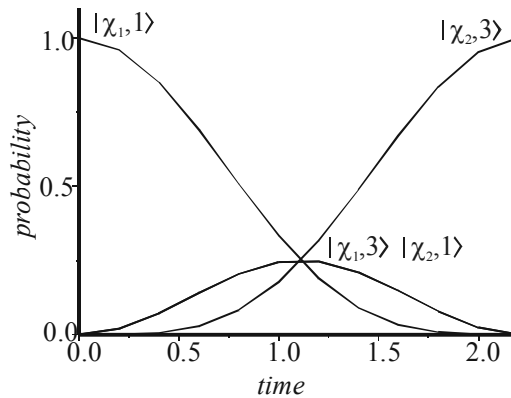
V čase $t = 1$ vlnová funkcia je špecifikovaná takto

$$\begin{aligned}
 |\Psi(1)\rangle &= U(1)|\Psi(0)\rangle = (U_R(1) + iU_I(1))|\chi_1,1\rangle \\
 &= (U_R(1) + iU_I(1))(1,0,0,0,0,0)^T \\
 &= (0.5780, 0, -0.3492 - 0.3492i, 0.3492 - 0.3492i, 0, -0.4220)^T
 \end{aligned} \tag{10.43b}$$

Konečne, v čase $t = 2.2$ vlnová funkcia má tvar

$$\begin{aligned}
 |\Psi(2.2)\rangle &= U(2.2)|\Psi(0)\rangle = (U_R(2.2) + iU_I(2.2))|\chi_1,1\rangle \\
 &= (U_R(2.2) + iU_I(2.2))(1,0,0,0,0,0)^T \\
 &= (0.0002, 0, -0.0107 - 0.0107i, 0.0107 - 0.0107i, 0, -0.9998)^T
 \end{aligned} \tag{10.43c}$$

To znamená, že pre $t = 2.2$ vlnová funkcia je skoro presne vyjadrená pomocou stavu $|\chi_2,3\rangle$, čo je aj v súhlase so skutočnosťou, že na vektor $|\chi_1,1\rangle$ aplikujeme dvakrát po sebe operátor $\sqrt{X}$, čo produkuje negáciu počiatočného stavu.



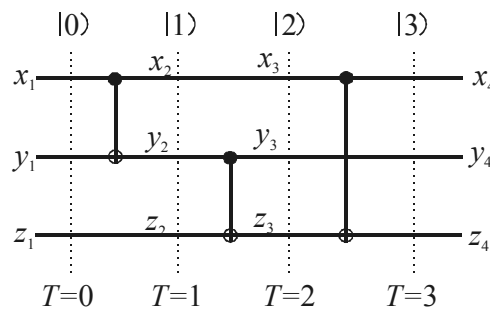
Obrázok 10.2. Priebehy pravdepodobností pre stavy $|\chi_1,1\rangle$, $|\chi_1,3\rangle$, $|\chi_2,1\rangle$ a $|\chi_2,3\rangle$, ktoré sú špecifikované vzťahom (10.33), keď počiatočný stav bol $|\Psi(0)\rangle = |\chi_1,1\rangle$. V čase $t = 2$ pôvodný stav $|\chi_1,1\rangle$ bol totálne nahradený stavom $|\chi_2,3\rangle$, čo je v súhlase so skutočnosťou, že kvadrát operátora $\sqrt{X}$ v čase $t = 2$ vykoná negáciu $|\chi_1,1\rangle$ na stav $|\chi_2,3\rangle$.

10.2 Zložitejšia implementácia Feynmanovho počítača pomocou troch operátorov C_{NOT}

Kvantová 2-qubitová brána riadenej negácie C_{NOT} (alebo Boolovej funkcie XOR) je určená vzťahom (7.3), jej maticová reprezentácia v báze stavov $\mathcal{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ má tvar

$$C_{NOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \quad (10.44)$$

Grafická reprezentácia tejto brány je znázornená na obr. 7.5. Pomocou troch brán C_{NOT} vytvoríme novú 3-qubitovú bránu znázornenú na obr. 11.3.



Obrázok 10.3.

Tabuľka 10.1. Argumenty a funkčné hodnoty 3-qubitovej brány z obr. 10.3

#	$T = 0$			$T = 1$			$T = 2$			$T = 3$		
	x_0	y_0	z_0	x_1	y_1	z_1	x_2	y_2	z_2	x_3	y_3	z_3
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	1	0	0	1	0	0	1
2	0	1	0	0	1	0	0	1	1	0	1	1
3	0	1	1	0	1	1	0	1	0	0	1	0
4	1	0	0	1	1	0	1	1	1	1	1	0
5	1	0	1	1	1	1	1	1	0	1	1	1
6	1	1	0	1	0	0	1	0	0	1	0	1
7	1	1	1	1	0	1	1	0	1	1	0	0

$$G = C_{NOT}(x, y) \otimes |1\rangle\langle 0| + C_{NOT}(y, z) \otimes |2\rangle\langle 1| + C_{NOT}(x, z) \otimes |3\rangle\langle 2| \quad (10.45)$$

kde symbol $C_{NOT}(x, y)$ reprezentuje 2-qubitový operátor pôsobiaci na „premenne“ x a y ,

$$\begin{aligned} \langle x, y, z | C_{NOT}(x, y) | x', y', z' \rangle &= \langle x, y | \underbrace{C_{NOT}(x, y) | x', y' \rangle}_{|x', x' \oplus y' \rangle} | z | z' \rangle = \langle x, y | x', x' \oplus y' \rangle \langle z | z' \rangle \\ &= \langle x | x' \rangle \langle y | x' \oplus y' \rangle \langle z | z' \rangle \end{aligned} \quad (10.46a)$$

podobný tvar majú aj ostatné dva operátory

$$\langle x, y, z | C_{NOT}(y, z) | x', y', z' \rangle = \langle x | x' \rangle \langle y | y' \rangle \langle z | y' \oplus z' \rangle \quad (10.46b)$$

$$\langle x, y, z | C_{NOT}(x, z) | x', y', z' \rangle = \langle x | x' \rangle \langle y | y' \rangle \langle z | x' \oplus z' \rangle \quad (10.46c)$$

Maticová reprezentácia operátora G má tvar

$$\mathbf{G} = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{C}_{NOT}(x,y) & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{C}_{NOT}(y,z) & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{C}_{NOT}(x,z) & \mathbf{0} \end{pmatrix} \quad (10.47)$$

Jebotlivé operátory riadenej negácie $\mathbf{C}_{NOT}(x,y)$, $\mathbf{C}_{NOT}(y,z)$, $\mathbf{C}_{NOT}(x,z)$ majú maticové reprezentácie v báze $\mathcal{B} = \{|000\rangle, |001\rangle, \dots, |111\rangle\}$

$$\mathbf{C}_{NOT}(x,y) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} \end{pmatrix}, \quad (10.48a)$$

$$\mathbf{C}_{NOT}(y,z) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{X} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{X} \end{pmatrix} \quad (10.48b)$$

$$\mathbf{C}_{NOT}(x,z) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{X} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{X} \end{pmatrix} \quad (10.48c)$$

Poznamenajme, že tieto maticové reprezentácie sú tvorené symetrickými maticami.

Hamiltonián systému je definovaný vzťahom

$$H = G + G^+$$

Celková báza v ktorej je definovaný hamiltonián H je tvorená tenzorovým súčinom množín obsahujúcej 3-qubitové vektory $\{|x, y, z\rangle; x, y, z = 0, 1\}$ a časových vektorov $\{|i\rangle; i = 0, 1, 2, 3\}$

$$B_{tot} = \{|x, y, z\rangle\} \otimes \{|i\rangle\} = \left\{ |\chi_{\alpha, i}\rangle = \underbrace{|\alpha\rangle}_{|x, y, z\rangle} \otimes |i\rangle \right\} \quad (10.49)$$

ktorá obsahuje $8 \times 4 = 32$ elementov. Maticová reprezentácia hamiltoniánu H v báze B_{tot} má tvar reálnej symetrickej matice typu (32×32)

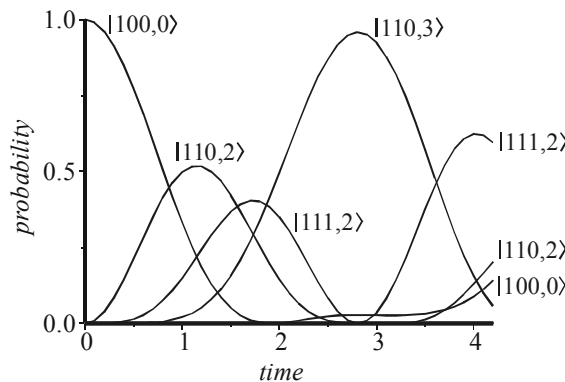
$$H = G + G^+ = \begin{pmatrix} \mathbf{0} & C_{NOT}(x, y) & \mathbf{0} & \mathbf{0} \\ C_{NOT}(x, y) & \mathbf{0} & C_{NOT}(y, z) & \mathbf{0} \\ \mathbf{0} & C_{NOT}(y, z) & \mathbf{0} & C_{NOT}(x, z) \\ \mathbf{0} & \mathbf{0} & C_{NOT}(x, z) & \mathbf{0} \end{pmatrix} \quad (10.50)$$

