UNIVERZA V MARIBORU

FAKULTETA ZA NARAVOSLOVJE IN MATEMATIKO

Oddelek za matematiko in računalništvo

MAGISTRSKO DELO

Tinkara Marčec

Maribor, 2018

UNIVERZA V MARIBORU

FAKULTETA ZA NARAVOSLOVJE IN MATEMATIKO

Oddelek za matematiko in računalništvo

Magistrsko delo

KVANTNO RAČUNALNIŠTVO IN GROVERJEV ALGORITEM

na študijskem programu 2. stopnje Matematika

Mentor:

izr. prof. dr. Drago Bokal

Kandidatka:

Tinkara Marčec

Somentor:

doc. dr. Amor Chowdhury

Maribor, 2018

ZAHVALA

Zahvaljujem se mentorju izr. prof. dr. Dragu Bokalu in somentorju doc. dr. Amor Chowdhuryju za pomoč, trud in strokovno vodenje pri izdelavi magistrske naloge.

Iskrena hvala staršem in vsem, ki so mi v času študija stali ob strani in me vzpodbujali. Zahvaljujem se tudi Žigu za vsakodnevno podporo in razumevanje.

Vsem iskreno hvala.

KVANTNO RAČUNALNIŠTVO IN GROVERJEV ALGORITEM

program magistrskega dela

V magistrskem delu povzemite matematične podlage kvantnega računalništva, orišite fizikalne temelje te nove veje na meji med računalništvom in matematiko in se posebej posvetite Groverjevemu algoritmu za učinkovito iskanje po neurejeni zbirki podatkov.

Razmislite, v kakšnem odnosu je Groverjev algoritem z NP-polnimi problemi in na primeru ilustrirajte, kakšne pohitritve lahko dosežemo z njim. Če bi ga uporabili za razbijanje kriptografskega ključa, s kakšnim ukrepom bi dosegli enako stopnjo varnosti, kot pred razvojem algoritma?

Osnovni viri:

1. C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, C. Monroe, *Complete 3-Qubit Grover search on a programmable quantum computer*, Nature Communications volume 8, Article number: 1918 (2017).

2. A. Holobar, *Kvantno računalništvo in kriptografija*, Fakulteta za elektrotehniko, računalništvo in informatiko, Inštitut za računalništvo, Maribor, 2016.

3. J. Watrous, *Quantum computation lecture notes*, University of Waterloo, 2006.

izr. prof. dr. Drago Bokal

doc. dr. Amor Chowdhury

**MARČEC, T.: Kvantno računalništvo in Groverjev algoritem.
Magistrsko delo, Univerza v Mariboru, Fakulteta za naravoslovje in matematiko, Oddelek za matematiko in računalništvo, 2018.**

IZVLEČEK

Magistrsko delo obravnava teoretičen pristop k razumevanju kvantnega računalništva in opisuje kvantni algoritem kot primer uporabnosti hitro se razvijajočega področja. Delo je razdeljeno na štiri dele. V prvem delu je podrobeneje opisana matematična podlaga, potrebna za razumevanje kvantnega računanja, ki obsega kompleksna števila, vektorske prostore in razširitve ter linearne transformacije. Drugi del opisuje fizikalne osnove in temeljne definicije ter razlage kvantne mehanike, iz katere se razvija področje kvantnega računalništva. Kvantni mehaniki sledi poglavje kvantnega računalništva, v katerem so predstavljeni osnovni koncepti in elementi, s katerimi je možno graditi kvantne algoritme. Predstavljen je tudi model kvantnega računanja, katerega se poslužujejo raziskovalci in razvijalci na področju odkrivanja novih kvantnih algoritmov. V zadnjem delu magistrske naloge je opisan Groverjev algoritem, eden izmed prvih kvantnih algoritmov, ki prikazuje uporabnost kvantnega računalništva v prihodnosti.

Ključne besede: linearne transformacije, kvantno računalništvo, kubit, kvantna vrata, kvantno vezje, Groverjev algoritem.

Math. Subj. Class. (2010): 15A04 Linearne transformacije,
68Q12 Kvantni algoritmi.

MARČEC, T.: Quantum computing and Grover's algorithm.
Master Thesis, University of Maribor, Faculty of Natural Scicences and Mathematics, Department of Mathematics and Computer Science, 2018.

ABSTRACT

The master thesis investigates a theoretical approach to the understanding of quantum computing and describes quantum algorithm as an example of usability in a rapidly evolving field. The thesis is divided into four parts. In the first part, the mathematical basis needed to understand quantum computation, comprising complex numbers, vector spaces and extensions, along with linear transformations, is described in more detail. The second part describes the physical basics and basic definitions and explanations of quantum mechanics, from which the field of quantum computing develops. Then follows the chapter of quantum computing, in which the basic concepts and elements for constructing quantum algorithms are presented. In this chapter quantum computing model is described. It is used by researchers and developers in the field of discovering new quantum algorithms. In the last part of the master's thesis, one of the first quantum algorithms, Grover's algorithm, is described, which presents the usability of quantum computing in the future.

Keywords: linear transformation, quantum computing, qubit,
quantum gates, quantum circiut, Grover's algorithm.

Math. Subj. Class. (2010): 15A04 Linear transformations,
68Q12 Quantum algorithms.

Kazalo

Slike

Uvod

Tema magistrskega dela sodi v področje kvantnega računalništva. Le–to z opiranjem na zakone kvantne mehanike poskuša razviti algoritme, ki se bodo v prihodnosti izvajali na kvantnih računalnikih. Njihov razvoj je trenutno v zgodnji fazi, razvijalci se trudijo, da jim bo v prihodnosti uspelo ustvariti učinkovit kvantni računalnik, ki bo v računski moči močno prekašal klasičnega. Čeprav je do njegove splošne uporabe še dolga pot, je znanih dovolj informacij o delovanju kvantnega računalnika, da se lahko prične implementacija primernih algoritmov. Razvoj kvantega računalnika in algoritmov torej poteka vzporedno.

Namen magistrskega dela je seznanitev z razvijajočim se področjem kvantnega računalništva, ki prinaša nove možnosti za uporabo matematičnih znanj pri razvijanju algoritmov v drugačni dimenziji programiranja, kot jo poznamo danes.

Delo je organizirano v pet poglavij. Prvi dve poglavji služita podrobnemu opisu matematičnih konceptov, potebnih za razumevanje kvantnega računanja. V prvem poglavju opišemo kompleksna števila in vektorske razširitve, saj kvantno računalništvo temelji na aritmetiki kompleksnih števil. Drugo poglavje je namenjeno opisu linearnih transformacij, ki so osnova kvantnega računanja. Naštejemo in opišemo tudi nekaj primerov linearnih transformacij, ki se pojavijo na področju kvantne mehanike. V naslednjem poglavju predstavimo osnovne fizikalne in kvantnomehanske koncpete, za lažje razumevanje kvantnega računalništva, saj se je le–to razvilo iz osnovnih načel in konceptov kvantne mehanike. Sledi poglavje kvantnega računalništva, v katerem podrobneje opišemo in predstavimo posamezne elemente računanja. Predstavimo tudi uporaben model kvantnega računanja, s pomočjo katerega se razvijajo kvantni algoritmi. V zadnjem poglavju magistrske naloge predstavimo splošen proces delovanja že obstoječih kvantnih algoritmov in opišemo delovanje Groverjevega algoritma, ki pohitri reševanje NP–polnih problemov in iskanje po nestrukturirani bazi.

Poglavje 1

Kompleksna števila in razširitve vektorskih prostorov

1.1 Kompleksna števila

Vsebina podpoglavja je povzeta po [1], [16].

Kvantna mehanika in kvantno računalništvo temeljita na aritmetiki kompleksnih števil, zato najprej navedemo nekaj njihovih lastnosti, ki nam služijo kot osnova pri opisovanju kvantnomehanskih konceptov.

Kompleksna števila predstavljajo razširitev realnih števil, kjer lahko korenimo tudi negativna števila. Kompleksno število predstavlja urejeni par (a, b), kjer sta $a, b \in \mathbb{R}$. Množico kompleksnih števil označimo kot

$$\mathbb{C} = \{(a, b) \mid a, b \in \mathbb{R}\},$$

na kateri sta definirani računski operaciji seštevanja in množenja na naslednji način

$$(a, b) + (c, d) = (a + c, b + d) \tag{1.1}$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc). \tag{1.2}$$

Če z i označimo tako imenovano imaginarno enoto, ki predstavlja par $(0, 1)$, iz navedenega

sledi $i^2 = -1$. Za vsak $z = (a, b) \in \mathbb{C}$ dobimo zapis

$$z = (a, 0) + (0, b) = (a, 0) + (0, 1)(0, b) = a + ib, \qquad a, b \in \mathbb{R}. \tag{1.3}$$

Število a pri tem predstavlja realno komponento števila z ($a = Re(z)$), b pa njeno imaginarno komponento ($b = Im(z)$). Tako se nam porodi naraven način predstavitve kompleksnih števil v ravnini, pri čemer absciso imenujemo realna, ordinato pa imaginarna os.
Kriterij za enakost kompleksnih števil je enakost pripadajočih realnih števil po koordinatah. Naj bosta $z = a + bi$ in $w = c + di$ kompleksni števili. Potem velja

$$z = w \Leftrightarrow a = c \text{ in } b = d. \tag{1.4}$$

Poleg že definiranega seštevanja in množenja kompleksnih števil poznamo še odštevanje, deljenje in konjugiranje. Odštevanje kompleksnih števil je analogno seštevanju, deljenje pa je definirano na naslednji način

$$\frac{a+ib}{c+id} = \left(\frac{a+ib}{c+id} \cdot \frac{c-id}{c-id}\right) = \frac{ac+bd}{c^2+d^2} + i\frac{bc-ad}{c^2+d^2}, \quad \text{kjer } c^2 + d^2 \neq 0. \tag{1.5}$$

Kompleksna števila lahko tudi konjugiramo. Operacijo konjugiranja označimo z *, konjugirano kompleksno število pa z $\overline{z}$. Naj bo $z = a + ib$ kompleksno število. Potem je njegovo konjugirano število $z^* = \overline{z} = a - ib$. Nadalje velja $z \cdot \overline{z} = a^2 + b^2$.
Operacija konjugiranja se izkaže za uporabno pri izračunu absolutne vrednosti kompleksnega števila

$$|z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}. \tag{1.6}$$

Absolutna vrednost kompleksnega števila, dobljena s pomočjo Pitagorovega izreka, predstavlja razdajo kompleksnega števila od koordinatnega izhodišča, oziroma dolžino vektorja $\overline{0z}$.

Kompleksna števila so *komutativen obseg* oziroma *polje*.

Polarne koordinate

Kompleksno število, izraženo v polarnih koordinatah, predstavimo s kotom φ in radijem r, kar poenostavi marsikateri izračun. Radij kompleksnega števila $z = a + ib$ izrazimo kot njegovo absolutno vrednost, saj le-ta predstavlja dolžino vektorja $\overline{0z}$

$$r = |z| = \sqrt{z\overline{z}} = \sqrt{a^2 + b^2}. \tag{1.7}$$

Kotu φ pravimo tudi argument kompleksnega števila z, $\varphi = Arg(z)$ in ga izračunamo kot

$\varphi = \arctan \frac{a}{b}$.
Geometrijsko si lahko komponento a kompleksnega števila $z = a + ib$ predstavljamo kot $\cos\varphi \cdot |z|$, komponento b pa kot $\sin\varphi \cdot |z|$, kjer je φ kot med realno osjo in vektorjem $\overline{0z}$. Iz take geometrijske predstave dobimo polarni zapis kompleksnega števila

$$z = |z| \cdot (\cos\varphi + i \sin\varphi). \tag{1.8}$$

Kompleksno število lahko v polarnih koordinatah zapišemo tudi kot

$$z = re^{i\varphi}, \tag{1.9}$$

kar izhaja iz Eulerjeve formule, opisane v naslednjih odstavkih.
Eksponentno funkcijo e^x lahko s pomočjo Taylorjeve vrste v okolici točke 0 izrazimo kot vsoto

$$e^x = \sum_{n=0}^{\infty} \frac{x^n}{n!}. \tag{1.10}$$

Če kot eksponent vzamemo $x = i\varphi$ dobimo

$$e^{i\varphi} = \sum_{n=0}^{\infty} \frac{(i\varphi)^n}{n!} = \left(1 - \frac{\varphi^2}{2!} + \frac{\varphi^4}{4!} - \frac{\varphi^6}{6!} + \cdots\right) + i\left(\frac{\varphi}{1!} - \frac{\varphi^3}{3!} + \frac{\varphi^5}{5!} + \cdots\right). \tag{1.11}$$

Elementi v okepajih predstavljajo razvoj funkcij $\cos\varphi$ in $\sin\varphi$ v Taylorjevo vrsto, kar nas pripelje do **Eulerjeve formule**

$$e^{i\varphi} = \cos\varphi + i\sin\varphi. \tag{1.12}$$

1.2 Vektorski prostori in razširitve

V poznejših poglavjih magistrske naloge podrobneje predstavimo kvantno računalništvo, pri katerem za enoto informacije uporabjamo kvantni bit oziroma kubit. Ker si lahko kubit predstavljamo kot vektor, je za razumevanje tega koncepta potrebno znanje o vektorskih prostorih in bazah, kar opišemo v tem podpoglavju. Vpeljemo tudi definicijo normiranih prostorov in skalarnega produkta ter definiramo Hilbertov prostor, ki nam služi kot osnova za abstraktni matematični model v kvantni mehaniki. Poglavje zaključimo s pregledom nekaterih uporabnih lastnosti Hilbertovih prostorov.

1.2.1 Osnovni pojmi vektorskih prostorov

Vsebina podpoglavja je povzeta po [6], [19]. Oznaka $\mathbb{F}$ predstavlja eno izmed polj $\mathbb{R}$ in $\mathbb{C}$.

Definicija 1.1 *Množica X je vektorski prostor nad poljem $\mathbb{F}$, če obstajata taki operaciji*
$+ : X \times X \to X, \quad (x, y) \mapsto x + y \quad \forall x, y \in X \quad$ *(seštevanje)*
$\cdot : \mathbb{F} \times X \to X, \quad (\lambda, x) \mapsto \lambda \cdot x \quad \forall \lambda \in \mathbb{F}, \ \forall x \in X \quad$ *(množenje s skalarjem),*
da velja:

1. $(x + y) + z = x + (y + z) \quad \forall x, y, z \in X,$
2. $x + y = y + x \quad \forall x, y \in X,$
3. $\exists 0 \in X : x + 0 = 0 + x = 0 \quad \forall x \in X,$
4. $\forall x \in X \exists - x \in X : x + (-x) = 0,$
5. $\lambda(x + y) = \lambda x + \lambda y \quad \forall \lambda \in \mathbb{F}, \ \forall x, y \in X,$
6. $(\lambda + \mu)x = \lambda x + \mu x \quad \forall \lambda, \mu \in \mathbb{F}, \ \forall x \in X,$
7. $(\lambda\mu)x = \lambda(\mu x) \quad \forall \lambda, \mu \in \mathbb{F}, \ \forall x \in X,$
8. $1 \cdot x = x \quad \forall x \in X.$

Elemente iz $\mathbb{F}$ imenujemo skalarji, elemente iz X pa vektorji.

