KVANTNO RAČUNALNIŠTVO

ENEJ CAF

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Predstavljen je princip delovanja kvantnih računalnikov in pet obstoječih tipov različnih kubitov. Uvodoma je opisan zgodovinski razvoj področja kvantnega računalništva, ki mu sledita opisa kubitov in kvantne prepletenosti. V nadaljevanju so pod drobnogled vzeti osnovni tipi kvantnih vrat in univerzalni nabori le-teh. Sledi pregled DiVincenzovega kriterija, dekoherence in kvantnega odpravljanja napak. Nato so predstavljeni še različni, za izdelavo kvantnih bitov, perspektivni fizikalni sistemi: jedrska magnetna resonanca, ujeti ioni, SQUID, kvantne pike in linearni optični računalnik.

QUANTUM COMPUTING

The article introduces theoretical principles in quantum computing and gives insight into five existing realisations of qubits. In the introduction historical background of quantum computing is presented, followed by the description of qubits, superposition and entanglement. Furthermore, elementary quantum gates and universal sets of gates are discussed. In addition, DiVincenzo criteria, decoherence and quantum error correction are presented. In the end, five types of promising physical systems used in existing qubits are pointed out: nuclear magnetic resonance, trapped ions, superconducting quantum interference device, quantum dots and linear optical quantum computer.

1. Uvod

Kvantna mehanika, kot jo poznamo danes, se je pričela razvijati v dvajsetih letih prejšnjega stoletja, sčasoma pa se je razvilo tudi več različnih razlag. Najstarejša in najbolj razširjena interpretacija, ki se je bom držal tudi znotraj članka, je kopenhagenska interpretacija, ki se je oblikovala okrog let 1925 in 1927, zlasti pod vplivom danskega fizika Nielsa Bohra in njegovega nemškega kolega Wernerja Heisenberga. Bistvo te interpretacije je povzeto v petih postulatih:

1. Kvantni sistem je opisan z vektorjem $|\psi\rangle$ v Hilbertovem prostoru.
2. Merljivi fizikalni količini oz. opazljivki ustreza hermitski operator $\hat{A} = \hat{A}^\dagger$.
3. Za sistem v stanju $|\psi\rangle$ izrazimo pričakovano vrednost kot $\langle\psi|\,\hat{A}\,|\psi\rangle$.
4. Časovni razvoj stanja je podan s Schrödingerjevo enačbo $i\hbar\frac{\mathrm{d}|\psi\rangle}{\mathrm{d}t} = \hat{H}\,|\psi\rangle$, kjer je $\hat{H}$ Hamiltonov operator.
5. Pri meritvi opazljivke A je rezultat meritve ena od lastnih vrednosti a, $\hat{A}\,|\psi\rangle = a\,|\psi\rangle$, pri čemer je verjetnost za tak izid $p_a = |c_a|^2$, kjer je c_a verjetnostna amplituda za razvoj stanja po lastnih vektorjih operatorja A: $|\psi\rangle = \sum_a c_a\,|a\rangle = \sum_a \langle a|\psi\rangle\,|a\rangle$.

Na nadaljnji razvoj so nato ključno vplivali predvsem udeleženci Solvayeve konference, kjer velja izpostaviti Von Neumanna kot matematika, ki je spisal prvo celovito delo o kvantni mehaniki [1] in s številnimi dokazi tlakoval pot Diracu in njegovemu formalizmu, ki je prinesel velike poenostavitve.

Z razvojem kvantne mehanike so se v letu 1970 izoblikovali tudi prvi zametki ideje o kvantnem računalništvu, ko sta Stephen Wiesner in Charlie Bennett v svojih razpravah prvič uporabila pojem kvantne informacijske teorije na podlagi kvantne prepletenosti [2]. V letu 1980 je Richard Feynman opazil, da je kvantni problem večih teles težko rešljiv za klasične računalnike zaradi eksponentno naraščajočega Hilbertovega prostora kvantnih stanj. Kvantni računalnik se je zdel naravna rešitev, zato je v letu 1981 na konferenci, ki sta jo organizirala IBM in MIT, znanstvenike s področja

računalništva izzval naj izdelajo računalnik, ki bo temeljil na kvantni fiziki v smislu nadzorovane obdelave z atomi ali posameznimi molekulami, kar bi omogočilo bistven preskok v velikostem redu računalniških komponent in prispevalo k reševanju določenih problemov. Kasneje se je večje zanimanje za to področje pojavilo v letu 1994, ko je Peter Shor pokazal, da je razcep na praštevila možno izvesti s polinomsko časovno zahtevnostjo na kvantnih računalnikih, kar je za klasične računalnike problem z subeksponentno časovno zahtevnostjo[1]. Področje je nato postalo zelo perspektivno za različne veje znanosti in je konstantno razvijajoče, zato smo priča veliko novim dosežkom praktično vsako leto.

Z namenom, da bi predstavil to hitro razvijajoče področje znanosti, bom v nadaljevanju najprej opisal teoretične osnove delovanja kvantnih računalnikov in njihove prednosti. Nato bom izpostavil nekaj načinov, s katerimi so znanstveniki do sedaj uspeli realizirati tovrstne naprave in izzive, s katerimi se pri tem srečujejo.

2. Delovanje kvantnega računalnika

Za razvoj kvantnega računalništva je bila ključna zamisel, da lahko kot računalniški bit uporabimo kvantni dvonivojski sistem, na primer jedrski spin ali polarizacijo posameznega fotona. Velika sprememba, ki je prišla z idejo, je veliko nižji velikostni red elementov, kamor lahko shranimo informacijo, hkrati pa nam je jasno, da sistema ne bomo več obravnavali klasično, temveč v kvantno mehanskem formalizmu operatorjev in vektorjev stanj. Kvantni biti imajo torej lastnosti, kot sta superpozicija in prepletenost, ki ju lahko s pridom uporabimo. Kvantne lastnosti takšnih sistemov namreč dopuščajo direktne izračune problemov kvantne narave, kjer so prisotni enaki omenjeni pojavi, česar klasični računalniki ne zmorejo.

Za operacije na bitih torej uvedemo opazljivkam prirejene hermitske operatorje, ki bodo nadomestili klasična vrata. V praksi takšne operatorje učinkovito ponazorimo z matrikami. Pri tem se je potrebno zavedati, da operatorjem ustreza določena eksperimentalna postavitev, s katero tudi merimo stanje našega sistema v skladu s von Neumannovo meritvijo in petim postulatom kvantne mehanike, kjer si lahko zamislimo postavitev pri znanem Stern-Gerlachovem eksperimentu za meritev S_z – operatorja projekcije spinske vrtilne količine na os z. Pri tem vemo, da se rezultat poskusa do trenutka meritve unitarno razvija s Hamiltonovim operatorjem kot generatorjem časovnega razvoja. Ko meritev zaključimo, kvantni sistem ni več izoliran od klasičnega. Dobimo dodatno ireverzibilno sklopitev z okolico oziroma klasičnim makroskopskim sistemom z velikim številom delcev. Opisanemu pojavu pravimo sesedanje valovne funkcije.

Kvantna meritev je torej precej drugačna od klasične. V eksperimentu, kjer merimo splošno fizikalno opazljivko A, ki je povezana s hermitksim operatorjem $\hat{A} = \hat{A}^\dagger$, je posledica meritve projekcija na enega od lastnih vekotrjev $\hat{A}$. Rezultati meritev so torej lastne vrednosti operatorja $\hat{A}$, ki jih označimo z λ_n. V kolikor poskus ponavljamo, se bo povprečna vrednost naših izmerkov približevala pričakovani vrednosti:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \lambda_n = \langle \hat{A} \rangle \,.$$

Ko nam uspe postaviti ustrezno eksperimentalno okolje, kjer lahko ustvarimo določena stanja, nanje delujemo v obliki operatorjev in izvedemo meritve, pa je velik izziv programabilnost kvantnih računalnikov v obliki programskih jezikov, kot to počnemo na klasičnih računalnikih. Na tem področju

[1] Poskus so uspeli izvesti 10 let kasneje na IBM-ovem računalniku s kubiti iz spinskih stanj jeder (podobno kot pri MRI).

obstaja že kar nekaj jezikov, kot so QPL, QML in LIQ$Ui|>$, in programskih paketov na primer v obliki knjižnic za Python, ki omogočajo upravljanje vezij na prototipih kvantnih računalnikov preko spletnih storitev in simulacije na lastnem klasičnem računalniku. Takšni paketi so na primer Qiskit, Ocean, ProjectQ in Forest.

Sedaj, ko smo spoznali osnovno idejo delovanja kvantnega računalnika, si poglejmo stvari še nekoliko bolj podrobno in formalno.

2.1 Klasični bit

Bit je okrajšava za klasični bit, ki ga udejanimo s klasičnim dvonivojskim sistemom. Biti lahko zavzamejo zgolj Boolovi vrednosti 0 in 1, zato jih predstavimo z dvema ortonormiranima stanjema: $|0\rangle$ in $|1\rangle$ oz. v 2-D vektorskem prostoru: $\begin{bmatrix}1\\0\end{bmatrix}$ in $\begin{bmatrix}0\\1\end{bmatrix}$. Za netrivialne izračune uporabimo več bitov, ki jih sestavljamo s tenzorskim produktom. Za dva bita na primer dobimo bazo štirih ortogonalnih stanj:

$$|0\rangle \otimes |0\rangle = |00\rangle\,,\ |0\rangle \otimes |1\rangle = |01\rangle\,,\ |1\rangle \otimes |0\rangle = |10\rangle\ \text{ in }\ |1\rangle \otimes |1\rangle = |11\rangle\,, \tag{1}$$

pri čemer je sistem vedno točno v enem od zapisanih stanj. V splošnem lahko na tak način z n biti predstavimo eno izmed 2^n različnih konfiguracij, ki jih lahko dobimo s tenzorskimi produkti danih stanj. Za bolj praktično predstavo lahko stanjem pripišemo števila. Za naš primer na primer: $|00\rangle \to 1$, $|01\rangle \to 2$, $|10\rangle \to 3$ in $|11\rangle \to 4$, s čimer lahko opišemo štiri različna števila, v klasičnem računalniku z dvema bitoma pa lahko shranimo potem le eno, na primer 3.

2.2 Kubit

Kubit je poslovenjeni izraz za angleško besedo *qubit*, ki pomeni kvantni bit in je v praksi lahko na primer nuklearni spin velikosti $\frac{1}{2}$ ali nepolariziran foton. Za razliko od bita nismo omejeni zgolj na dve klasični stanji $|0\rangle$ in $|1\rangle$, ampak kubit $|\psi_1\rangle$ predstavimo kot superpozicijo stanj: $c_0\,|0\rangle + c_1\,|1\rangle$ z amplitudama c_0 in c_1, kjer velja pogoj normalizacije $|c_0|^2 + |c_1|^2 = 1$. Pomembna razlika pri tem je, da so kubiti predstavljeni s kvantnimi stanji, ki zavzemajo zvezen nabor vrednosti, ki jih lahko ponazorimo s točkami na Blochovi sferi.

Kot pri bitih, si tudi za kubite želimo posplošitev na n kubitov, kar imenujemo kvantni register. Začnimo spet na primeru dveh kubitov. Ker imamo kvantni dvonivojski sistem, bo baza prostora enaka kot za primer bitov v enačbi 1. Po prejšnji definiciji tvorimo stanje dveh kubitov kot superpozicijo vseh stanj bitov:

$$|\psi\rangle = a_{00}\,|00\rangle + a_{01}\,|01\rangle + a_{10}\,|10\rangle + a_{11}\,|11\rangle\ \text{ in normalizacijo }\ \langle\psi|\psi\rangle = 1. \tag{2}$$

Kvantni register torej zapišemo bistveno drugače kot klasičnega. Na podlagi izkušenj s klasičnimi biti bi namreč pričakovali, da sistem dveh bitov tvorimo s tenzorskim produktom med njima. Za dva poljubna kubita $|\psi_1\rangle$ in $|\psi_2\rangle$ bi na tak način dobili:

$$|\psi_1\rangle \otimes |\psi_2\rangle = (c_0\,|0\rangle + c_1\,|1\rangle) \otimes (d_0\,|0\rangle + d_1\,|1\rangle) = c_0d_0\,|00\rangle + c_0d_1\,|01\rangle + c_1d_0\,|10\rangle + c_1d_1\,|11\rangle\,.$$

Ta relacija je poseben primer zveze za dva kubita v enačbi (2), kjer velja $a_{00}\,a_{11} = a_{10}\,a_{01}$, kar vidimo z enačenjem vektorskih komponent v obeh zapisih. Splošni kvantni register lahko torej predstavlja tudi neproduktno oz. prepleteno stanje[2], kar rezultira v posebnih lastnostih, ki jih bom opisal v

[2]Izvorni Schrödingerjev izraz je *verschränkt* oz. *entangled* v angleški literaturi.

poglavju (2.3) .