Počiatkový stav v čase $t = 0$ je určený vektorom $|\Psi(0)\rangle = |\chi_{0,0}\rangle = |0, 0, 0\rangle \otimes |0\rangle$, Podobne ako v predchádzajúcej kapitole, vektory z báze B_{tot} vyjadríme ako stĺpcové vektory

$$|\chi_{1,0}\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |\chi_{2,0}\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, |\chi_{3,0}\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, |\chi_{8,3}\rangle = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} \quad (10.51)$$

Formula (10.29) v tomto prípade reálneho hamiltoniánu má tento tvar

$$\begin{aligned} |\Psi(t)\rangle &= U(t) |\Psi(0)\rangle = e^{-iHt} |\Psi(0)\rangle = e^{-iHt} |\chi_{1,0}\rangle \\ &= \left(\underbrace{\sum_{k=1}^{32} \cos \lambda_k t \cdot \mathbf{x}_k \mathbf{x}_k^T}_{U_R(t)} + i \underbrace{(-1) \sum_{k=1}^{32} \sin \lambda_k t \cdot \mathbf{x}_k \mathbf{x}_k^T}_{U_I(t)} \right) |\chi_{1,0}\rangle \\ &= U_R(t) |\chi_{1,0}\rangle + i U_I(t) |\chi_{1,0}\rangle \\ &= (\alpha_1 + i\beta_1, \alpha_2 + i\beta_2, \dots, \alpha_{32} + i\beta_{32})^T \end{aligned} \quad (10.52)$$



Obrázok 10.4.

V čase $t = 0$ vlnová funkcia má tvar

$$|\Psi(0)\rangle = |\chi_1, 1\rangle = (1, 0, 0, 0, 0, 0)^T \quad (10.53a)$$

V čase $t = 1$ vlnová funkcia je špecifikovaná takto

$$\begin{aligned} |\Psi(1)\rangle &= U(1)|\Psi(0)\rangle = (U_R(1) + iU_I(1))|100, 0\rangle \\ &= 0.5767|100, 0\rangle - 0.7058i|110, 2\rangle - 0.3856|111, 2\rangle + 0.1432i|110, 3\rangle \end{aligned} \quad (10.53b)$$

V čase $t = 2.9$ vlnová funkcia má tvar

$$\begin{aligned} |\Psi(2.9)\rangle &= U(2.9)|\Psi(0)\rangle = (U_R(2.9) + iU_I(2.9))|100, 0\rangle \\ &= -0.1632|100, 0\rangle + 0.0133i|110, 2\rangle + 0.1882|111, 2\rangle + 0.9684i|110, 3\rangle \end{aligned} \quad (10.53c)$$

To znamená, že pre $t = 2.9$ vlnová funkcia je skoro presne vyjadrená pomocou stavu $|110, 3\rangle$, čo je aj v súhlase so skutočnosťou, že ak na vektor $|100, 0\rangle$ aplikujeme postupne tri operátory C_{NOT} stav $|100\rangle$ sa nám zmení na stav $|110\rangle$. Tento výsledok môžeme jednoducho verifikovať pomocou tabuľky 10.1, kde vidíme, že stav $|100\rangle$ v stĺpci pre $T = 0$ sa transformuje na stav $|110\rangle$ pre $T = 3$.

11. prednáška

Kvantové algoritmy I – Deutschov a Jozsov algoritmus a Simonov algoritmus

Kvantové algoritmy patria medzi najdôležitejšiu časť modernej oblasti informatiky, ktorá sa nazýva kvantové počítanie. Reprezentujú spojenie medzi kvantovou mechanikou a teóriou algoritmov klasickej počítačovej vedy, ktorá je založená na paradigme klasického počítania reprezentovanej univerzálnym Turingovým strojom a/alebo von Neumannovou architektúrou sekvenčných počítačov. Použitie zákonitostí kvantovej mechaniky, menovite princípu superpozície, umožňuje zaviesť vnútorný paralelizmus, ktorý otvára úplne nové možnosti pre implementáciu rôznych algoritmov, ktoré na klasických počítačoch (ekvivalentných s univerzálnym Turingovým strojom) boli nepredstaviteľné. Týmto spôsobom klasické algoritmy mohli byť preformulované na kvantovú verziu, čo obvykle znamenalo redukciiu ich numerickej zložitosti a teda aj ich podstatnú akceleráciu. Tento jav otvára úplne nové a netušené možnosti riešenia numerických problémov, ktoré sa doteraz zdali neriešiteľné (obvykle sa uvádzalo, že na procesore, ktorý vykonáva x špeciálnych operácií za sekundu, výpočet by trval y sekúnd, čo je podstatne viac, ako čas od *big bang* až po súčasnosť, t. j. 4.4×10^{17} sekúnd). Tak napríklad (Martin Nowak, 18. február 2005) zistenie, že číslo $2^{25964951}-1$ je prvočíslo, vyžadovalo obrovské mnohomesačné úsilie na gridovskej sieti stoviek PC počítačov s intelovskými PENTIUM procesormi, pozri obr. 11.1.

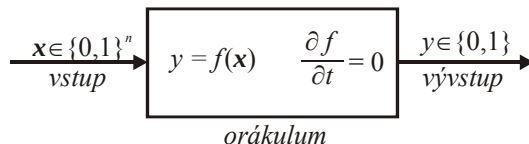


Obrázok 11.1. Poštové razítko z mesta Urbana, štát Illinois, oznamuje objav z r. 1963, že číslo $2^{11213}-1$ je prvočíslo.

Riešenie týchto a podobných problémov pomocou kvantových algoritmov (ktoré žiaľ vyžadujú zatiaľ neexistujúci nový hardware – kvantové počítače) bude dosiahnuté v priebehu niekoľkých sekúnd alebo minút. Táto potenciálna možnosť neobyčajne znervózňuje počítačových vedcov, ktorí pracujú v teórii moderných kryptovacích systémov, ktoré sú obvykle založené na skutočnosti, že nejaké číslo je prvočíslo, alebo je súčinom dvoch alebo viacerých prvočísel. Bezpečnosť týchto kódov vychádza z predpokladu, že verifikácia vyššie uvedených skutočností je numericke neobyčajne náročný problém, preto pravdepodobnosť „prelomenia“ kódu je veľmi malá. Tento predpoklad je platný len na klasických počítačoch, použitie kvantových počítačov ho falzifikuje, čo má za dôsledok hľadanie takých kryptovacích systémov, ktoré by aj pre kvantové počítače boli obtiažne prelomiteľné.

V kvantových algoritmoch sa intenzívne využíva metóda orákula, čo môžeme interpretovať ako zapuzdrený software, s dobre definovaným vstupom a výstupom, ktorý vstup zobrazí na binárny výstup – odpoveď, áno/nie. Spôsob implementácie orákula užívateľovi je neznámy, preto z jeho pohľadu orákulum môže byť interpretované ako čierna skrinka, nevieme akým spôsobom je vstup zobrazovaný na binárnych výstup typu áno/nie.

Obvykle sa predpokladá, že orákulum poskytne okamžité odpoveď, potom sa nemusí započítavať do časovej zložitosti algoritmu. V prípade, že tento čas je konečný, musí sa započítavať do časovej zložitosti algoritmu, jeho príspevok k časovej zložitosti je lineárny vzhľadom k počtu „dotazov“ na orákulum.



Obrázok 11.. Znázornenia orákula ako zariadenia, ktoré zobrazuje vstup na výstup, pričom toto zobrazenie je v čase nemenné. Užívateľ nemá prostriedky, aby zistil, akým spôsobom je toto zobrazenie implementované.

