

Kvantni logički sklopovi

Pavlić, Bruno

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Rijeka / Sveučilište u Rijeci**

Permanent link / Trajna poveznica: <https://um.nsk.hr/um:nbn:hr:194:714467>

Rights / Prava: [In copyright](#)/[Zaštićeno autorskim pravom.](#)

Download date / Datum preuzimanja: **2025-04-03**



Repository / Repozitorij:

[Repository of the University of Rijeka, Faculty of Physics - PHYRI Repository](#)



Sveučilište u Rijeci
Fakultet za Fiziku



Kvantni logički sklopovi

Bruno Pavlić

Diplomski rad

Rijeka, 2022.

Sveučilište u Rijeci
Fakultet za Fiziku
Diplomski studij Fizika i matematika



Bruno Pavlić

Kvantni logički sklopovi

Diplomski rad

Mentor: izv. prof. dr. sc. Zoran Kaliman

Rijeka, 2022.

Sažetak

Ovaj rad nadahnut je člankom *Quantum technology: the second quantum revolution*. Iznesen je rezultat John S. Bella kojim se odbacuje teorija skrivenih varijabli u kvantnoj mehanici i time se opovrgava teza Alberta Einsteina o *spooky-action at the distance* pri spregnutim česticama. Dan je pregled osnovnih pojmova kvantnog računanja. Uvodi se pojam qubita te reprezentacije istog na Blochovoj sferi. Definirana su najčešće korištena kvantna logička vrata i njihovo djelovanje te se izdvaja Cliffordova grupa unitarnih transformacija. Ističe se efikasnost korištenja kvantnih logičkih sklopova sastavljenih od vrata van Cliffordove grupe na kvantnom računalu, kao i rezultat o nemogućnosti kloniranja nepoznatog kvantnog stanja, ali moguća teleportacija istog. Korištenjem spomenutih kvantnih logičkih vrata, izvodi se Deutschov algoritam. Pomoću kvantnog Fourierovog transformata, prikazan je Shorov algoritam za faktorizaciju broja $N = 21$. Na kraju dan je osvrt na trenutni položaj kvantnog računala u odnosu na klasična te se objašnjava BB84 protokol.

Ključne riječi: **qubit, spregnutost, logička vrata, logički sklop, kvantni algoritam, kvantno računalo**

Sadržaj

| | | |
|----------|--|-----------|
| 1 | Uvod | 1 |
| 2 | Qubit | 3 |
| 2.1 | Mjerenje qubita | 3 |
| 2.2 | Blochova sfera | 5 |
| 2.3 | Sustavi sastavljeni od više qubita | 7 |
| 2.3.1 | Spregnuta stanja | 7 |
| 2.4 | Rad Einstein – Podolsky – Rosen | 8 |
| 2.4.1 | Bellova nejednakost | 10 |
| 3 | Kvantni logički sklopovi | 12 |
| 3.1 | Klasični logički sklopovi | 13 |
| 3.1.1 | Logička vrata I, AND | 13 |
| 3.1.2 | Logička vrata ILI, OR | 13 |
| 3.1.3 | Logička vrata NE, NOT | 14 |
| 3.1.4 | Logička vrata ekskluzivno ILI, XOR | 14 |
| 3.2 | Kvantni logički sklopovi | 14 |
| 3.2.1 | Paulijeva logička vrata | 14 |
| 3.2.2 | Hadamardova vrata | 17 |
| 3.2.3 | Operator faznog pomaka | 18 |
| 3.2.4 | Kvadratni korijen iz NOT vrata | 19 |
| 3.2.5 | C_{NOT} vrata | 19 |
| 3.2.6 | SWAP vrata | 23 |
| 3.3 | Univerzalnost kvantnog računala | 25 |
| 3.3.1 | Cliffordova grupa | 25 |
| 3.3.2 | Kvantno izvođenje klasičnih logičkih operacija | 27 |
| 3.4 | Kvantna teleportacija i <i>No-cloning</i> teorem | 28 |
| 3.4.1 | <i>No-cloning</i> teorem | 28 |
| 3.4.2 | Kvantna teleportacija | 29 |
| 4 | Kvantna računala i algoritmi | 32 |
| 4.1 | Deutschov algoritam | 32 |
| 4.2 | Shorov algoritam | 34 |
| 4.2.1 | Kvantni Fourierov transformat | 35 |
| 4.2.2 | Shorov algoritam za faktorizaciju | 36 |
| 4.3 | Budućnost kvantnih računala | 38 |
| 4.4 | Životni vijek qubita | 40 |

SADRŽAJ

| | |
|---------------------------|-----------|
| 5 Zaključak | 41 |
| A Metodčki dodatak | 42 |

1 Uvod

Početak novog stoljeća, dvojica kvantnih fizičara, Jonathan Dowling i Gerard J. Milburn [1] objavljuju članak *Quantum technology: the second quantum revolution* u kojem navode kako se civilizacija nalazi u sredini druge kvantne revolucije. Prva kvantna revolucija započela je pokušajem rješavanja problema zračenja crnog tijela, odnosno rješavanja problema „ultraljubičaste katastrofe“ kako je isti nazvao Paul Ehrnefest. Max Planck, vođen idejom kvantizirane energije oscilatora, izvodi relaciju za intenzitet zračenja crnog tijela u ovisnosti o frekvenciji zračenja i temperaturi. Godine 1924. godine na Sveučilištu u Parizu, pod mentorstvom Paula Langevina, fizičar plemićkog podrijetla Louis-Victor-Pierre-Raymond de Broglie, temeljeno na radu Maxa Plancka i Alberta Einsteina, u svojem doktoratu daje pretpostavku o valno – čestičnoj prirodi elektrona. Tri godine kasnije, L. Germer i C. J. Davisson dobivaju ogibnu sliku elektrona na kristalima, čime je de Broglieva pretpostavka dokazana. Werner Heisenberg, zajedno s M. Bornom i P. Jordanom objavljuju 1925. godine tri članka kojima su razvili matričnu mehaniku, u kojoj se fizičke veličine reprezentiraju matricama. Nadahnut de Broglievom hipotezom, 1926. godine austrijski fizičar Erwin Schrödinger objavljuje rad *An Undulatory Theory of the Mechanics of Atoms and Molecules* u kojem, želeći pobliže istražiti fenomen valne prirode tvari, uvodi jednadžbu propagacije vala, koja njemu u čast nosi ime Schrödingerova jednadžba:

$$\Delta\Psi + \frac{8 \cdot \pi^2 \cdot m}{h^2}(E - V)\Psi = 0.$$

Vremenski – ovisna Schrödingerova jednadžba je linearna diferencijalna jednadžba drugog reda po prostoru i prvog reda po vremenu:

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

gdje je $\hbar = \frac{h}{2\pi}$ reducirana Planckova konstanta. Rješenja Schrödingerove jednadžbe [2] su stacionarna stanja ¹ određene ukupne energije ² te je svaka linearna kombinacija rješenja Schrödingerove jednadžbe rješenje Schrödingerove jednadžbe. Dvije godine kasnije, u radu *The quantum theory of the electron*, engleski fizičar Paul Adrien Maurice Dirac kombinira specijalnu relativnost sa Schrödingerovom jednadžbom i dobiva relativističku valnu jednadžbu elektrona. Godine 1930., objavljuje knjigu *The Principles of Quantum Mechanics* u kojem pokazuje ekvivalentnost matrične i valne kvantne mehanike. Daljnji razvoj kvantne mehanike obilježile su rasprave tada vodećih fizičara o interpretacijama iste. 1935. godine, Albert Einstein, temeljeno na teoremu John von Neumanna, zajedno s Borisom Podolskim i Nathan Rosenom zaključuje kako valna funkcija ne može dati potpun opis realnosti. Tridesetak godina kasnije, John S. Bell, pronalazi grešku u von Neumannovom

¹Gustoća vjerojatnosti $|\Psi(x, t)|^2$ ne ovisi o vremenu.

²Svako mjerenje ukupne energije daje rezultat $\langle H \rangle = E$.

teoremu te odbacuje Einsteinovu teoriju skrivenih varijabli. Krajem drugog svjetskog rata, engleski matematičar Alan Turing, radio je na dešifriranju poruka sa *Enigme*, kriptografskog uređaja koji su koristile sile osovine, ponajviše Njemačka. Uspjeh Alana Turinga i suradnika pomogao je ubrzati okončanje drugog svjetskog rata te se upravo on smatra ocem računalnih znanosti. Već 1947. godine izumljen je tranzistor, za koji su 1956. trojica fizičara iz Bellova laboratorija, John Bardeen, Walter H. Brattain i William Shockley dobili Nobelovu nagradu za fiziku. Ubrzani razvoj tranzistora i njihovo smanjenje u veličini, koji se opisuje i Mooreovom zakonitosti³, doveo je do mikroskopskih integriranih krugova. Dakako, broj tranzistora u integriranom krugu može se povećavati do granice koju dopuštaju zakoni fizike, dakle, do tranzistora reda veličine atoma. Prva kvantna revolucija otkrila je ljudima stvarno lice prirode, a uloga druge kvantne revolucije je korištenjem znanja o kvantnim sistemima i istraživanjima fenomena kvantne mehanike primijeniti iste u informacijskim tehnologijama. Potrebno je ovladati kvantnim principima poput kvantizacije, Heisenbergova načela neodređenosti, superpozicije, tuneliranja, kvantne spregnutosti i dekoherencije u svrhu razvoja instrumenata i tehnologija. Sam cilj ovladavanja principa kvantne mehanike je kreiranje kvantnog računala, a čiji rad ovisi o preciznim mjerenjima (eng. *Quantum metrology*), mogućnosti ispravljanja grešaka (eng. *Quantum control*) te komunikacijskim protokolima (eng. *Quantum communication*). Smatra se kako je to računalo sposobno brže i točnije obavljati zadatke prijenosa informacija, a pruža mogućnosti sigurnije enkripcije podataka. Unazad nekoliko godina, razvoj kvantnih računala budi zanimanje šire publike, što se može očitati po naslovima znanstveno - popularnih stranica i časopisa. Velike tehnološke kompanije, poput Microsofta i IBM-a, ulažu znatna sredstva u razvoj te tehnologije, tako je 2019. godine tvrtka IBM predstavila je prvo komercijalno dostupno kvantno računalo *IBM Quantum System One*. Sve to, utječe na mišljenje kako je ta tehnologija ovdje, spremna za korištenje, ali ipak njena sposobnost i upotreba ne potvrđuju predstavljeno. 2022. godine Nobelova nagrada za fiziku dodijeljena je Alain Aspectu, John F. Clauseru te Walnut Creeku za eksperimente sa spregnutim fotonima, utvrđivanje kršenja Bellove nejednakosti te uvođenje značajnih inovacija u kvantnim informatičkim znanostima.

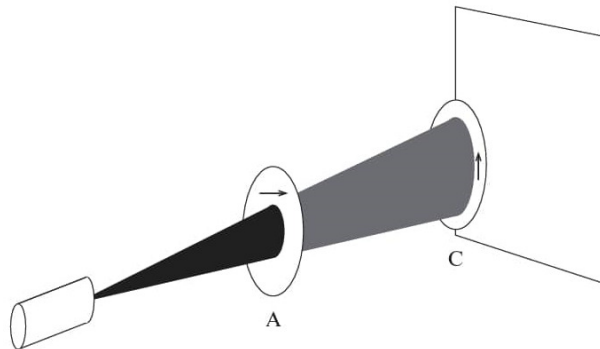
³1965. godine, Gordon Moore je opazio kako se svaki dvije godine broj tranzistora u integriranom krugu udvostruči.

2 Qubit

Klasično, **bit** (eng. *Basic Indissoluble information uniT*) brojčana je jedinica količine informacija, a također označava odabir između dva brojčana stanja 0 ili 1 (*Binary digiT*), odnosno njima svaku alternativu. U kvantnom slučaju, odgovarajuća jedinica informacije zove se **qubit**. To je kvantnomehanički sustav koji se može izmjeriti u jednom od dva stanja, koja se najčešće u Diracovoj bra-ket notaciji označavaju s $|0\rangle$ i $|1\rangle$. Fizičku realizacija kvantnog bita moguće je ostvariti, na primjer, spinom elektrona (spin gore i spin dolje), stanjem polarizacije fotona i nuklearnim spinom atoma. Osnovna je razlika između bita i qubita ta što qubit može biti u superpoziciji stanja prije mjerenja, dok bit može biti u samo jednom od dva stanja, 0 ili 1. I više, qubite možemo mjeriti na više načina, ali samo jednom, dok klasične bitove možemo mjeriti samo na jedan način, ali više puta.