Definicija 1.2 *Neprazna podmnožica Y vektorskega prostora X je podprostor vektorskega prostora X, če je tudi sama vektorski prostor.*

Trditev 1.3 *Velja naslednja ekvivalenca*

$$Y \subseteq X \text{je podprostor} \iff \forall \lambda, \mu \in \mathbb{F}, \ \forall y_1, y_2 \in Y : \lambda y_1 + \mu y_2 \in Y.$$

Definicija 1.4 *Naj bo X vektorski prostor nad $\mathbb{F}$.* ***Linearna kombinacija*** *vektorjev $x_1, x_2, \ldots, x_n \in X$ je vsak vektor oblike $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n$, kjer so $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$ koeficienti te linearne kombinacije.*
Če obstajajo taki skalarji $\lambda_1, \ldots, \lambda_n \in \mathbb{F}$, ne vsi enaki 0, da je $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n = 0$, potem so vektorji $x_1, x_2, \ldots, x_n$ ***linearno odvisni****.*
Če vektorji niso linearno odvisni, pravimo da so ***linearno neodvisni****.*

Definicija 1.5 ***Linearna lupina*** *množice vektorjev $\{x_1, \ldots, x_n\}$ iz vektorskega prostora $\mathbb{F}$ je množica vseh linearnih kombinacij vektorjev $x_1, \ldots, x_n$, ki jo označimo kot*

$$\mathcal{L}(\{x_1, \ldots, x_n\}) = \{\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_n x_n \mid \lambda_1, \ldots, \lambda_2 \in \mathbb{F}\}.$$

Trditev 1.6 *Naj bo X vektorski prostor in $x_1, x_2, \ldots, x_n \in X$. Linearna lupina $\mathcal{L}(\{x_1, \ldots, x_n\})$ je najmanjši podprostor prostora X, ki vsebuje vse vektorje $x_1, x_2, \ldots, x_n$.*

Definicija 1.7 *Podmnožica Y vektorskega prostora X je **ogrodje**, če velja $\mathcal{L}(Y) = X$.*

Definicija 1.8 *Podmnožica B vektorskega prostora X je **baza** prostora X, če velja:*

1. *B je linearno neodvisna,*
2. *$\mathcal{L}(B) = X$.*

Izrek 1.9 *Množica vektorjev $\{b_1, \ldots, b_n\}$ je baza vektorskega prostora X natanko tedaj, ko lahko vsak vektor iz X zapišemo na enoličen način kot linearno kombinacijo vektorjev $b_1, \ldots, b_n$.*

Dokaz. ($\Rightarrow$) Naj bo $\{b_1, \ldots, b_n\}$ baza prostora X in $x \in X$. Po definiciji baze lahko x zapišemo kot linearno kombinacijo baznih vektorjev. Tako je potrebno pokazati le še enoličnost:
Recimo, da lahko vektor x zapišemo kot linearno kombinacijo baznih vektorjev na dva načina: $x = \alpha_1 b_1 + \ldots + \alpha_n b_n = \beta_1 b_1 + \ldots + \beta_n b_n, \quad$ kjer so $\alpha_i, \beta_i \in F, \ \forall i \in \{1, \ldots, n\}$.
Iz zgornjega zapisa dobimo enakost $(\alpha_1 - \beta_1)b_1 + \ldots + (\alpha_n - \beta_n)b_n = 0$.
Ker so bazni vektorji linearno neodvisni, velja
$\alpha_i - \beta_i = 0 \quad \forall i \in \{1, \ldots, n\} \quad \Longrightarrow \quad \alpha_i = \beta_i \quad \forall i \in \{1, \ldots, n\}$.
($\Leftarrow$) Sedaj predpostavimo, da lahko vsak vektor iz X na enoličen način zapišemo kot linearno kombinacijo vektorjev $b_1, \ldots, b_n$. Dokazati je potrebno, da je $\{b_1, \ldots, b_n\}$ baza.
Zadošča videti, da so vektorji $b_1, \ldots, b_n$ linearno neodvisni. Zapišimo ničelni vektor kot linearno kombinacijo izbranih vektorjev
$\lambda_1 b_1 + \ldots + \lambda_n b_n = 0 \quad$ kjer so $\lambda_i \in \mathbb{F}, \ \forall i \in \{1, \ldots, n\}$.
Potem velja $\lambda_1 b_1 + \ldots + \lambda_n b_n = 0 = 0b_1 + \ldots + 0b_n$.
Ker pa predpostavka določa enoličnost zapisa, sledi $\lambda_1 = \lambda_2 = \ldots = \lambda_n = 0$

□

Definicija 1.10 *Vektorski prostor X je **končno razsežen** (oziroma končno dimenzionalen), če obstaja taka končna podmnožica $Y \subseteq X$, da je $\mathcal{L}(Y) = X$. V nasprotnem primeru je vektorski prostor neskončno razsežen.*

Izrek 1.11 *Vse baze končno razsežnega vektorskega prostora imajo isto število elementov.*

Definicija 1.12 *Naj bo X končno razsežen vektorski prostor nad $\mathbb{F}$. Številu vseh elementov v bazi pravimo* ***dimenzija*** *vektorskega prostora X in jo označimo z $dim(X)$.*

Definicija 1.13 *Naj bo X končno razsežen vektorski prostor nad $\mathbb{F}$. Množica $\{x_1, \ldots, x_n\}$ je* ***maksimalna linearno neodvisna*** *podmnožica prostora X, če velja:*

1. *$\{x_1, \ldots, x_n\}$ so linearno neodvisni,*
2. *$\{x_1, \ldots, x_n, w\}$ so linearno odvisni $\quad \forall w \in X$.*

Izrek 1.14 *Vsaka maksimalna linearno neodvisna podmnožica končno razsežnega vektorskega prostora X je baza tega prostora.*

Izrek 1.15 *Naj bo X končno razsežen vektorski prostor in $dim(X) = n$. Naj bo $\{x_1, \ldots, x_k\}$ linearno neodvisna podmnožica prostora X. Če je $k < n$, potem obstajajo taki vektorji $\{x_{k+1}, x_{k+2}, \ldots, x_n\}$, da je $\{x_1, \ldots, x_k, x_{k+1}, \ldots, x_n\}$ baza vektorskega prostora X. Z drugimi besedami: vsako linearno neodvisno podmnožico lahko razširimo do baze.*

1.2.2 Normirani prostori

Vsebina podpoglavja je povzeta po [19].

Preden vpeljemo pojem Hilbertovega prostora, je potrebno vektorski prostor opremiti z normo.

Definicija 1.16 *Naj bo X vektorski prostor nad $\mathbb{F}$. Preslikava $||.|| : X \to \mathbb{R}$ se imenuje* ***norma****, če velja:*

1. $||x|| \geq 0 \quad \forall x \in X$,
2. $||x|| = 0 \Longrightarrow x = 0$,
3. $||\lambda x|| = |\lambda| ||x|| \quad \forall x \in X, \ \forall \lambda \in \mathbb{F}$,
4. $||x + y|| \leq ||x|| + ||y|| \quad \forall x, y \in X$.

Vektorski prostor, opremljen s to preslikavo, imenujemo ***normirani prostor*** *in ga označimo kot $(X, ||.||)$.*

1.2.3 Hilbertovi prostori

Vsebina podpoglavja je povzeta po [3], [6].

V normiranih prostorih lahko elemente oziroma vektorje seštevamo, množimo s skalarji ter jim s pomočjo norme določimo dolžine. Če normiranim prostorom dodamo operacijo skalarnega produkta, lahko definiramo Hilbertove prostore, ki se izkažejo za uporabne predvsem v fiziki na področjih kvantne mehanike in termodinamike.

Kot motivacijo za vpeljavo skalarnega produkta v poljubnem vektorskem prostoru nad $\mathbb{F}$ si ogljemo definicijo skalarnega produkta v prostoru geometrijskih vektorjev $\mathbb{R}^3$.
Za poljubna vektorja $\vec{a} = (a_1, a_2, a_3)$ in $\vec{b} = (b_1, b_2, b_3)$ je njun skalarni produkt enak

$$\vec{a} \cdot \vec{b} = a_1 b_1 + a_2 b_2 + a_3 b_3. \tag{1.13}$$

Opazimo, da je skalarni produkt preslikava $\mathbb{R}^3 \times \mathbb{R}^3 \longrightarrow \mathbb{R}$. Geometrijsko lahko skalarni produkt izračunamo po formuli $\vec{a} \cdot \vec{b} = |\vec{a}||\vec{b}| \cos\varphi$, kjer je $\varphi \in [0, \pi]$ kot med vektorjema $\vec{a}$ in $\vec{b}$, $|\vec{a}|$ in $|\vec{b}|$ pa njuni dolžini.
Splošnejši pojem skalarnega produkta v poljubnem vektorskem prostoru nad $\mathbb{F}$ vpeljemo z naslednjo definicijo.

Definicija 1.17 *Naj bo X vektorski prostor nad poljem $\mathbb{F}$. Preslikavi $< ., . >: X \times X \longrightarrow \mathbb{F}$ pravimo* ***skalarni produkt****, če veljajo naslednje lastnosti:*

1. $< x, x > \in \mathbb{R}^+ \cup \{0\} \quad \forall x \in X$ *in*
   $< x, x >= 0 \Leftrightarrow x = 0$ *(pozitivna definitnost),*
2. $< x, y >= \overline{< y, x >} \quad \forall x, y \in X$ *(poševna simetričnost),*
3. $< \alpha x + \beta y, z >= \alpha < x, z > + \beta < y, z >$
   $\forall \alpha, \beta \in \mathbb{F},\ \forall x, y, z \in X$ *(linearnost v prvi komponenti).*

Opomba 1.18 *Iz točk 2. in 3. definicije je razvidno:*

(*i*) $< x, 0 >= 0 =< 0, x > \quad \forall x \in X,$
(*ii*) $< z, \alpha x + \beta y >= \overline{\alpha} < z, x > + \overline{\beta} < z, y >$
$\forall \alpha, \beta \in \mathbb{F}\ \forall x, y, z \in X$ *(poševna linearnost v drugi komponenti).*

V nadaljevanju poglavja se bo X nanašal na vektorski prostor nad poljem $\mathbb{F}$ s skalarnim produktom.

Definicija 1.19 *Preslikavi* $||.|| : X \longrightarrow \mathbb{R}$ *s predpisom* $||x|| = \sqrt{< x, x >} \quad \forall x \in X$ *pravimo* ***norma, porojena s skalarnim produktom****.*
Razdalja med vektorjema $x, y \in X$ *pa je definirana kot* $d(x, y) = ||x - y||$.

Definicija 1.20 *Velja naslednje:*

(*i*) *Neničelna vektorja* $x, y \in X$ *sta pravokotna (ali* ***ortogonalna****), če je* $< x, y >= 0$.

(*ii*) *Množica* $Y \subseteq X$ *je ortogonalna, če sta vsaka dva različna elementa iz* Y *pravokotna.*

(*iii*) *Vektor* x *je* ***normiran****, če je* $||x|| = 1$.

(*iv*) *Množica* $Y \subseteq X$ *je* ***ortonormirana****, če je ortogonalna in je vsak njen element normiran.*

Trditev 1.21 *Če je* $Y \subseteq X$ *ortogonalna množica brez vektorja* 0*, potem je* Y *linearno neodvisna.*

Opomba 1.22

(*i*) *S posebnim postopkom, imenovanim Gramm-Schmidtova ortogonalizacija, lahko iz poljubne baze prostora dobimo ortogonalno bazo.*
(*ii*) *Vsak končno razsežen vektorski prostor s skalarnim produktom premore ortonormirano bazo (vektorje, dobljene z Gramm-Schmidtovo ortogonalizacijo le normiramo).*
(*iii*) *Za ortonormirane baze velja neodvisnost skalarnega produkta od baznih elementov.*

Opomba 1.23 *Vemo, da ima vektor različne koordinate glede na različne baze. Če je* $b = \{b_1, \ldots, b_n\}$ *baza vektorskega prostora* X*, lahko poljuben vektor* $x \in X$ *zapišemo kot* $v = \sum_{i=1}^{n} \alpha_i b_i$*, kjer so* α_i *komponente vektorja glede na bazo* B*. Če je baza* B *ortonormirana, lahko izračun komponent vektorja poenostavimo s trikom skalarnega produkta. Posamezno komponento vektorja dobimo z izračunom:* $< b_i, v >= \alpha_i$.

Definicija 1.24 *Prostor je poln, če je v njem vsako Cauchyjevo zaporedje konvergentno.*

Definicija 1.25 ***Hilbertov prostor*** *je poln vektorski prostor nad* $\mathbb{F}$ *na katerem je definirana operacija skalarnega produkta* $< ., . >$*, ki poraja normo tega prostora.*

Opomba 1.26 *Ker nas v nadaljevanju zanimajo le algebrajske lastnosti Hilbertovih prostorov, lastnosti Cauchyjevih zaporedij ne bomo podrobneje preučevali.*

Ob koncu omenimo dve neenakosti, ki veljata v Hilbertovih prostorih in ju posredno uporabljamo v nadaljnjih poglavjih.

Izrek 1.27 (Neenakost Cauchy-Schwarz-Bunjakovski) *Za poljubna $x, y \in X$ velja neenakost*

$$| < x, y > | \leq ||x|| \cdot ||y||. \tag{1.14}$$

Trditev 1.28 (Trikotniška neenakost) *Za poljubna $x, y \in X$ velja neenakost*

$$||x + y|| \leq ||x|| + ||y||. \tag{1.15}$$

Poglavje 2

Linearne transformacije

Prejšnje poglavje je namenjeno matematičnim osnovam za definiranje kvantnega bita, to poglavje pa je namenjeno obnovi teorije, ki služi kot podlaga za vpeljavo kvantnih logičnih vrat. V začetku se spomnimo nekaj trditev o inverznih matrikah ter definiramo osnovne pojme linearnih transformacij in z njimi povezanih matrik. Spomnimo se prehoda na novo bazo, opišemo posebne primere linearnih transformacij, ki jih nadalje uporabimo v kvantni mehaniki, ter definiramo lastne vrednosti in lastne vektorje.
Vsi vektorski prostori v tem poglavju so končno razsežni, vsebina je povzeta po [6].

Izrek 2.1 *Naj bo M poljubna kvadratna matrika. Veljajo naslednje trditve:*

(*i*) *Če je $Mv = 0$ za poljuben neničelni vektor v, matrika M nima inverza.*
(*ii*) *Matrika je obrnljiva natanko tedaj, ko je njena determinanta različna od 0.*
(*iii*) *Če je $Mv = 0$ za poljuben neničelni vektor v, potem je $det(M) = 0$.*

Definicija 2.2 *Naj bosta U in V vektorska prostora nad $\mathbb{F}$. Preslikavi $\mathcal{A} : U \longrightarrow V$ pravimo* ***linearna preslikava*** *(ali* ***linearna transformacija*** *ali linearni operator), če velja:*

(*i*) $\mathcal{A}(x + y) = \mathcal{A}(x) + \mathcal{A}(y) \quad \forall x, y \in U,$
(*ii*) $\mathcal{A}(\lambda x) = \lambda \mathcal{A}(x) \quad \forall \lambda \in \mathbb{F},\ \forall x \in U.$

Matriki prirejena linearna preslikava

Vsaki matriki $A \in M_{m\times n}(\mathbb{F})$ lahko priredimo linearno preslikavo $\mathcal{A}_A : \mathbb{F}^n \longrightarrow \mathbb{F}^m$ s predpisom $\mathcal{A}_A(x) = Ax \quad \forall x \in \mathbb{F}^n$.