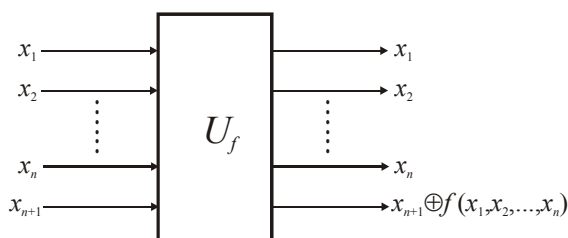
Pre jednoduchosť orákulum budeme špecifikovať ako Boolovu funkciu, obr. 11.1

$$f: \{0,1\}^n \rightarrow \{0,1\} \quad (11.1)$$

ktorá zobrazuje n -rozmerný binárny vektor $x \in \{0,1\}^n$ na binárny argument $f(x) \in \{0,1\}$. Problém reprezentácie Boolovej funkcie pomocou unitárneho zobrazenia bol študovaný v kapitole 9.1.5. Aplikácia unitárneho zobrazenia priradeného Boolovej funkcii (11.1) má tvar

$$\begin{aligned} U_f |x_1 x_2 \dots x_n, x_{n+1}\rangle &= U_f |x_1 x_2 \dots x_n\rangle \otimes |x_{n+1}\rangle \\ &= |x_1 x_2 \dots x_n\rangle \otimes |x_{n+1} \oplus f(x_1, x_2, \dots, x_n)\rangle \\ &= |x_1 x_2 \dots x_n, x_{n+1} \oplus f(x_1, x_2, \dots, x_n)\rangle \end{aligned} \quad (11.2)$$

Diagramatická reprezentácia tejto formule je znázornená na obr. 11.2.



Obrázok 11.2. Diagramatická interpretácia unitárneho operátora, ktorý realizuje Boolovu funkciu f obsahujúcu n premenných. Kvantová brána obsahuje $n+1$ vstupov a výstupov, posledná premenná x_{n+1} obsahuje na výstupe hodnotu Boolovej funkcie

11.1 Deutschov a Jozsov algoritmus

Tento kvantový algoritmus bol navrhnutý Deutschom v r. 1985 [xx] ako prvý algoritmus využívajúci vnútorný paralelizmus kvantových systémov, do podoby prezentovanej v tejto kapitole bol zovšeobecnený Deutschom a Jozsom v r. 1992 [xx] (pozri obr. 11.3).

Budeme študovať Boolovu funkciu $f: \{0,1\}^n \rightarrow \{0,1\}$. Táto funkcia sa nazýva *konštantná*, ak $\forall x, x' \in \{0,1\}^n: f(x) = f(x')$, t. j. pre každý argument $x \in \{0,1\}^n$ funkčná hodnota $f(x)$ je konštantná (0 alebo 1). Funkcia sa nazýva *vyvážená* (angl. balanced), ak množinu $\{0,1\}^n$ môžeme rozložiť na dve disjunktné časti rovnakej mohutnosti, $\{0,1\}^n = A \cup B$ a $|A| = |B| = 2^{n-1}$, aby platilo $\forall (x \in A) \forall (x' \in B): f(x) \neq f(x')$. Príklady týchto funkcií pre $n=2$ sú uvedené v tab. 11.1.

Tabuľka 11.1. Príklad konštantnej a vyváženej funkcie

x_1	x_2	konštantná funkcia	vyvážená funkcia (XOR)
0	0	1	0
0	1	1	1
1	0	1	1
1	1	1	0



Obrázok 11.3. David Deutsch, britský fyzik a informatik (narodený v Izraeli rodičom, pochádzajúcim z Rakúska), jeden zo zakladateľov kvantového počítania, pôsobiaci v Centre for Quantum Computation, University of Oxford. Je predstaviteľom mnoho-svetovej interpretácie kvantovej mechaniky (analogický prístup k sémantickej interpretácii výrokov v neklasických logikách zaviedol v polovici 60. rokov americký logik a filozof Saul Kripke).

Klasický algoritmus na zistenie toho, či funkcia f je konštantná alebo vyvážená, spočíva v tom, že preveríme polovicu riadkov plus jeden riadok tabuľky pravdivostných hodnôt funkcie, pomocou týchto údajov môžeme jednoznačne rozhodnúť, či funkcia je konštantná alebo vyvážená. To znamená, že zložitosť tohto postupu je $O(N)$, kde $N = 2^n$ je počet hodnôt argumentov funkcie f .

Pre lepšie pochopenie základných myšlienok Deutschovho algoritmu budeme diskutovať jeho najjednoduchšiu verziu pre $n = 1$, t. j. pre Boolove funkcie 1-premennej s dvoma hodnotami argumentu (s 0 a 1). V tomto jednoduchom prípade, funkcia f je vyvážená vtedy a len vtedy, ak $f(0) \neq f(1)$. Ukážeme, že na rozdiel od klasického algoritmu, kde na zistenie toho, či funkcia je konštantná alebo vyvážená potrebujeme dva pokusy, v kvantovom počítaní nám stačí len jeden pokus.

Pôvodný Deutschov algoritmus môžeme prehľadne vyjadriť pomocou týchto krokov:

1. krok. Inicializuje sa 2-qubitový register v stave $|\psi_1\rangle = |01\rangle = |0\rangle \otimes |1\rangle$.
2. krok. Aplikuje sa Hadamardov operátor na jednotlivé qubity v stave $|\psi_1\rangle$.

$$\begin{aligned}
 |\psi_2\rangle &= U_H^{\otimes 2} |\psi_1\rangle = (U_H |0\rangle) \otimes (U_H |1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle) \otimes (|0\rangle - |1\rangle) \\
 &= \frac{1}{2}(|0,0\rangle + |1,0\rangle - |0,1\rangle - |1,1\rangle)
 \end{aligned}
 \tag{11.3}$$

3. krok. Aplikuje sa orákulum reprezentované unitárnym operátorom U_f , ktorý je priradený Boolovej funkcii f (pozri (11.2))

$$\begin{aligned}
 |\psi_3\rangle &= U_f |\psi_2\rangle = \frac{1}{2} U_f (|0, 0 \oplus f(0)\rangle + |1, 0 \oplus f(1)\rangle - |0, 1 \oplus f(0)\rangle - |1, 1 \oplus f(1)\rangle) \\
 &= \frac{1}{2} (|0, f(0)\rangle + |1, f(1)\rangle - |0, \bar{f}(0)\rangle - |1, \bar{f}(1)\rangle) \\
 &= \frac{1}{2} (|0\rangle \otimes (|f(0)\rangle - |\bar{f}(0)\rangle) + |1\rangle \otimes (|f(1)\rangle - |\bar{f}(1)\rangle)) \\
 &= \frac{1}{2} \sum_{x=0,1} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)
 \end{aligned} \tag{11.4}$$

4. krok. Aplikuje sa Hadamardov operátor na prvý qubit stavu $|\psi_3\rangle$

$$\begin{aligned}
 |\psi_4\rangle &= U_H |\psi_3\rangle = \frac{1}{2} \sum_{x=0,1} (-1)^{f(x)} U_H |x\rangle (|0\rangle - |1\rangle) \\
 &= \frac{1}{2} \sum_{x=0,1} [(-1)^{f(x)} |0\rangle + (-1)^{x+f(x)} |1\rangle] \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \\
 &= \begin{cases} |0\rangle & (\text{pre } f(0) = f(1)) \\ |1\rangle & (\text{pre } f(0) \neq f(1)) \end{cases} \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
 \end{aligned} \tag{11.5}$$

5. krok. Aplikuje sa meranie k prvému qubit v báze $\{|0\rangle, |1\rangle\}$, v prípade, že funkcia je konštantná, dostaneme stav $|0\rangle$ s jednotkovou pravdepodobnosťou, v opačnom prípade, ak je funkcia vyvážená, dostaneme stav $|1\rangle$ s jednotkovou pravdepodobnosťou.

Týmto sme dokázali, že v kvantovom počítaní stačí použiť jeden pokus na jednoznačnú špecifikáciu toho, či funkcia f s jedným argumentom je konštantná alebo vyvážená.

V čom sa odlišuje kvantový algoritmus od klasického algoritmu? V *druhom kroku* sme aplikovali Hadamardov operátor na stav $|\psi_1\rangle = |01\rangle = |0\rangle \otimes |1\rangle$ na zostrojenie superpozície všetkých 2-qubitových stavov, čo je v klasickom prístupe nemožné. Tento prechod od jedného stavu k superpozícii všetkých možných stavov reprezentuje v kvantových algoritmoch vnútorný paralelizmus, ktorý je principiálne dôležitý pre výhodnosť kvantových algoritmov pred klasickými algoritmi. V *treťom kroku* aplikujeme orákulum jedinou operáciou na všetky stavy systému, čo je možné, podobne ako v predchádzajúcom prípade, len v kvantových algoritmoch. Táto skutočnosť je prejavom už zmieneného vnútorného paralelizmu kvantových algoritmov. V klasickom algoritme, keď chceme vyhodnotiť pomocou orákula všetky elementy z nejakej množiny, tak musíme aplikovať orákulum jednotlivo a postupne ku všetkým elementom množiny.