V splošnem potem n kubitov predstavlja normalizirano superpozicijo vseh 2^n bitnih stanj. Pri tem pa moramo biti zelo pozorni, saj po izreku Holeva [3, 4] iz takšnega kvantnega sistema pridobimo informacijo velikosti največ n klasičnih bitov, kar ustreza največjemu številu med seboj ortogonalnih stanj.

Večja razlika med biti in kubiti je tudi v operacijah, ki jih izvajamo na obeh sistemih. Reverzibilni operaciji za bite sta tako identiteta in sprememba med vrednostima bita $|0\rangle \leftrightarrow |1\rangle$, kar nam omogoča prehod med vsemi možnimi permutacijami. Pomembna operacija je tudi meritev, s katero določimo vrednost bita, ki ostane nespremenjena po meritvi. Na drugi strani so reverzibilne operacije na kubitih unitarni operatorji. Meritev pa je ireverzibilna operacija na kvantnem registru, s katero z določeno verjetnostjo izmerimo eno od možnih stanj. V izmerjeno stanje se po meritvi sesede celoten kvantni register.

2.3 Kvantno prepletena stanja

Prepletena stanja so po definiciji takšna, da jih ne moremo razčleniti kot produkt stanj iz ločenih Hilbertovih prostorov $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_N\rangle \in H_1 \otimes H_2 \cdots \otimes H_N$, ampak predstavljajo nerazdružljivo celoto, torej posameznega delca ne moremo opisati do potankosti brez drugih. Takšne delce lahko razmaknemo poljubno daleč in bodo še vedno ostali prepleteni. Sisteme s takšnimi stanji je torej najpreprosteje simulirati na kvantnih računalnikih, veliko razvoja pa se v zadnjem času odvija na področju kvantne komunikacije z izkoriščanjem prepletenosti.

Posvetimo se sedaj zgledu v dvodimenzionalnemu Hilbertovem prostoru s stanji oblike, ki je zapisana v enačbi (2). Pod drobnogled vzemimo na primer prepleteno stanje dveh kubitov v sistemih 1 in 2: $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. Če posamezna kubita razmaknemo, še zmeraj ostaneta prepletena, zanima pa nas, kaj se zgodi, če ju pomerimo. Če pride najprej do meritve v prvem sistemu, je rezultat katerokoli od stanj $|0\rangle$ in $|1\rangle$ z verjetnostjo 1/2. Če nato pride do meritve v drugem sistemu, se izkaže, da bo rezultat popolnoma koreliran, čeprav se to opazovalcu v drugem sistemu ne bi posvetilo, razen če bi komuniciral z opazovalcem v prvem sistemu. Torej, če smo v prvem sistemu izmerili stanje $|0\rangle$, bo v drugem rezultat meritve zagotovo $|1\rangle$, če pa bi v prvem sistemu izmerili $|1\rangle$, bomo v drugem dobili $|0\rangle$. Opazimo, da izid meritve v prvem sistemu v trenutku vpliva na meritev v drugem na poljubni razdalji.

Obnašanje prepletenih delcev, ki dajeta vtis, kot da sta se o rezultatu meritve dogovorila vnaprej, je zmotilo tudi Einsteina. V letu 1935 je v članku s Podolskym in Rosenom [5] predlagal uvedbo skritih spremenljivk, ki bi določale vnaprejšnji dogovor o rezultatu meritve in pod vprašaj postavil pravilnost kvantne mehanike. Problem je ostal na filozofski ravni miselnih eksperimentov do leta 1965, ko je Bell predlagal meritev korelacij med posameznimi stanji in zapisal slavno Bellovo neenakost [6]. Če bi bila kvantna mehanika pravilna, bi korelacije kršile neenakost, kar se je tudi izkazalo v poznejših eksperimentih. Primer takšnih stanj so prepletena Bellova stanja, ki jih bomo srečali tudi v nadaljevanju:

$$|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$$
$$|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)\,. \tag{3}$$

Zanimivi zgledi uporabe prepletenih stanj se pojavijo pri načinih komunikacije med dvema sistemoma z ločenima Hilbertovima prostoroma H_1 ter H_2, ki sta povezana s kvantnim kanalom tako, da med sabo lahko izmenjujeta kubite na primer v obliki fotonov. Zamislimo si, da lahko v prvem sistemu pripravimo stanje $|0\rangle$ ali stanje $|1\rangle$, ki ga pošljemo v drugi sistem, kjer z meritvijo ugotovimo, katero od stanj smo pripravili v prvem sistemu. S tem smo s poslanim kubitom, prenesli informacijo enega bita. V resnici je to tudi najbolje, kar lahko storimo, kar je posledica izreka Holeva [3].

Zdaj pa si zamislimo nekoliko drugačen primer. V sistemih ena in dva imamo kubita, ki tvorita prepleteno kvantno stanje — na primer $|\phi^+\rangle$, ki je eno od Bellovih stanj iz enačb (3). To lahko dosežemo s pripravo dveh prepletenih kubitov, ki ju dostavimo v prvi in drugi sistem. Sedaj si lahko zamislimo protokol, ki ga lahko izvedemo tudi po daljšem časovnem obdobju in ga poznamo v obeh sistemih:

Protokol:

- V prvem in drugem sistemu imamo prepletena kubita, ki tvorita stanje $|\phi^+\rangle$.
- V prvem sistemu, lahko pred pošiljanjem izvedemo eno od štirih operacij:
  1. I (ne naredimo ničesar).
  2. σ_x (rotacija za π okrog osi x).
  3. σ_y (rotacija za π okrog osi y).
  4. σ_z (rotacija za π okrog osi z).

  Operacije v prvem sistemu transformirajo začetno stanje prepletenih kubitov v štiri stanja Bellove baze (3):

  1. $|\phi^+\rangle \xrightarrow{I} |\phi^+\rangle$.
  2. $|\phi^+\rangle \xrightarrow{\sigma_x} |\psi^+\rangle$.
  3. $|\phi^+\rangle \xrightarrow{\sigma_y} |\psi^-\rangle$.
  4. $|\phi^+\rangle \xrightarrow{\sigma_z} |\phi^-\rangle$.
- Kubit pošljemo iz prvega sistema v drugega.
- V drugem sistemu izvedemo meritev stanja kubitov tako, da lahko razločimo med stanji Bellove baze.

V drugem sistemu z meritvijo torej lahko ugotovimo, katera od štirih operacij je bila storjena na začetnem stanju. Če potegnemo analgojo s prejšnjimi primeri, lahko vsaki od operacij priredimo stanje v bazi $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ oz. števila od 1 do 4, torej lahko z enim poslanim kubitom posredujemo dva klasična [7]. Poleg tega je tak način pošiljanja informacije varen, saj v primeru prestreženega kubita v kvantnem kanalu, iz njega ne bi dobili nobene informacije, saj ima poslani kubit gostotno matriko $\rho = \frac{1}{2}\,\mathrm{I}$. Celotna informacija je torej skrita v korelacijah kubitov v prvem in drugem sistemu, zato bi za prestrezanje informacij potrebovali oba kubita. Takšnemu načinu komuniciranja pravimo gosto kodiranje (*dense coding*). Seveda pa pri tem ne gre za kršenje izreka Holeva, saj je bilo v resnici na začetku potrebno razposlati oba kubita. Tako si lahko mislimo, da smo v prvem sistemu najprej ustvarili stanje $|\phi^+\rangle$, poslali kubit v drugi sistem in nato izvedli zapisani protokol. Ključna pridobitev pri tem je, da lahko prvi korak razdelitve kubitov v oba sistema izvedemo dolgo preden želimo poslati sporočilo.

Za področje računalništva je zanimiv tudi pojav kvantne teleportacije, pri kateri lahko s klasično informacijo prenašamo kvantno [8].

2.4 Kvantna vrata

Sedaj ko smo spoznali nekaj osnovnih lastnosti kubitov in temeljne razlike, ki jih ločujejo od bitov, se lahko vprašamo, kako na njih izvajamo računske operacije?

Kot je do sedaj že jasno v kvantnem sistemu ne operiramo s klasičnimi vrati na primer OR, AND, NOR, NAND, XOR in XNOR, ampak za kvantno računanje na stanjih sistema izvedemo različne unitarne transformacije[3], ki jim pravimo kvantna vrata. Tvoriti želimo takšna vrata, da lahko iz dane linearne kombinacije stanj $|0\rangle$ in $|1\rangle$ preidemo v poljubno novo kombinacijo.

2.4.1 Vrata za posamezni kubit

Zaenkrat vemo, da lahko v bazi stanj $\{|0\rangle, |1\rangle\}$ operatorje zapišemo v obliki matrike z elementi sestavljenimi iz tenzorskih produktov posameznih stanj v Diracovem zapisu:

$$A = \begin{bmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{bmatrix} = a_{0,0} |0\rangle \langle 0| + a_{0,1} |0\rangle \langle 1| + a_{1,0} |1\rangle \langle 0| + a_{1,1} |1\rangle \langle 1| . \tag{4}$$

Za začetek obravnave različnih kvantnih vrat pričnimo s standardnimi fizikalnimi operatorji (identiteta in Paulijeve matrike), nato pa postopno tvorimo standardne tipe kvantnih vrat. Izpeljemo relacije med tenzorskimi produkti v zapisu (4) in Paulijevimi matrikami:

$$\begin{gathered} |0\rangle \langle 0| = \tfrac{\mathrm{I}+\sigma_z}{2}, \quad |1\rangle \langle 1| = \tfrac{\mathrm{I}-\sigma_z}{2}, \\ |0\rangle \langle 1| = |0\rangle \langle 0| \, \sigma_x = \tfrac{\mathrm{I}+\sigma_z}{2}\sigma_x = \tfrac{\sigma_x + i\sigma_y}{2} \quad \text{in} \quad |1\rangle \langle 0| = \sigma_x |0\rangle \langle 0| = \sigma_x \tfrac{\mathrm{I}+\sigma_z}{2} = \tfrac{\sigma_x - i\sigma_y}{2}. \end{gathered} \tag{5}$$

Dodati velja, da je naša baza sestavljena iz lastnih vektorjev σ_z: $\sigma_z |0\rangle = 1 |0\rangle$ in $\sigma_z |1\rangle = -1 |1\rangle$. Za izračune se pogosto uporablja tudi baza σ_x $\{|+\rangle, |-\rangle\}$, zelo redko pa zasledimo bazo σ_y. Opremljeni z relacijami (5) lahko posplošeno matriko iz enačbe (4) zapišemo v obliki Paulijeve dekompozicije:

$$A = \frac{a_{0,0} + a_{1,1}}{2} \, \mathrm{I} + \frac{a_{0,1} + a_{1,0}}{2} \, \sigma_x + i \, \frac{a_{0,1} - a_{1,0}}{2} \, \sigma_y + \frac{a_{0,0} - a_{1,1}}{2} \, \sigma_z. \tag{6}$$

Opremljeni z nekaj več formalizma, si lahko sedaj ogledamo operacije na kubitih. Za začetek, si zaželimo, da bi lahko zamenjali stanja kubita na primer iz $|0\rangle$ v $|1\rangle$ in obratno. V ta namen uvedemo Paulijeva vrata.

- Paulijeva vrata
Paulijeva vrata X označujemo s simbolom $-\boxed{\mathrm{X}}-$ ali $-\oplus-$, kar predstavlja delovanje matrike $\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = |0\rangle \langle 1| + |1\rangle \langle 0|$ na vektor stanja. Iz zapisa s tenzorskim produktom je jasno, da vrata zamenjajo amplitudi stanj $|0\rangle$ in $|1\rangle$, torej predstavljajo ekvivalent klasični operaciji NOT.