Linearni preslikavi prirejena matrika

Velja tudi, da lahko s pomočjo dane linearne preslikave konstruiramo njeno matriko. Naj bo $\mathcal{A} : U \longrightarrow V$ poljubna linearna preslikava in $B = \{u_1, \ldots, u_n\}$ baza prostora U ter $C = \{v_1, \ldots, v_m\}$ baza prostora V. Potem velja, da lahko vsak vektor $\mathcal{A}(u_j) \in V$ razvijemo po bazi C. Ker lahko vsak vektor zapišemo kot linearno kombinacijo baznih vektorjev, lahko linearno transformacijo $\mathcal{A}$ vektorjev iz baze B zapišemo na naslednji način

$\mathcal{A}(u_1) = a_{11}v_1 + a_{21}v_2 + \ldots + a_{m1}v_m,$

$\mathcal{A}(u_2) = a_{12}v_1 + a_{22}v_2 + \ldots + a_{m2}v_m,$

$\vdots$

$\mathcal{A}(u_n) = a_{1n}v_1 + a_{2n}v_2 + \ldots + a_{mn}v_m$ za neke skalarje $a_{i,j} \in \mathbb{F}$.

Če skalarje zapišemo v matriko

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix},$$

pravimo taki matriki matrika linearne preslikave glede na bazi B in C in jo označimo kot $\mathcal{A}[B, C]$.

Opomba 2.3 *Matrika $\mathcal{A}[B, C]$ je določena enolično glede na urejeni bazi B in C. To pomeni, da je odvisna od izbire baz B in C ter od vrstnega reda baznih elementov.*

2.1 Prehod na novo bazo

Vsebina podpoglavja je povzeta po [6].

Definicija 2.4 *Naj bosta $B = \{u_1, \ldots, u_n\}$ in $C = \{v_1, \ldots, v_n\}$ urejeni bazi vektorskega prostora U. Naj bodo $p_{ij} \in \mathbb{F}$ taki skalarji, da velja*

$v_1 = p_{11}u_1 + p_{21}u_2 + \ldots + p_{n1}u_n,$

$v_2 = p_{12}u_1 + p_{22}u_2 + \ldots + p_{n2}u_n,$

$\vdots$

$v_n = p_{1n}u_1 + p_{2n}u_2 + \ldots + p_{nn}u_n.$

Potem matriko $P[B,C] = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{pmatrix}$

imenujemo ***matrika prehoda*** *od baze B do baze C.*
Dodatno velja, da je matrika $P[B,C]$ *obrnljiva in* $P[B,C]^{-1} = P[C,B]$.

Naslednji izrek nam pove, kako se spremeni matrika linearne preslikave $\mathcal{A} : U \longrightarrow V$, če spremenimo bazi prostorov U in V.

Izrek 2.5 *Naj bo* $\mathcal{A} : U \longrightarrow V$ *poljubna linearna preslikava. Naj bosta* $B_1 = \{u_1, \ldots, u_n\}$ *in* $B_2 = \{u_1', \ldots, u_n'\}$ *bazi prostora U ter* $C_1 = \{v_1, \ldots, v_n\}$ *in* $C_2 = \{v_1', \ldots, v_n'\}$ *bazi prostora V. Potem velja*

$$\mathcal{A}[C_2, B_2] = P[C_2, C_1]\mathcal{A}[C_1, B_1]P[B_1, B_2]. \tag{2.1}$$

Če imamo na razpolago ortonormirano bazo, se izračun matrike bistveno poenostavi. Ker so bazni vektorji v ortonormirani bazi med sabo pravokotni in enotske dolžine, lahko pri iskanju matrike linearne transformacije uporabimo trik skalarnega produkta, ki smo ga omenili že pri izračunu komponent vektorja. Posamezen element matrike dobimo s skalarnim produktom baznega vektorja in vektorja, dobljenega z njegovo linearno preslikavo.
Naj bo $C = \{c_1, \ldots, c_m\}$ ortonormirana baza vektorskega prostora V in $\mathcal{A} : V \longrightarrow V$ poljubna linearna preslikava. Matriko linearne preslikave glede na bazo C dobimo na naslednji način

$$A = \mathcal{A}[B,C] = \begin{pmatrix} < c_1, \mathcal{A}(c_1) > & < c_1, \mathcal{A}(c_2) > & \cdots & < c_1, \mathcal{A}(c_n) > \\ < c_2, \mathcal{A}(c_1) > & < c_2, \mathcal{A}(c_2) > & \cdots & < c_2, \mathcal{A}(c_n) > \\ \vdots & \vdots & \ddots & \vdots \\ < c_m, \mathcal{A}(c_1) > & < c_m, \mathcal{A}(c_2) > & \cdots & < c_m, \mathcal{A}(c_n) > \end{pmatrix},$$

kjer je $B = \{b_1, \ldots, b_n\}$ poljubna (ne nujno ortonormirana) baza prostora V [13].

2.2 Posebni primeri linearnih transformacij v kvantni mehaniki

Vsebina podpoglavja je povzeta po [11], [13].

Adjugirani operatorji

Definicija 2.6 *Naj bo M $n \times m$ matrika.* ***Adjungirano*** *matriko $M^\dagger$ dobimo tako, da na matriki M uporabimo operaciji transponiranja in konjugiranja: $M^\dagger = (M^T)^*$.*
Naj bo $\mathcal{A} : V \longrightarrow W$ linearna transformacija z matriko M. Potem je linearna preslikava $\mathcal{A}^* : W \longrightarrow V$ z matriko $M^\dagger$ adjungirana preslikava preslikave $\mathcal{A}$.

Unitarni operatorji

Izrek 2.7 *Naj bo $\mathcal{U} : V \longrightarrow V$ linearna transformacija. Naslednje trditve so ekvivalentne:*

(*i*) *Linearna transformacija $\mathcal{U}$ je unitarna, če ohranja dolžine vektorjev*

$$||\mathcal{U}v|| = ||v||, \quad \forall v \in V. \tag{2.2}$$

(*ii*) *Linearna transformacija $\mathcal{U}$ je unitarna, če ohranja skalarni produkt*

$$< \mathcal{U}v, \mathcal{U}w > = < v, w >, \quad \forall v, w \in V. \tag{2.3}$$

(*iii*) *Linearna transformacija $\mathcal{U}$ je unitarna, če ima njena matrika v ortonormirani bazi ortonormirane vrstice (in stolpce).*

Definicija 2.8 *Matriko M unitarne transformacije imenujemo* ***unitarna****.*

Trditev 2.9 *Za unitarno matriko velja enakost*

$$M^\dagger M = M M^\dagger = \mathbb{I}. \tag{2.4}$$

Hermitski operatorji

Definicija 2.10 *Matrika M, ki je enaka svoji adjungirani matriki je* ***hermitska***

$$M \text{ je hermitska} \Longleftrightarrow M^\dagger = M. \tag{2.5}$$

Nadalje, hermitski operator je linearna transformacija, katere matrika je hermitska (v kateri koli bazi).

Ob koncu poglavja se spomnimo definicije lastnih vrednosti, ki predstavljajo edine možne rezultate meritev fizikalnega sistema v kvantni mehaniki, kar podrobneje predstavimo v naslednjih poglavjih.

Definicija 2.11 *Naj bo $\lambda \in \mathbb{F}$. λ je **lastna vrednost** linearne preslikave $\mathcal{A} : V \longrightarrow V$, če obstaja tako neničelni vektor $v \in V$, da je*

$$\mathcal{A}v = \lambda v. \tag{2.6}$$

*Pravimo, da je v **lastni vektor**, ki pripada lastni vrednosti λ.*
*Dodatno velja, da množica vseh lastnih vektorjev, ki pripadajo lastni vrednosti λ, skupaj z vektorjem 0 tvori podprostor $\{v \in V | \mathcal{A}x = \lambda x\}$, ki ga imenujemo **lastni podprostor**.*

Opomba 2.12

(*i*) *Lastne vrednosti preslikav in njihovih matrik sovpadajo.*
(*ii*) *Lastni vektorji, ki pripadajo različnim lastnim vrednostim, so med sabo linearno neodvisni.*

Poglavje 3

Fizikalne osnove in kvantna mehanika

3.1 Fizikalne osnove

Za razumevanje konceptov kvantne mehanike je potrebno poznati določene fizikalne pojme, katerih se spomnimo v tem podpoglavju.

Mehanika

Mehanika je veja fizike, ki proučuje gibanje in mirovanje teles ter gibanje teles pod vplivom sil. Gibanje je relativno, kar pomeni, da je odvisno od okolice, glede na katero ga opazujemo. Gibajoče se telo ima **gibalno količino** G, ki predstavlja produkt mase telesa in njegove hitrosti, $G = mv$. Če na telo deluje sila, se mu gibalna količina spremeni. Odvisno od velikosti sile, se gibalni količini spremenita hitrost in/ali smer. Sila tako pove spremembo gibalne količine v enoti časa, kar lahko zapišemo kot $F = \frac{\Delta G}{\Delta t} = \frac{\Delta(mv)}{\Delta t} = m\frac{\Delta v}{\Delta t} = ma$, kjer je a pospešek.

Kinetična energija telesa z maso m, ki se giblje translatorno (t. j. gibanje, pri katerem se vsi deli telesa gibajo z enakimi hitrostmi in pospeški) s hitrostjo v, je enaka $W_k = \frac{mv^2}{2}$. Med gibanjem se kinetična energija telesa spreminja, če sile opravljajo delo. Sprememba kinetične energije telesa je enaka delu vseh sil, ki nanj delujejo, $A = \Delta W_k$. **Potencialna energija** je energija, ki jo ima telo zaradi svoje lege v polju sil. Primer potencialne energije je težnostna potencialna energija, ki jo izračunamo po enačbi $W_p = mgh$, kjer je m masa opazovanega telesa, g gravitacijski pospešek in h višina telesa glede na zemeljsko površje.

Če na telo deluje le njegova teža, velja izrek o ohranitvi kinetične in potencialne energije $\frac{mv^2}{2} + mgh = konstanta$.

Valovanje

Valovanje je zaporedje motenj, ki se razširjajo skozi snov ali prostor. Povzročitelj motenj je izvor valovanja.

Valovanje, ki potuje po napeti vrvi je **potujoče valovanje**, vendar potuje le motnja, vsak delec vrvi pa niha na svojem mestu. Občutek, da se delci po vrvi premikajo, imamo zaradi tega, ker le-ti ne nihajo sočasno. Tako krivulja odmikov posameznih delcev potuje s hitrostjo $v = \lambda f$, kjer je λ valovna dolžina, f pa frekvenca valovanja. Frekvenca je število ponavljajočih se dogodkov glede na časovno enoto. Valovna dolžina je razdalja med sosednjima hriboma ali doloma in je tem večja, čim večja je hitrost valovanja in čim manjša je frekvenca izvora. Rečemo tudi, da je valovna dolžina pot, ki jo valovanje prepotuje v nihajnem času izvora, ki ga dobimo kot $t_0 = \frac{1}{f}$.

Interferenca je pojav, pri katerem več različnih valovanj vpliva na nihanje delcev. Kjer se valovni hribi prvega in drugega valovanja ujemajo, se skupna amplituda poveča, v nasprotnem primeru se skupno valovanje oslabi. Rezultat interference potujočih valovanj, ki imata enaki amplitudi, širita pa se v nasprotnih smereh, je **stoječe valovanje**.

Valovanje lahko delimo tudi na **mehansko**, pri katerem nihajo delci snovi in se lahko razširja le skozi snov, in na **elektromagnetno**, ki je valovanje v električnem in magnetnem polju. Ker elektromagnetno valovanje ni vezano na snov, se lahko širi tudi skozi brezzračni prostor.
Širjenje elektromagnetnega valovanja
Električni naboj v okolici ustvarja električno polje. Če se nabit delec v električnem polju giblje, se ustvari njemu pripadajoče magnetno polje. Ob spremembi hitrosti nabitega delca, ki je izvor valovanja, se v njegovi okolici spremenita jakost električnega in gostota magnetnega polja. Nastala sprememba se v vse smeri razširja skozi prostor, kar pomeni, da po prostoru potuje elektromagnetni val. Če se hitrost delca stalno spreminja, se ustvari elektromagnetno valovanje. Vse vrste elektromagnetnih valov se skozi vakuum razširjajo enako hitro s svetlobno hitrostjo $c = 3 \cdot 10^8 \frac{m}{s}$.
Elektormagnetni spekter
Razdelitev elektromagnetnih valov po frekvencah oziroma valovnih dolžinah imenujemo elektromagnetni spekter. Svetlobo sestavlja ozek pas elektromagnetnih valov z valovnimi dolžinami od 0.4 µm do 0.8 µm. Valovi z večjimi frekvencami in manjšimi valovnimi dolžinami od svetlobe so še ultarvijolični, rentgenski in gama žarki. Valovi z manjšimi frekvencami in večjimi valovnimi dolžinami pa so infrardeči, mikrovalovi in radijski valovi [10], [14].

3.2 Kvantna mehanika

3.2.1 Osnovna načela kvantne mehanike

V 19. stoletju, času uradnega odkritja atomov, so znanstveni preboji pripeljali do razvoja novih teorij, predvsem na področju podatomskega raziskovanja. S pomočjo eksperimentov najpomembnejših znanstvenikov tistega časa, kot so Dalton, Thomson in Rutherford, je bil ustvarjen model atoma, ki je v grobem v uporabi še danes. Z raziskovanjem podatomskega področja pa s klasično fiziko ni bilo več mogoče opisati pojavov kot so stabilnost atoma, fotoelektrični efekt, sevanje črnega telesa ipd. Tako se je v začetku 20. stoletja pričela razvijati nova veja fizike, kvantna mehanika, ki je zagotovila temelje nekaterim najpomembnejšim odkritjem v znanosti. Je teorija, ki proučuje vedenje najmanjših delcev na podlagi verjetnosti.

V nadaljevanju opišemo glavna načela, na katerih sloni kvantna mehanika.

1. NAČELO: Kvantizacija

Definicija 3.1 ***Kvant*** *je najmanjša možna diskretna enota neke fizikalne količine, kot je na primer energija ali snov.*

Pojem kvant je prvi vpeljal nemški fizik Max Planck, ki je ugotovil, da telesa lahko oddajajo in prejemajo energijo le v nezveznih količinah, ki jih je poimenoval kvanti. Ko je Einstein pokazal, da svetloba obstaja tudi v kvantizirani obliki (fotoni), so ta koncept uporabili pri atomski zgradbi. Iskanje stabilnega atomskega jedra je Nielsa Bohra, enega izmed najpomembnejših znanstvenikov na področju kvantne mehanike, pripeljalo do ugotovitve, da energijska stanja elektronov zavzamejo le diskretne vrednosti. Elektronu v atomu se ob trku s fotonom lahko poveča energija, vendar le, če ima ta energija točno določeno vrednost. Pravimo, da je takrat elektron v vzbujenem stanju. Elektron iz vzbujenega stanja zelo hitro preide nazaj, pri čemer odvečno energijo odda v obliki fotona s točno določeno frekvenco, kar je enostavno pokazati eksperimentalno. Ko so elektroni najbližje jedru, imajo najnižjo možno energijo, ki se ne more več zmanjšati. Energijska stanja elektrona so tako primer kvantizirane količine.