V ďalšej časti tejto kapitoly vykonáme zovšeobecnenie použitej metódy pre Boolove funkcie s dvoma alebo viacerými argumentmi, $n \geq 2$:

1. krok. Inicializuje sa $(n+1)$ -qubitový register v stave $|\psi_1\rangle = |\mathbf{0}, 1\rangle = \underbrace{|00\dots 0\rangle}_{n\text{-krát}} \otimes |1\rangle$.
2. krok. Aplikuje sa Hadamardov operátor na jednotlivé qubity v stave $|\psi_1\rangle$

$$\begin{aligned}
 |\psi_2\rangle &= U_H^{\otimes(n+1)} |\psi_1\rangle = \underbrace{(U_H |0\rangle) \otimes (U_H |0\rangle) \otimes \dots \otimes (U_H |0\rangle)}_{n\text{-krát}} \otimes (U_H |1\rangle) \\
 &= \frac{1}{2^{n/2}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
 \end{aligned} \tag{11.6}$$

3. krok. Aplikuje sa orákulum reprezentované unitárnym operátorom U_f , ktorý je priradený Boolovej funkcii f (pozri (11.2))

$$\begin{aligned}
 |\psi_3\rangle &= U_f |\psi_1\rangle = \frac{1}{2^{n/2}} U_f \left(\sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right) \\
 &= \frac{1}{2^{n/2}} \sum_{\mathbf{x} \in \{0,1\}^n} |\mathbf{x}\rangle \otimes \frac{1}{\sqrt{2}} \underbrace{(|f(\mathbf{x})\rangle - |\bar{f}(\mathbf{x})\rangle)}_{(-1)^{f(\mathbf{x})}(|0\rangle - |1\rangle)} \\
 &= \frac{1}{2^{n/2}} \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
 \end{aligned} \tag{11.7}$$

4. krok. Aplikuje sa Hadamardov operátor na prvých n qubitov, po algebraických úpravách dostaneme (použijeme formulu z príkladu 11.1)

$$\begin{aligned}
 |\psi_4\rangle &= U_H^{\otimes n} |\psi_3\rangle = \\
 &= \frac{1}{2^{n/2}} \sum_{\mathbf{x}' \in \{0,1\}^n} \left(\sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{\mathbf{x} \cdot \mathbf{x}' + f(\mathbf{x})} \right) |\mathbf{x}'\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)
 \end{aligned} \tag{11.8a}$$

kde $\mathbf{x} \cdot \mathbf{x}' = x_1 x'_1 + x_2 x'_2 + \dots + x_n x'_n$ je skalárny súčin. Predpokladajme, že f je konštantná funkcia, potom sumácia v zátvorke je nenulová len pre $\mathbf{x}' = 0$; to znamená, že pre konštantnú funkciu f stavový vektor $|\psi_4\rangle$ obsahuje len $|0\rangle$. V opačnom prípade, ak funkcia f je vyvážená, potom sumácia v zátvore pre $\mathbf{x}' = 0$ je nulová, potom stavový vektor $|\psi_4\rangle$ neobsahuje stav $|0\rangle$. Tieto závery vyjadríme tak, že (11.8) prepíšeme do tvaru

$$|\psi_4\rangle = \frac{1}{2^{n/2}} \left\{ \begin{array}{l} |0\rangle \quad (f \text{ je konštantná}) \\ \sum_{\mathbf{x}' \in \{0,1\}^n} |\mathbf{x}'\rangle \quad (f \text{ je vyvážená}) \end{array} \right\} \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \tag{11.8b}$$

5. krok. Aplikuje sa meranie k prvému n -qubitovému stavu $|0\rangle$, ak ho nameráme, potom funkcia f je konštantná, v opačnom prípade, ak oho nenameráme, funkcia f je vyvážená.

Týmto sme dokázali, že meraním stavov prvých n qubitov s určitou zistíme vlastnosť (konštantnosť alebo vyváženosť) funkcie f .

Príklad 11.1. Dokážte formulu

$$U_H^{\otimes n} |\mathbf{x}\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{x}' \in \{0,1\}^n} (-1)^{\mathbf{x} \cdot \mathbf{x}'} |\mathbf{x}'\rangle$$

kde $\mathbf{x} \cdot \mathbf{x}' = x_1 x'_1 + x_2 x'_2 + \dots + x_n x'_n$ je skalárny súčin dvoch binárnych vektorov $\mathbf{x} = (x_1 x_2 \dots x_n) \in \{0,1\}^n$ a $\mathbf{x}' = (x'_1 x'_2 \dots x'_n) \in \{0,1\}^n$.

Príklad 11.2. Diskutujte vlastnosti výrazu

$$\sum_{x \in \{0,1\}^n} (-1)^{x \cdot x' + f(x)}$$

pre konštantnú a vyváženú Boolovu funkciu f .

Príklad 11.3. V príklade 11.1 je použitý skalárny súčin, diskutujte dôsledky predpokladu, keď sumácia v skalárnom súčine je definovaná ako XOR operácia (súčet modulo 2).

11.2 Simonov algoritmus

D. Simon v r. 1994 [xx] navrhol kvantový algoritmus, ktorý bol stimulovaný Deutschovým a Jozsovim algoritmom, avšak Boolovu funkciu špecifikoval iným spôsobom. Nech $f: \{0,1\}^n \rightarrow \{0,1\}^n$ je „vektorová“ Boolova funkcia, ktorá zobrazuje binárne reťazce dĺžky n na binárne reťazce taktiež dĺžky n . Budeme predpokladať, že funkčné hodnoty funkcie f sú špecifikované orákulom, kde vstup je argument $x \in \{0,1\}^n$ a výstup je funkčná hodnota $y = f(x) \in \{0,1\}^n$.

Definícia 11.1. Boolova funkcia $f: \{0,1\}^n \rightarrow \{0,1\}^n$ sa nazýva **periodická** vtedy a len vtedy, ak existuje taký nenulový vektor (**perióda**) $p = (p_1 p_2 \dots p_n) \in \{0,1\}^n$, aby bola splnená podmienka

$$\forall (x, y \in \{0,1\}^n): (x \neq y) \wedge (f(x) = f(y)) \Leftrightarrow x = y \oplus p \quad (11.9)$$

V prípade, že funkcia f je 1-1-značná, potom nie je periodická (perióda p neexistuje). Ak funkcia f je konštantná, potom táto funkcia je periodická tak, že každý binárny vektor $p \in \{0,1\}^n$ je periódou.

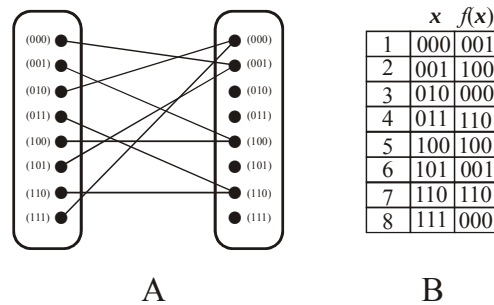
Veta 11.1. Boolova funkcia $f: \{0,1\}^n \rightarrow \{0,1\}^n$ je periodická s periódou p vtedy a len vtedy, ak

$$\forall (x \in \{0,1\}^n) \exists! (y \in \{0,1\}^n): (x \neq y) \wedge (f(x) = f(y)) \wedge (x = y \oplus p) \quad (11.10)$$

Ilustrácia tejto vety je znázornená na obr. 11.4. Jej dôkaz vykonáme v dvoch krokoch:

(1) $\Rightarrow$, predpokladajme je periodická s periódou p , potom podľa definície (11.1) platí relácia, ktorá je skoro totožná s reláciou (11.10) dokazovanej vety, odlišuje sa jedine podmienkou jednoznačnosti existencie dvojice x a y . Predpokladajme, že existujú dva rôzne vektory y a y' , ktoré vyhovujú relácii (11.10), t. j. musí platiť $x = y \oplus p$ a $x = y' \oplus p$, „riešením“ týchto rovníc dostaneme $y = x \oplus p$ a $y' = x \oplus p$, z čoho plynie $y = y'$, čo je v kontradikcii s pôvodným predpokladom, že vektory y a y' sú rôzne. Týmto sme dokázali, že definičná podmienka (11.9) implikuje podmienku (11.10) z dokazovanej vety.

(2) $\Leftarrow$, predpokladajme platnosť podmienky (11.10) pre periódu p , potom automaticky musí platiť aj definičná podmienka (11.9), t. j. funkcia f je periodická. $\square$



Obrázok 11.4. Znáozornenie periodického zobrazenia $f: \{0,1\}^3 \rightarrow \{0,1\}^3$ s periódou $p = (010)$. Z obrázku vyplýva, že dva rôzne argumenty x a y , medzi ktorými existuje vzťah $x = y \oplus p$, sú vždy zobrazené práve na jeden obraz $f(x) = f(y) \in \{0,1\}^3$, hovoríme, že zobrazenie je 2-na-1.

Problém hľadania periódy Boolovej funkcie je veľmi dôležitý v kryptografii; ak vieme v polynomiálnom čase nájsť periódu funkcie, potom vieme aj v polynomiálnom čase prelomiť *RSA kryptovací algoritmus* s verejným kľúčom. Simonov algoritmus bol silnou inšpiráciou pre Shooru [xx] pri návrhu jeho kvantového algoritmu pre nájdenie faktorizácie prirodzeného čísla na súčin prvočísel.