Nekoliko težje je videti, kaj predstavljata ostala dva operatorja. Paulijeva vrata Y zapišemo s simbolom $-\boxed{\mathrm{Y}}-$ in Paulijeva vrata Z s simbolom $-\boxed{\mathrm{Z}}-$. Oba operatorja predstavljata rotacije za kot π okrog pripisanih osi (y in z) in jim pripadata znani Paulijevi matriki: $\sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = -i |0\rangle \langle 1| + i |1\rangle \langle 0|$ in $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle \langle 0| - |1\rangle \langle 1|$.

Naučili smo se, kako lahko med sabo menjamo stanja, vendar pa opazimo, da z rabo posameznih Paulijevih vrat vedno znova ostanemo na polih Blochove sfere — ne moremo doseči superpozicije

[3] Unitarni operator U: $UU^\dagger = U^\dagger U = \mathrm{I}$

stanj. S tem namenom uvedemo naslednja standardna vrata.

- Hadamardova vrata
V želji po pretvorbi stanj $|0\rangle$ in $|1\rangle$ v superpozicijo obeh, si zamislimo delovanje vrat v obliki:

$$H\,|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ in } H\,|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Takšna vrata zapišemo s simbolom $-\boxed{\text{H}}-$ v kvantnem vezju, najpreprosteje pa jih izračunamo v Diracovem zapisu: $H\,|n\rangle = \frac{1}{\sqrt{2}}(|1-n\rangle + (-1)^n\,|n\rangle)$, kjer je $n \in \{0,1\}$.

Za potrebe predstave si lahko pomagamo tudi z matričnim zapisom:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix} = \frac{1}{\sqrt{2}}\left(\sigma_z + \sigma_x\right). \tag{7}$$

Vrata si lahko predstavljamo kot rotacijo okoli osi $\hat{n}$: $e^{-i\frac{\theta}{2}\hat{n}\cdot\vec{\sigma}} = \cos(\frac{\theta}{2})\mathrm{I} - i\sin(\frac{\theta}{2})\hat{n}\cdot\vec{\sigma}$. Če skalarni produkt razpišemo po komponentah in primerjamo z izrazom (7), vidimo, da gre za rotacijo za kot $\theta = \pi$ okrog osi $\frac{1}{\sqrt{2}}(\hat{e}_x + \hat{e}_z)$ na Blochovi sferi, kjer sta $\hat{e}_x$ in $\hat{e}_z$ enotska vektorja v smeri osi.

Zanimivo pa je izraziti operator tudi kot produkt rotacij okrog y in z osi: $\frac{1}{\sqrt{2}}\left(\sigma_z + \sigma_x\right) = \frac{1}{\sqrt{2}}\,\sigma_z\,(\mathrm{I} + i\sigma_y)$. Uporabimo še eksponentni zapis matrike[4] in zapišemo $\frac{\mathrm{I}+i\sigma_y}{\sqrt{2}} = e^{i\frac{\pi}{4}\sigma_y}$ in analogno še $\sigma_z = -i\sigma_z = e^{-\pi/2}e^{i\frac{\pi}{2}\sigma_z}$, kar nas pripelje do zapisa:

$$H = e^{-\pi/2}e^{i\frac{\pi}{2}\sigma_z}e^{i\frac{\pi}{4}\sigma_y},$$

ki ga pogosto zapišemo brez faznega faktorja.

S Hadamardovi vrati lahko zapišemo superpozicijo stanj, če pa si želimo zapisa v vsej splošnosti, pa potrebujemo še vrata, ki so sposobna spreminjati fazo.

- Vrata faznega premika in vrata T ter S
Pri vratih T gre za primer faznih vrat $R(\phi) = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 0\\ 0 & e^{i\phi}\end{bmatrix}$, kjer je ϕ enak $\pi/4$. Označujemo jih s simbolom $-\boxed{\text{T}}-$ v kvantnem vezju. Vrata S definiramo kot $S = T^2$ in imajo simbol $-\boxed{\text{S}}-$ v kvantnem vezju. Ker vrata faznega premika premikajo stanji $R(\phi)\,|0\rangle = |0\rangle$ in $R(\phi)\,|1\rangle = e^{i\phi}\,|1\rangle$, lahko vidimo, da se verjetnost za meritev stanja ne spremeni, spremeni pa se kvantna faza. Takšna rotacija predstavlja vrtež okrog osi $\hat{e}_z$ na Blochovi sferi, tako da se nam zariše zemljepisna širina na krogli. S Hadamardovimi in faznimi vrati lahko torej pridemo do poljubno izbrane linearne kombinacije stanj kubita v vezju:

$$R(\pi/2+\phi)\,H\,R(2\theta)\,H\;|0\rangle = \cos(\theta)\,|0\rangle + e^{i\phi}\sin(\theta)\,|1\rangle\,.$$

2.4.2 Vrata za več kubitov

Vrata za več kubitov v resnici ustrezajo matrikam, ki jih razširimo na večjo bazo. Najprej si poglejmo, kako lahko posplošimo vrata za operatorje na enem stanju.

[4] $e^{ixA} = \cos(x)\mathrm{I} + i\sin(x)A$

- Vzporedna vrata
Poglejmo si zapis dvojih splošnih vzporednih vrat A in B za posamezni kubit v bazi $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$:

$$A \otimes B = \begin{bmatrix} a_{0,0} & a_{0,1} \\ a_{1,0} & a_{1,1} \end{bmatrix} \otimes \begin{bmatrix} b_{0,0} & b_{0,1} \\ b_{1,0} & b_{1,1} \end{bmatrix},$$

s čimer dobimo bločno matriko skupne velikosti 4×4.

Primer takšnih vrat, ki se pogosto uporabljajo, so vzporedna Hadamardova vrata:

$$H \otimes H \otimes \cdots \otimes H = H^{\otimes n}$$

za n vzporednih vrat. Kadar pripravimo n kubitov v stanju $|00\ldots0\rangle$ dobimo superpozicijo 2^n vseh možnih stanj v registru z enakimi koeficienti oz. enako verjetnostjo za izid meritve. Torej

$$H^{\otimes n} |00\ldots0\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=1}^{2^n} \sum_{k=1}^{n} |i_k\rangle .$$

Na primer $H^{\otimes 2} |00\rangle = \frac{1}{\sqrt{2^2}}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$.

S tem smo zgolj posplošili spoznanje iz prejšnjega poglavja o tem, da lahko zapišemo poljubno linearno kombinacijo posameznega stanja, na več kubitov. Ker pa si posebej želimo delovati tudi na prepletena stanja, imamo veliko motivacijo še za konstruiranje vrat, s katerimi je to mogoče.

- Kontrolna vrata
Za delovanje na prepletenih stanjih torej uvedemo kontrolna vrata. V bazi $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ vrata zapišemo kot bločno diagonalno matriko iz identitete in splošne matrike U. Najpogosteje se uporabljajo vrata, kjer je U ena od Paulijevih matrik:

$$C_{x,\,y,\,z} = \begin{bmatrix} \mathrm{I} & 0 \\ 0 & \sigma_{x,\,y,\,z} \end{bmatrix}. \tag{8}$$

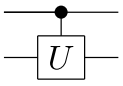
Kontrolna vrata v splošnem delujejo na dveh ali več kubitih, z razširitvijo matrike po istem principu, in predstavljajo operacijo: "Če je A res, potem naredi B." Poglejmo si na primer, kako delujejo $CNOT = C_x$ vrata, ki so najpogosteje v rabi. Kot vhod sprejmejo kontrolni $|k\rangle$ (*control*) in ciljni $|c\rangle$ (*target*) kubit ter nato izvedejo operacijo $|k\rangle |c\rangle \to |k\rangle |c \oplus k\rangle$, kar pomeni, če je stanje kontrolnega kubita $|1\rangle$, potem je ciljno stanje obrnjeno, v nasprotnem primeru pa ciljno stanje ostane nespremenjeno. Po dogovoru je na shemah v vezju linija, ki vsebuje majhno odebeljeno piko kontrolno stanje, linija z operatorjem pa ciljno. Simbol za $CNOT$ vrata je:


.

V splošnem uporabimo delovanje poljubnega unitarnega operatorja za en kubit U, ki ga predstavimo z matriko U, ki nadomesti $\sigma_{x,\,y,\,z}$ v definiciji (8). Splošno delovanje kontrolnih vrat je torej:

$$|k\rangle |c\rangle \to |k\rangle\ U^k |c\rangle . \tag{9}$$

Če je $k = 0$ operator ne deluje. Oznaka takšnih vrat v kvantnem vezju je podobna prejšnji:

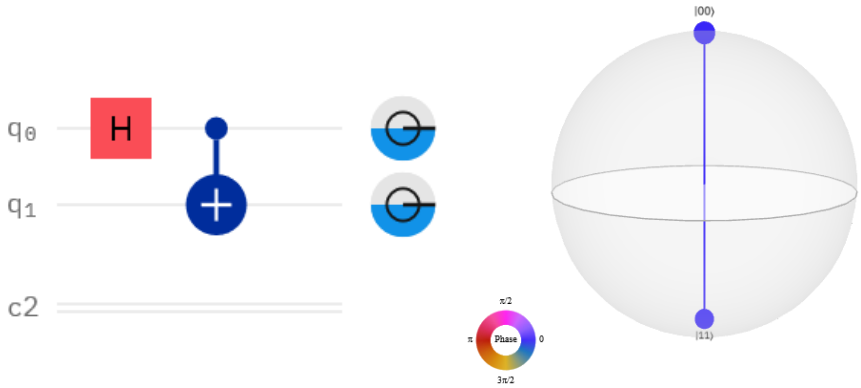


.

Poglejmo si še poučen zgled uporabe takšnih vrat za tvorbo prepletenih stanj. Oglejmo si, kako bi iz stanja $|00\rangle$ tvorili Bellovo stanje $|\phi^+\rangle$ iz enačbe (3). Shema vezja je prikazana na sliki 1a. S Hadamardovimi vrati najprej delujemo na prvi kubit:

$$(H \otimes I)\,|00\rangle = \left\{ \frac{1}{\sqrt{2}} \big(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1| \big)\ |0\rangle \right\} |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$$

Nato upoštevamo še način delovanja vrat na ciljni bit glede na kontrolnega po enačbi (9). Dobimo končni rezultat, ki je prikazan na sliki 1b: $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\phi^+\rangle$.



(a) Shema za ustvarjanje Blochovih stanj. **(b)** Blochova sfera s faznim diagramom.

Slika 1. Na sliki a) je prikazan poskus z dvemo kubitoma $|00\rangle \to |\phi^+\rangle$. Končni stanji sta prikazani na Blochovi sferi an sliki b) z modro barvo, kar pomeni, da nimata faznega zamika. Stanji izmerimo z enako verjetnostjo kot ponazarjata teoretična števca na koncu linije pri a).

- Toffolijeva vrata ali dvojna kontrolna NOT vrata

Delujejo podobno kot $CNOT$, vendar delujejo na treh kubitih. Opazujejo torej dve kontrolni liniji in izvedejo operacijo na ciljni liniji, če sta obe kontrolni stanji $|1\rangle$. Simbol za Toffolijeva vrata je:

.

Podobno kot prej lahko z bločno matriko tudi Toffolijeva vrata posplošimo za splošno matriko U, ki predstavlja unitarni operator.

Spoznali smo kar nekaj vrat, v splošnem pa bi bilo težko pripraviti eksperimentalni sistem, na katerem bi lahko izvajali tako širok nabor operatorjev, kot jih želimo uporabiti. Želja po tem, da bi z omejenim naborom vrat, ki jih lahko učinkovito implementiramo v naš kvantni računalnik, opisali vse možne operatorje, nam daje motivacijo za študij univerzalne množice kvantnih vrat.

2.4.3 Univerzalna množica vrat

Univerzalna množica vrat predstavlja končno množico vrat, s katerimi lahko opišemo katerikoli unitarni operator (matriko) poljubno dobro.

Definicija 1. Množica kvantnih vrat G je univerzalna, če za vsak $\epsilon > 0$ in katerokoli unitarno matriko U na n kubitih obstaja zaporedje vrat $g_1, g_2, \ldots, g_i$ iz G tako da velja:

$$||U - U_{g_i} \ldots U_{g_2} U_{g_1}|| \leq \epsilon. \tag{10}$$

Normo definiramo kot $\max_{|\psi\rangle} ||(U - U') |\psi\rangle ||$, kjer so $|\psi\rangle$ vsa normirana kvantna stanja v prostoru stanj.