2.1 Mjerenje qubita

Jedan od najjednostavnijih kvantnomehaničkih mjernih uređaja su polarizacijski filtri. Postavimo li ispred izvora svjetlosti dva polarizacijska filtra (Slika 1.) [3], međusobno okomite polarizacije, na projekcijskom platnu se ne opaža svjetlost, odnosno vjerojatnost da se foton nađe između dva filtra te kasnije između drugog filtra i platna je nula. No, kada bi se između

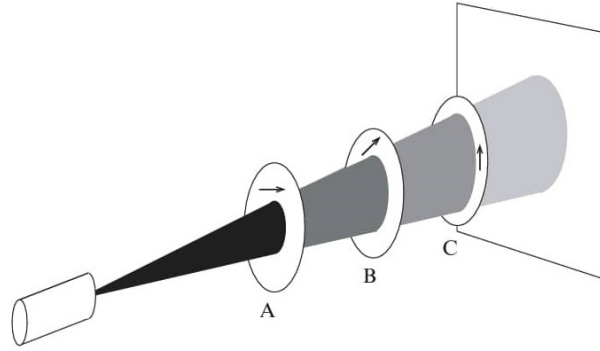


Slika 1: Filtri međusobno okomite polarizacije

dva filtra postavio treći (Slika 2.), polarizacije 45° u odnosu na oba, na platnu opažamo svjetlost. Nastavimo li tako i dalje s dodavanjem filtera, primijetimo porast intenziteta svjetla što se opaža na platnu. Ako proizvoljnu polarizaciju zapišemo kao

$$|\psi\rangle = \alpha|\uparrow\rangle + \beta|\rightarrow\rangle,$$

tako da vrijedi uvjet normalizacije $\alpha^2 + \beta^2 = 1$ te foton dolazi do horizontalnog polarizacijskog filtra, $|\uparrow\rangle$, vjerojatnost transmisije iznosi α^2 , a apsorpcije β^2 . Time je prolaskom kroz filter svjetlost horizontalno polarizirana. Vjerojatnost prolaza kroz vertikalno polarizirani filter, $|\rightarrow\rangle$ iznosi 0. Neka je sada umetnut treći filter između prva dva, tako da s oboje zatvara



Slika 2: 3 polarizacijska filtera

kut mjere 45° , $|\nearrow\rangle$. Horizontalno polarizirano svjetlo koje je prošlo kroz prvi filter, možemo zapisati pomoću para ortogonalnih smjerova $|\nearrow\rangle$ i $|\searrow\rangle$ kao

$$|\rightarrow\rangle = \frac{1}{\sqrt{2}}(|\nearrow\rangle - |\searrow\rangle).$$

Time smo prešutno promijenili bazu. Tako predočeno, jasno je kako fotoni koji su prošli kroz filter 1 imaju vjerojatnost 0.5 da prođu kroz drugi filter. Time fotoni koji su prošli oba filtera imaju polarizaciju u smjeru vektora baze $|\nearrow\rangle$. Kako vrijedi

$$|\nearrow\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle + |\rightarrow\rangle),$$

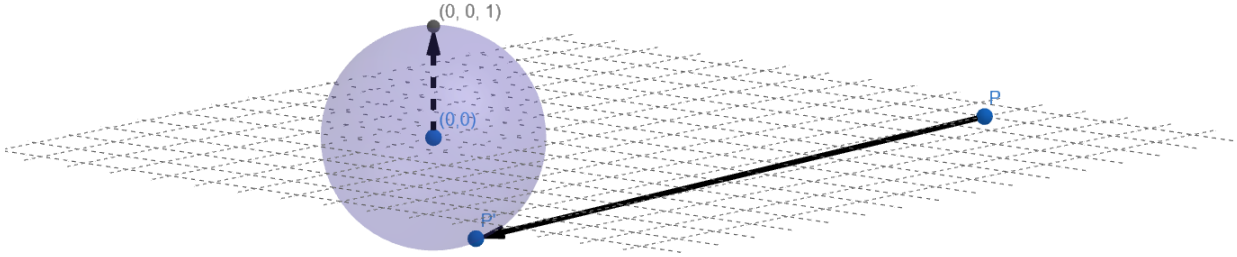
kroz treći, vertikalno polarizirani filter, ipak prolazi svjetlost, zato što postoji vertikalna komponenta vektora $|\nearrow\rangle$. Skup svih mogućih stanja kvantnomehaničkog sistema zove se prostor stanja. Nadalje, vrijedi da qubit može biti opisan svakim kvantnomehaničkim sistemom koji se može reprezentirati dvodimenzionalnim kompleksnim vektorskim prostorom, uz uvjet raspoznavanja dva linearno nezavisna vektora, $|0\rangle$ i $|1\rangle$. I više, ako zahtijevamo normiranost, dolazimo do skupa ortonormiranih vektora, odnosno baze prostora. Uobičajeno, za vektore baze uzimamo

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Kažemo da je kvantno stanje $|\Psi\rangle$ superpozicija baznih stanja, odnosno elemenata baze $\{|0\rangle, |1\rangle\}$, ako je ono netrivialna linearna kombinacija vektora baze, odnosno vrijedi

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle, \alpha \neq 0, \beta \neq 0.$$

Svaki mjerni uređaj, prema postulatima kvantne mehanike, mora imati dva intrizično određena stanja mjerenja, kojima odgovaraju ortonormirani vektori $|a\rangle$ i $|b\rangle$ koji čine bazu vektorskog prostora. Tako na primjeru s polarizacijskim filterima, koje shvaćamo kao mjerne uređaje, treći filter, koji je zatvarao kut mjere 45° s prva dva, možemo shvatiti kao uređaj s bazom $\{|\nearrow\rangle, |\searrow\rangle\}$. Odabir baze je nužan kako bi mjerenjem došli do ispravnog, determinističkog



Slika 3: Stereografska projekcija, 1. Ishodište kompleksne ravnine $(0,0)$ preslika se u sjeverni pol, $(0,0,1)$. Svakoj točki kompleksne ravnine P pridružena je jedinstvena točka P' na jediničnoj sferi.

rezultata. Mjerenjem dolazi do kolapsa valne funkcije, što znači da se mijenja stanje kvantnog sistema. Valja napomenuti kako mjerenjem možemo iz qubita saznati samo jedan bit klasične informacije.

2.2 Blochova sfera

Cilj je pronaći odgovarajuću geometrijsku reprezentaciju prostora stanja jednog qubita. Neka je bijektivno preslikavanje τ dano s,

$$\begin{aligned}\tau : c_1 |0\rangle + c_2 |1\rangle &\mapsto \mathcal{C} = \frac{c_2}{c_1} \in \mathbb{C} \\ \tau : |1\rangle &\mapsto \infty\end{aligned}$$