Klasický prístup k hľadaniu periódy zobrazenia $f: \{0,1\}^n \rightarrow \{0,1\}^n$ je exponenciálne náročný (množina $\{0,1\}^n$ obsahuje $N = 2^n$ elementov, preto pri prehľadávaní všetkých možných dvojíc musíme vykonať $2^n(2^n-1)/2$ dvojíc aktivácií orákula. Ako bude ukázané neskôr, Simonov kvantový algoritmus rieši tento problém v zložitosti $O(n)$, takže predstavuje exponenciálnu akceleráciu klasického algoritmu.

Podobne ako v predchádzajúcom príklade budeme prezentovať Simonov algoritmus pomocou jeho jednotlivých krokov:

1. krok. Inicializuje sa $2n$ -qubitový register v stave $|\psi_1\rangle = |\mathbf{0}\rangle \otimes |\mathbf{0}\rangle = \underbrace{|00\dots 0\rangle}_{n\text{-krát}} \otimes \underbrace{|00\dots 0\rangle}_{n\text{-krát}}$.

2. krok. Aplikuje sa Hadamardov operátor na prvých n qubitov v stave $|\psi_1\rangle$

$$\begin{aligned}
 |\psi_2\rangle &= U_H^{\otimes n} |\psi_1\rangle = \underbrace{(U_H |\mathbf{0}\rangle) \otimes (U_H |\mathbf{0}\rangle) \otimes \dots \otimes (U_H |\mathbf{0}\rangle)}_{n\text{-krát}} \otimes |\mathbf{0}\rangle \\
 &= \frac{1}{2^{n/2}} \left(\sum_{x \in \{0,1\}^n} |x\rangle \right) \otimes |\mathbf{0}\rangle
 \end{aligned}
 \tag{11.11}$$

3. krok. Aplikuje sa unitárny operátor U_f na prvých n qubitov stavu $|\psi_2\rangle$, ďalších n qubitov je použitých na funkčnú hodnotu (pozri (11.2))

$$|\psi_3\rangle = U_f |\psi_2\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle |f(x)\rangle
 \tag{11.12}$$

4. krok. Aplikuje sa Hadamardov operátor na prvých n qubitov, použijeme formulu z príkladu 11.1, po algebraických úpravách dostaneme

$$\begin{aligned}
 |\psi_4\rangle &= U_H^{\otimes n} |\psi_3\rangle = \frac{1}{2^{n/2}} \sum_{\mathbf{x} \in \{0,1\}^n} (U_H^{\otimes n} |\mathbf{x}\rangle) |f(\mathbf{x})\rangle \\
 &= \frac{1}{2^n} \sum_{\mathbf{x}, \mathbf{x}' \in \{0,1\}^n} (-1)^{\mathbf{x} \cdot \mathbf{x}'} |\mathbf{x}'\rangle |f(\mathbf{x})\rangle \\
 &= \frac{1}{2^{n+1}} \sum_{\mathbf{x}, \mathbf{x}' \in \{0,1\}^n} \left[(-1)^{\mathbf{x} \cdot \mathbf{x}'} + (-1)^{(\mathbf{x} \oplus \mathbf{p}) \cdot \mathbf{x}'} \right] |\mathbf{x}'\rangle |f(\mathbf{x})\rangle
 \end{aligned} \tag{11.13}$$

Pri prechode od druhého do tretieho riadku sme použili skutočnosť, že transformácia $\mathbf{x} \mapsto \mathbf{x} \oplus \mathbf{p}$ zachováva množinu binárnych vektorov $\{0,1\}^n$, potom platí

$$\begin{aligned}
 \sum_{\mathbf{x}, \mathbf{x}' \in \{0,1\}^n} (-1)^{\mathbf{x} \cdot \mathbf{x}'} |\mathbf{x}'\rangle |f(\mathbf{x})\rangle &= \sum_{\mathbf{x}, \mathbf{x}' \in \{0,1\}^n} (-1)^{(\mathbf{x} \oplus \mathbf{p}) \cdot \mathbf{x}'} |\mathbf{x}'\rangle |f(\mathbf{x} \oplus \mathbf{p})\rangle \\
 &= \sum_{\mathbf{x}, \mathbf{x}' \in \{0,1\}^n} (-1)^{(\mathbf{x} \oplus \mathbf{p}) \cdot \mathbf{x}'} |\mathbf{x}'\rangle |f(\mathbf{x})\rangle
 \end{aligned} \tag{11.14}$$

kde sme použili skutočnosť, že funkcia f má periódu $\mathbf{p}$. Použitím tejto relácie dostaneme vzťah z tretieho riadku. Druhý člen v hranatej zátvorke (11.13) môže byť vyjadrený takto

$$(-1)^{(\mathbf{x} \oplus \mathbf{p}) \cdot \mathbf{x}'} = (-1)^{\mathbf{x} \cdot \mathbf{x}'} (-1)^{\mathbf{p} \cdot \mathbf{x}'} \tag{11.15}$$

potom finálny tvar (11.13) pre $|\psi_4\rangle$ má tvar

$$|\psi_4\rangle = \frac{1}{2^{n+1}} \sum_{\mathbf{x}, \mathbf{x}' \in \{0,1\}^n} \left[(-1)^{\mathbf{x} \cdot \mathbf{x}'} (1 + (-1)^{\mathbf{p} \cdot \mathbf{x}'}) \right] |\mathbf{x}'\rangle |f(\mathbf{x})\rangle \tag{11.16}$$

Všetky vektory $\mathbf{x}'$ môžeme rozdeliť do dvoch tried, prvá (druhá) trieda je určená podmienkou $\mathbf{x}' \cdot \mathbf{p} = 1$ ($\mathbf{x}' \cdot \mathbf{p} = 0$), pričom predpokladáme, že pri definícii skalárneho súčinu je použitá operácia súčtu XOR (súčet modulo 2) potom

$$|\psi_4\rangle = \begin{cases} 0 & (\text{pre } \mathbf{p} \cdot \mathbf{x}' = 1) \\ \frac{1}{2^{n-1}} \sum_{\mathbf{x}' \in \{0,1\}^n} \left(\sum_{\mathbf{y} \in I_f} (-1)^{\mathbf{x}_y \cdot \mathbf{x}'} |\mathbf{y}\rangle \right) |\mathbf{x}'\rangle & (\text{pre } \mathbf{p} \cdot \mathbf{x}' = 0) \end{cases} \tag{11.17}$$

kde sme použili označenie $\mathbf{y} = f(\mathbf{x}) \in I_f = f(\{0,1\}^n) \subseteq \{0,1\}^n$, kde I_f je množina funkčných hodnôt zobrazenia f (image), a $\mathbf{x}_y$ je argument, ktorý je zobrazený na $\mathbf{y}$; poznamenajme, že ku každému obrazu $\mathbf{y}$ existujú dva argumenty $\mathbf{x}_y$ a $\mathbf{x}'_y$.

5. krok. Aplikuje sa meranie k prvému n -qubitovému stavu $|\mathbf{x}'\rangle$, ak ho nameriame (s pravdepodobnosťou $1/2^{n-1}$), potom platí $\mathbf{p} \cdot \mathbf{x}' = 0$.

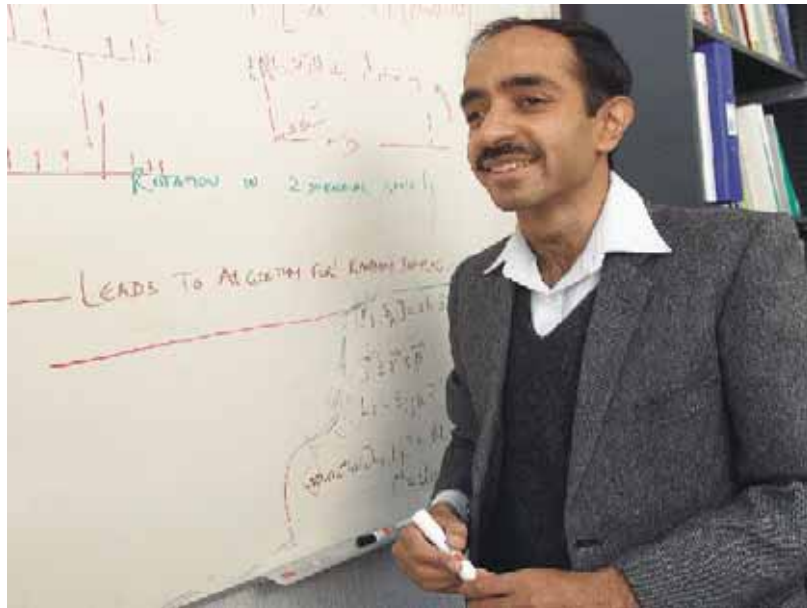
Naznačeným postupom zostrojíme sadu binárnych vektorov $\{\mathbf{x}'_1, \mathbf{x}'_2, \dots, \mathbf{x}'_q\}$, ktoré vyhovujú podmienke $\mathbf{p} \cdot \mathbf{x}' = 0$, t. j. zostrojili sme systém homogénnych rovníc

$$\begin{aligned}
 \mathbf{p} \cdot \mathbf{x}'_1 &= 0 \\
 \mathbf{p} \cdot \mathbf{x}'_2 &= 0 \\
 &\dots\dots\dots \\
 \mathbf{p} \cdot \mathbf{x}'_q &= 0
 \end{aligned} \tag{11.18}$$

Riešením tohto systému pomocou Gaussovej eliminačnej metódy zostrojíme vektor $\mathbf{p}$.