Končna natančnost je posledica tega, da s končno množico vrat (števno množico) ne moremo opisati eksaktno neskončne množice vrat (neštevne množice) in gre za učinkovit približek. O tem govori Solovay–Kitaev izrek (str. 618, [9]), ki nam zagotavlja, da lahko učinkovito opišemo katerikoli unitarni operator do natančnosti $\epsilon > 0$ z $\mathcal{O}(m \log^c(\frac{m}{\epsilon}))$ vrati iz univerzalne množice vrat, kjer je $c \approx 2$.

V želji po tvorbi takšne množice si poglejmo ključne lastnosti, na katere moramo biti pri tem pozorni:

- z vrati iz množice lahko ustvarimo superpozicijo stanj,
- z njimi lahko ustvarimo prepletenost stanj,
- v množici ne smejo biti zgolj realna vrata.

Pogosto dodamo še pogoj, da množica vrat ni podmnožica Cliffordove množice[5] C_n, ki ni univerzalna, a vendarle ustreza prvim trem lastnostim, zato v sebi vsebuje mnogo potencialnih kadnidatov za univerzalno množico. Ta pogoj je torej predvsem praktične narave, saj se izkaže, da je velikokrat lažje pokazati, da je množica vrat podmnožica Cliffordove množice, kot da ni univerzalna množica.

Kljub temu pa je C_n zelo pomembna, saj zanjo velja Gottes-Knillov izrek. Ta pravi, da je lahko simulacija unitarnih transformacij iz omenjene množice na stabiliziranih stanjih[6] učinkovita na klasičnem računalniku, kar je osnova večine klasičnih simulatorjev za kvantne računalnike. Za n kubitov takšna simulacija potrebuje $\mathcal{O}(n)$ operacij, merjenje opazljivk pa ima lahko red $\mathcal{O}(n^2)$ po Aaronson in Gottesmanovem algoritmu [**?**].

Da zares pridobimo univerzalno množico, ponavadi C_n razširimo do univerzalne množice z dodajanjem vrat, ki niso njen element, najpogosteje vrata T ali pa Toffolijeva vrata. Primeri univerzalnih množic so: $\{CNOT, H, T\}$, $\{\text{Toffoli}, H\}$, $CNOT$ in vsa vrata za en kubit.

V praksi se izkaže, da je nekatere množice vrat bolje implementirati kot druge na različnih kvantnih sistemih. Veliko vlogo pri tem ima tudi to, kako popravljamo napake i pri dekoherence.

2.4.4 Poskus z univerzalno množico kvantnih vrat

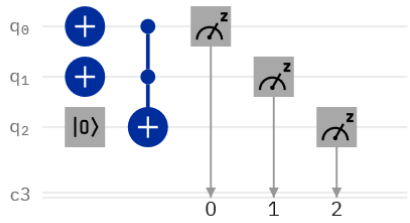
Za ilustracijo opisa splošnih vrat z univerzalno množico so Toffolijeva vrata nadomeščena z elementi univerzalne množice $\{CNOT, H, T\}$. Izbrano nadomestno vezje je še relativno preprosto, kot lahko vidimo v vezju na sliki 2.

[5] Cliffordova množica je množica unitarnih transformacij, ki normalizira Paulijevo množico za n kubitov P_n: $P_n = \{\pm 1, \pm i\} \times \{\text{I}, \sigma_x, \sigma_y, \sigma_z\}^{\otimes n}$. Formalno potem zapišemo Cliffordovo množico kot:

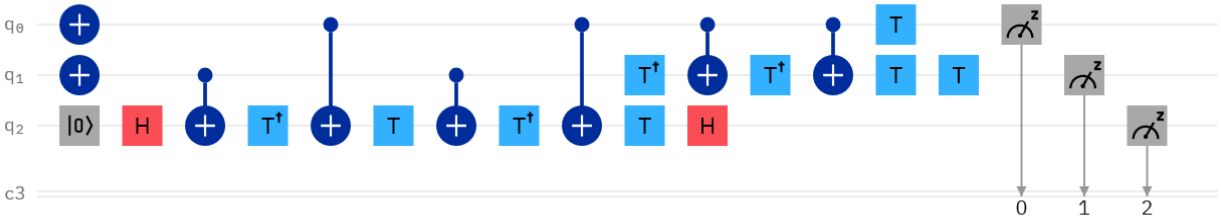
$$C_n = \{U : \; UP_nU^\dagger = P_n\}.$$

Definiciji za C_n očitno zadoščajo Paulijeve matrike, pokažemo pa lahko tudi, da velja na primer: $HXH^\dagger = Z$, $SXS^\dagger = Y$, $CNOT(X \otimes I)CNOT^\dagger$, torej so vsebovana tudi vrata $H \in C_1$, $S \in C_1$ in $CNOT \in C_2$. Vrata $CNOT$, H, S lahko generirajo celotno Cliffordovo množico.

[6] Cliffordova množica je lahko generirana zgolj s pomočjo H, $CNOT$ in $R(\phi)$ (namesto S) vrat, zato je lahko stabilizirano vezje sestavljeno zgolj iz teh treh vrat. Stanja v takšnem vezju so stabilizirana stanja.



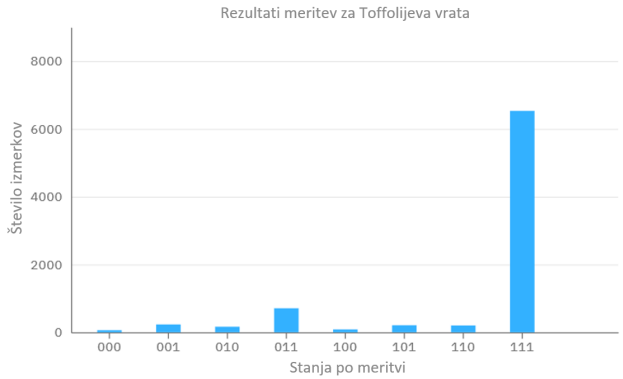
(a)



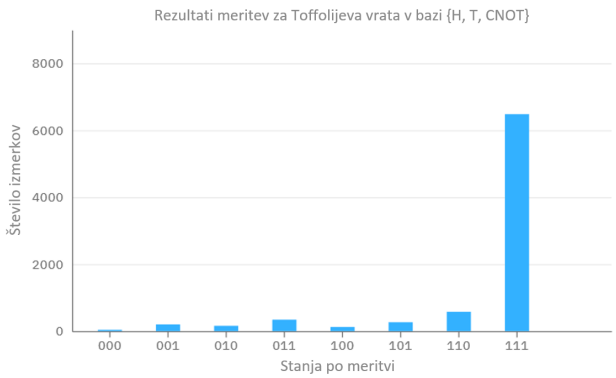
(b)

Slika 2. Prikazani sta vezji za Toffolijeva vrata, ki sta narisani v orodju IBM Quantum Composer za vhodno stanje $|110\rangle$ (začetna oznaka $q_0 = q_1 = |1\rangle$ po delovanju vrat NOT, $q_2 = |0\rangle$). Na sliki a) vidimo Toffolijeva vrata, na sliki b) pa njihov nadomestek v bazi $\{CNOT, H, T\}$. Na koncu vidimo še simbol sivih števcev za opravljanje meritev.

Teoretično bi za vhodno stanje $|110\rangle$ pričakovali rezultat $|111\rangle$ z verjetnostjo 1, vendar se izkaže, da v praksi ni povsem tako. Poskusi za obe vezji so bili izvedeni na na IBM-ovem kvantnem računalniku z imenom *ibmq_santiago* v Čilu s petimi superprevodnimi kubiti, rezultati pa so bili primerljivi za obe vezji. Ker se je za uporabo kvantnih računalnikov potrebno prijaviti v uporabniške čakalne vrste, je število poskusov za uporabnika v vrsti omejeno na 8192, za kar je računalnik potreboval približno 15 s. Poskus pri tem pomeni pripravo stanja, izvedbo operacij v vezju in meritev končnega stanja. Primer izida poskusa je prikazan na sliki 3.



(a) Rezultati implementacije Toffolijevih vrat.



(b) Rezultati implementacije nadomestnega vezja.

Slika 3. Pri obeh poskusih sta dobljena podobno visoka vrhova v teoretično predvidenem stanju. Opazimo tudi zašumljenost rezultatov na drugih stanjih, ki izgleda naključno in je spet popolnoma drugačna ob nadaljnih ponovitvah poskusa.

Kljub temu da se je rezultat po izvedbi poskusa z zelo veliko streli dobro ujemal, je bil poskus ponovljen z namenom, da bi ugotovili, kakšna bi bila odstopanja med ponovitvami ob različnih ča-

sih dneva zaradi vplivov iz okolice. Dobljeni rezultati za število izmerkov v stanju $|111\rangle$ po poskusih so zbrani v tabeli 1.

n	Toffoli [ ]	Toffoli{T, H, CNOT} [ ]	Toffoli{T, H, CNOT, S} [ ]
1	6530	6473	6242
2	6135	6466	6202
3	5864	6482	6088
4	5793	6266	5785
5	6461	6274	6438

Tabela 1. Prikazane so vrednosti, ki predstavljajo število izmerkov v stanju $|111\rangle$ po izvedenem poskusu s 8192 streli v celoti, n pa je zaporedno število poskusa. Po stolpcih lahko izračunamo povprečne verjetnosti za izid poskusa. Za Toffolijeva vrata kot samostojen operator dobimo $p_1 = 0.75\,(1 \pm 0.06)$, v bazi {H, T, CNOT}: $p_2 = 0.78\,(1 \pm 0.02)$ in še dodatno z nadomestnim operatorjem $S = T^2$: $p_3 = 0.75\,(1 \pm 0.06)$.

Kljub kar precej zašumljenim poskusom za implementacijo vrat in njihovega nadomestka z univerzalno množico, dobimo dovolj podobne rezultate v okviru napake pri p_1 in p_2, da je prikaz uporabe univerzalne množice vrat uspel. V nasprotju s pričakovanji opazimo, da v okviru napake ni bilo opazne razlike med zašumljenostjo pri rabi nadomestnega vezja za Toffolijeva vrata, prav tako ni bilo večjih sprememb, ko je bilo nadomestno vezje nadgrajeno z uporabo operatorja S, kar bi v principu moralo prispevati k večji natančnosti [10]. S tem lahko zaključimo, da so v okviru danih napak, ki so posledica interakcije z okolico in nenatančnosti pri meritvah, vse tri množice enakovredne.

3. Izdelava kvantnih računalnikov

3.1 DiVincenzov kriterij

Ko kvantna vrata prepišemo v vezje, ki shematično predstavlja izvedbo algoritma, se začnemo zanimati za izdelavo kvantnega računalnika, ki bo zmogljivejši od klasičnih pri izvajanju algoritmov za določene probleme. Obstaja 5 minimalnih pogojev, ki jim je potrebno zadostiti. Omenjeni kriterij je med raziskovanjem pri IBM-u zasnoval ameriški fizik DiVincenzo [11].

1. **Razširljiv fizikalni sistem z dobro določenimi kubiti.**
   Če želimo, da so kubiti kot nosilci informacije dobro določeni, moramo dobro poznati njihove lastnosti, na primer energijski spekter in interakcijske lastnosti tako z drugimi kubiti v kvantnem registru kot tudi z okolico. Ponavadi v kontekstu kubitov govorimo o dvonivojskih sistemih, vendar bi praktično dobili dobro aproksimacijo takšnega sistema, če bi vzeli večnivojski sistem z zelo nizkimi verjetnostmi za zasedenost višjih energijskih stanj. Dodatna zahteva je še enostavna razširljivost, kar pomeni, da lahko dodamo večje število kubitov. Zahteva ni ključna za poskuse v kvantnih komunikacijah, kjer lahko kvantno teleprotacijo in gosto kodiranje izvajamo z nekaj kubiti, vendar pa je precej bolj pomembna za računske probleme. Za potrebe reševanja problemov iz atomske fizike s klasičnimi interakcijami na primer potrebujemo med 50 in 100 kubitov [12].

2. **Možnost nastavljanja kubitov na enostavno začetno stanje.**
   Pogoj predstavlja dejstvo, da potrebujemo znano začetno stanje kvantnega registra, na katerem potem izvajamo nadaljnje operacije. Prav tako je zelo pomembno, da so večji računalniki sposobni sproti odpravljati napake, ki nastanejo zaradi dekoherence in drugih motenj, za kar je potrebno v vmesnem procesu ponastavljati stanja.