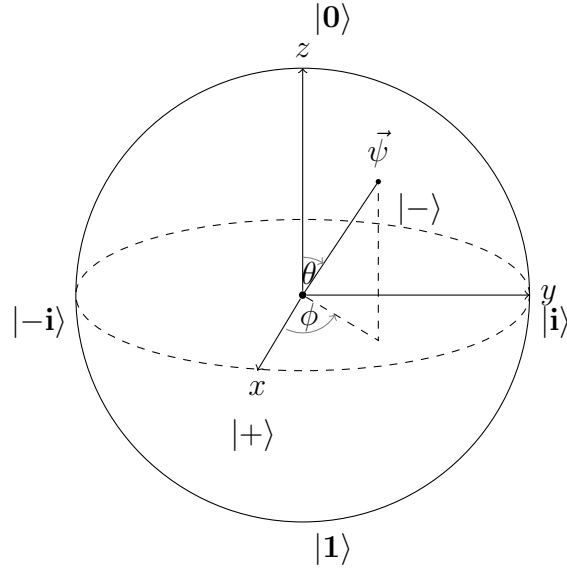
Ako dva ili više vektora predstavljaju istu realizaciju kvantnog stanja, kažemo da se oni razlikuju do na globalnu fazu, imaginarnu jedinicu $e^{i\phi}$, odnosno vrijedi $|x\rangle = e^{i\phi} |x'\rangle$, pa je moguće napraviti redukciju na kvocijentni prostor. S druge strane, relativna faza označava kut u kompleksnoj ravnini između dva kompleksna broja, c_1 i c_2 . Globalna faza nema fizičkog značaja za kvantni sistem, dok dva stanja s različitim relativnim fazama označavaju realizacije dvaju različitih kvantna stanja. Svakom kompleksnom broju $\mathcal{C} = a + bi$ moguće je pridružiti točku (x, y, z) na jediničnoj sferi koristeći stereografsku projekciju Π (slika 3.) [3],

$$\begin{aligned}\Pi : (a, b) &\mapsto \left(\frac{2a}{|z|^2 + 1}, \frac{2b}{|z|^2 + 1}, \frac{1 - |z|^2}{|z|^2 + 1} \right) \\ \Pi : \infty &\mapsto (0, 0, -1)\end{aligned}\tag{1}$$

Time su jednoznačno određene točke, odnosno stanja na sferi, a neke od istaknutijih su

$$\begin{aligned}\Pi(|0\rangle) &= (0, 0, 1), & \Pi(|1\rangle) &= (0, 0, -1), & \Pi(|+\rangle) &= (1, 0, 0), \\ \Pi(|-\rangle) &= (-1, 0, 0), & \Pi(|i\rangle) &= (0, 1, 0), & \Pi(|-i\rangle) &= (0, -1, 0).\end{aligned}$$

Time je stanje $|0\rangle$ sjeverni pol Blochove sfere, a stanje $|1\rangle$ južni pol Blochove sfere. Neka je sada na Blochovoj sferi odabrana proizvoljna točka, odnosno stanje jednog qubita. Kut



Slika 4: Blochova sfera

što ga sa \mathbf{z} -osi zatvara radij-vektor te točke označimo s θ , $\theta \in [0, \pi]$ a kut što ga s x -osi zatvara ortogonalna projekcija radij-vektora točke na xy -ravninu s ϕ , $\phi \in [0, 2\pi]$. Tada se proizvoljno stanje može zapisati kao

$$|\Phi\rangle = e^{-i\frac{\phi}{2}} \cos \frac{\theta}{2} |0\rangle + e^{i\frac{\phi}{2}} \sin \frac{\theta}{2} |1\rangle. \quad (2)$$

Vektori ortonormirane baze Hilbertovog prostora su parovi antipodalnih točaka na Blochovoj sferi pa tako skup $\{|+\rangle, |-\rangle\}$ predstavlja Hadamardova baza, a skup $\{|0\rangle, |1\rangle\}$ standardna baza. Primijetimo kako antipodalne točke imaju suprotne predznake komponentata, a kako vrijede relacije $\theta = \arccos \frac{z}{r}$ i $\phi = \arctan \frac{y}{x}$, prilikom zrcaljenja oko ishodišta, mjera kuta ϕ se ne mijenja, dok se mjera kuta θ uveća za π . Tako dva antipodalna stanja pišemo kao:

$$\begin{aligned} |\Phi_1\rangle &= e^{-i\frac{\phi}{2}} \cos \frac{\theta}{2} |0\rangle + e^{i\frac{\phi}{2}} \sin \frac{\theta}{2} |1\rangle, \\ |\Phi_2\rangle &= e^{-i\frac{\phi}{2}} \cos \frac{\theta + \pi}{2} |0\rangle + e^{i\frac{\phi}{2}} \sin \frac{\theta + \pi}{2} |1\rangle. \end{aligned}$$

Sada je skalarni umnožak:

$$\begin{aligned} \langle \Phi_1 | \Phi_2 \rangle &= \left(e^{i\frac{\phi}{2}} \cos \frac{\theta}{2} \langle 0| + e^{-i\frac{\phi}{2}} \sin \frac{\theta}{2} \langle 1| \right) \left(e^{-i\frac{\phi}{2}} \cos \frac{\theta + \pi}{2} |0\rangle + e^{i\frac{\phi}{2}} \sin \frac{\theta + \pi}{2} |1\rangle \right) \\ \langle \Phi_1 | \Phi_2 \rangle &= \cos \frac{\theta}{2} \cos \frac{\theta + \pi}{2} \langle 0|0\rangle + \sin \frac{\theta}{2} \sin \frac{\theta + \pi}{2} \langle 1|1\rangle \\ \langle \Phi_1 | \Phi_2 \rangle &= \cos \frac{\theta}{2} \cos \frac{\theta + \pi}{2} + \sin \frac{\theta}{2} \sin \frac{\theta + \pi}{2} \\ \langle \Phi_1 | \Phi_2 \rangle &= \cos -\frac{\pi}{2} \\ \langle \Phi_1 | \Phi_2 \rangle &= 0 \end{aligned}$$

Skalarni umnožak stanja $|\Phi_1\rangle$ s $|\Phi_1\rangle$ je:

$$\begin{aligned}\langle\Phi_1|\Phi_1\rangle &= \left(e^{i\frac{\phi}{2}} \cos \frac{\theta}{2} \langle 0| + e^{-i\frac{\phi}{2}} \sin \frac{\theta}{2} \langle 1| \right) \left(e^{-i\frac{\phi}{2}} \cos \frac{\theta}{2} |0\rangle + e^{i\frac{\phi}{2}} \sin \frac{\theta}{2} |1\rangle \right) \\ \langle\Phi_1|\Phi_1\rangle &= \cos^2 \frac{\theta}{2} + \sin^2 \frac{\theta}{2} \\ \langle\Phi_1|\Phi_1\rangle &= 1.\end{aligned}$$

Skalarni umnožak stanja $|\Phi_2\rangle$ s $|\Phi_2\rangle$ je:

$$\begin{aligned}\langle\Phi_2|\Phi_2\rangle &= \left(e^{i\frac{\phi}{2}} \cos \frac{\theta + \pi}{2} \langle 0| + e^{-i\frac{\phi}{2}} \sin \frac{\theta + \pi}{2} \langle 1| \right) \left(e^{-i\frac{\phi}{2}} \cos \frac{\theta + \pi}{2} |0\rangle + e^{i\frac{\phi}{2}} \sin \frac{\theta + \pi}{2} |1\rangle \right) \\ \langle\Phi_1|\Phi_1\rangle &= \cos^2 \frac{\theta + \pi}{2} + \sin^2 \frac{\theta + \pi}{2} \\ \langle\Phi_1|\Phi_1\rangle &= 1.\end{aligned}$$

Time je pokazano da stanja pridružena antipodalnim točkama Blochove sfere čine ortonormiranu bazu Hilbertovog prostora.