12. prednáška

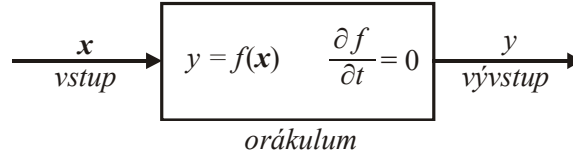
Kvantové algoritmy II – Groverov algoritmus prehľadávania



Obrázok 12.1. Americký teoretický informatik Lov K. Grover, ktorý pracuje v Bellovych laboratóriách v Murray Hill NJ, USA.

Predstavme si, že stojíme pred problémom ako v neusporiadanej databáze obsahujúcej N položiek máme nájsť špecifikovanú položku. Ako príklad tejto úlohy môže byť problém nájsť v bratislavskom telefónnom zozname meno užívateľa telefónu na základe daného telefónneho čísla. Jednoduchá stratégia ako riešiť túto úlohu spočíva v tom, že si telefónny zoznam rozdelíme na dve polovice a náhodne vyberieme jednu z nich. Ak máme šťastie (s 50% pravdepodobnosťou), nájdeme vo vybranej polovici telefónneho zoznamu užívateľa, ktorého telefónne číslo sa zhoduje s daným číslom. Jednoduchými úvahami sa dá dokázať, že musíme prehľadať $N/2$ položiek s pravdepodobnosťou $P = 1/2$, čiže zložitosť tohto jednoduchého prehľadávacieho algoritmu je $o(N)$. Ukazuje sa, že tento výsledok pre počítače, ktoré majú von Neumannovu architektúru už nemôže byť vylepšený nejakou inou stratégiou prehľadávania (iná situácia nastane, ak použijeme počítač s paralelnou architektúrou, potom výsledok uvedený vyššie môže byť podstatne vylepšený). Groverov kvantový algoritmus rieši túto úlohu tak, že s vysokou pravdepodobnosťou je potrebné vykonať len $\sqrt{N}$ prehľadávanií, čiže zložitosť z lineárnej $o(N)$ klesla na $o(N^{1/2})$.

Prv než pristúpime k formulovaniu kvantového Groverovho algoritmu, definujme **orákulum** ako uzavretý systém, ktorý má špecifikovaný vstup a výstup, pričom na výstupe je zobrazenie vstupu a toto zobrazenie je v celej histórii orákula nemenné a taktiež nepoznáme štruktúru tohto zobrazenie, pozri obr. 12.2.



Obrázok 12.2. Znázornenia orákula ako zariadenia, ktoré zobrazuje vstup na výstup, pričom toto zobrazenie je v čase nemenné. Užívateľ nemá prostriedky, aby zistil, akým spôsobom je toto zobrazenie implementované.

Pre jednoduchosť predpokladajme, že orákulum je špecifikované Boolovou funkciou

$$f : \{0,1\}^n \rightarrow \{0,1\} \quad (12.1)$$

Označme $\mathbf{a} \in \{0,1\}^n$ ako **riešenie** orákula, potom platí

$$f(\mathbf{x}) = \begin{cases} 1 & (\text{ak } \mathbf{x} = \mathbf{a}) \\ 0 & (\text{ak } \mathbf{x} \neq \mathbf{a}) \end{cases} \quad (12.2)$$

Aby táto úloha bola výpočtovo zaujímavá, musíme predpokladať, že počet riešení M je o mnoho rádov menší ako počet $N = 2^n$ všetkých možných argumentov funkcie f , $M \ll N = 2^n$. Tak napríklad pre $n = 100$ a jedno existujúce riešenie, $M = 1$, orákulum len jeden argument z množiny obsahujúcej $2^{100} \approx 10^{30}$ možných argumentov ohodnotí funkčnou hodnotou 1.

Nech orákulum je kvantové, jeho špecifikácia pomocou stavových vektorov nech má tvar $|\mathbf{x}\rangle|q\rangle$, kde $|\mathbf{x}\rangle$ indexový register orákula obsahujúci n binárnych položiek a $|q\rangle$ je qubit orákula. Kvantové orákulum je špecifikované unitárnym operátorom O

$$O|\mathbf{x}\rangle|q\rangle = |\mathbf{x}\rangle|q \oplus f(\mathbf{x})\rangle \quad (12.3)$$

ktorý zmení qubit orákula, ak $\mathbf{x}$ je riešenie. Táto definícia operátora O nám umožňuje skontrolovať, či binárny vektor $\mathbf{x} \in \{0,1\}^n$ je riešenie, v prvom kroku si pripravíme stavový vektor $|\mathbf{x}\rangle|0\rangle$, v druhom kroku aplikujeme naň operátor O , ak sa zmení orákulový qubit, potom $\mathbf{x}$ je riešenie. V kvantovom algoritme prehľadávania je výhodné špecifikovať orákulový stav ako vektor $(|0\rangle - |1\rangle)/\sqrt{2}$. Ak $\mathbf{x}$ nie je riešenie, potom táto časť stavového vektora sa nemení, v opačnom prípade, ak $\mathbf{x}$ je riešenie, potom na základe (12.3) táto časť zmení znamienko

$$O|\mathbf{x}\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \quad (12.4)$$

To znamená, že orákulový stav $(|0\rangle - |1\rangle)/\sqrt{2}$ sa v priebehu aplikácie operátora O nemení, čiže môže byť vynechaný ako nepodstatný

$$O|\mathbf{x}\rangle = (-1)^{f(\mathbf{x})} |\mathbf{x}\rangle \quad (12.5)$$

Tieto úvodné úvahy môžeme zosumarizovať tak, že orákulum (operátor O) označí všetky stavové vektory $|\mathbf{x}\rangle$, pre ktoré platí $\mathbf{x} = \mathbf{a}$ (t. j. sú riešením) tak, že zmení fázu ich stavového vektora, v opačnom prípade, ak platí $\mathbf{x} \neq \mathbf{a}$ (t. j. nie sú riešením) tak, ich fáza sa zachováva.

Operátor orákula môžeme formálne vyjadriť takto

$$O = 1 - 2|\mathbf{a}\rangle\langle\mathbf{a}| \quad (12.6)$$

Lahko sa presvedčíme, že takto špecifikovaný operátor orákula vyhovuje podmienke (12.5): pre $\mathbf{x} \neq \mathbf{a}$ dostaneme

$$O|x\rangle = (1 - 2|a\rangle\langle a|)|x\rangle = |x\rangle - 2\underbrace{|a\rangle\langle a|x\rangle}_0 = |x\rangle \quad (12.7a)$$

pre $x = a$ dostaneme

$$O|a\rangle = (1 - 2|a\rangle\langle a|)|a\rangle = |a\rangle - 2\underbrace{|a\rangle\langle a|a\rangle}_1 = -|a\rangle \quad (12.7b)$$

Operátor orákula zachováva stavové vektory $|x\rangle$, ktoré sú ortogonálne k riešeniu $|a\rangle$, a zmení znamienkou stavového vektora riešenia $|a\rangle$. Táto transformácia má jednoduchú interpretáciu, jeho pôsobenie na ľubovoľný vektor z 2^n lineárneho priestoru $\{|x_1, \dots, x_n\rangle\}$ spočíva v jeho zobrazení do hyperroviny ortogonálnej k vektoru $|a\rangle$, ktoré zachováva komponentu ležiacu v hyperrovine a mení znamienko komponenty kolineárnej so s riešením $|a\rangle$.

Niekoľko môže namietat', že teoretický prístup ku konštrukcii kvantového prehľadávacieho algoritmu, ktorý predpokladá existenciu orákula, je pofiderný. Dôvodí sa, že postulát existencie orákula je vlastne ekvivalentný s predpokladom, že poznáme riešenie problému. V tejto súvislosti musíme poznamenať, že je potrebné rozlišovať medzi tým, že poznáme riešenie a tým, že sme schopný rekognoskovať, či x je riešenie alebo nie. Používané orákulum je založené na druhej skutočnosti, preveruje či dané x je riešenie alebo nie, nič nám nehovorí o tom, aké je správne riešenie.