3. **Dekoherenčni časi veliko daljši kot časi izvajanja vrat.**
   Dekoherenčni čas je posledica interakcije z okoljem, zaradi česar čista kvantna stanja prehajajo v mešanico čistih stanj. Na dekoherenčni čas vplivajo tudi interakcije z drugimi kubiti iz registra in navsezadnje tudi začetno stanje sistema. Če na sistemu ne bi izvajali postopkov za odstranjevanje napak, potem bi moral biti dekoherenčni čas daljši od časa izvajanja našega algoritma. Ker pa v praksi vedno izvajamo takšne postopke, moramo v resnici čas med zaporednima popravljanjema stanj optimizirati, tako da bo krajši od dekoherenčnega časa. Ker takšen postopek lahko izvajamo najhitreje tik pred in tik po vratih, je logična zahteva, da mora biti dekoherenčni čas vsaj tako dolg kot čas delovanja vrat. Seveda si želimo, da je čas dekoherence veliko daljši od časa delovanja vrat, saj to pomeni, da sistem ne potrebuje prepogostega popravljanja in je bolj stabilen.

   Pri izvajanju vrat dejansko na kvantno stanje delujemo z motnjo v obliki ustreznega generatorja $\hat{G}$ vrat $U(t) = e^{i\frac{\hat{G}}{\hbar}t}$, kot je na primer Hamiltonjan generator operatorja časovnega razvoja. Zato smo si v teoretično orientiranem uvodu predstavljali, da idealna vrata hipno delujejo za točno določen čas, torej jih lahko preprosto vklapljamo in izklapljamo. V realnem sistemu pa lahko takšno hipno delovanje vzbudi višja stanja sistema, paziti pa moramo tudi na interakcije z ostalimi kubiti in okoljem. Zaradi tega delujemo s posameznimi vrati previdneje, torej bolj počasi, kar določa tipične čase izvajanja vrat. Tipične vrednosti se seveda zelo razlikujejo med tipi kvantnih računalnikov, enako velja tudi za dekoherenčne čase.

4. **Univerzalna množica kvantnih vrat.**
   Za učinkovito izvajanje operacij potrebujemo univerzalno množico vrat, pri čemer imamo več možnosti, kot je predstavljeno v poglavju 2.4.3. V praksi se lahko izkaže, da je nekatere množice lažje implementirati kot druge, ali pa so lahko celo bolj natančne.

5. **Možnost meritve posameznega kubita.**
   Na sistemu mora biti možno pomeriti posamezni kubit, meritev pa mora biti natančna in učinkovita. Seveda je idealna meritev popolnoma zanesljiva in se izvede hipno, v praksi pa je meritev učinkovita z neko verjetnostjo in traja nekaj časa. Naša želja je torej, da jo izvedemo dovolj hitro, torej hitreje od dekoherenčnega časa, saj moramo drugače implementirati dodatna vrata za odpravljanje napak. Zaradi nenatančnosti meritev moramo poskuse ponoviti, lahko jih izvajamo tudi vzporedno na več različnih računalnikih. Zgled je narejen v poglavju 2.4.4.

3.2 Dekoherenca

V DiVincenzovem kriteriju si prizadevamo za čim bolj stabilne kubite, ki ostanejo v superpoziciji stanj toliko časa, da lahko izvedemo operacije iz našega vezja. To dosežemo s čim šibkejšo sklopitvijo z okolico, kar pa se odraža tudi v tem, da z zunanjimi vplivi težje delujemo na sistem. Torej težje izvajamo naša kvantna vrata. Prav zaradi tega si želimo odpravljanja napak med algoritmom tako, da dobimo ustrezen kompromis med obema zahtevama.

Dekoherenca lahko na kvantnih računalnikih povzroči veliko napak, na primer spreminjanje kvantne faze $|0\rangle - |1\rangle \to |0\rangle + |1\rangle$ ali pa majhne spremembe amplitude $c\,|0\rangle \to (c+\epsilon)\,|0\rangle$. Manjše napake se lahko hitro nakopičijo in preidejo v večje, kot je na primer največkrat navedena obrat bita (*bit-flip*): $|1\rangle \to |0\rangle$.

Najpogosteje se kot mera za dekoherenco uporablja dekoherenčni čas τ_D, ki pove, koliko časa traja, da pride do opaznega obrata bita $|1\rangle \to |0\rangle$ zgolj pod vplivom okolice oziroma da bomo z opazno

veliko verjetnostjo izmerili stanje $|0\rangle$. Če takšno stanje pustimo pri miru še nekaj dekoherenčnih časov, bo stanje sistema povsem naključno.

Za odpravljanje napak pa je mogoče bolj informativno razmerje dekoherenčnega časa z oceno za čas delovanja vrat, ki mora biti veliko večje od 1.

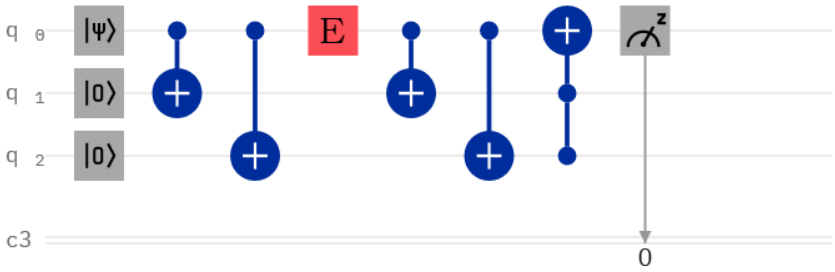
3.3 Kvantno odpravljanje napak

Za izvedbo daljših algoritmov je torej ključno vpeljati tudi odpravljanje napak, ki nastanejo zaradi dekoherence. V klasičnih računalnikih, kjer je edina možna napaka obrat bita, to rešujemo s ponavljanjem. Informacijo po kanalu, na katerem prihaja do motenj, pošljemo večkrat in pogledamo, kakšen je najbolj pogost izid, kjer upamo oz. predpostavimo, da pride do napake v manjšem številu izidov. Takšen pristop pa v kvantnem računalništvu ne pride v poštev zaradi nezmožnosti kloniranja kvantne informacije. Poleg tega se napake v kvantnih sistemih razvijajo zvezno s časom in niso diskretne kot v klasičnem svetu in je tudi zato obravnava same napake povsem drugačna. Dodatno se razlikuje tudi zaznavanje napak, saj ob kvantni meritvi zmotimo sistem.

Ena prvih metod na tem področju je nastala po predlogu Asherja Peresa leta 1985 [13], ki je pokazala, da lahko s tremi fizičnimi kubiti zapišemo informacijo vsebovano v enem idealnem kubitu in ga pri tem zavarujemo pred obratom bita. Kasneje sta v letih 1995 Shor [**?**] in 1996 Steane [14] rešitev posplošila na kodo za odpravljanje poljubne napake na posameznem kubitu, pri čemer informacijo v enem idealnem kubitu zapišemo s petimi fizičnimi kubiti.

Osnovna ideja kvantnih vezij z odpravljanjem napak je torej, da povečamo število kubitov in nekoliko prilagodimo vezje. V praksi velja ocena, da lahko za poljubno kompleksen kvantni algoritem, ki traja poljubno dolgo, izvajamo uspešno odpravljanje napak, če pride do največ ene napake na vsakih 10^4 računskih operacij (str. 119, [15]).

Kot zgled si poglejmo, kako bi zavarovali kubit (q_0), ki nosi informacijo, kjer predpostavimo, da je edina možna napaka, ki se zgodi v vezju, obrat bita na enem od kubitov (ne hkrati na večih). Ta predpostavka je tu zgolj zaradi lažje predstavljivosti vezja in ni realistična. Na sliki 4 je na primer prikazan obrat bita z rdečo na kubitu q_0, lahko pa se zgodi tudi na q_1 ali q_2.



Slika 4. Shema vezja, ki odpravi obrat bita (rdeč simbol "E") na kubitu q_0. S sivo je označena meritev na klasičnem kanalu c_3. Vezje deluje tudi, če bi obrat bita prestavili po vezju navzdol na q_1 ali q_2. *Opomba: Obrat bita v resnici implementiramo z vrati NOT, vendar je tu drugačna oznaka izbrana zaradi jasnosti.*

Ideja vezja z dodatnima kubitoma je to, da osnovno stanje $|\psi\rangle = c_0|0\rangle + c_1|1\rangle$ razširimo v stanje $|\psi'\rangle = c_0|000\rangle + c_1|111\rangle$, ki nastopa pred območjem, kjer nastopi obrat bita "E", po katerem dobimo $|\psi''\rangle = c_0|100\rangle + c_1|011\rangle$. V nadaljevanju pa lahko s kombinacijo kontrolnih in Toffolijevih vrat popravimo vsako permutacijo v stanjih $|100\rangle$ in $|011\rangle$, tako da bomo na q_0 ponovno dobili $|\psi\rangle$.

3.4 Tipi kvantnih računalnikov

V tem poglavju je prestavljenih nekaj najpogostejših tipov kvantnih računalnikov in njihove prednosti ter slabosti. Pri tem so izpuščeni hladni atomi, ki so posebej pomembni za kvantne simulatorje. Slednji omogočajo proučevanje kvantnih sistemov, ki jih težko analiziramo v laboratoriju in so praktično nemogoči za simuliranje na klasičnih superračunalnikih. Za primer si zamislimo, da omenjene hladne atome pridobimo s hlajenjem v pasti, nato pa kondenzat z atomi iz pasti prestavimo v periodični optični potencial, kar omogoča natančno simuliranje kristalnih struktur. To je pripravno za opazovanje pojavov, kot so na primer Blochove oscilacije. Primerov uporabe hladnih atomov in kvantnih simulatorjev je veliko, v nadaljevanju pa se bomo bolj posvetili tipom kubitov za kvantne računalnike, kakršne smo si zamislili uvodoma.

3.4.1 NMR kvantni računalnik

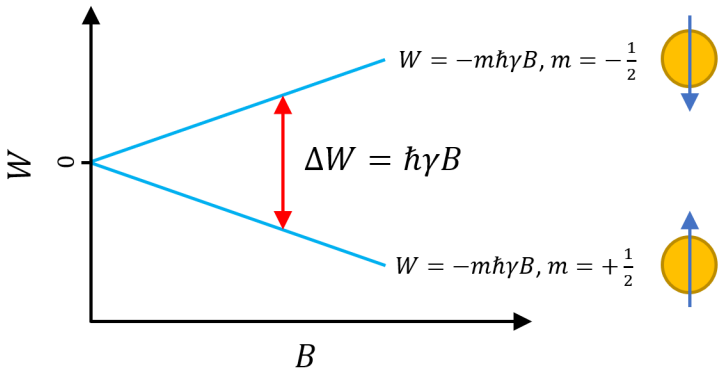
Prvi poskus izdelave je bil prav računalnik, ki deluje s pomočjo jedrske magnetne resonance (NMR — *nuclear magnetic resonance*). Do pojava pride, ko so jedra izpostavljena konstantnemu magnetnemu polju, nato pa vključimo še drugo nihajoče magnetno polje, kar se uporablja na primer za kemijske analize, v fiziki materialov in slikanje z magnetno resonanco v medicini (MRI). Velik napredek pri razvoju NMR metod je spodbudil tudi razvoj takšnih kvantnih računalnikov.

Večina atomskih jeder ima magnetni moment in spin, h kateremu prispevajo spini in obhodna vrtilna količina vseh protonov in nevtronov v jedru. Pri tem se zavedamo, da je spin jeder s sodim število protonov in nevtronov enak 0, z lihim številom obeh pa je celoštevilski. Polovične spine dobimo za jedra s sodim številom protonov in lihim številom nevtronov ali obratno. Ko jedra postavimo v magnetno polje, se spin ob interakciji s poljem polarizira in se nekateri protoni poravnajo v smeri magnetnega polja (paralelna stanja), spet drugi se obrnejo v obratni smeri (antiparalelna stanja). Tako kot pri klasičnem NMR-ju tudi v kvantnem računalništvu uporabljamo jedra s spinom 1/2 (sodo-liha, liho-soda jedra npr. ^{1}H, ^{13}C, ^{19}F, ^{15}N).