2.3 Sustavi sastavljeni od više qubita

Klasično, „snaga“ procesora raste linearno s porastom broja tranzistora. U odnosu na klasične procesore, „snaga“ kvantnih procesora raste eksponencijalno s porastom broja qubita. U 2^n -dimenzionalnom Hilbertovom prostoru $V_1 \otimes V_2 \otimes \dots \otimes V_n$ standardno odabiremo ortonormiranu bazu

$$\mathcal{B} = \{|v_1 v_2 \dots v_n\rangle = |v_1\rangle \otimes |v_2\rangle \otimes \dots \otimes |v_n\rangle \mid v_i = 0, 1, \forall i \in \{1, 2, \dots, n\}\}. \quad (3)$$

Za $n = 2$, uzimamo standardno bazu

$$\mathcal{B} = \{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}. \quad (4)$$

Tada se svaki vektor Φ iz Hilbertovog prostora $V_1 \otimes V_2$ može prikazati kao linearna kombinacija vektora baze

$$\Phi = \alpha |00\rangle + \beta |01\rangle + \gamma |10\rangle + \delta |11\rangle, \alpha, \beta, \gamma, \delta \in \mathbb{C},$$

tako da vrijedi uvjet normalizacije

$$|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1.$$

2.3.1 Spregnuta stanja

Valna funkcija stanja nekog sustava prilikom mjerenja kolapsira u jedno od dozvoljenih stanja i time je iz nje moguće izvući samo jednu klasičnu informaciju. Kako bismo pomoću qubita saznali sve pohranjene informacije, koristimo se parovima spregnutih čestica. Prostor

stanja sustava od n qubita ima $2^n - 1$ kompleksnu dimenziju [3], odnosno potrebno je $2^n - 1$ kompleksnih brojeva kako bi se opisao sustav n qubita. Time je jednoznačan prikaz kvantnog stanja ostvaren ako je jedan od skalara α_i realan broj različit od nule, u prikazu

$$\Phi = \alpha_0 |0 \cdots 00\rangle + \alpha_1 |0 \cdots 01\rangle + \cdots + \alpha_{2^n-1} |1 \cdots 11\rangle. \quad (5)$$

Kažemo da je stanje Φ u Hilbertovom prostoru $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ prostora separabilno, ako se ono može zapisati kao tenzorski produkt $\Phi = |v_1\rangle \otimes \cdots \otimes |v_n\rangle$, inače kažemo da je stanje spregnuto. Kod spregnutih stanja, cjelinu nije moguće opisati isključivo pomoću dijelova od kojih je sastavljena. Primjetimo, zapis iz 3 predstavlja nespregnuto stanje. Umjesto ranije spomenute standardne baze Hilbertovog prostora $V_1 \otimes V_2$, koristi se i Bellova baza

$$\mathcal{B}' = \left\{ \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \right\}.$$

Vektori Bellove baze su spregnuti. Uzmimo za primjer $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ i pretpostavimo da postoji dekompozicija

$$\begin{aligned} \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) &= (\alpha |0\rangle + \beta |1\rangle) \otimes (\gamma |0\rangle + \delta |1\rangle), \\ \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) &= \alpha\gamma |00\rangle + \alpha\delta |01\rangle + \beta\gamma |10\rangle + \beta\delta |11\rangle. \end{aligned}$$

Slijedi:

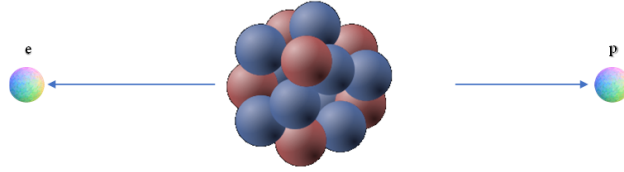
$$\begin{aligned} \alpha \cdot \gamma &= 0 & \alpha \cdot \delta &= \frac{1}{\sqrt{2}} \\ \beta \cdot \delta &= 0 & \beta \cdot \gamma &= -\frac{1}{\sqrt{2}} \end{aligned}$$

što dovodi do kontradikcije. Zaključujemo da je stanje $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ spregnuto. S druge strane, vektori standardne baze su separabilni, pa tako vrijedi

$$\begin{aligned} |00\rangle &= |0\rangle \otimes |0\rangle, & |01\rangle &= |0\rangle \otimes |1\rangle, \\ |10\rangle &= |1\rangle \otimes |0\rangle, & |11\rangle &= |1\rangle \otimes |1\rangle. \end{aligned}$$

2.4 Rad Einstein – Podolsky – Rosen

1935. godine u časopisu *Physical review*, A. Einstein, B. Podolsky i N. Rosen objavljuju rad [4] *Može li se kvantno-mehanički opis fizičke stvarnosti smatrati kompletnim?*. U radu, kompletnost fizičke teorije dana je zahtjevom: „Svaki element fizičke realnosti mora imati odgovarajući element u fizičkoj teoriji.“ Polazi se od pretpostavke da valna funkcija u potpunosti može opisati sustav. Također, prema postulatima kvantne mehanike fizičke observable reprezentiraju se hermitskim operatorima. Prema Heisenbergovoj relaciji za nekomutirajuće



Slika 5: Emisija para elektron - pozitron iz nestabilne jezgre

observable slijedi kako nije moguće istovremeno točno odrediti očekivane vrijednosti oba operatora, na primjer operator položaja i operator impulsa, što je poznata relacija dana s

$$\Delta x_i \Delta y_j \geq \frac{\hbar}{2} \delta_{ij}. \quad (6)$$

Prema njihovom misaonom eksperimentu, sustavi 1 i 2 međudjeluju u intervalu $0 \leq t \leq T$. Stanja oba sustava za $t < 0$ su poznata, stanje združenog sustava 1 + 2 za $t > T$ određuje se rješavanjem Schrödingerove jednačbe, a stanja pojedinačnih sustava 1 i 2 za $t > T$ nije moguće odrediti radi kolapsa valne funkcije. U radu, dolazi se do zaključka kako je moguće odrediti istovremeno odrediti svojstvene vrijednosti nekomutirajućih fizičkih veličina, te zaključuju kako valna funkcija ne pruža potpuni opis fizičke realnosti. Zamislimo nestabilnu jezgru koja prilikom raspada stvara par elektron – pozitron [5]. Kako je promjena angularnog momenta jezgre jednaka nuli, tada prema zakonu očuvanja angularnog momenta stvoreni par elektron – pozitron mora imati spinove suprotnih smjerova. Neka je dvoje promatrača, Alice i Bob na relativističkim udaljenostima, svaki s mjernim uređajem. Uređaji mjere iznos spina u smjerovima \hat{a} i \hat{b} . Valna funkcija para elektron – pozitron dana je s