Definujme **Groverov operátor**

$$G = (2|\psi\rangle\langle\psi| - I)O \quad (12.8)$$

kde O je orákulum (12.6) a $|\psi\rangle$ je n -qubitový stavový vektor, ktorý je možno zostrojiť (9.6) pomocou aplikácie Hadamardových operátorov na $|\theta\rangle = |0\rangle \otimes \dots \otimes |0\rangle$

$$\begin{aligned} |\psi\rangle &= (H|0\rangle) \otimes (H|0\rangle) \otimes \dots \otimes (H|0\rangle) = (H \otimes H \otimes \dots \otimes H)|00\dots 0\rangle \\ &= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \dots \otimes (|0\rangle + |1\rangle) = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \end{aligned} \quad (12.9)$$

Matematické vlastnosti tohto operátora G sú základom pre implementáciu Groverovho kvantového algoritmu pre prehľadávanie.

Veta 12.1. Aplikácia operátora $R_\psi = (2|\psi\rangle\langle\psi| - I)$ na stavový vektor $|\phi\rangle = \sum_{y=0}^{2^n-1} \alpha_y |y\rangle$ poskytuje

$$R_\psi |\phi\rangle = \sum_{y=0}^{2^n-1} [2\langle\alpha\rangle - \alpha_y] |y\rangle \quad (12.10)$$

kde $\langle\alpha\rangle = (1/2^n) \sum_y \alpha_y$ je priemerná hodnota koeficientov α_y .

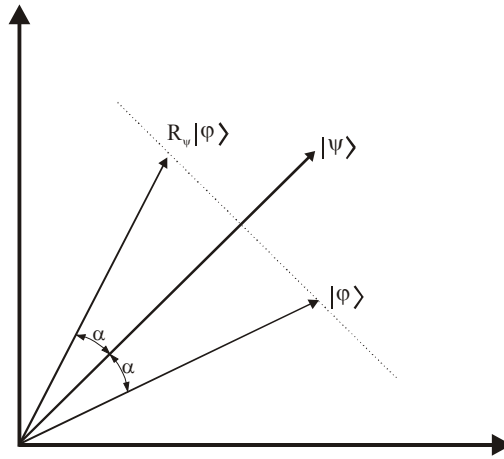
Operátor $R_\psi = (2|\psi\rangle\langle\psi| - I)$ môžeme vyjadriť takto

$$R_\psi = 2|\psi\rangle\langle\psi| - I = \frac{1}{2^{n-1}} \sum_{x,x'=0}^{2^n-1} |x\rangle\langle x'| - I \quad (12.11)$$

aplikovaním tejto formuly na $|\phi\rangle$ dostaneme

$$\begin{aligned}
 R_\psi |\phi\rangle &= \frac{1}{2^{n-1}} \sum_{x,x',y=0}^{2^n-1} \alpha_y \underbrace{\langle x'|y\rangle}_{\delta_{xy}} |x\rangle - \sum_{y=0}^{2^n-1} \alpha_y |y\rangle \\
 &= \sum_{x=0}^{2^n-1} \underbrace{\left(\frac{2}{2^n} \sum_{y=0}^{2^n-1} \alpha_y \right)}_{\langle \alpha \rangle} |x\rangle - \sum_{y=0}^{2^n-1} \alpha_y |y\rangle = \sum_{y=0}^{2^n-1} (2\langle \alpha \rangle - \alpha_y) |y\rangle
 \end{aligned} \tag{12.12}$$

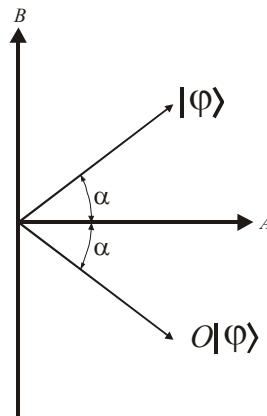
Operátor $R_\psi = (2|\psi\rangle\langle\psi| - I)$ sa nazýva niekedy aj ako operátor inverzie vzhľadom k priemernej hodnote. Jeho geometrická interpretácia je znázornená na obr. 12.3.



Obrázok 12.3. Aplikácia operátora R_ψ na vektor $|\phi\rangle$ spočíva v jeho reflexii vzhľadom k vektoru $|\psi\rangle$.

Podobným spôsobom môžeme interpretovať aj pôsobenie orákula O na vektor stavový vektor $|\phi\rangle$. Tento vektor rozdelíme na dve časti, prvá časť obsahuje vektory $|x\rangle$, ktorú nie sú riešením, zatiaľ čo druhá časť bude obsahovať vektory, ktoré sú riešením

$$|\phi\rangle = \sum_x \alpha_x |x\rangle = \underbrace{\sum_{x \in A} \alpha_x |x\rangle}_{|\phi_A\rangle} + \underbrace{\sum_{x \in B} \alpha_x |x\rangle}_{|\phi_B\rangle} = |\phi_A\rangle + |\phi_B\rangle \tag{12.13}$$



Obrázok 12.4. Grafická interpretácia pôsobenia orákula O na stavový vektor $|\phi\rangle$, ktorá spočíva v reflexii tohto vektora v hyperrovine obsahujúcej vektory $|x\rangle$, ktoré nie sú riešeniami.

Orákulum O je špecifikované takto

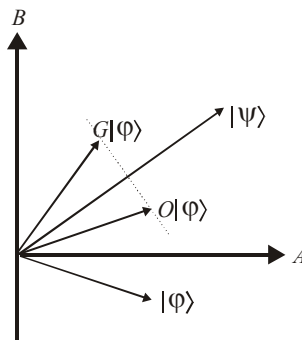
$$O|x\rangle = \begin{cases} |x\rangle & (|x\rangle \in A) \\ -|x\rangle & (|x\rangle \in B) \end{cases} \quad (12.14)$$

Aplikácia orákula na stav $|\phi\rangle$ je určená takto

$$O|\phi\rangle = O(|\phi_A\rangle + |\phi_B\rangle) = |\phi_A\rangle - |\phi_B\rangle \quad (12.15)$$

Grafická interpretácia aplikácie orákula O na vektor $|\phi\rangle$ je znázornená na obr. 12.4.

Spojením týchto dvoch interpretácií operátorov R_ψ a O môžeme zostrojiť grafickú interpretáciu Groverovho operátora G , ktorý je súčinom týchto dvoch operátorov, $G = R_\psi O$, pozri obr. 12.5.



Obrázok 12.5. Grafická interpretácia pôsobenia Groverovho operátora G na stavový vektor $|\phi\rangle$. V prvom kroku vykonáme reflexiu vektora $|\phi\rangle$ vzhľadom k hyperrovine reprezentovanej osou A . V druhom kroku vykonáme reflexiu R_ψ vzhľadom k vektoru $|\psi\rangle$. Spojením týchto dvoch reflexií dostaneme rotáciu vektora $|\phi\rangle$ na výsledný vektor $G|\phi\rangle$.

Obrátime našu pozornosť na analytické vyjadrenie tvorby vektora $G|\psi\rangle$, vektor $|\psi\rangle$ rozdelíme na dve normalizované časti

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{N}} \sum_x |x\rangle = \sqrt{\frac{N-M}{N}} \underbrace{\frac{1}{\sqrt{N-M}} \sum_{x \in A} |x\rangle}_{|\psi_A\rangle} + \sqrt{\frac{M}{N}} \underbrace{\frac{1}{\sqrt{M}} \sum_{x \in B} |x\rangle}_{|\psi_B\rangle} \\ &= \sqrt{\frac{N-M}{N}} |\psi_A\rangle + \sqrt{\frac{M}{N}} |\psi_B\rangle \end{aligned} \quad (12.16)$$

kde $N = 2^n$, $|B| = M$, $|A| = N - M$. Aplikácia operátora O k takto upravenému stavovému vektoru $|\psi\rangle$ je špecifikovaná týmto jednoduchým vzťahom

$$O|\psi\rangle = O\left(\sqrt{\frac{N-M}{N}} |\psi_A\rangle + \sqrt{\frac{M}{N}} |\psi_B\rangle\right) = \sqrt{\frac{N-M}{N}} |\psi_A\rangle - \sqrt{\frac{M}{N}} |\psi_B\rangle \quad (12.17)$$

Aplikácia operátora R_ψ k $O|\psi\rangle$ sa získa pomocou geometrickej interpretácie tohto operátora, pozri obr. 12.6.