Stanji $|0\rangle$ (paralelno stanje) in $|1\rangle$ (antiparalelno stanje) v magnetnem polju imata energijsko razliko (str. 131, [16]):

$$\Delta W = W_{M_J} - W_{M_J+1} = g\mu_j B = \hbar\gamma B,$$

kjer je M_J spinsko kvantno magnetno število, g giromagnetni moment jedra, μ_j jedrski magneton, γ giromagnetno razmerje in B gostota magnetnega polja. Tako smo tvorili dvonivojski sistem, ponazorjen na sliki 5, ki si ga želimo za konstrukcijo kubitov.



Slika 5. Prikazan je graf energije v odvisnosti od gostote magnetnega polja za dvonivojski sistem jedra s pol celim spinom.

Prehod med nivojema je možen z nihajočim magnetnim poljem z resonančno frekveco: $\nu = \Delta W/h$. Za doseganje visokih frekvenc torej potrebujemo čim močnejša polja ($\nu \propto B$), ki jih dobimo s superprevodnimi magneti. Poskusa pa ne delamo zgolj na eni molekuli. Pri prehodu v radiofrekvenčnem spektru imajo oddani fotoni energijo reda 1 μeV, zato je posamezne fotone zelo težko zaznati. Poleg tega je za nukleone porazdeljene po Boltzmannovi porazdelitvi proces vzbuditve fotona iz višjega v nižje stanje precej redek ($1/10^4$ str. 5, [17]). S tem namenom se uporablja ansamble reda velikosti 10^{18} do 10^{19} molekul. V tako velikih vzorcih pa velja opomniti, da nimajo vsa jedra enake resonančne frekvence zaradi vpliva elektronov, kar imenujemo kemijski premik (*chemical shift*) in se pogosto upošteva s semi-empiričnimi kemijskimi približki (str. 236 [18]). Ker imamo tako velike vzorce in merimo povprečje, se privzame, da takšna meritev ne vpliva na stanja spinov jeder (str. 103, [19]).

Ideja kvantnega NMR računalnika, kot sta ga v letu 1998 zasnovala Gershenfeld and Chuang [20], je, da lahko molekulo predstavimo kot kvantni računalnik, katerega stanja so določena z orientacijo spinov jeder v molekuli (paralelna in antiparalelna stanja). Izberemo molekule, ki jih ni težko pridobiti in imajo jedra s spinom 1/2 ter dolgima relaksacijskima časoma T_1 in T_2. Poleg tega izbiramo molekule z različnimi jedri, ali pa enakimi jedri z različnimi kemijskimi premiki frekvence vzbujanja, da lahko delujemo na točno določeno jedro. Nato s sekvencami radiofrekvenčnih pulzov, ki jih poznamo iz NMR, tvorimo kvantna logična vrata in tako ustvarimo unitarne transformacije sistema. Na ta način lahko naredimo sisteme z nekaj kubiti. Leta 2001 je na primer IBM izvedel Schorov algoritem na 7 kubitnemu računalniku [21].

Eksperimentalne tehnike NMR-ja so zelo razvite (meritev, priprava vzorcev in pulzov), dekoherenčni časi pa so daljši od nekaj sekund, kar v veliki meri zadošča DiVincenzovim kriterijem. Žal pa z dodajanjem kubitov v sistem pada intenziteta signala za približno polovico, če uporabljamo trenutno pripravljena psevdo čista stanja[7]. Zaradi tega takšna začetna stanja niso prava pot k razširitvi kvantnega registra NMR računalnikov [17], saj jih, kljub temu da je dodajanje novih kubitov v sistem zelo preprosto, v praksi potem ne moremo pomeriti.

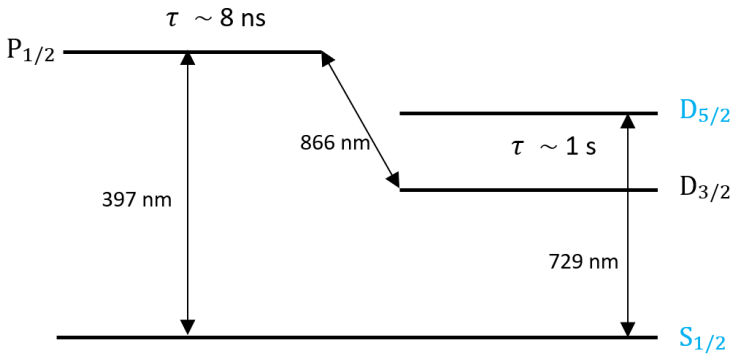
3.4.2 Kvantni računalnik z ujetimi ioni

V tem načinu poskušamo nabite delce, na primer ione, ujeti v zaprtem prostoru s pomočjo elektromagnetnega polja, čemur rečemo kvantna past. Ker po Earnshawovem izreku [23] ne moremo zadržati nabitih delcev v statističnem ravnovesju le z elektrostatskimi efekti, najpogosteje uporabljamo Paulijeve in Penningove pasti [24]. V pasteh ustvarimo elektrostatsko kvadrupolno polje v obliki sedla, nato pa dodamo izmenično kvadrupolno polje za Paulijevo past ali pa močno magnetno polje vzdolž osi za Penningovo. Kubit je torej shranjen v stabilnih elektronskih stanjih posameznega iona pri nizki temperaturi, ki nam zagotavlja stabilnost orbit iona v pasti. Več ionov pa lahko zložimo tudi v verige tako, da pripravimo kvantni register. V takšnih pogojih so ioni skoraj popolnoma izolirani od okolice, za kvantno posredovanje informacije pa interagirajo v skupni ionski pasti preko elektromagnetne interakcije.

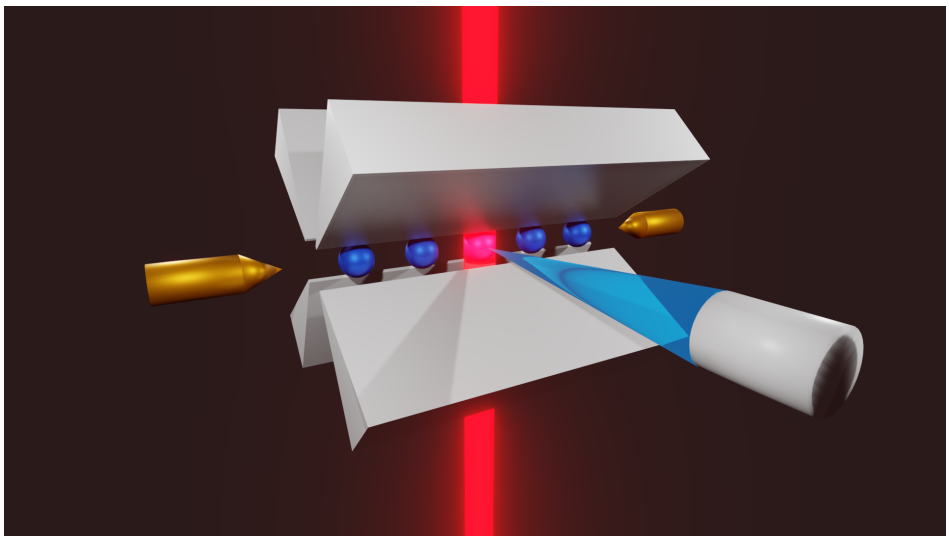
Na tem mestu se seveda pojavi vprašanje, kako pa v ionu dejansko tvorimo kubit, saj imamo lahko

[7] Psevdo čista stanja so oblike $\rho = \frac{1-\epsilon}{2^n}\mathrm{I}_{2^n} + \epsilon\,|\psi\rangle\langle\psi|$, kjer je $|\psi\rangle$ čisto stanje, ϵ pa je čistost. Ta stanja so torej mešana $\mathrm{Tr}\rho^2 \neq 1$ z majhnim deležem čistega stanja ϵ. Pri NMR poskusih so uporabna, ker se v času razvija le njihov čisti del, mešani pa ostane nespremenjen: $\rho(t) = \hat{U}\rho(t=0)\hat{U}(t)^\dagger = \frac{1-\epsilon}{2^n}\mathrm{I}_{2^n} + \epsilon\hat{U}(t)\,|\psi\rangle\langle\psi|\,\hat{U}(t)^\dagger$, kjer je $U(t) = e^{-\frac{i}{\hbar}\hat{H}(t)}$ propagator. Ker pričakovano vrednost spina, ki je relevantna za poskus, izračunamo kot $\mathrm{Tr}(\rho\sigma)$, mešani del odpade. Zaradi tega jih uporabimo kot nadomestek za čista začetna stanja, ki jih je težko pridobiti [22, 17].

več elektronskih stanj. Pripravo si bomo najlažje ogledali na primeru. Vzemimo ion $^{40}Ca^{+}$, z nivoji prikazanimi na sliki 6. Osnovno stanje kubita bo najnižje elektronsko stanje $S_{1/2}$. Za izbiro drugega dvonivojskega stanja smo pozorni na višje nivoje $P_{1/2}$, $D_{5/2}$ in $D_{3/2}$. Prehod iz $P_{1/2}$ v $S_{1/2}$ je dipolni prehod in se zgodi praktično spontano v nekaj nanosekundah, zato ni primeren za tvorbo stabilnega dvonivojskega sistema. Izkaže se, da je precej stabilno stanje $D_{5/2}$, kjer prehod ni dipolen, zato si ta nivo izberemo za višje stanje našega dvonivojskega sistema. Ker je med izbranima nivojema še nivo $D_{3/2}$, na ion konstantno svetimo z laserjem z valovno dolžino 866 nm, da ta nivo izničimo tako, da ga vzbujamo v stanje $P_{1/2}$. Zanimivo je še, da lahko pogosto uporabimo tudi preostale nivoje. Pri $^{40}Ca^{+}$ na primer $P_{1/2}$ za Dopplerjevo hlajenje iona. Pri tem na ion svetimo z nekoliko višjo valovno dolžino, kot je potrebna za prehod (397 nm). Če se atom giblje proti viru laserskega snopa zaradi Dopplerjevega pojava opazi svetlobo z manjšo valovno dolžino in z večjo verjetnostjo absorbira foton. S časoma ion preide v osnovno stanje tako, da v naključni prostorski kot izseva foton s karakterističnо valovno dolžino. Ker ima ion večjo verjetnost za absorpcijo fotona v smeri, v katero se giblje, bo zaradi tega izgubljal hitrost.



Slika 6. Shema nivojev in prehodov za ion $^{40}Ca^{+}$. Označene so valovne dolžine laserja za vzbujanje prehoda med stanji in ocena za čas preživet v vbujenem stanju τ. Z modro sta označena nivoja s katerima tvorimo kubit. Podatki za sliko so pridobljeni iz [25].



Slika 7. Prikazana je poenostavljena shema eksperimentalne postavitve verige ionov ujetih v past. Štiri stranske elektrode označene s sivo barvo ustvarjajo statično kvadrupolno polje, imamo pa še prečno magnetno polje, ki je usmerjeno vzdolž verige ionov označenih s temnomodro. Z rdečo je shematsko prikazano delovanje laserja, s svetlomodro pa je ponazorjen prehod fotonov do CCD kamere, ki jih zaznava.

Na posamezne kubite v takšnem registru lahko vplivamo z laserjem. Vemo, da s sinusno nihajočo elektromagnetno motnjo svetlobe na dvonivojskem sistemu povzročimo, da verjetnost za zasedenost posameznih stanj oscilira z Rabijevo frekvenco. Podobno lahko z zaporedjem elektromagnetnih pulzov dosežemo poljubno superpozicijo obeh nivojev. Poleg tega pa je z laserjem možno inducirati tudi sklopitev z ostalimi kubiti v verigi (prepletenost). Na ta način pripravimo tudi začetna stanja. Meritev poteka tako, da laser z valovno dolžino, ki ustreza enemu od energijskih nivojev, vzbuja ion. Ob prehodu iz vzbujenega stanja ion odda fotone, ki jih lahko zaznamo npr. s CCD kamero. Če se ion sesede v drugo stanje kubita, potem ne bo oddal fotona, kljub interakciji z laserjem. S poznavanjem zaporedja oddanih fotonov lahko določimo stanje iona, ki predstavlja kubit. Za ponovno uporabo pa je potrebno ion na novo ohladiti. Shema eksperimenta, ki predstavlja kvantni računalnik z verigo ujetih ionov, je prikazana na sliki 7.

3.4.3 Kvantni računalnik s SQUID

SQUID (*superconducting quantum interference device*) je mikronsko majhen obroč iz dveh superprevodnih spojev povezanih preko tankih izolatorskih plasti, kot je prikazano na sliki 8b. Narisan je primer z dvema spojema, v praksi pa se uporabljajo tudi obroči z več tovrstnimi spoji. Za boljše razumevanje delovanja si najprej poglejmo ozadje superprevodnosti in spojev.