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|e+\rangle |p-\rangle - |e-\rangle |p+\rangle). \quad (7)$$

Alice pomoću mjernog uređaja odredi kako je pozitron spina gore, odnosno u odnosu na svoj smjer mjerenja dobije vrijednost $+\frac{1}{2}$. Time je urušila valnu funkciju te ona postaje

$$|\Psi\rangle = |e-\rangle |p+\rangle.$$

Zapišemo li pozitivan smjer mjerenja Bobovog uređaja pomoću polarnih kutova θ i ϕ , gdje je θ kut između pozitivnih dijelova vektora mjernih uređaja Alice i Boba

$$|\hat{b}+\rangle = \sin \frac{\theta}{2} e^{i\frac{\phi}{2}} |p+\rangle + \cos \frac{\theta}{2} e^{-i\frac{\phi}{2}} |p-\rangle,$$

slijedi da je vjerojatnost da i Bob u odnosu na svoj smjer mjerenja dobije vrijednost $+\frac{1}{2}$ jednaka

$$P(+\hat{b}) = |\langle \hat{b}+ | p+\rangle|^2 = \sin^2 \frac{\theta}{2},$$

a vjerojatnost da mjerenjem utvrdi vrijednost $-\frac{1}{2}$ jednaka

$$P(-\hat{b}) = 1 - \sin^2 \frac{\theta}{2} = \cos^2 \frac{\theta}{2}.$$

Primijetimo, odaberu li Alice i Bob isti smjer mjerenja, $\theta = 0^\circ$ pa je vjerojatnost da Bob izmjeri vrijednost $-\frac{1}{2}$ jednaka

$$P(-\hat{b}) = \cos^2 0 = 1.$$

Kako prema postulatima specijalne teorije relativnosti klasična informacija ne može putovati brzinom većom od brzine svjetlosti, Albert Einstein [6] je zagovarao stajalište kako je informacija intrinzično sadržana u česticama prilikom napuštanja nestabilne jezgre, odnosno da postoji lokalna skrivena varijabla koja u sebi nosi tu, promatraču nepoznatu informaciju do mjerenja.

2.4.1 Bellova nejednakost

Prema [5] i [7], pretpostavimo li da postoji funkcija očekivane vrijednosti spina elektrona duž osi \hat{a} tako da je $\sigma_e \equiv \sigma_e(\mathcal{W}, \hat{a})$, gdje je \mathcal{W} n -vektor skrivenih varijabli. Slijedi:

$$\sigma_e(\mathcal{W}, \hat{a}) = -\sigma_p(\mathcal{W}, \hat{a}) = \pm \frac{1}{2}.$$

Očekivana vrijednost umnoška $\sigma_e(\mathcal{W}, \hat{a}) \cdot \sigma_p(\mathcal{W}, \hat{b})$ dana je s

$$\int d^n \mathcal{W} \rho(\mathcal{W}) \cdot \sigma_e(\mathcal{W}, \hat{a}) \cdot \sigma_p(\mathcal{W}, \hat{b}).$$

Neka je \hat{c} treći vektor duž kojeg je moguće obaviti mjerenje. Koristeći činjenicu da je $\sigma_e^2(\mathcal{W}, a) = \sigma_p^2(\mathcal{W}, a) = \frac{1}{4}$ slijedi

$$\langle \sigma_e(\hat{a})\sigma_e(\hat{b}) \rangle - \langle \sigma_e(\hat{a})\sigma_e(\hat{c}) \rangle = - \int d^n \mathcal{W} \rho(\mathcal{W}) \cdot \sigma_e(\mathcal{W}, \hat{a}) \cdot \sigma_p(\mathcal{W}, \hat{b})(1 - 4\sigma_e(\mathcal{W}, \hat{b})\sigma_e(\mathcal{W}, \hat{c})).$$

Kako je $|\sigma_e(\mathcal{W}, \hat{a}) \cdot \sigma_p(\mathcal{W}, \hat{b})| \leq \frac{1}{4}$ slijedi Bellova nejednakost:

$$|\langle \sigma_e(\hat{a})\sigma_e(\hat{b}) \rangle - \langle \sigma_e(\hat{a})\sigma_e(\hat{c}) \rangle| \leq \frac{1}{4} \left(1 + 4 \langle \sigma_e(\hat{b})\sigma_e(\hat{c}) \rangle_{\mathcal{W}} \right) \quad (8)$$

Kvantnomehanički, očekivana vrijednost umnoška

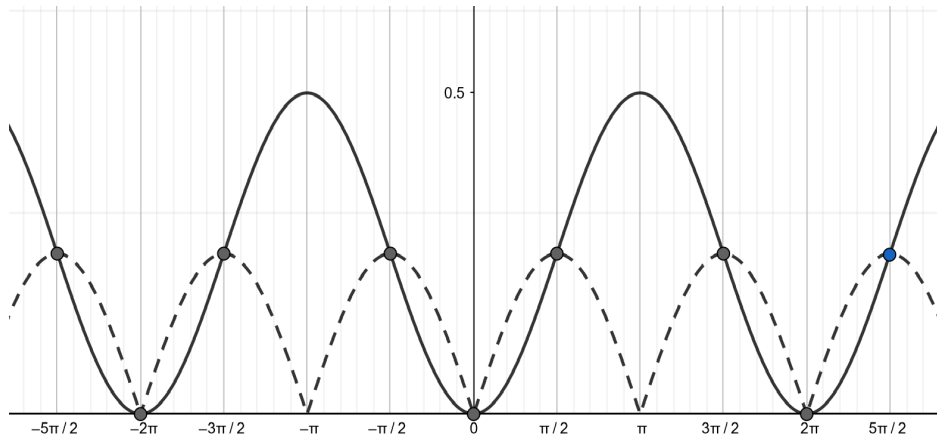
$$\langle \sigma_e(\hat{a})\sigma_e(\hat{b}) \rangle = -\frac{1}{4} \cos \theta = -\frac{1}{4} \hat{a} \cdot \hat{b}.$$

Bellova nejednakost mora vrijediti za svaki izbor vektora $\hat{a}, \hat{b}, \hat{c}$ pa tako i za vekore:

$$\begin{aligned} \hat{a} \cdot \hat{b} &= 0, \\ \hat{c} &= \sin \phi \hat{a} + \cos \phi \hat{b}, \end{aligned}$$

Dobivena nejednakost je tada:

$$\left| \frac{1}{4} \sin \phi \right| \leq \frac{1}{4} (1 - \cos \phi), \quad (9)$$



Slika 6: Grafički prikaz nejednadžbe 9 - isprekidanom linijom prikazan je graf funkcije $|\frac{1}{4} \sin \phi|$, a punom linijom prikazan je graf funkcije $\frac{1}{4}(1 - \cos \phi)$.