2. NAČELO: Valovno–delčni dualizem

Definicija 3.2 *Za snov na mikroskopski ravni veljajo lastnosti delca in vala, čemur pravimo* ***valovno–delčni dualizem****.*

Eden izmed najpomembnejših eksperimentov kvantne mehanike je eksperiment z dvojno režo, katerega je že v 19. stoletju zasnoval Young, in pokazal, da se svetloba obnaša kot valovanje. Ekperiment vključuje izvor svetlobnega valovanja, ploščo z dvema režama ter zaslon. Če ploščo z režama osvetlimo z virom svetlobe, se na zaslonu prikaže interferenčni vzorec, sestavljen iz svetlih in temnih prog. Ker se interferenca pojavi pri valovanju, ta eksperiment pokaže, da svetlobo lahko obravnavamo kot valovanje.

Leta 1905 je Einstein uvedel drugačen koncept dojemanja svetlobe, pri čemer je sklepal, da čeprav se svetloba vede kot valovanje, je sestavljena iz kvantiziranih količin, ki jih imenujemo fotoni. Vendar, če je svetloba sestavljena iz fotonov, se morata pri prej omenjenem eksperimentu na zaslonu pokazati odseva obeh rež. Številni eksperimenti so s pomočjo detektorjev fotonov potrdili to teorijo. Če eksperiment izvedemo enako kot prej, vendar z detektorjem za vsak foton preverimo, skozi katero režo je potoval, se na zaslonu pojavita le odseva rež. Takoj ko odstranimo detektor fotonov, se interferenčni vzorec spet pojavi. Iz teh rezultatov je razviden velik vpliv meritev. Če ne merimo posameznega fotona, se bo obnašal kot val, drugače kot delec.

Schrödingerjeva enačba

Einsteinova teorija je sprožila nadaljna raziskovanja in kmalu so ugotovili, da če lahko gledamo na svetlobo, ki je elektromagnetno valovanje, kot na delec, lahko tudi na delec gledamo kot na val. Francoski fizik Louis de Broglie je v svoji hipotezi navedel, da Einsteinova enačba za gibalno količino,

$$P = \frac{h}{\lambda}, \tag{3.1}$$

kjer je h Planckova konstanta, ki opisuje velikosti kvantov, velja tudi za delce z maso. Valovna dolžina delca se lahko izračuna iz zgornje enačbe kot

$$\lambda = \frac{h}{P} = \frac{h}{mv}. \tag{3.2}$$

Hipotezo so potrdili z eksperimentom z dvojno režo, na enak način kot pri svetlobi, vendar so skozi režo namesto fotonov spuščali elektrone. Rezultat eksperimenta je bil enak opisanemu v prejšnjem odstavku. Ob svoji hipotezi je Broglie pokazal, da elektroni tvorijo stoječe valovanje. Le–to pomeni kvantizacijo elektronskih orbit okrog jedra atoma, kar je v skadu z Bohrovim atomskim modelom.

Nedolgo zatem je avstrijski fizik Erwin Schrödinger zapisal znano Schrödingerjevo enačbo, ki pravi, da lahko vso snov obravnavamo z valovno funkcijo. Enačba opisuje spremembe sistema skozi čas, pri čemer so lastnosti sistema določene le verjetnostno. V posplošeni

obliki jo zapišemo kot

$$i\hbar\frac{d\Psi(x,t)}{dt} = \hat{H}\Psi(x,t), \tag{3.3}$$

kjer je i imaginarna enota, $\hbar$ reducirana Planckova konstanta ($\hbar = \frac{h}{2\pi}$), $\Psi(x,t)$ valovna funkcija v času t in položaju x, $\hat{H}$ pa Hamiltonov operator, ki opisuje energijo sistema in ga opišemo v nadaljnjih poglavjih. Ker lahko na vsak delec gledamo kot na val, mu pripada valovna funkcija $\Psi(x,t)$. Le–ta opisuje trenutno stanje delca in podaja amplitude verjetnosti, iz katerih lahko izračunamo verjetnosti posameznih stanj. Valovna funkcija nam torej pove spreminjanje verjetnosti določenih lastnosti opazovanega delca ali sistema.

3. NAČELO: Heisenbergovo načelo nedoločenosti

Načelo nedoločenosti, ki ga je razvil nemški fizik Werner Heisenberg, pove, da ne moremo istočasno z gotovostjo poznati nekaterih parov lastnosti. V najpogosteje navedenem primeru sta ti lastnosti položaj in gibalna količina delca, merjena ob istem času. Eno ali drugo količino lahko poznamo, vendar ne obeh hkrati. Načelo lahko razumemo kot posledico valovno–delčnega dualizma, saj na elektron lahko gledamo kot na delec ali val, vendar ne oboje hkrati. Takoj ko izmerimo položaj elektrona, na elektron gledamo kot na delec, saj je valovanje (oz. valovna funkcija) le mera za izračun verjetnosti položaja. Ko imamo položaj elektrona, o njegovi gibalni količini ne vemo nič in obratno [14], [21].

3.2.2 Koncepti kvantne mehanike

Diracova notacija

Diracova notacija bra-ket, imenovana po angleškem fiziku Paulu Diracu, matematično predstavlja zapis vektorja s kompleksnimi koeficienti. Ket vektor je predstavljen kot

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}. \tag{3.4}$$

Bra vektor je transponiran vektor pripadajočega ket vektorja s konjugiranimi koeficienti

$$\langle a| = (a_1^* \; a_2^* \; \cdots \; a_n^*). \tag{3.5}$$

Množenje bra in ket vektorja nam da njun skalarni produkt

$$\langle a|b\rangle = (a_1^* \; a_2^* \; \cdots \; a_n^*) \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix} = a_1^* b_1 + a_2^* b_2 + \cdot + a_n^* b_n \; \in \mathbb{C}. \tag{3.6}$$

Hitro opazimo, da velja

$$\langle a|b\rangle = \langle b|a\rangle^* . \tag{3.7}$$

Kot pri običajnem množenju matrik z vektorji velja, da pri množenju matrik s ket vektorji, spet dobimo ket vektor [13].

Matematični model na primeru polarizacije fotona

Kvantna mehanika vsak opazovani sistem obravnava kot matematični model v kompleksnem Hilbertovem prostoru, kar se je v večih letih raziskovanja izkazalo kot primeren pristop za opis kvantnomehanskih pojavov.

Naslednja enačba predstavlja matematično podlago kvantnomehanskim konceptom, ki so jih vrsto let eksperimentalno razvijali

$$H\,|a\rangle = \lambda_a\,|a\rangle\,. \tag{3.8}$$

Z matematičnega vidika hitro opazimo pomen zgornje enačbe. H predstavlja hermitsko matriko linearne transformacije ($H = H^\dagger$), $|a\rangle$ je lastni vektor matrike H, λ_a pa njegova pripadajoča lastna vrednost, ki je realno število. Ta zapis lahko uporabimo kot opis sistema. Hermitska matrika, ki je matrika linearne transformacije, predstavlja merljivo lastnost opazovanega sistema. Lastni vektorji so vsa možna stanja sistema, lastne vrednosti pa predstavljajo rezultate meritve. Pri tem velja, da lastni vektorji dane matrike predstavljajo ortonormirano bazo. Vsi vektorji opazovanega sistema so enotski. Razlog, da je temu tako, je možnost izračuna verjetnosti posameznih stanj, kar razložimo v nadaljevanju [13].

Sedaj navedimo nekaj aksiomov, s katerimi fizikalni sistem pretvorimo v matematični model:

1. Vsak sistem lahko prenesemo na Hilbertov prostor, pri čemer vsako stanje sistema ustreza točki na enotski sferi Hilbertovega prostora.

2. Vsaka merljiva lastnost sistema ustreza nekemu operatorju (oziroma njegovi pripadajoči matriki) Hilbertovega prostora. Ta operator (matrika) je vedno Hermitski.

3. Edini možni merljivi rezultati opazovane lastnosti so realna števila, ki so lastne vrednosti transformacijske matrike. Pri tem lastni vektorji pripadajočih lastnih vrednosti tvorijo ortonormirano bazo prostora stanj $\{|x_i\rangle\}$. Iz tega sledi, da lahko vsak vektor zapišemo kot linearno kombinacijo lastnih vektorjev

$$|\psi\rangle = \sum_i a_i \, |x_i\rangle \, . \tag{3.9}$$

4. Za ortonormirano bazo Hilbertovega prostora $\{|x_i\rangle\}$ velja enakost

$$\sum_i |x_i\rangle \, \langle x_i| = \mathbf{I}, \tag{3.10}$$

pri čemer je $|x_i\rangle \, \langle x_i|$ operator, ki porodi matriko. V splošnem je transformacija $|v\rangle \, \langle v|$ operator projekcije vektorja $|x\rangle$ na vektor $|v\rangle$

$$|v\rangle \, \langle v| \, (|x\rangle) = \langle v|x\rangle \, |v\rangle \, . \tag{3.11}$$

5. Verjetnost, da bo meritev opazovane lastnosti za stanje $|\psi\rangle = \sum_i a_i \, |x_i\rangle$ enaka λ_i, je $|a_i|^2$, kjer je λ_i pripadajoča lastna vrednost stanja $|x_i\rangle$. Povprečna pričakovana vrednost meritve λ_i po večih merjenjih je

$$\langle \psi|H|\psi\rangle = \sum_i |a_i|^2 \lambda_i, \tag{3.12}$$

kjer H predstavlja merljivo lastnost.

6. Če je meritev opazovane lastnosti H enaka λ_k za pripadajoč lastni vektor $|x_k\rangle$, se stanje sistema "zruši" (kolapsira) v lastni vektor $|x_k\rangle$. Naslednje meritve kolapsiranega stanja vrnejo lastno vrednost λ_k z gotovostjo 1 [5], [13].

Za lažjo predstavo opišemo sistem s pomočjo eksperimenta, v katerem opazujemo polarizacijo svetlobe. Za poskus rabimo izvir nepolarizirane svetlobe (npr. žarnico) ter nekaj polarizacijskih filtrov za proučevanje polarizacije fotonov. Polarizacijski filter si lahko intuitivno predstavljamo kot "režo", za katero so fotoni, ki jih prepušča, polarizirani v enaki smeri kot je "reža"nastavljena. Če najprej namestimo navpičen filter, bo za njim vsa svetloba polarizirana navpično, njena intenziteta, ki je odvisna od kota med polarizacijama, bo jasno manjša (intenziteta bo polovična, ker je povprečna vrednost $\cos^2(\theta)$ enaka $\frac{1}{2}$, kjer je θ kot med polarizacijo fotona ter polarizatorjem, pri čemer predpostavimo enakomerno porazdeljenost polarizacije fotonov). Če za navpično polariziranim filtrom namestimo enak filter, se ne bo na intenziteti svetlobe poznalo nič, saj bodo skozi drugi filter prišli vsi fotoni, kot so skozi prvega. Sedaj sukamo drugi filter in opazimo, da skozenj prihaja vedno manj

svetlobe, dokler ni nameščen pravokotno na prvi filter. Takrat filter zadrži vso svetlobo. Intenziteta svetlobe, ki prehaja skozi drugi filter, se izračuna po enačbi $I = I_0 cos^2(\theta)$, kjer je I_0 začetna intenziteta svetlobe (intenziteta po prvem filtru), θ pa kot med merjenima polarizacijama. Tak sistem lahko prenesemo v Hilbertov prostor, kjer horizontalno polarizacijo obravnavamo kot vektor $|x\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, vertikalno polarizacijo pa kot vektor $|y\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Horizontalna in vertikalna polarizacija sta bazni stanji sistema, vektorja $|x\rangle$ in $|y\rangle$ pa predstavljata ortonormirano bazo.

Skalarni produkt dveh možnih stanj $\langle x|y\rangle$ nam predstavlja *verjetnostno amplitudo*, ki pove, kakšne so možnosti prehoda fotonov skozi stanje $|x\rangle$, če je pripravljen v stanju $|y\rangle$.

Verjetnostna amplituda nam še ne pove *verjetnosti*. Le–to dobimo s kvadriranjem skalarnega produkta

$$|\langle x|y\rangle|^2 = \langle x|y\rangle \langle y|x\rangle . \tag{3.13}$$

Če nadaljujemo s poskusom in med vertikalno ter horizontalno polarizirana filtra vrinemo tretjega, katerega polarizacija ni vzporedna prejšnjima, se za zadnjim filtrom pojavi nekaj svetlobe. Vsi fotoni, ki pridejo skozi prvi filter, imajo enako energijo in polarizacijo, vendar jih skozi drugi polarizator pride le določeno število. Ne moremo z gotovostjo napovedati, kateri izmed fotonov bo prišel skozi, lahko izračunamo le njegovo verjetnost. Ta nenavaden pojav lahko pojasnimo s pojmom *superpozicije* (oziroma linearne kombinacije) posameznih fotonov. Vsak foton lahko zapišemo kot vektor linearne kombinacije baznih vektorjev. Ker v opisanem eksperimentu bazo predstavljata vektorja vertikalne in horizontalne polarizacije, lahko vsako stanje sistema (smer polarizacije) zapišemo kot

$$|\Theta\rangle = \alpha |x\rangle + \beta |y\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}, \tag{3.14}$$

pri čemer je $|\Theta\rangle$ enotski vektor, Θ pa kot med opazovanima polarizacijama. Ker imamo vsak vektor predstavljen na enotski sferi Hilbertovega prostora, velja enakost

$$\alpha^2 + \beta^2 = 1, \quad \alpha, \beta \in \mathbb{C}. \tag{3.15}$$

V našem primeru α predstavlja verjetnostno amplitudo, da bo foton, polariziran pod kotom Θ od polarizatorja $|x\rangle$ prišel skozi polarizator $|x\rangle$, in je enaka $cos(\Theta)$, β pa predstavlja verjetnostno amplitudo, da bo isti foton prišel skozi polarizator $|y\rangle$. Verjetnost prehoda skozi posamezni (bazni) polarizator pa dobimo s kvadriranjem verjetnostne amplitude.

Opazovana merljiva lastnost je tako v našem primeru meritev vertikalne ali horizontalne

polarizacije. Hermitski operator te lastnosti oziroma njemu pripadajoča matrika je oblike $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$. Je ena izmed *Paulijevih matrik*, in se hitro izračuna iz enačbe (3.8), lastnih vektorjev in pripadajočih lastnih vrednosti (predpostavimo njuni vrednosti). Lastni vrednosti kot rezultat meritve povesta, ali je posamezni foton šel skozi polarizator ali ne.

Matematično formulacijo konkretnega sistema, opisanega z zgornjim eksperimentom, lahko tudi posplošimo. V splošnem lahko vsako stanje sistema zapišemo kot

$$|\psi\rangle = \sum_i a_i |x_i\rangle = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \end{pmatrix}, \tag{3.16}$$

kjer vektorji $|x_i\rangle$ predstavljajo neksončno ortonormirano bazo nekega Hilbertovega prostora. Pri tem velja

$$\sum_i a_i a_i^* = 1 \tag{3.17}$$

in

$$P(x_i) = |a_i|^2 = a_i a_i^*, \tag{3.18}$$

kjer je $P(x_i)$ verjetnost, da bo stanje $|\psi\rangle$ izmerjeno v stanju $|x_i\rangle$. To verjetnost dobimo iz izračuna kvadrata skalarnega produkta $\langle x_i|\psi\rangle^2$, pri čemer upoštevamo ortonormiranost baze.