Superprevodnost lahko na mikroskopskem nivoju razložimo v skladu s teorijo BCS tako, da se elektroni privlačijo in tvorijo vezana stanja — Cooperjeve pare, ki se obnašajo kot bozoni s spinom 0, nabojem $e = -2e_0$ in maso $m = 2m_e$, torej bodo pri dovolj nizkih temperaturah vsi pari v osnovnem energijskem stanju sistema. Koherenčna dolžina parov je dovolj velika, da se prekrivajo, poleg tega pa se ujemajo še relativne faze parov. Posledično so superprevodniki kvantno koherentni na makroskopskih razdaljah. Zaradi tega lahko utemeljimo obravnavo superprevodnikov na osnovi fenomenološke Ginzburg-Landauove teorije, kjer je osrednja količina kompleksna makroskopska valovna funkcija Ψ, ki je ureditveni parameter za superprevodno stanje in sestoji iz amplitude in faze: $\Psi = |\Psi|e^{i\delta}$. Takšno funkcijo ponavadi normaliziramo s pogojem $\int_V \Psi^*\Psi \mathrm{d}\mathbf{r}^3 = N$, kjer integriramo po volumnu, N pa je celotno število Cooperjevih parov v materialu. S tem preidemo na zapis $\Psi = \sqrt{n(\mathbf{r})}e^{i\delta}$, kjer je $n(\mathbf{r})$ lokalna gostota parov.

Če staknemo dva superprevodnika preko tanke plasti izolatorja, temu pravimo Josephsonov spoj, ki je prikazan na sliki 8a. Tak spoj brez dodatne priklopljene napetosti lahko obravnavamo kot potencialno oviro, preko katere lahko Cooperjevi pari tunelirajo. Za ravni stik se reševanje zaradi simetrije poenostavi na odvisnost zgolj od koordinate x, katere nosilna os pravokotno prebada spoj. Z reševanjem Schrödingerjeve enačbe na območju $|x| < a$, kjer velja $V > E$, lahko izračunamo gostoto verjetnostnega toka:

$$j_x = \frac{\kappa e\sqrt{n_1 n_2}}{\sinh^2(2\kappa a)}\ \sin(\delta_2 - \delta_1) = j_c \sin(\delta_2 - \delta_1), \tag{11}$$

kjer je $\kappa = \frac{\sqrt{2m(V-E)}}{\hbar}$, n_1 in n_2 pa sta številski gostoti na straneh spoja. Iz enačbe (11) je razvidna povezava s kritičnim tokom j_c in sinusom razlike faz. Velja torej, da na superprevodnem spoju ne bomo opazili toka Cooperjevih parov, če bomo imeli na obeh straneh enako kvantno fazo. Tak rezultat je pričakovan, saj je za nastavek valovne funkcije $\psi(\mathbf{r}) = \sqrt{n(\mathbf{r})}\, e^{i\delta(\mathbf{r})}$ gostota verjetnostnega toka izračunana kot $\mathbf{j} = \frac{e\hbar n(\mathbf{r})}{m}\nabla\delta$. Ker vemo, da je v osnovnem energijskem stanju gibalna količina $\mathbf{p} = m\mathbf{v} = \frac{m}{n(\mathbf{r})e}\,\mathbf{j} = \hbar\nabla\delta$ enaka 0, velja $\nabla\delta = 0$ oziroma je kvantna faza δ konstantna po celotnem superprevodniku in dobimo ravnovesno stanje.

V kolikor je napetost med spojema enaka 0, se razlika med fazama ne spreminja v času, torej je edini pogoj za neničelni tok $\delta_2 - \delta_1 \neq n\pi$. Če pa na spoj priključimo napetost, bo razlika faz lahko odvisna tudi od časa. Za ta namen je potrebno rešiti sistem dveh sklopljenih Schrödingerjevih enačb z različnima nastavkoma na straneh in karakteristično sklopitveno konstanto K, ki jo lahko povežemo z rezultatom s prejšnje strani. Zaradi preprostosti kar izrazimo rešitev sistema:

$$\hbar\frac{\partial n_1}{\partial t} = -\hbar\frac{\partial n_2}{\partial t} = 2K\sqrt{n_1 n_2}\sin(\delta_2 - \delta_1), \tag{12}$$

$$\hbar\frac{\partial}{\partial t}(\delta_2 - \delta_1) = 2eU. \tag{13}$$

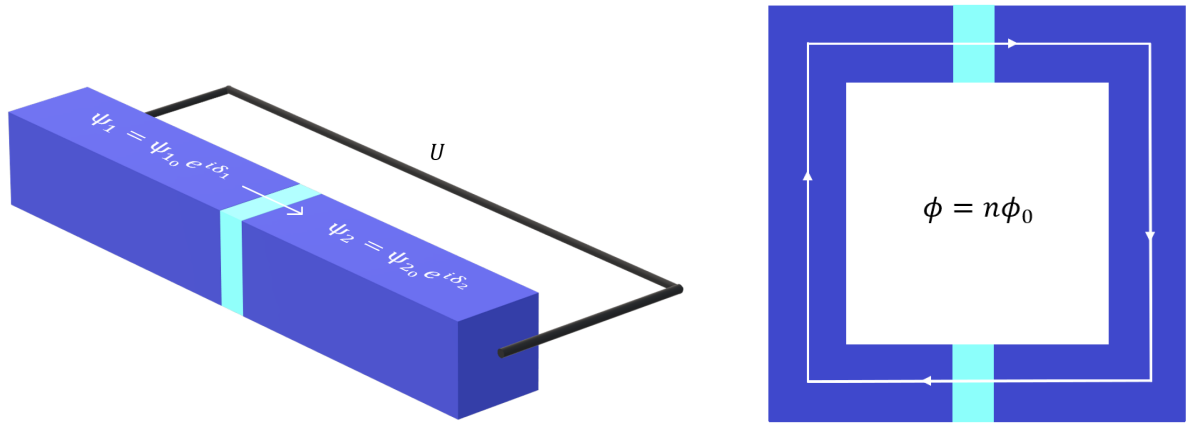
V enačbi (12) opazimo, da se številska gostota ene strani povečuje ravno toliko, kolikor se druga zmanjšuje. Tok na posamezni strani je enak odvodu številske gostote po času, zato ponovno dobimo zvezo:

$$I = I_c \sin(\delta_2 - \delta_1), \tag{14}$$

kjer je kritični tok $I_c = 2K\sqrt{n_1 n_2}/\hbar$. Ob vplivu napetosti pa se s časom spreminja tudi razlika faz:

$$\delta_2 - \delta_1 = \delta_0 + \frac{2eU(t)}{\hbar}\,t. \tag{15}$$

Ob priključitvi konstantne napetosti z vstavljanjem enačbe (15) v enačbo (14) vidimo, da bomo na spoju prejeli izmenični tok.



(a) Shema superprevodnega spoja s tanko izolatorsko plastjo. **(b)** Shema SQUID-a z dvema spojema.

Slika 8. Na shemi a) je prikazan Josephsonov spoj priključen na napetost U. Tanek izolatorski spoj je obarvan svetlomodro, superprevodnik pa je prikazan v temno modri barvi. Na sliki b) je prikazan SQUID sestavljen iz dveh takšnih povezanih spojev. V notranjosti SQUID-a, po katerem teče supertok, dobimo kvantiziran magnetni pretok.

Sedaj lahko hitro opazimo uporabno vrednost superprevodnih obročev SQUID. Če si zamislimo preprost obroč z dvema Josephsonovima spojema na vsaki strani (glej sliko 8b), vemo, da je zgolj v notranjosti takšnega obroča prisotno magnetno polje. Zato lahko zapišemo:

$$2\pi n + \delta_2 - \delta_1 = \frac{e}{\hbar}\oint \mathbf{A}(\mathbf{r})\cdot \mathrm{d}\mathbf{r} = \frac{e}{\hbar}\oint_S \nabla\times\mathbf{A}(\mathbf{r})\cdot \mathrm{d}\mathbf{S} = \frac{e}{\hbar}\oint_S \mathbf{B}(\mathbf{r})\cdot \mathrm{d}\mathbf{S} = \frac{e}{\hbar}\Phi_B, \tag{16}$$

kjer je razlika faz izražena za valovni funkciji, ki opisujeta vsako stran obroča. Magnetni pretok, ki ga obkroža supertok, pa je kvantiziran s kvantom magnetnega pretoka $\Phi_0 = \frac{h}{2e_0}$. Na tak način tvorimo kubit, katerega osnovno in višje stanje sta pri različnih vrednostih kvantiziranega magnetnega

pretoka in ki ustrezata na primer stanjema s supertokom v nasprotnih smereh po obroču. Pri tem je pomembno tudi število Josephsonovih spojev. Supertok v obroču brez spojev bi bil stacionaren, saj nimamo nobene upornosti, posledično pa je tudi magnetni pretok od časa neodvisen. Z dodajanjem spojev v obroč dodamo dinamiko, tako da lahko pridobimo različne kvantizirane vrednosti pretoka. Dodajanje spojev pa je v principu ugodno tudi zato, ker lahko s tem povečamo dekoherenčni čas takšnega kubita.

Kvantna vrata lahko na tovrstnih kubitih izvajamo s spreminjanjem magnetnega polja in mikrovalovi. Ko pa imamo enkrat tehnično izpopolnjene tovrstne kubite, meritev stanj izvajamo kar z dodatnimi SQUID-i. Z izdelavo tovrstnih kvantnih sistemov se ukvarja na primer podjetje DWave [26].

3.4.4 Kvantne pike

Kvantne pike so polprevodniške nanostrukture, pogosto imenovane tudi umetni atomi, ki so že nekaj časa predmet raziskav na različnih področjih industrijske nanotehnologije. Velikost kvantnih pik je nekaj nanometrov in so narejene tako, da zadržujejo gibanje elektronov in vrzeli v prostoru.

Primer takšne uporabe je spinski kubit iz kvantne pike, v kateri je ujet le en elektron. Enokubitne operacije se izvajajo z magnetnimi pulzi, na pike pa lahko vplivamo tudi z laserjem. Za izvedbo dvokubitnih vrat lahko kvantne pike sklopimo preko spoja, ki si ga predstavljamo kot pregrado, skozi katero lahko delci tunelirajo. Če je potencial takšne pregrade visok, je tuneliranje med pikama prepovedano in se stanja kubitov ne razvijajo v času. Če pa je potencial pregrade dovolj nizek, lahko tak spoj opišemo s Hubbardovim modelom [27], ki v limiti močne odbojne interakcije preide v Heisenbergov model. Med dvema pikama zapišemo:

$$H(t) = J(t)\,\mathbf{S_1} \cdot \mathbf{S_2}, \tag{17}$$

s časovno odvisno sklopitveno konstanto $J(t) = 4t_0^2(t)/u$, ki jo lahko vklapljamo ali izklapljamo z matričnim elementom za tuneliranje $t_0(t)$. u je karakteristična energija, ki je potrebna za nabitje kvantne pike, $\mathbf{S_i}$ pa je spinski operator velikosti $1/2$ za kvantno piko i. Na tak način lahko tvorimo primere kontrolnih vrat. Z ustrezno dolgim pulzom lahko s takšnim Hamiltonjanom generiramo operator razvoja: $U = e^{-i\pi \mathbf{S_1}\cdot\mathbf{S_2}}$, ki je enaka učinku vrat SWAP (str. 127, [15]):

$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Takšen model (17) podaja dober opis, če zadostimo naslednjim pogojem [27]:

- Lahko zanemarimo višja stanja delca v piki. To dobro velja, če je energijski razmak med nivoji ΔE večji od termične energije delcev: $\Delta E \gg kT$.
- Čas pulza τ_P mora biti daljši od $\hbar/\Delta E$, da preprečimo skoke v višja orbitalna stanja.
- $u > t_0(t)$ za vse čase, kar zagotavlja natančnost Heisenbergove sklopitve.
- Čas dekoherence τ_D mora biti bistveno daljši od trajanja pulza: $\tau_D \gg \tau_P$.