Použitím vzťahu (12.16) a geometrickej interpretácie znázornenej na obr. 12.16 môžeme stavový vektor $|\psi\rangle$ písať takto

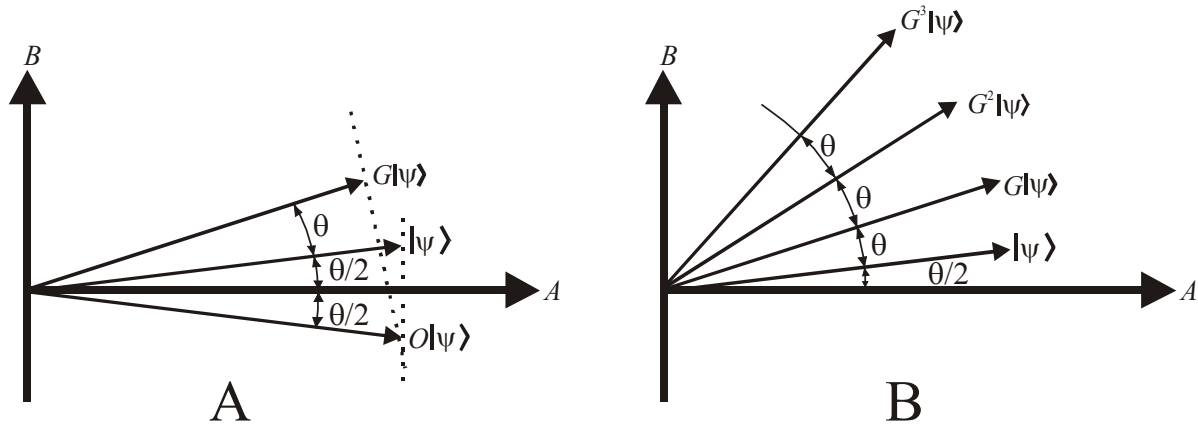
$$|\psi\rangle = \cos \frac{\vartheta}{2} |\psi_A\rangle + \sin \frac{\vartheta}{2} |\psi_B\rangle \quad (12.18a)$$

pričom

$$\cos \frac{\vartheta}{2} = \sqrt{\frac{N-M}{N}} \quad (12.18b)$$

Použijúc analógiu s týmto vzťahom (12.18a) môžeme podľa obr. 12.6 písať vektor $G|\psi\rangle$ takto

$$G|\psi\rangle = \cos \frac{3\vartheta}{2} |\psi_A\rangle + \sin \frac{3\vartheta}{2} |\psi_B\rangle \quad (12.19)$$



Obrázok 12.6. (A) Grafická interpretácia pôsobenia Groverovho operátora G na stavový vektor $|\psi\rangle$ špecifikovaný (12.9). Grafická interpretácia opakovaného pôsobenia G na stavový vektor $|\psi\rangle$.

Opakované použitie Groverovho operátora G na stavový vektor $|\psi\rangle$ dáva (pozri obr. 12.6, diagram B)

$$G^k |\psi\rangle = \cos \frac{(2k+1)\vartheta}{2} |\psi_A\rangle + \sin \frac{(2k+1)\vartheta}{2} |\psi_B\rangle \quad (12.20)$$

Opakovaným použitím Groverovho operátora dosiahneme, že transformovaný stav $G^k |\psi\rangle$ je skoro rovnobežný s osou B , potom musí platiť

$$\frac{(2k+1)\vartheta}{2} \approx \frac{\pi}{2} \Rightarrow k \approx \frac{\pi - \vartheta}{2\vartheta} \Rightarrow k \approx \frac{\pi}{2\vartheta} \quad (12.21)$$

Uhol ϑ získame z (12.18b) za predpokladu, že $N \gg M$, pravá strana (12.18b) môže byť zjednodušená na $1 - M/(2N)$, potom

$$\vartheta = 2 \arccos \left(1 - \frac{M}{2N} \right) \approx 2 \left(\frac{M}{N} \right)^{1/2} \quad (12.22)$$

Dosadením tohto výsledku do (12.21) dostaneme špecifikáciu k , ktoré je potrebné k tomu, aby $G^k |\psi\rangle$ bol rovnobežný s osou B

$$k \approx \left\lceil \frac{\pi}{4} \left(\frac{N}{M} \right)^{1/2} \right\rceil \quad (12.23)$$

Aplikovaním k -krát Groverového operátora na stav $|\psi\rangle$, kde k je prirodzené číslo špecifikované (12.23), modifikovaný (k -krát rotovaný) stavový vektor $G^k|\psi\rangle$ je veľmi blízky vektoru $|\psi_B\rangle$, t. j. vektor $G^k|\psi\rangle$ obsahuje s vysokou pravdepodobnosťou len qubity, ktoré sú orákulum špecifikované ako riešenie; ostatné stavy, ktoré nie sú orákulum špecifikované ako riešenie, majú skoro nulovú pravdepodobnosť výskytu.

Groverov algoritmus prehľadávania zosumarizujeme do formy jednoduchého algoritmu takto:

Algoritmus 12.1.

Vstup:

(1) Orákulum O , ktoré vyhodnotí, či stavový n -qubitový vektor $|x\rangle$ je riešenie alebo nie je riešenie, orákulum je špecifikované funkciou $f: \{0,1\}^n \rightarrow \{0,1\}$, kde $f(x) = 0$, pre $|x\rangle$, ktoré nie je riešenie alebo $f(x) = 1$, pre $|x\rangle$, ktoré je riešenie; potom $O|x\rangle = (-1)^{f(x)}|x\rangle$.

(2) $n+1$ quibitov v stave $|0\rangle$.

Výstup:

(1) Stav riešenia $|a\rangle$.

Procedúra:

(1) Vytvor inicializovaný stav $|\psi_{ini}\rangle = |0\rangle$.

(2) Vytvor $|\psi\rangle = H^{\otimes n}|\psi_{ini}\rangle = (1/2^{n/2})\sum|x\rangle$.

(3) Urči $k \approx \lceil (\pi/4)(N/M)^{1/2} \rceil$, ktoré špecifikuje mocninu Groverovho operátora G

(4) Opakovane k -krát aplikuj Groverov operátor, $|\psi^{(i)}\rangle = G^{(i-1)}|\psi^{(i-1)}\rangle$, kde $G^{(i-1)}$ je Groverov operátor vytvorený vzhľadom k vektoru $|\psi^{(i-1)}\rangle$, pričom $|\psi^{(0)}\rangle = |\psi\rangle$.

(5) Pomocou merania aplikovaného na $|\psi^{(k)}\rangle$ zostroj $|a\rangle$.

12.1 Ilustračný príklad Groverovho algoritmu.

Nech $N = 2^4 = 16$, t. j. neštruktúrovaná databáza obsahuje 16 položiek, $\mathcal{D} = \{p_1, p_2, \dots, p_{16}\}$, postulujeme, že položka p_{10} obsahuje hľadanú informáciu (ihla v kope sena). Stavový vektor

$$|\psi\rangle = \frac{1}{4} \sum_{x=0}^{15} |x\rangle = \frac{1}{4} (|0000\rangle + |0001\rangle + \dots + |1111\rangle)$$

Budeme počítat' $G|\psi\rangle = (2|\psi\rangle\langle\psi| - 1)O|\psi\rangle$, kde unitárny operátor reprezentuje orákulum špecifikované takto

$$O|x\rangle = \begin{cases} |x\rangle & (\text{pre } x \neq 9) \\ -|x\rangle & (\text{pre } x = 9) \end{cases}$$

Potom

$$O|\psi\rangle = \frac{1}{4} \sum_{\substack{x=0 \\ (x \neq 9)}}^{15} |x\rangle - \frac{1}{4} |9\rangle$$

V ďalšom kroku aplikujeme na tento výsledok operátor $R_\psi = (2|\psi\rangle\langle\psi| - 1)$, po jednoduchých úpravách dostaneme (pozri obr. 12.3 a rov. (12.12))

$$G|\psi\rangle = R_\psi O|\psi\rangle = \frac{3}{16} \sum_{\substack{x=0 \\ (x \neq 9)}}^{15} |x\rangle + \frac{11}{16} |9\rangle$$

Ak tento proces zopakujeme, pre aplikáciu druhej mocniny Groverovho operátora dostaneme

$$G^2|\psi\rangle = \frac{5}{64} \sum_{\substack{x=0 \\ (x \neq 9)}}^{15} |x\rangle + \frac{61}{64} |9\rangle$$

Hodnota maximálnej mocniny k operátora G je určená vzťahom (12.13)

$$k = \lceil \pi \rceil = 3$$

táto tretia mocnina Groverovho operátora má tvar

$$G^3|\psi\rangle = -\frac{13}{256} \sum_{\substack{x=0 \\ (x \neq 9)}}^{15} |x\rangle + \frac{251}{256} |9\rangle$$

Ďalšie aplikácie už by viedli k zhoršovaniu výsledku, t. j. $G^4|\psi\rangle, G^5|\psi\rangle, \dots$ už by sa vzdŕaľovali od riešenia $|9\rangle$. Ak vykonáme meranie nad $G^3|\psi\rangle$ s pravdepodobnosťou blízkou jednej dostaneme riešenie $|9\rangle$.