Če se vrnemo na enačbo (3.8), lahko definiramo operatorje za izračun najpomembnejših količin, ki so pozicija delca, njegova gibalna količina in energija. Izračuni operatorjev vključujejo uporabo valovne funkcije in Schrödingerjeve enačbe in jih ne bomo izpeljevali.
Operator pozicije delca je oblike

$$\hat{X} = -\frac{id}{dx}, \tag{3.19}$$

pri čemer lastna vrednost enačbe $\hat{X}|\psi\rangle = x|\psi\rangle$ predstavlja pozicijo delca z valovno funkcijo $|\psi\rangle$.
Operator gibalne količine

$$\hat{P} = -\frac{i\hbar d}{dx} \tag{3.20}$$

kot lastno vrednost vrne gibalno količino opazovanega delca $\hat{P}|\psi\rangle = p|\psi\rangle$.

Operator energije imenujemo *Hamiltonov operator*

$$\hat{H} = -\frac{\hbar^2}{2m}\frac{d^2}{dx^2} + u(x), \tag{3.21}$$

ki pomnožen z valovno funkcijo predstavlja Schrödingerjevo enačbo. S tem operatorjem torej preverjamo, kako se energija sistema spreminja skozi čas $\hat{H}\,|\psi\rangle = E\,|\psi\rangle$.

Sedaj imamo matematični model kvantnega sistema. Če želimo opazovano lastnost izmeriti večkrat in pri tem opazovati dobljene meritve (lastne vektorje), je potrebno narediti več kopij sistema, ker stanja po večih meritvah ene lastnosti ostanejo nespremenjena (šesti aksiom pove, da se stanja sistema po meritvi kolapsirajo v merjena stanja in v teh ostanejo). Tako je povprečna vrednost meritve po N merjenjih enaka

$$\overline{m} = \frac{1}{N}\sum_{i=1}^{N}\lambda_i \tag{3.22}$$

in

$$lim_{N\to\infty}\overline{m} = \mu. \tag{3.23}$$

Pričakovana vrednost meritve sistema H v stanju $|\psi\rangle$ je torej

$$\mu = \sum_i |a_i|^2\lambda_i, \tag{3.24}$$

ki jo označimo in izračunamo kot $\langle\psi|H|\psi\rangle$, pri čemer vrstni red množenja ni pomemben [5].

V zadnjem delu poglavja še pojasnimo pojem **kvantne prepletenosti** (angl. entanglement). Če imata dva delca isto valovno funkcijo, rečemo, da sta prepletena, kar pomeni, da so njune lastnosti povezane. Takoj ko izmerimo lastnost enega delca, povzročimo kolaps valovne funkcije. Z meritvijo posameznega delca nemudoma vplivamo tudi na drugega, čeprav sta lahko na poljubnih medsebojnih razdaljah. Eksperimentalno pokažemo prepletenost tako, da s posebno napravo spustimo dva prepletena fotona (prepletenost se doseže s temu namenjenimi napravami) in ju pošljemo v nasprotnih smereh ter izmerimo polarizacijo prvega. V trenutku meritve smo spremenili polarizacijo obeh fotonov naenkrat. Če je bil prvi foton polariziran navpično, je polarizacija drugega fotona nujno navpična, ampak v nasprotni smeri prvega. Pojav še danes bega znanstvenike, saj edina možna razlaga pove, da delca komunicirata v vsakem trenutku. To bi pomenilo, da bi se informacije širile hitreje kot svetloba, kar je v nasprotju s splošno relativnostno teorijo [21].

Poglavje 4

Kvantno računalništvo

V 90. tih letih 20. tega stoletja se je začel razvoj kvantnega računalništva, katerega začetnik je bil Richard Feynman, ki je ugotovil, da klasični računalniki ne morejo učinkovito simulirati procesov kvantne mehanike. Osnovni razlog za to je, da splošno kvantno stanje predstavlja superpozicijo 2^n klasičnih stanj, kar podrobneje razložimo tekom poglavja. Klasični računalniki preprosto niso tako zmogljivi, da bi v doglednem času lahko izvedli netrivialne izračune. Tako se je začel intenziven razvoj kvantnega računalnika in algoritmov, ki traja še danes.

Kvantni računalniki izkoriščajo lastnosti kvantne mehanike, s čimer pohitrijo računske procese. Rezultat ohranjanja informacije v superpoziciji ali prepletenosti so bistveno hitrejši algoritmi, kot jih uporabljamo na klasičnih računalnikih.

V poglavju opišemo osnovne elemente kvantnega računalništva, potrebne za razvoj algoritmov, prenesemo matematični koncept kvantne mehanike na sistem kvantnega računalnika ter opišemo model kvantnega računanja na osnovi kvantnega vezja.

4.1 Elementi kvantnega računalništva

Glavni komponenti kvantnega računalništva sta pomnilnik, sestavljen iz kvantnih bitov, ter procesor, ki izvaja operacije s kvantnimi logičnimi vrati.

4.1.1 Kvantni pomnilnik

Kubit

Fundamentalna enota klasične informacije je bit, ki lahko zavzame vrednosti 0 ali 1. V kvantnem računalništvu predstavlja analogijo klasičnemu bitu kvantni bit, ali *kubit*, ki predstavlja osnovno enoto kvantne informacije.

Definicija 4.1 *Kvantni bit ali **kubit** je najenostvnejši kvantni sistem, katerega stanje lahko opišemo kot superpozicijo stanj* $|0\rangle$ *in* $|1\rangle$*, ki predstavljata standardno ortonormirano bazo sistema. Prostor stanj je kompleksen Hilbertov prostor* $\mathbb{C}^2$*.*

Splošno stanje kubita je tako

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{4.1}$$

kar v Hilbertovem prostoru predstavimo z vektorjem $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. Pri tem velja $\alpha, \beta \in \mathbb{C}$ in

$$|\alpha|^2 + |\beta|^2 = 1. \tag{4.2}$$

Sistem z dvema stanjema lahko predstavimo s tridimenzionalno enotsko sfero, ki jo imenujemo *Blochova sfera* (slika 4.1). Vsako stanje kubita predstavlja točko na Blochovi sferi. Severni in južni pol sta bazni stanji $|0\rangle$ in $|1\rangle$, vsaka točka na ekvatorju pa superpozicija teh stanj z enako verjetnostno amplitudo. Splošno stanje opišemo s pomočjo sfernih koordinat

$$|\Psi\rangle = \cos\left(\frac{\phi}{2}\right)|0\rangle + e^{i\theta}\sin\left(\frac{\phi}{2}\right)|1\rangle\,, \quad 0 < \theta < \pi,\ 0 < \phi < 2\pi, \tag{4.3}$$

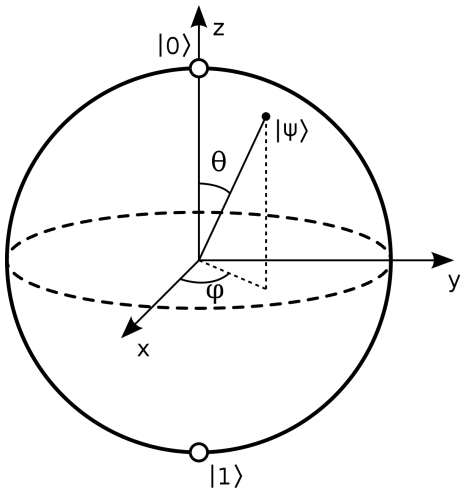
kjer je ϕ polarni kot, θ pa kot med z-osjo in enotskim vektorjem stanja.

Pomembni lastnosti Blochove sfere sta ortogonalnost nasprotnih točk in možnost rotacije okrog x, y, in z-osi, kar v nadaljevanju predstavimo s kvantnimi opreatorji. Če sta točki na Blochovi sferi zamaknjeni za azimutni kot π, sta ortogonalni in predstavljata neko bazo v Hilbertovem prostoru. V splošnem velja ekvivalenca

$$\vec{r_\Phi} = -\vec{r_\theta} \Leftrightarrow \langle\Phi|\theta\rangle = 0, \tag{4.4}$$

kjer sta $\vec{r_\Phi}, \vec{r_\theta}$ enotska vektorja na Blochovi sferi [18], [20].

Opomba 4.2 *Blochova sfera ni podmnožica pripadajočega Hilbertovega prostora, ampak predstavlja le orodje za vizualizacijo sistema z dvema baznima stanjema.*



Slika 4.1: Blochova sfera.

Nad kvantnim bitom izvajamo le unitarne operacije ali meritev:

1. *Izvedba meritve:* Naj bo superpozicija kubita oblike $\begin{pmatrix}\alpha\\ \beta\end{pmatrix}$. Če nad tem kubitom izvedemo meritev, kot rezultat meritve dobimo 0 z verjetnostjo $|\alpha|^2$, ali 1 z verjetnostjo $|\beta|^2$. Rečemo, da se kubit kolapsira v eno izmed možnih baznih stanj, njemu prirejen vektor pa dobi obliko $\begin{pmatrix}1\\ 0\end{pmatrix}$ ali $\begin{pmatrix}0\\ 1\end{pmatrix}$. Rezultat meritve je *klasična informacija.*
2. *Izvedba unitarne operacije:* Vsaka unitarna matrika U, prirejena neki linearni transformaciji, spremeni superpozicijo kubita, predstavljenega z vektorjem v, v superpozicijo Uv [20].

Pri razvijanju kvantnih računalnikov se poslužujejo različnih realizacij kubitov. Kubit je lahko sistem z dvema ortogonalnima polarizacijama fotona ali spin elektrona ali atomskega jedra ipd. Spin je eno izmed kvantnih števil, s katerim opišemo delec, in ima le dve možni vrednosti, spin gor in spin dol, ki predstavljata standardno ortonormirano bazo [8].

Tenzorski produkt

Ker lahko posamezni kubit prenesemo na kompleksni Hilbertov prostor, rabimo pri računanju z n kubiti nov vektorski prostor, ki ga dobimo s tenzorskim produktom n Hilbertovih prostorov $\mathcal{H} \otimes \ldots \otimes \mathcal{H}$.

Nadalje definirani tenzorski produkt dveh vektorskih prostorov lahko intuitivno prenesemo na višje dimenzije.

Definicija 4.3 *Naj bosta $\mathcal{H}_1$ in $\mathcal{H}_2$ Hilbertova prostora z bazama $\mathcal{B}_1$ in $\mathcal{B}_2$. Potem je tudi*

tenzorski produkt

$$\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2 = \{ \sum_{|i\rangle \in \mathcal{B}_1} \sum_{|j\rangle \in \mathcal{B}_2} c_{i,j} \, |i,j\rangle \, | c_{i,j} \in \mathbb{C} \} \tag{4.5}$$

Hilbertov prostor z bazo $\mathcal{B} = \mathcal{B}_1 \otimes \mathcal{B}_2$ *in skalarnim produktom* $\langle i,j|i',j'\rangle = \langle i|i'\rangle \langle j|j'\rangle$*, kjer* $|i\rangle, |i'\rangle \in \mathcal{B}_1 \quad |j\rangle, |j'\rangle \in \mathcal{B}_2$*. Dimenzija prostora* $\mathcal{H}$ *je* nm*, kjer je* n *dimenzija prostora* $\mathcal{H}_1$*,* m *pa dimenzija prostora* $\mathcal{H}_2$

Definicija 4.4 *Naj bosta* $x \in \mathcal{H}_1, y \in \mathcal{H}_2$*, oblike* $x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$, $y = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$*. Potem je njun tenzorski produkt* $x \otimes y$ *matrika dimenzije* $n \times m$*, kjer* $(x \otimes y)_{i,j} = x_i y_j$*.*

Trditev 4.5 *Naj bodo* $x \in \mathcal{H}_1, y \in \mathcal{H}_2, z \in \mathcal{H}_3$*. Veljajo naslednje lastnosti:*

(i) $(x \otimes y) \otimes z = x \otimes (y \otimes z)$,

(ii) $x \otimes (y + z) = x \otimes y + x \otimes z \quad in \quad (x + y) \otimes z = x \otimes z + y \otimes z$,

(iii) $\alpha(x \otimes y) = (\alpha x) \otimes y = x \otimes (\alpha y), \quad \alpha \in \mathbb{C}$,

(iv) $x \otimes y \neq y \otimes x$.

Opomba 4.6 *Tenzorski produkt dveh stanj kubitov* $|\psi\rangle, |\phi\rangle$ *zapišemo kot* $|\psi\rangle \otimes |\phi\rangle = |\psi\rangle \, |\phi\rangle$*. Oznaka za tenzorski produkt baznih stanj* $|i\rangle, |j\rangle$ *je* $|i,j\rangle$*.*

Stanje, ki ga dobimo kot tenzorski produkt dveh stanj imenujemo *kombinirano stanje*. Če kombinirano stanje lahko zapišemo kot tenzorski produkt dveh ali več stanj, so ta stanja *ločljiva*, v nasprotnem primeru pa so med sabo *prepletena*. Taka stanja ustrezajo kvantnomehanski lastnosti prepletenosti, opisani ob koncu tretjega poglavja [9], [22].

Kvantni register

Kvantni register je nabor n kvantnih bitov, ki ga lako zapišemo s tenzorskim produktom

$$|e\rangle = |e_{n-1}\rangle \otimes |e_n\rangle \otimes \ldots \otimes |e_0\rangle \, . \tag{4.6}$$

Kvantni register dveh kubitov ima štiri bazna stanja $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ in se lahko nahaja v enem izmed teh stanj ali pa je v njihovi superpoziciji

$$|\Psi\rangle = \alpha_0 |00\rangle + \alpha_1 |01\rangle + \alpha_2 |10\rangle + \alpha_3 |11\rangle . \tag{4.7}$$

V kvantnem registru z n kubiti je lahko shranjenih 2^n klasičnih števil. Elemente standardne ortonormirane baze takega kvantnega registra za lažjo preglednost označujemo kot $|0\rangle, |1\rangle, \ldots, |N-1\rangle$, kjer je $N = 2^n$ [9].

4.1.2 Kvantni operatorji

Iz prejšnjega poglavja vemo, da se stanje sistema skozi čas spreminja preko Schrödingerjeve enačbe, dokler ga ne izmerimo. Kvantni operatorji oziroma kvantna logična vrata, opisana v nadaljnjih odstavkih, predstavljajo analogijo reševanju časovno odvisne Schrödingerjeve enačbe v kvantnem računalništvu, saj spreminjajo stanje sistema ter s tem določajo verjetnosti za posamezno meritev. Delovanje kvantnih vrat označujemo s simboli, ki jih zapisujemo v diagramu poteka kvantnega računanja.

Vsebina podpoglavja je povzeta po [15], [20], [22].