što vrijedi za intervale

$$\left\langle \frac{\pi}{2} + 2k\pi, \frac{3\pi}{2} + 2k\pi \right\rangle, k \in \mathbb{Z},$$

odnosno ne vrijedi za intervale

$$\left\langle -\frac{\pi}{2} + 2k\pi, \frac{\pi}{2} + 2k\pi \right\rangle, k \in \mathbb{Z}.$$

Time je pokazano kako je kvantna mehanika nekonzistentna s teorijom skrivenih varijabli. Spregnuta stanja i njihova mjerenja nije moguće objasniti pomoću teorije skrivenih varijabli. Eksperimentalni podaci dobiveni od 1972. godine pa nadalje su u skladu s mjerenjima predviđenim kvantnom mehanikom, no radi tehničkih ograničenja, tek unazad dvadeset godina dobiveni su službeni rezultati poput rada [8] *Experimental loophole-free violation of a Bell inequality using entangled electron spins separated by 1.3 km* koji potvrđuju narušenje Bellove nejednakosti.

3 Kvantni logički sklopovi

Za početak, navest ćemo dva rezultata linearne algebre koji su od velikog značaja za objašnjenje matematičkog alata koji se koristi prilikom mjerenja qubita. [9]

Propozicija 3.1. Svojtveni vektori hermitskog operatora s pripadajućim, međusobno različitim, svojtvenim vrijednostima su ortogonalni.

Propozicija 3.2. Svaki hermitski operator može se dijagonalizirati.

Navedene propozicije vode nas do zaključka kako hermitski operatori definiraju jedinstveni rastav na direktnu sumu međusobno ortogonalnih potprostora. [3] Time prostor V možemo zapisati kao direktnu sumu $V = V_1 \oplus V_2$ gdje je $V_1 \perp V_2$. Sada možemo definirati preslikavanje koje zovemo projekcija na potprostor, odnosno operator projekcije

$$P_i : V \rightarrow S_i,$$

gdje je

$$P_i |v\rangle = |v_i\rangle, |v_i\rangle \in V_i.$$

S tako zadanom kompozicijom, mjerni uređaj bilježi vjerojatnost $|P_i |\psi\rangle|^2$ da početno stanje $|\Psi\rangle$ kolapsira u stanje $|\psi'\rangle = \frac{P_i |\psi\rangle}{|P_i |\psi\rangle|}$. Prisjetimo li se zapisa proizvoljne polarizacije

$$|\psi\rangle = \alpha |\uparrow\rangle + \beta |\rightarrow\rangle,$$

time je definira rastav prostora kao

$$V = V_{|\uparrow\rangle} \oplus V_{|\rightarrow\rangle}.$$

Time prethodno razmatrane horizontalno, odnosno vertikalno, polarizirane filtre poistovjećujemo s operatorima projekcije

$$P_{\uparrow} : V \rightarrow V_{|\uparrow\rangle},$$

$$P_{\rightarrow} : V \rightarrow V_{|\rightarrow\rangle},$$

te su vjerojatnosti apsorpcije, odnosno transmisije dane s

$$|P_{\uparrow} |\psi\rangle|^2 = \alpha^2,$$

$$|P_{\rightarrow} |\psi\rangle|^2 = \beta^2.$$

Dobiveni rezultati u skladu su onima iz 2.1.

3.1 Klasični logički sklopovi

Osnovni klasični logički sklopovi temeljeni su na osnovnim logičkim operacijama ⁴:

I (eng. *AND*; \wedge), **ILI** (eng. *OR*; \vee) te **NE** (eng. *NOT*, \neg).

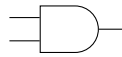
Također postoje i složeni, izvedeni logički sklopovi, poput logičkih vrata ekskluzivno **ILI**, **XOR**, koja su izvedena pomoću osnovnih logičkih operacija **I**, **ILI** i **NE**, odnosno možemo ih izraziti kao

$$(p \vee q) \wedge \neg(p \wedge q).$$

Klasični logički sklopovi izvode se pomoću tranzistora. U daljnjem tekstu dana je tablica istinitosti za pojedina logička vrata kao i pripadajući simbol. Također, primijetimo kako su jedino logička vrata **NE** povratna, odnosno, znajući izlaznu vrijednost bita moguće je odrediti ulaznu vrijednost bita. To je ostvarivo i u jednom od četiri slučaja logičkih vrata **I**, kada je izlazna vrijednost bita 1.

3.1.1 Logička vrata I, AND

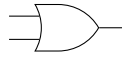
| p | q | $p \wedge q$ |
|-----|-----|--------------|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |



Slika 7: Tablica istinitosti i simbol za logička vrata I (AND)

3.1.2 Logička vrata ILI, OR

| p | q | $p \vee q$ |
|-----|-----|------------|
| 1 | 1 | 1 |
| 1 | 0 | 1 |
| 0 | 1 | 1 |
| 0 | 0 | 0 |

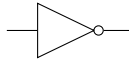


Slika 8: Tablica istinitosti i simbol za logička vrata ILI (OR)

⁴U logici sudova koristi se termin propozicionalni veznik, odnosno veznik, i to je svaka funkcija $f : \{0, 1\}^n \rightarrow \{0, 1\}, \forall n \in \mathbb{N}$.

3.1.3 Logička vrata NE, NOT

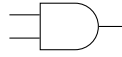
| p | $\neg p$ |
|-----|----------|
| 1 | 0 |
| 0 | 1 |



Slika 9: Tablica istinitosti i simbol za logička vrata NE (NOT)

3.1.4 Logička vrata ekskluzivno ILI, XOR

| p | q | $p \wedge q$ |
|-----|-----|--------------|
| 1 | 1 | 1 |
| 1 | 0 | 0 |
| 0 | 1 | 0 |
| 0 | 0 | 0 |



Slika 10: Tablica istinitosti i simbol za logička vrata ekskluzivno ILI (XOR)

3.2 Kvantni logički sklopovi

Kvantna logička vrata su svaka promjena kvantnog stanja qubita, odnosno unitarne transformacije qubita. Geometrijski shvaćeno, to su rotacije na Blochovoj sferi. Grafički ih prikazujemo pomoću paralelnih horizontalnih pravaca i kvadratića, gdje svaka linija odgovara jednom qubitu, a kvadratići promjeni stanja jednog qubita. U daljnjem tekstu, uzet ćemo u obzir standardnu bazu za sustave od jednog, odnosno dva qubita.

3.2.1 Paulijeva logička vrata

Sljedeće transformacije odnose se na sustave od jednog qubita [3]. Hermitske i unitarne matrice

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \text{ i } Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},$$

su Paulijeve matrice ⁵ koje s jediničnom matricom

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

⁵Paulijeve matrice dobile su ime u čast Austrijskog fizičara Wolfganga Ernsta Paulia.

čine skup Paulijevih logičkih vrata ⁶.