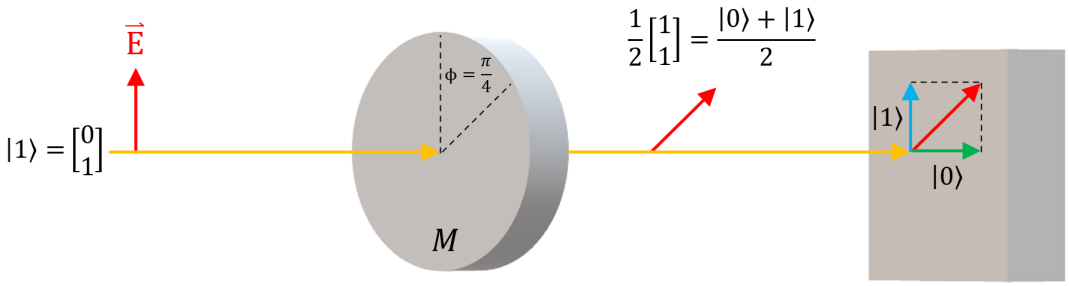
V splošnem je ta pristop zelo obetaven, saj lahko sistem kvatnih pik z obstoječo tehnologijo zelo razširimo na daljše verige kubitov. Vendar pa kljub temu da je sistem precej odporen na različne vplive iz okolice, obstaja problem dekehorence zaradi sklopitve spina jeder iz katerih je sestavljena pika in spina elektrona v njeni notranjosti.

3.4.5 Linearni optični računalnik (LOQC)

Fotoni imajo kar nekaj pripravnih lastnosti, ki so obetavne za uporabo v obliki kubitov, kjer kvantno informacijo nosijo v polarizaciji. Poleg tega jih lahko po optičnih vlaknih pošiljamo na velike razdalje praktično brez večjih izgub informacije. Relativno preprosto je ustvariti tudi prepletena kvantna stanja na vhodu. Kar pa se izkaže za težavno je to, kako pripravimo fotone do tega, da med sabo interagirajo, kar je nujno potrebno za izvajanje kvantnih algoritmov.

To težavo lahko odpravimo z uporabo nelinearnih optičnih komponent, kar pa še zmeraj zagotovi, da bo med sabo interagiralo le malo število fotonov, torej bomo potrebovali veliko ponovitev poskusa, da bi dobili iskane izide. To težavo so že v letu 2001 rešili E. Knill, R. Laflamme in G. Milburn, ki so ugotovili, da lahko kvantni računalnik naredijo brez interakcij med fotoni [28]. Tako so na sistemu z linearnimi optičnimi komponentami s prepletenimi stanji na vhodu in s specifičnimi meritvami na nekaterih od fotonov dosegli željene izide. Tak pristop imenujemo linearno optično kvantno računalništvo ali v izvirniku *linear optical quantum computing* (LOQC). Velika prednost je, da lahko uporabimo veliko poznanega optičnega formalizma za zrcala, žarkovne delilnike, filtre, poleg tega pa imamo tudi zelo dovršene detektorje fotonov.

Kot zgled si poglejmo, kako z optičnim komponentam prirejeno matriko tvorimo kvantna vrata, na primer takšna, za tvorbo superpozicije stanj. Za lažjo predstavo vzamemo kar linearni polarizator s prepustno smerjo za kot 45°, ki ga opišemo z matriko $M = \frac{1}{2}\begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$, in skozenj spustimo polarizirano svetlobo zapisano z Jonesovim vektorjem $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Na ta način dobimo superpozicijo stanj $\frac{1}{2}(|0\rangle + |1\rangle)$, enak rezultat pa bi dobili tudi za vhodno stanje $|0\rangle$. Shema takšnega poskusa je predstavljena na sliki 9. Podobno pa lahko z zrcalom in žarkovnim delilnikom tvorimo Hadamardova vrata, ki smo jih predhodno uporabili za tvorbo superpozicije.



Slika 9. Shema delovanja linearnega polarizatorja M pod kotom $\phi = 45°$ na polarizirano svetlobo.

Slabša plat linearnih optičnih računalnikov je, da potrebujemo veliko število vhodnih fotonov in relativno veliko število linearnih optičnih komponent. Pomembno se je zavedati, da so takšni procesi nedeterministični in je potrebno poskuse velikokrat ponoviti, glavni vir napake pa ni dekoherenca, ki praktično ni prisotna, ampak absorbcija.

LOQC računalniki že vrsto let izkazujejo svoj velik potencial, v letošnjem akademskem letu pa je prišlo do bolj odmevnega preboja, ki so ga decembra 2020 kitajski znanstveniki objavili v reviji Science in s tem pokazali kvantno prevlado na problemu vzorčenja bozonov, kjer z vzorčenjem iz verjetnostne porazdelitve sipanih bozonov poskušamo oceniti pričakovano vrednost permanente matrike [29]. Pojmu kvantne prevlade lahko sicer na konkretnem problemu ustrezajo različne tehnične definicije, vendar gre v osnovi za to, da lahko kvantni računalnik reši izbrani problem, ki ga noben klasični ne bi v uresničljivem času. Pravimo, da kvantni računalnik prinese superpolinomsko pospe-

šitev algoritma na klasičnem računalniku oz. da je razlika časovne zahtevnosti večja od polinomske. Da so uspešno zadostili temu kriteriju, so znanstveniki zasnovali optični sistem Jiuzhang, ki ima 100 vhodov in izhodov, 300 žarkovnih delilnikov ter 75 zrcal. Velikost izhodnega prostora stanj je 10^{30}, njegova hitrost vzorčenja pa je približno 10^{14}-krat večja kot na superračunalnikih. Zadnja vrednost je izračunana glede na japonski superračunalnik Fugaku, ki bi, če pretvorimo v leta, potreboval nekaj več kot 600 milijonov let za rešitev tega problema.

4. Zaključek

Po dvajsetih letih izrazitega napredka in razglasitve kvantne prevlade v okviru nekaterih problemov, se bo kvantno računalništvo zagotovo skokovito razvijalo tudi v prihodnje, predvsem z različnimi še bolj izpopolnjenimi načini izdelave, kjer sem nekatere izmed najbolj perspektivnih predstavil v članku. Področje privlači tudi velike vlagatelje, kot sta IBM in Google, zato si lahko v bližnji prihodnosti obetamo še več presenetljivih dosežkov ter zanimivih odkritij.

V zadnjem času se veliko raziskuje tudi na področju kvantnega strojnega učenja [30]. Velik potencial le-tega se kaže na primer za statistično fiziko, fiziko kondenzirane snovi in za fiziko delcev, kjer je na primer potrebno obdelati ogromne količine podatkov, če želimo poiskati korelacije med začetnimi in končnimi delci, ki nastanejo preko neperturbativnih procesov. V ta namen bi na kvantnem računalniku lahko implementirali tenzorsko nevronsko mrežo (TN). Prednost tenzorskih nevronskih mrež pred standardnimi metodami, kot so globoke nevronske mreže (DNN) in pospešena odločitvena drevesa (BDT), je, da lahko kvantno navdahnjene TN izkoristijo kvantno naravo problema bolje, kot to na primer počnejo DNN [31]. Poleg tega imajo TN izjemno učinkovit način za merjenje korelacij in križne entropije ter omogočajo veliko stiskanje nevronske mreže praktično brez izgub. Takšne mreže bi torej bilo mogoče implementirati na kvantne računalnike v bližnji prihodnosti, s trenutno dosegljivimi visokimi vrednostmi stopnje šuma na precej omejenem številu kubitov [30].

LITERATURA

[1] J. v. Neumann, *Mathematische Grundlagen der Quantenmechanik*, Monatshefte für Mathematik und Physik **40**, A31 (1933).

[2] S. Wiesner, *Conjugate coding*, ACM SIGACT News **15**, 78 (1983).

[3] A. Holevo, *The capacity of the quantum channel with general signal states*, IEEE Transactions on Information Theory **44**, 269 (1998).

[4] D. Kafri and S. Deffner, *Holevo's bound from a general quantum fluctuation theorem*, Physical Review A **86** (2012).

[5] A. Einstein, B. Podolsky, and N. Rosen, *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?*, Physical Review **47**, 777 (1935).

[6] *Predavanja iz kvantne optike na univerzi Humboldt, poglavje 6: kvantna prepletenost*, Spletna stran: https://www.physik.hu-berlin.de/de/nano/lehre/quantenoptik08/Chapter6, [ogled: 16. 3. 2021].

[7] A. K. J. Preskill, *Predavanja iz kvantnega računalništva na univerzi Calteh, poglavje 4: kvantna prepletenost*, Spletna stra: http://theory.caltech.edu/ preskill/ph229/notes/chap4.pdf, [ogled: 20. 3. 2021].

[8] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, *Experimental quantum teleportation*, Nature **390**, 575 (1997).

[9] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, 2010.

[10] P. Niemann, A. Gupta, and R. Drechsler, *T-depth Optimization for Fault-Tolerant Quantum Circuits*, in *2019 IEEE 49th International Symposium on Multiple-Valued Logic (ISMVL)*, IEEE, 2019.

[11] D. P. DiVincenzo, *The Physical Implementation of Quantum Computation*, Fortschritte der Physik **48**, 771 (2000).

[12] D. S. Abrams and S. Lloyd, *Quantum Algorithm Providing Exponential Speed Increase for Finding Eigenvalues and Eigenvectors*, Physical Review Letters **83**, 5162 (1999).

[13] A. Peres, *Reversible logic and quantum computers*, Physical Review A **32**, 3266 (1985).

[14] A. M. Steane, *Error Correcting Codes in Quantum Theory*, Physical Review Letters **77**, 793 (1996).

[15] R. Žitko, *Kvantne in računalniške tehnologije*, DMFA, Ljubljana, 2017.

[16] J. Strnad, *Fizika, 4. del*, DMFA, Ljubljana, 2018.

[17] J. Jones, *Nuclear Magnetic Resonance Quantum Computation*, Spletna stran: https://nmr.physics.ox.ac.uk/pdfs/lhnmrqc.pdf, [ogled: 15. 3. 2021].

[18] I. P. Gerothanassis, A. Troganis, V. Exarchou, and K. Barbarossou, *Nuclear magnetic resonance (NMR) spectroscopy: Basic principles and phenomena, and their applications to chemistry, biology and medicine, journal = Chem. Educ. Res. Pract.*, **3**, 229 (2002).

[19] S. Akama, *Elements of Quantum Computing*, Springer International Publishing, 2015.

[20] N. A. Gershenfeld and I. L. Chuang, *Bulk Spin-Resonance Quantum Computation*, Science **275**, 350 (1997).

[21] L. M. K. Vandersypen, M. Steffen, G. Breyta, C. S. Yannoni, M. H. Sherwood, and I. L. Chuang, *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*, Nature **414**, 883 (2001).

[22] D. G. Cory, M. D. Price, and T. F. Havel, *Nuclear magnetic resonance spectroscopy: An experimentally accessible paradigm for quantum computing*, Physica D: Nelectronicar Phenomena **120**, 82 (1998).

[23] *Earnshaw's theorem*, dostopno na: https://en.wikipedia.org/wiki/Earnshaw%27s_theorem, [ogledano: 14. 3. 2021].

[24] *Ion traps*, Spletna stran: https://en.wikipedia.org/wiki/Ion_trap, [ogled: 14. 3. 2021].

[25] J. Eschner, *Quantum computation with trapped ions*, dostopno na: https://www.icfo.eu/-images/publications/Proc.06-002.pdf, [ogledano: 20. 3. 2021].

[26] *Introduction to the D-Wave Quantum Hardware*, Spletna stran: https://www.dwavesys.com-/tutorials/background-reading-series/introduction-d-wave-quantum-hardware, [ogled: 1. 4. 2021].

[27] D. Loss and D. P. DiVincenzo, *Quantum computation with quantum dots*, Physical Review A **57**, 120 (1998).

[28] E. Knill, R. Laflamme, and G. J. Milburn, *A scheme for efficient quantum computation with linear optics*, Nature **409**, 46 (2001).

[29] H.-S. Zhong et al., *Quantum computational advantage using photons*, Science **370**, 1460 (2020).

[30] W. Huggins, P. Patil, B. Mitchell, K. B. Whaley, and E. M. Stoudenmire, *Towards quantum machine learning with tensor networks*, Quantum Science and Technology **4**, 024001 (2019).

[31] T. Felser, M. Trenti, L. Sestini, A. Gianelle, D. Zuliani, D. Lucchesi, and S. Montangero, *Quantum-inspired Machine Learning on high-energy physics data*, 2021.