Definicija 4.7 *Kvantni operatorji ali* ***kvantna logična vrata*** *so unitarne linearne transformacije, ki spreminjajo stanje enega ali več kvantnih bitov v novo stanje. Za matriko unitarne linearne transformacije U velja enakost $UU^\dagger = \mathbb{I}$.*

Opomba 4.8 *Pogoj za unitarnost je pomemben s stališča ohranjanja dolžin vektorjev. Če si predstavljamo stanje kubita kot vektor na Blochovi sferi pred transformacijo, tudi po transformaciji predstavlja neko stanje, zato mora ležati na Blochovi sferi.*

Opomba 4.9 *Ker so kvantni operatorji po definiciji obrnljive matrike (inverz vsake transformacije U je $U^\dagger$), je pri kvantnem računanju vsaka operacija obrnljiva. Pri klasičnem računanju bi se morali za tak pogoj omejiti le na računanje z bijektivnimi funkcijami.*

Eno–kubitna kvantna vrata

Najenostavnejši primer unitarnih transformacij so kvantna vrata, ki delujejo na enem kubitu. Predstavimo jih z unitarno matriko dimenzije 2×2.

Hadamardova vrata

Hadamardova vrata predstavimo z matriko

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

Standardno stanje $|0\rangle$ Hadamardova vrata pretvorijo v $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, stanje $|1\rangle$ pa v $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$.
Če uporabimo Hadamardova vrata hkrati na n kubitih v stanju $|0\rangle$, dobimo stanje enotne superpozicije $|s\rangle$, kjer imajo vsi bazni vektorji enako verjetnostno amplitudo

$$|s\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle . \tag{4.8}$$

Hadamardova vrata so sama sebi inverz, $HH = \mathbb{I}$, kar pomeni, da če na stanje kubita dvakrat delujemo s Hadamardovimi vrati, dobimo stanje enako začetnemu. Le–to razloži pojav *kvantne interference*. Rezultat dvakratnega delovanja Hadamardovih vrat na stanje $|0\rangle$, vrne stanje $|0\rangle$. Po drugem delovanju Hadamardovih vrat je verjetnostna amplituda, da dobimo stanje $|1\rangle$ iz stanja $|0\rangle$ po absolutni vrednosti enaka verjetnostni amplitudi, da dobimo stanje $|1\rangle$ iz stanja $|1\rangle$, vendar ima nasprotni predznak. Zato se medsebojno izničita oziroma *destruktivno interferirata*. Nasprotno sta verjetnostni amplitudi za stanje $|0\rangle$ pozitivni in *interferirata konstruktivno*. Zato velja, da meritev začetnega stanja $|0\rangle$ po dvakratnem delovanju Hadamardovih vrat vrne stanje $|0\rangle$ z verjetnostjo 1.

Simbol, ki označuje delovanje Hadamardovih vrat na kubit prikazuje naslednja slika:

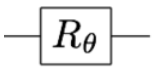
Slika 4.2: Hadamardova vrata.

Fazna vrata

Matrika kvantnih faznih vrat je oblike

$$\Phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Ta vrata stanja $|0\rangle$ ne spreminjajo, stanje $|1\rangle$ pa transformirajo v $e^{i\theta}|1\rangle$, kjer je θ azimutni kot na Blochovi sferi.



Slika 4.3: Fazna vrata.

Za fazna vrata uporabljamo več različnih oznak, eno izmed njih prikazuje zgornja slika.

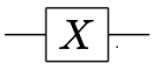
Paulijeva vrata

Poznamo Paulijeva X, Y in Z kvantna vrata, ki predstavljajo vrtenje na Blochovi sferi za π radianov.

Paulijeva X vrata predstavljajo vrtenje okrog osi x

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

Oznaka v diagramu:



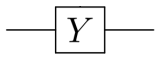
Slika 4.4: Paulijeva X vrata.

Ta vrata lahko predstavimo tudi kot vrata NOT, saj obrnejo stanje kvantnega bita. Bazno stanje $|0\rangle$ pretvorijo v $|1\rangle$ in obratno. Tudi ta vrata so sama sebi inverz, zato velja enakost $XX = \mathbb{I}$.

Paulijeva Y vrata opišejo vrtenje okrog osi y

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

Oznaka v diagramu:

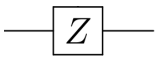


Slika 4.5: Paulijeva Y vrata.

Paulijeva Z vrata, ki so ekvivalentna vrtenju okrog osi z, so le poseben primer faznih vrat, kjer je $\theta = \pi$

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Oznaka v diagramu:



Slika 4.6: Paulijeva Z vrata.

Več–kubitna kvantna vrata

Analogno enokubitnim vratom lahko n–kubitna vrata predstavimo z unitarno matriko dimenzije $2^n \times 2^n$.

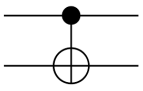
CNOT vrata

Nadzorovana NE (CNOT ali controlled–NOT) vrata delujejo nad dvema kvantnima bitoma, pri čemer izberemo kontrolni in ciljni kubit. Delujejo tako, da negirajo stanje ciljnega kubita le, če je kontrolni kubit v stanju $|1\rangle$, kar opiše matrika

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

Kombinacija operatorjev Hadamardovih in CNOT vrat poveže vhodna kubita v stanje prepletenosti.

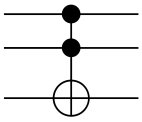
Delovanje CNOT vrat, kjer je prvi kubit kontrolni, označimo s simbolom:



Slika 4.7: CNOT vrata.

Toffolijeva vrata

Toffolijeva vrata ali dvojna nadzorovana NE vrata delujejo nad tremi kubiti, kjer je spet potrebno izbrati ciljni kubit, ostala dva sta kontrolna. Vrata negirajo stanje ciljnega kubita le, če sta oba kontrolna bita v stanju $|1\rangle$. Predstavljena so z matriko dimenzije 8×8, ki je analogna matriki CNOT vrat. Oznaka za delovanje Toffolijevih vrat, kjer sta prva dva kubita kontrolna, je:



Slika 4.8: Toffolijeva vrata.

Univerzalni set logičnih vrat

Pri klasičnih računalnikih logična operatorja NAND (negirani in) in NOR (negirani ali) predstavljata univerzalni set logičnih vrat, ki lahko izračunata katerokoli funkcijo. V kvantnem računalništvu ta set predstavljajo eno–kubitna in CNOT vrata. Z njimi lahko zgradimo katerokoli unitarno operacijo na n kubitih.

Opomba 4.10 *Vsa zgoraj opisana kvantna vrata so matrike linearnih transformacij v standardni bazi.*

4.2 Model kvantnega računanja

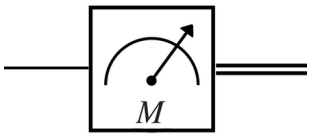
Ob koncu poglavja elemente kvantnega računalništva združimo v celoto kot model na osnovi kvantnega vezja, ki se uporablja za ponazoritev nadzorovanega spreminjanja stanj kvantnih bitov oziroma poteka algoritmov. Osnovna ideja približa in poenostavi razumevanje spreminjanja sistema skozi čas.

Vsebina podpoglavja je povzeta po [22].

Model temelji na izdelavi **kvantnega vezja**, predstavljenega z diagramom poteka, ki vsebuje začetna stanja kubitov, kvantna logična vrata in meritev. Vsak kubit je predstavljen s horizontalno črto, operacije in meritev pa označujejo posebni simboli. Simboli za operacije so navedeni pri posameznih kvantnih vratih. Potek kvantnega računanja, kjer enoto informacije predstavlja kubit, skrajšano zapišemo v treh korakih:

1. *Priprava:* Priprava kubitov v superpozicijo baznih stanj v standardni bazi.
2. *Razvoj:* Izvedba operacij s kvantnimi vrati.
3. *Meritev:* Meritev, ki povzroči kolaps superpozicije možnih stanj in vrne klasično informacijo.

V diagramu poteka se uporablja več možnih simbolov za meritev, najpogostejši je prikazan na spodnji sliki, kjer vzporedni črti predstavljata klasično informacijo po meritvi:



Slika 4.9: Simbol za meritev.

Opomba 4.11 *Edina neobrnljiva operacija izvedena nad stanji kvantnih bitov je meritev. Le–to pove 6. aksiom kvantne mehanike.*

Poglavje 5

Groverjev algoritem

5.1 Kvantni algoritmi

Kvantni algoritmi, skupki kvantnih vrat in registrov, izkoriščajo superpozicijo kvantnih stanj, pri čemer je v kvantnih registrih sočasno shranjenih več števil. Ponavadi so predstavljeni z diagramom poteka kvantnega vezja, ki se pričnejo z nekaj vhodnimi kubiti in končajo z meritvijo, oziroma sledijo poteku kvantnega računanja priprava–razvoj–meritev pri modelu kvantnega vezja. So verjetnostni algoritmi, saj je meritev posameznega stanja odvisna od verjetnosti, dobljene iz amplitude baznega stanja. Verjetnost točne napovedi je večja pri večjem številu vzorcev, zato je potrebno za natančnejše izračune posamezni algoritem večkrat ponoviti.

V splošnem so za pohitritev nad klasičnimi algoritmi potrebni trije pogoji:

1. *Superpozicija*: Ker lahko vsako stanje zapišemo kot superpozicijo baznih stanj

$$|\psi\rangle = \sum_{x=0}^{N-1} \alpha_x |x\rangle , \tag{5.1}$$

   lahko v enem stanju hranimo $N = 2^n$ klasičnih informacij.

2. *Paralelizem*: Če je stanje $|\psi\rangle$ že v superpoziciji nekaterih baznih stanj, deluje operator U na vsa bazna stanja hkrati, kar imenujemo *kvantni paralelizem*

$$U \sum_{x=0}^{N-1} \alpha_x |x\rangle = \sum_x \alpha_x U |x\rangle . \tag{5.2}$$

   Ravno superpozicija in paralelizem omogočata pohitritive kvantnih algoritmov do mere, ki ji klasični algoritmi niso kos.

3. *Kvantna interferenca*: Kvantna interferenca, razložena na primeru dvakratnega delovanja Hadamardovih vrat, poveča verjetnost, da bo izmerjeno željeno stanje ter zmanjša verjetnosti za meritev ostalih. Interferenca tako dovoljuje spreminjanje stanj v superpoziciji [22].

Zelo uporabna kvantnomehanska lastnost je tudi prepletenost kubitov, ki pa je med algoritmi manj razširjena. Koristna je predvsem na področju prenosa klasičnih informacij s pomočjo kubitov in kvantnega teleportiranja.

Računska zahtevnost kvantnih algoritmov

Dva osnovna razreda računske zahtevnosti sta **P**(polinomski) in **NP**(nedeterministično polinomski), kjer razred **P** vsebuje računske probleme rešljive v polinomskem času, **NP** pa je razred problemov, za katere lahko pravilnost rešitve ugotovimo v polinomskem času. Razred **NP** vsebuje tudi **NP–polne** probleme, ki so najtežji problemi v **NP** in so prevedljivi na **NP** probleme. Če bi uspeli najti polinomski algoritem, ki reši **NP–poln** problem, bi bili polinomsko rešljivi vsi **NP** problemi, kar bi pomenilo, da sta razreda **P** in **NP** enaka. Vemo, da je razred **P** vsebovan v razredu **NP**, vendar ne vemo ali velja enakost $\mathbf{P} = \mathbf{NP}$.

Čeprav vemo, da lahko kvantni algoritmi učinkovito rešijo nekatere **NP** probleme, ki po mnenju mnogih niso v razredu **P** (npr. faktorizacija), še ni znano, ali lahko hitro rešijo vse **NP** probleme.

Razreda **P** in **NP** se nahajata v razredu **P–SPACE**, ki vsebuje probleme, rešljive s pomnilnikom polinomske velikosti, pri katerem čas obdelave ni omejen.

Za reševanje problemov s kvantnimi algoritmi lahko definiramo nov razred **BQP**, ki učinkovito reši probleme na kvantnih računalnikih z dovoljeno mejno verjetnostno napako. Neznana je točna relacija med razredi **BQP** in **P, NP, P–SPACE**, vemo pa, da kvantni računalniki učinkovito rešijo vse **P** probleme, ne morejo pa rešiti problemov izven **P–SPACE** v doglednem času. Tako razred **BQP** leži nekje med **P–SPACE** in **P** [17].

Splošni računski proces

Kvantni računalnik deluje na število x z določeno funkcijo f in kot rezultat vrne $f(x)$. Če je x n–bitno celo število, $f(x)$ pa m–bitno celo število, za računanje potrebujemo vsaj $n + m$ kubitov. Za dejanski računski proces so potrebni še dodatni kubiti, ki jih za lažji zapis poteka trenutno zanemarimo. Kvantni register je sestavljen iz vhodnega in izhodnega registra, pri čemer vhodni register hrani začetnih n kubitov, izhodni pa m kubitov, dobljenih s funkcijo f. Z vhodnim in izhodnim registrom upravljamo istočasno, pri poteku kvantnega računanja pa sledita že opisanemu poteku kvantnega računanja:

1. *Priprava:* Na tem koraku se vhodni register postavi v stanje superpozicije baznih stanj, kar lahko dosežemo z delovanjem Hadamardovih vrat.

2. *Razvoj:* Za vsa vhodna stanja algoritem izračuna vrednosti funkcije f. Tako je v izhodnem registru shranjena superpozicija vseh možnih rezultatov $f(x)$ za vsak x v vhodnem registru.

3. *Meritev:* Izvede se meritev izhodnega registra, kjer se superpozicija možnih izidov funkcije f kolapsira v eno izmed možnih stanj. Hkrati meritev izhodnega registra povzroči kolaps superpozicije stanj vhodnega registra. Tako v vhodnem registru ostane vrednost x, ki prispeva k izmerjeni vrednosti $f(x)$. Če je $f(x)$ enak za različne vrednosti x, bo v vhodnem registru po meritvi ostala superpozicija teh vrednosti [9].

Funkcija f je izvedena s pomočjo kvantnih vrat oziroma transformacije U_f na naslednji način

$$U_f(|x\rangle_n |y\rangle_m) = |x\rangle_n |y \oplus f(x)\rangle_m . \tag{5.3}$$

Operator $\oplus$ predstavlja seštevanje po modulu 2, oziroma deluje enako kot kvantna vrata CNOT.

Če je začetna vrednost izhodnega registra enaka $y = 0$, je stanje po delovanju vrat enako

$$U_f(|x\rangle_n |y\rangle_m) = |x\rangle_n |f(x)\rangle_m . \tag{5.4}$$

Stanje vhodnega registra ostane nespremenjeno, v izhodnem registru pa je samo vrednost funkcije $f(x)$.

Večina funkcij f ne more biti izvedena učinkovito (z majhnim številom kvantnih vrat), zato veliko učinkovitih klasičnih algoritmov kvantni računalniki izvajajo počasneje kot klasični. Tako ni nujno, da je vsak kvantni algoritem hitrejši in efektivnejši od klasičnega, obstajajo pa trije razredi kvantnih algoritmov, ki klasične prekašajo. V prvi razred spadajo algoritmi, ki temeljijo na (kvantni) Fouriejevi transformaciji, orodju, ki se na široko uporablja pri klasičnem računanju. Ti algoritmi rešijo faktorizacijske probleme v eksponentno hitrejšem času kot najboljši znani klasični algoritmi. Najbolj znana sta Deutsch–Jozsa in Shorov algoritem. V drugem razredu so simulacijski algoritmi, ki simulirajo kvantne sisteme. V tretjem razredu pa se nahajajo kvantni iskalni algoritmi, katerih osnovo predstavlja Groverjev algoritem [8], [9], [15].

Kvantni iskalni algoritmi

Kvantni iskalni algoritmi rešijo naslednji problem: v nestrukturiranem iskalnem prostoru velikosti N poiščejo element, ki zadošča znani lastnosti. Klasično bi za reševanje opisanega problema v naslabšem primeru potrebovali N operacij, kvantni iskalni algoritem pa najde element z le $\sqrt{N}$ operacijami. Kvantni iskalni algoritmi tako kvadratično pohitrijo

iskanje. Čeprav so počasnejši v primerjavi z algoritmi, ki temeljijo na kvantni Fouriejevi transformaciji, jih lahko uporabimo za večji spekter reševanja problemov [8], [22].

5.2 Groverjev algoritem

Groverjev algoritem, ki ga je zasnoval in leta 1996 objavil Lov Grover, predstavlja osnovo kvantnih iskalnih algoritmov, ki so uporabni za pohitritev reševanja NP–polnih problemov ter iskanja elementa po nestrukturirani bazi.

5.2.1 Opis

Vsebina podpoglavja je povzeta po [4].

Definicija 5.1 *Cilj Groverjevega algoritma je pri dani množici N elementov* $X = \{x_1, x_2, \ldots, x_N\}$ *iz nestrukturirane baze in funkciji* $f : X \longrightarrow \{0, 1\}$ *s predpisom:*

$$f(x) = \begin{cases} 0 & x \neq x^* \\ 1 & x = x^* \end{cases} \tag{5.5}$$

najti element x^**, da je* $f(x^*) = 1$*.*

Nestrukturirano iskanje najlažje pojasnimo z iskanjem elementa po neurejeni bazi. Kot primer lahko navedemo iskanje po telefonskem imeniku, kjer imamo dano telefonsko številko ter ji želimo najti pripadajoče ime. Ker številke niso urejene po velikosti, lahko na klasičen način po vrsti preverjamo posamezne številke in ko pridemo do prave, dobimo željeno informacijo o imenu. Tak način je zelo zamuden, saj je ustrezno številko enostavno prepoznati, vendar jo je med velikim številom podatkov težko najti. Kvantni pristop temelji na definiranju 'oracle' funkcije, ki označi dano številko in z uporabo superpozicije in paralelizma pohitri iskanje na celotni bazi podatkov.

Klasični pristop

Klasični pristop iskanja željenega vhoda posamično preverja vse možne vhode pri dani množici N elementov. V najslabšem primeru potrebuje $N - 1$ korakov, v povprečju torej $\frac{N}{2}$ korakov. Časovna zahtevnost je tako enaka $O(N)$.

Kvantni pristop

Kvantni pristop iskanja željenega podatka s pomočjo superpozicije hkrati preverja več možnih vhodov, kar močno pohitri iskanje. Pri opisu algoritma predpostavimo, da obstaja le ena rešitev iskalnega problema, torej le en tak $x^* \in X$, da je $f(x^*) = 1$.

Groverjev algoritem je sestavljen iz treh glavnih korakov in končne meritve. Predpostavimo, da imamo n začetnih kubitov. Vseh možnih stanj je tako $2^n = N$.

1. **Priprava začetnih stanj v stanje superpozicije**
   Začetno stanje vseh kubitov je enako $|0\rangle$. Na vsak kubit delujemo s Hadamardovimi vrati, da dobimo stanje enotne superpozicije

   $$|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \,. \tag{5.6}$$

2. **Delovanje oracle funkcije** O
   Hitro opazimo, da funkcija f iz definicije ni obrnljiva, zato je ne moremo uporabiti kot kvantna vrata v algoritmu. Oracle funkcijo zato definiramo na naslednji način

   $$O\,|x\rangle = (-1)^{f(x)}\,|x\rangle = \begin{cases} |x\rangle & |x\rangle \neq |x^*\rangle \\ -\,|x\rangle & |x\rangle = |x^*\rangle \,. \end{cases} \tag{5.7}$$

   S tako definicijo oracle operatorja shranimo informacijo o željenem vhodu v fazo stanja kubita. Groverjev algoritem tako pri dani funkciji O poišče tako stanje $|x^*\rangle$, da je $O\,|x^*\rangle = -\,|x^*\rangle$.
3. **Delovanje operatorja amplitudnega ojačanja** G
   Operator amplitudnega ojačanja poveča verjetnostno amplitudo pred stanjem $|x^*\rangle$ in zmanjša amplitude ostalih vektorjev $|x\rangle$. Matematično ga zapišemo kot

   $$G = 2\,|\psi\rangle\,\langle\psi| - \mathbb{I}. \tag{5.8}$$

   Kot že vemo, operator $|\psi\rangle\,\langle\psi|$ predstavlja projekcijo na vektor $|\psi\rangle$, operator G pa je zrcaljenje preko vektorja $|\psi\rangle$, kar pokažemo s preprosto izpeljavo.
   Naj bo $|w\rangle$ enotski vektor, nad katerim bomo prezrcalili vektor $|v\rangle$. Vektor $|v\rangle$ lahko zapišemo kot vsoto vzporednega vektorja z $|w\rangle$ in nanj pravokotnega

   $$|v\rangle = |v_v\rangle + |v_p\rangle \,, \tag{5.9}$$

   kjer velja

   $$|v_v\rangle = k\,|w\rangle \,, \tag{5.10}$$

$$\langle w|v_p\rangle = 0 \tag{5.11}$$

in

$$\langle w|v\rangle = \langle w|v_v\rangle + \langle w|v_p\rangle = \langle w|v_v\rangle + 0 = k\,\langle w|w\rangle = k. \tag{5.12}$$

Zato lahko vektorja $|v_v\rangle$ in $|v_p\rangle$ zapišemo kot

$$|v_v\rangle = \langle w|v\rangle\,|w\rangle \tag{5.13}$$

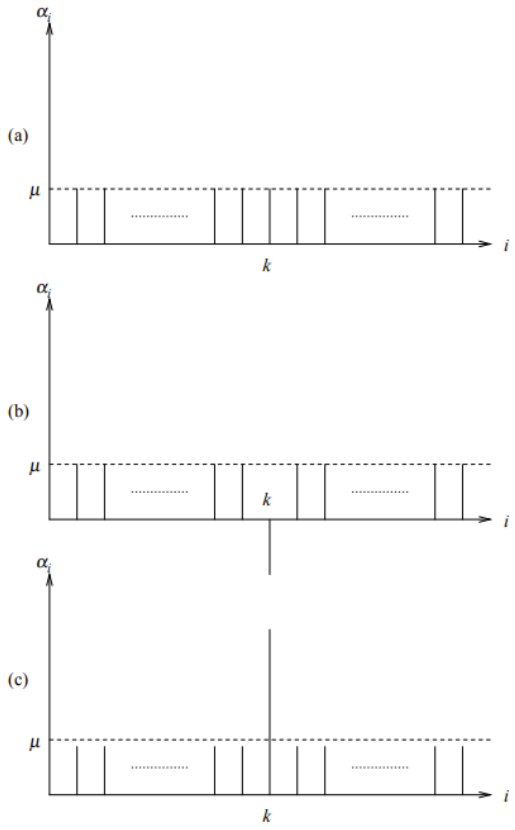
$$|v_p\rangle = |v\rangle - \langle w|v\rangle\,|w\rangle\,. \tag{5.14}$$

Sedaj prezrcalimo vektor $|v\rangle$ preko $|w\rangle$ z operatorjem R_w

$$R_w\,|v\rangle = |v\rangle - 2\,|v_p\rangle = |v\rangle - 2(|v\rangle - \langle w|v\rangle\,|w\rangle) = 2\,\langle w|v\rangle\,|w\rangle - |v\rangle = (2\,|w\rangle\,\langle w| - \mathbb{I})\,|v\rangle\,. \tag{5.15}$$

Operator rotacije okrog vektorja $|w\rangle$ je tako $2\,|w\rangle\,\langle w| - \mathbb{I}$ in $R_\psi = G$.

Zgornje korake opisuje naslednja slika (5.1), ki prikazuje spreminjanje verjetnostnih amplitud posameznih baznih stanj tekom algoritma. Po zadostni ponovitvi drugega (b) in tretjega (c) koraka, se verjetnostna amplituda stanja $|x^*\rangle$ povečuje. Iz slike je razvidno, da delovanje operatorja G poveča amplitudo željenemu izhodu in zmanjša amplitude ostalim.



Slika 5.1: Spreminjanje verjetnostnih amplitud baznih stanj tekom izvedbe Groverjevega algoritma.

Geometrijska vizualizacija

Vsi operatorji in amplitude v Groverjevem algoritmu so realni, kar pomeni, da vsa stanja lahko predstavimo v realnem Hilbertovem prostoru. Le–to nam dovoljuje geometrijski prikaz poteka algoritma.

Za lažjo predstavo, kako operatorja O in G transformirata stanje superpozicije $|\psi\rangle$, pogledamo njuno geometrijsko vizualizacijo. Po prvem koraku se stanje nahaja v enotni superpoziciji vseh možnih baznih stanj, ki ga lahko zapišemo kot vsoto

$$|\psi\rangle = \frac{1}{\sqrt{N}}(\sum_{x \neq x^*} |x\rangle + |x^*\rangle). \tag{5.16}$$

Oglejmo si podprostor (ravnino), ki ga napenjata $|x^*\rangle$ in $|\psi\rangle$. Ta dva vektorja predstavljata bazo te ravine, ampak nista ortogonalna, saj je njun skalarni produkt enak: $\langle x^*|\psi\rangle = \frac{1}{\sqrt{N}}$. Da dobimo ortonormirano bazo ravnine, definiramo vektor, pravokoten na $|\psi\rangle$: $|\psi\rangle -$

$\frac{1}{\sqrt{N}}|x^*\rangle$, ter ga normiramo

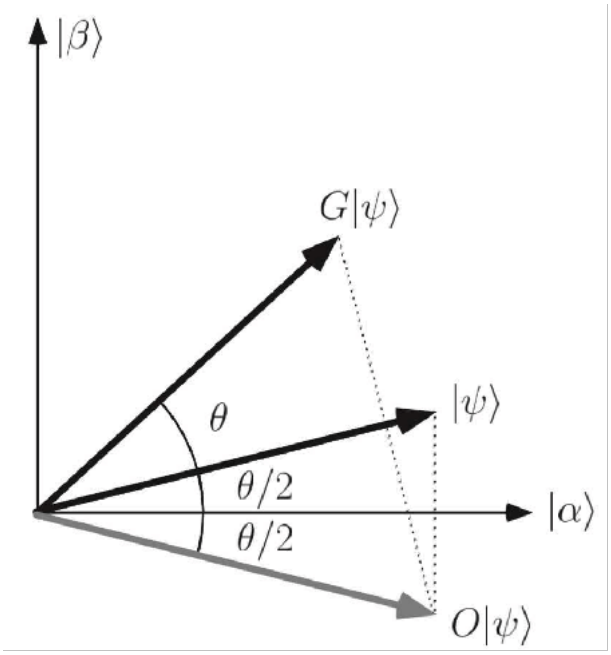
$$|\psi'\rangle = \frac{1}{\sqrt{2^n - 1}} \sum_{x \neq x^*} |x\rangle \,. \tag{5.17}$$

Vektorja $|x^*\rangle$ in $|\psi'\rangle$ tako tvorita ortonormirano bazo opazovane ravnine.

Operatorja O in G predstavljata rotacije vektorjev, kar pomeni, da poljuben vektor na tej ravnini preslikata v drug vektor na isti ravnini

$$a\,|x^*\rangle + b\,|\psi'\rangle \xrightarrow{DO} c\,|x^*\rangle + d\,|\psi'\rangle \,. \tag{5.18}$$

Operator O le negira amplitudo pred baznim vektorjem $|x^*\rangle$, zato začetno stanje $|\psi\rangle$ le prezrcali preko vektorja $|\psi'\rangle$ v opazovani ravnini. Nato operator G prezrcali dobljeni vektor $O\,|\psi\rangle$ preko vektorja $|\psi\rangle$, kar prikazuje naslednja slika. Vektorja $|\alpha\rangle$ in $|\beta\rangle$ predstavljata bazna vektorja $|\psi'\rangle$ in $|x^*\rangle$.



Slika 5.2: Geometrijski prikaz poteka Groverjevega algoritma.

Po večih ponovitvah operatorjev O in G se začetni vektor vedno bolj približuje željenemu $|x^*\rangle$. Zanima nas, kolikokrat je potrebno ponoviti delovanje opratorjev O in G, da bo verjetnost meritve vektorja $|x^*\rangle$ dovolj velika. Poglejmo, kako se spreminja kot med vektorjem $|\psi'\rangle$ in vektorjem $|\psi^r\rangle$:
$\Phi^{(0)} = \Theta$
$\Phi^{(1)} = \Theta + 2\Theta$

$\Phi^{(2)} = \Theta + 4\Theta$
$\vdots$
$\Phi^{(r)} = (2r+1)\Theta$

Opomba 5.2

1. *Na sliki (5.2) je kot* Θ *enak* $\frac{\theta}{2}$.
2. *Vektor* $|\psi^r\rangle$ *je vektor, dobljen iz začetnega vektorja* $|\psi\rangle = \left|\psi^0\right\rangle$ *po* r *ponovitvah delovanja operatorjev* O *in* G.

Opazovan vektor na ravnini, ki jo napenjata vektorja $|\psi'\rangle$ in $|x^*\rangle$ je po r korakih oblike

$$\left|\psi^{(r)}\right\rangle = \cos\Phi^{(r)}\left|\psi'\right\rangle + \sin\Phi^{(r)}\left|x^*\right\rangle. \tag{5.19}$$

Ker velja

$$P(|x^*\rangle) = \sin^2\Phi^{(r)} \tag{5.20}$$

in

$$\max(\sin^2\Phi^{(r)}) \Longleftrightarrow \max(\sin\Phi^{(r)}), \tag{5.21}$$

nas zanima, po koliko korakih, oziroma za kateri r, bo $\Phi^{(r)} = \frac{\pi}{2}$, da bo $P(|x^*\rangle) = 1$.

$$\Phi^{(r)} = (2r+1)\Theta = \frac{\pi}{2} \tag{5.22}$$

Sedaj poiščemo oceno za kot Θ s pomočjo operatorja projekcije

$$\left(\left|\psi'\right\rangle\left\langle\psi'\right|\right)|\psi\rangle = \left\langle\psi'\middle|\psi\right\rangle\left|\psi'\right\rangle. \tag{5.23}$$

Ker $\langle\psi'|\psi\rangle$ predstavlja dolžino projekcije vektorja $|\psi\rangle$ na $|\psi'\rangle$ velja

$$\cos\Theta = \left\langle\psi'\middle|\psi\right\rangle. \tag{5.24}$$

Po izračunu skalarnega produkta sledi

$$\cos\Theta = \sqrt{\frac{2^n - 1}{2^n}} \tag{5.25}$$

in

$$\sin\Theta = \sqrt{\frac{1}{2^n}} = \sqrt{\frac{1}{N}}. \tag{5.26}$$

$\Theta = \sin^{-1}\sqrt{\frac{1}{N}}$, ki ga za velike n-je lahko ocenimo kot

$$\sin\left(\sqrt{\frac{1}{N}}\right) \approx \sin^{-1}(\sqrt{\frac{1}{N}}) \approx \sqrt{\frac{1}{N}}. \tag{5.27}$$

Sledi

$$\Phi^{(r)} \approx (2r+1)\sqrt{\frac{1}{N}} = \frac{\pi}{2}, \tag{5.28}$$

$$r = \frac{\frac{\pi}{2}\sqrt{N-1}}{2} \approx \frac{\pi}{4}\sqrt{N} \approx \sqrt{N} = \sqrt{2^n}. \tag{5.29}$$

Iz zgornje ocene sledi, da je potrebno koraka v algoritmu ponoviti približno $\sqrt{2^n}$ krat, kjer je n število kubitov, da bo verjetnost meritve vektorja $\left|\psi^{(r)}\right\rangle$ zelo blizu 1. Lahko se zgodi, da meritev ne bo enaka željeni vrednosti, zato je potrebno algoritem večkrat pognati. **Časovna zahtevnost** algoritma je tako $O(\sqrt{2^n})$. Če je vrednost funkcije f enaka 1 za k različnih $x \in X$, pa lahko Groverjev algoritem preoblikujemo tako, da z verjetnostjo blizu 1 najde pravo rešitev v $O(\sqrt{\frac{2^n}{k}})$ korakih.

Poseben primer Groverjevaga algoritma je, ko imamo le dva kubita. Takrat je

$$\Phi^{(1)} = (2 * 1 + 1)\sin^{-1}(\frac{1}{2}) = \frac{\pi}{2} \tag{5.30}$$

in zato

$$P(\left|\psi^{(1)}\right\rangle = |x^*\rangle) = 1, \tag{5.31}$$

kar pomeni, da že po prvi iteraciji dobimo željeno vrednost z verjetnostjo 1.

Implementacija

Za delovanje algoritma na konkretnem primeru je vsakega izmed korakov potrebno implementirati oziroma zapisati z ustreznimi kvantnimi vrati. Prvi korak algoritma, stanje enotne superpozicije, dobimo z delovanjem že znanih Hadamardovih vrat na posamezni kubit. Oracle funkcije v drugem koraku algoritma ne moremo implementirati v splošnem, saj se od primera do primera razlikuje. Večina algoritmov pri njeni implementaciji uporablja dodatni kubit, ki je z ostalimi povezan s CNOT vrati. Njegovo začetno stanje je $|1\rangle$, na katerega delujemo s Hadamardovimi vrati. Potreben je iz stališča, da obrne amplitudo takrat, ko je stanje n kubitov v željenem stanju $|x^*\rangle$, kar zagotovi oracle funkcija. Dodatni kubit tako ustvari negativni predznak, saj velja $XH\,|1\rangle = -H\,|1\rangle$.

Delovanje operatorja G pa v splošnem lahko poenostavimo in delno implementiramo. Velja

$$G = 2\,|\psi\rangle\,\langle\psi| - \mathbb{I} = H(2\,|0\rangle\,\langle 0| - \mathbb{I})H, \tag{5.32}$$

kjer H predstavlja Hadamardova vrata. Tak zapis poenostavi implementacijo operatorja, saj je predstava zrcaljenja preko vektorja $|0\rangle$ bolj intuitivna. Pogljemo, zakaj velja zgornja enakost

$$G = H(2\,|0\rangle\,\langle 0| - \mathbb{I})H = 2H\,|0\rangle\,\langle 0|\,H - H\mathbb{I}H. \tag{5.33}$$

Ker je operator H sam sebi inverz, je $H\mathbb{I}H = \mathbb{I}$. Velja tudi, da delovanje Hadamardovih vrat na vektor $|0\rangle$ vrne stanje enotne superpozicije: $H\,|0\rangle = |\psi\rangle$. Zato sledi

$$G = 2\,|\psi\rangle\,\langle 0|\,H - \mathbb{I}. \tag{5.34}$$

Sedaj preverimo delovanje z $\langle 0|\,H$ na splošnem vektorju $|v\rangle$

$$\langle 0|\,H\,|v\rangle = \langle 0|Hv\rangle = \left\langle H^\dagger 0 \middle| v \right\rangle = \langle H0|v\rangle = \langle\psi|v\rangle\,. \tag{5.35}$$

Sledi

$$\langle 0|\,H = \langle\psi| \tag{5.36}$$

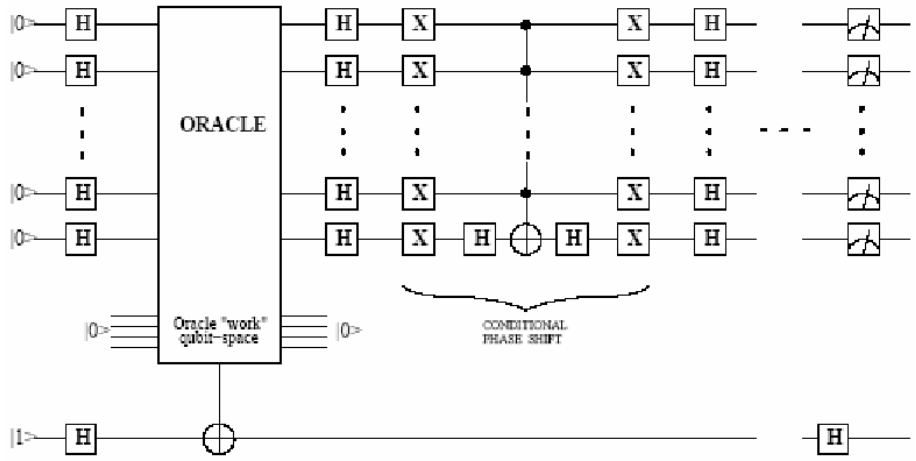
in

$$G = 2\left|\psi\right\rangle\left\langle\psi\right| - \mathbb{I} = H(2\left|0\right\rangle\left\langle 0\right| - \mathbb{I})H. \tag{5.37}$$

Tako operator G implementiramo z Hadamardovimi vrati na začetku in koncu, vmes pa uporabimo zrcaljenje preko vektorja $|0\rangle$, ki na vektorje v standardni bazi deluje na naslednji način

$$(2\left|0\right\rangle\left\langle 0\right| - \mathbb{I})\left|x\right\rangle = \begin{cases} -\left|x\right\rangle & x \neq 0 \\ \left|x\right\rangle & x = 0. \end{cases} \tag{5.38}$$

Zrcaljenje preko vektorja $|0\rangle$ torej obrne amplitudo vseh baznih stanj, razen $|0\rangle$. Implementacijo operatorja G in celotnega algoritma v modelu kvantnega vezja z n kubiti in dodatnim kubitom, potrebnim pri izračunu oracle funkcije predstavlja slika (5.3). Oracle funkcija zahteva dodatne kubite za lažjo implementacijo [4], [15].



Slika 5.3: Implementacija Groverjevega algoritma na modelu kvantnega vezja.

5.2.2 Uporaba

Algoritem je zaradi oracle funkcije, ki je specifična za posamezni primer, zelo splošen in se lahko uporabi na večjem številu problemov. V splošnem algoritem uporabimo za pohitritev NP-polnih problemov in iskanje po nestrukturirani bazi podatkov.

Pohitritev NP-polnih problemov

Kvantni iskalni algoritmi so lahko uporabni za pohitritev NP-polnih problemov. Eden izmed takih je preverjanje, ali dani graf vsebuje Hamiltonski cikel, ki sestoji iz dveh korakov:

1. Generiraj vrstni reda vozlišč grafa, kjer so dovoljena ponavljanja.

2. Za vsak vrstni red preveri, ali je Hamiltonski cikel. Če ne, ponovi prvi korak.

Ker je $n^n = 2^{n \log_2 n}$ različnih možnih vrstnih redov vozlišč, mora v najslabšem primeru algoritem preveriti toliko različnih kombinacij vozlišč. Časovna zahtevnost klasičnega algoritma je $O(p(n)2^{n \log_2 n})$, kjer je $p(n)$ polinom, potreben za preverbo Hamiltonovega cikla za posamezno množico vozlišč. Kvantni iskalni algoritem lahko pohitri to iskanje z definiranjem oracle funkcije, ki obrne amplitudo tistega vektorja, katerega komponente so množice vozlišč Hamiltonskega cikla

$$O\,|v_1, \ldots, v_n\rangle = \begin{cases} |v_1, \ldots, v_n\rangle & \{v_1, \ldots, v_n\} \text{ je Hamiltonski cikel} \\ -\,|v_1, \ldots, v_n\rangle & \{v_1, \ldots, v_n\} \text{ ni Hamiltonski cikel.} \end{cases} \tag{5.39}$$

Preverbo, ali je posamezna množica vozlišč Hamiltonski cikel opravimo klasično. Če predhodno preverimo, ali v danem grafu rešitev obstaja, lahko kvantni iskalni algoritem najde rešitev v času $O(p(n)2^{\frac{n \log_2 n}{2}})$.

Iskanje po nestrukturirani bazi

Kot smo že omenili, je pri klasičnem iskanju elementa po nestrukturirani bazi $2^n = N$ elementov, v najslabšem primeru potrebnih N preverjanj. Kvantni algoritem pohitri iskanje s pomočjo oracle funkcije, kar lahko opišemo na primeru iskanja kriptografskih ključev. Glavna ideja temelji na iskanju po prostoru vseh možnih dešifrirnih ključev $X = \{x_1, \ldots, x_N\}$. Vsak ključ je zaradi varnosti najprej šifriran s funkcijo g, ki je težko obrnljiva, tako da je po klasični poti praktično nemogoče ugotoviti inverz funkcije. Naj bo $y = g(x')$ dan šifriran ključ, katerega želimo dešifrirati. Želimo torej najti x', zato lahko problem razložimo kot iskanje inverza funkcije g. Definiramo funkcijo

$$f(x) = \begin{cases} 1 & g(x) = y \\ 0 & g(x) \neq y. \end{cases} \tag{5.40}$$

Nadalje le sledimo že opisanemu postopku Groverjevega algoritma, ki uspe najti pravi ključ v času $O(\sqrt{2^n})$. Čeprav je za velika števila n algoritem bistveno hitrejši, ne predstavlja velike nevarnosti razbitju določenih (simetričnih) šifrirnih ključev, saj pri podvojitvi dolžine ključev časovna zahtevnost iskanja ostane enaka kot pri klasičnem iskanju [2], [7], [12].

Zaključek

V magistrski nalogi smo se osredotočili na predstavitev teoretičnih podlag kvantnega računalništva. S predstavitvijo matematičnih konceptov ter osnovnih načel kvantne mehanike smo se približali razumevanju delovanja in uporabe kvantnih algoritmov.

Bistvena matematična področja, ki smo jih zajeli tekom magistrske naloge so kompleksna števila, vektorski prostori in linearne transformacije. Dotaknili smo se tudi osnovnih načel kvantne mehanike za lažje razumevanje konceptov, ki se pojavljajo na področju kvantnega računanja. V osrednjih poglavjih magistrske naloge smo predstavili kvantno računalništvo in opis Groverjevega algoritma. Podrobneje smo opisali osnovni model za izdelavo kvantnih algoritmov na podlagi kvantnega vezja, ki zajema pripravo kvantnih stanj, njihov razvoj s pomočjo kvantnih vrat oziroma linearnih transformacij in končno meritev stanj kubitov. Sledil je opis delovanja obstoječih algoritmov in podrobna razčlenitev delovanja Groverjevega algoritma.

Razčlenjena predstavitev kvantnega računanja pripomore k razumevanju hitro razvijajočega se področja kvantnega računalništva in lahko služi kot uvod v še neraziskana področja, ki jih prinaša razvoj kvantnih računalnikov.

Literatura

[1] I. Banič, T. Marčec, *Analiza 1 (zapiski iz predavanj)*, FNM UM, 2014.

[2] Bomb, *Grover's Algorithm + Quantum Zeno Effect + Vaidman* (online). (07. 2018). Dostopno na naslovu: `https://people.eecs.berkeley.edu/~vazirani/f04quantum/notes/lec10/lec11.pdf`.

[3] B. Brešar, T. Marčec, *Funkcionalna analiza (zapiski iz predavanj)*, FNM UM, 2018.

[4] Daytonellwanger, T. Marcec, *Introduction to Quantum Computing (zapiski iz video predavanj)*. Dostopno na naslovu: `https://www.youtube.com/watch?v=nZXq28oSSjM&list=PLIxlJjN2V90w3KBWpELOE7jNQMICxoRwc&index=19`

[5] B. Eagle, T. Marcec, *CosmoLearning Course (zapiski iz video predavanj)*. Dostopno na naslovu: `https://cosmolearning.org/video-lectures/schrdingers-equation-simple-derivation/`.

[6] D. Eremita, T. Marčec, *Linearna algebra (zapiski iz predavanj)*, FNM UM, 2014.

[7] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath, C. Monroe, *Complete 3-Qubit Grover search on a programmable quantum computer*, Nature Communications volume 8, Article number: 1918 (2017).

[8] M. Gregorič, *Kvantni računalniki (seminar)* (online). (06. 2018). Dostopno na naslovu: `http://mafija.fmf.uni-lj.si/seminar/files/2007_2008/Seminar_KvRacunalniki.pdf`.

[9] A. Holobar, *Kvantno računalništvo in kriptografija*, Fakulteta za elektrotehniko, računalništvo in informatiko, Inštitut za računalništvo, Maribor, 2016.

[10] R. Kladnik, *Pot k maturi iz fizike, fizika za srednješolce*, DZS, Ljubljana, 2011.

[11] T. Košir, *Sebiadjungirane, ortogonalne in normalne preslikave*(online). (04. 2018).Dostopno na naslovu: `https://www.fmf.uni-lj.si/~kosir/poucevanje/skripta/sebiadj.pdf`.

[12] C. Lavor, L.R.U. Manssur, R. Portugal, *Grover's Algorithm: Quantum Database Search* (online). (06. 2018). Dostopno na naslovu: `https://arxiv.org/pdf/quant-ph/0301079.pdf`.

[13] M. Loceff, *A Course in Quantum Computing* (online). (05. 2018). Dostopno na naslovu: `http://lapastillaroja.net/wp-content/uploads/2016/09/Intro_to_QC_Vol_1_Loceff.pdf`.

[14] I. Mele, M. Kralj, N. Železnik, *Oh to sevanje*, Presek Letnik 30 (2002/2003), str. 261–266.

[15] M. A. Nielsen *Quantum computing for the determined* (online). (05 2018). Dostopno na naslovu: `http://michaelnielsen.org/blog/quantum-computing-for-the-determined/`.

[16] D. Pagon, T. Marčec, *Algebra (zapiski iz predavanj)*, FNM UM, 2015.

[17] A. Steane, *Quantum computing*, University of Oxford, 1997.

[18] *Quantum computing explained* (online). (05. 2018). Dostopno na naslovu: `https://www.clerro.com/guide/580/quantum-computing-explained`.

[19] J. Valenza, *Linear Algebra: An Introduction to Abstract Mathematics*, Springer-Verlag, New York, 1993.

[20] J. Watrous, *Quantum computation lecture notes*, University of Waterloo, 2006.

[21] N. Zettili, *Quantum Mechanics Concepts and Applications* (online). (05. 2018). Dostopno na naslovu: `http://jsu.edu/depart/pes/physics/nzettili/front_toc_bk.pdf`.

[22] B. Ömer, *Structured Quantum Programming* (online). (07. 2018). Dostopno na naslovu: `http://tph.tuwien.ac.at/~oemer/doc/structquprog.pdf`.