Teorem 3.1. Paulijevi operatori baza su prostora linearnih operatora koji djeluju na dvodimenzionalni vektorski prostor.

Dokaz. Neka je dan proizvoljan linearan operator \mathbf{P} s matičnim zapisom. Tvrdimo da tada postoje jedinstveni skalari $\alpha, \beta, \gamma, \delta \in \mathbb{C}$ tako da vrijedi

$$\mathbf{P} = \begin{bmatrix} p_{00} & p_{01} \\ p_{10} & p_{11} \end{bmatrix} = \alpha \mathbf{I} + \beta \mathbf{X} + \gamma \mathbf{Y} + \delta \mathbf{Z}.$$

Rješavanjem sustava četiri jedandžbi s četiri nepoznanice, slijedi

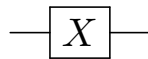
$$\begin{aligned} \alpha &= \frac{p_{00} + p_{11}}{2} & \beta &= \frac{p_{01} + p_{10}}{2} \\ \gamma &= \mathbf{i} \cdot \frac{p_{01} - p_{10}}{2} & \delta &= \frac{p_{00} - p_{11}}{2}. \end{aligned}$$

Kako sustav ima jedinstveno rješenje, skup Paulijevih logičkih vrata je baza prostora linearnih operatora koji djeluju na dvodimenzionalnom vektorskom prostoru. □

X vrata Kvantna logička vrata \mathbf{X} djeluju na jedan qubit unitarnom operacijom (10).

$$\mathbf{X} : |1\rangle \langle 0| + |0\rangle \langle 1| \quad (10)$$

Na slici 11 dan je simbol za Paulijeva logička vrata \mathbf{X} u kvantnom logičkom sklopu.



Slika 11: \mathbf{X} vrata

Djelovanje vrata \mathbf{X} na qubit $|0\rangle$ rezultira stanjem $|1\rangle$ i obratno:

$$\begin{aligned} \mathbf{X}|0\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle, \\ \mathbf{X}|1\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle. \end{aligned}$$

Na Blochovoj sferi, dana transformacija označava rotaciju za π oko x -osi. Unitaran operator \mathbf{X} ima svojstvene vektore $|+\rangle$ i $|-\rangle$ s pridruženim svojstvenim vrijednostima 1 odnosno -1 .

$$\begin{aligned} \mathbf{X}|+\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |+\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = 1 \cdot |+\rangle \\ \mathbf{X}|-\rangle &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} |-\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = -\frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = -1 \cdot |-\rangle \end{aligned}$$

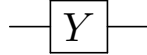
⁶U literaturi se koristi i naziv Paulijeve transformacije.

Logička vrata **X** analog su klasičnim logičkim vratima **NE**, ako preslikavanje $|0\rangle \mapsto |1\rangle$ i $|1\rangle \mapsto |0\rangle$ shvatimo kao negaciju.

Y vrata Kvantna logička vrata **Y** djeluju na jedan qubit unitarnom operacijom (11).

$$\mathbf{Y} : -i(|0\rangle\langle 1| - |1\rangle\langle 0|) \quad (11)$$

Na slici 12 dan je simbol za Paulijeva logička vrata **Y** u kvantnom logičkom sklopu.



Slika 12: **Y** vrata

Djelovanje vrata **Y** na qubit $|0\rangle$ rezultira stanjem $i|1\rangle$, a djelovanjem na qubit $|1\rangle$ rezultira stanjem $-i|0\rangle$:

$$\begin{aligned} \mathbf{Y}|0\rangle &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = i \begin{bmatrix} 0 \\ 1 \end{bmatrix} = i|1\rangle, \\ \mathbf{Y}|1\rangle &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -i \begin{bmatrix} 1 \\ 0 \end{bmatrix} = -i|0\rangle. \end{aligned}$$

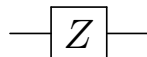
Na Blochovoj sferi, dana transformacija označava rotaciju za π oko y -osi. Unitaran operator **Y** ima svojstvene vektore $|i\rangle$ i $|-i\rangle$ s pridruženim svojstvenim vrijednostima 1 odnosno -1 .

$$\begin{aligned} \mathbf{Y}|i\rangle &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} |i\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix} = 1 \cdot |i\rangle \\ \mathbf{Y}|-i\rangle &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} |-i\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} -1 \\ i \end{bmatrix} = -1 \cdot |-i\rangle \end{aligned}$$

Z vrata Kvantna logička vrata **Z** djeluju na jedan qubit unitarnom operacijom (12).

$$\mathbf{Z} : |0\rangle\langle 0| - |1\rangle\langle 1| \quad (12)$$

Na slici 13 dan je simbol za Paulijeva logička vrata **Z** u kvantnom logičkom sklopu.



Slika 13: **Z** vrata

Djelovanje vrata \mathbf{Z} na qubit $|0\rangle$ on ostaje nepromijenjen, dok djelovanje na qubit $|1\rangle$ rezultira stanjem $-|1\rangle$:

$$\begin{aligned}\mathbf{Z}|0\rangle &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle, \\ \mathbf{Z}|1\rangle &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = - \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -|1\rangle.\end{aligned}$$

Na Blochovoj sferi, dana transformacija označava rotaciju za π oko z -osi. Svojevremeni vektori unitarnog operatora \mathbf{Z} su $|0\rangle$ i $|1\rangle$ s pridruženim svojstvenim vrijednostima 1 odnosno -1 .

3.2.2 Hadamardova vrata

Hadamardov unitarni operator djeluju na jedan qubit unitarnom operacijom (13).

$$\mathbf{H} = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|) \quad (13)$$

Hadamardov operator vektore standardne baze, $|0\rangle$ i $|1\rangle$ preslikava u vektore Hadamardove baze, $|+\rangle$ i $|-\rangle$.

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

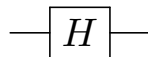
Matrični zapis operatora \mathbf{H} dan je s

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

Hadamardov operator je involucija, odnosno unitarni i hermitski operator

$$\mathbf{H} \cdot \mathbf{H}^\dagger = \left(\frac{1}{\sqrt{2}}\right)^2 \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \mathbf{I}$$

Na slici 14 dan je simbol za Hadamardova logička vrata \mathbf{H} u kvantnom logičkom sklopu.



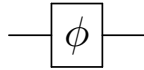
Slika 14: \mathbf{H} vrata

3.2.3 Operator faznog pomaka

Operator faznog pomaka djeluju na jedan qubit unitarnom transformacijom (14).

$$\mathbf{P}_\rho = |0\rangle\langle 0| + e^{i\rho}|1\rangle\langle 1| \quad (14)$$

Djelovanjem na proizvoljno stanje $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, sustav prelazi u stanje $|\Psi'\rangle = \alpha|0\rangle + \beta \cdot e^{i\rho}|1\rangle$ čime je promijenjena relativna faza ako je $\rho \neq 2k\pi, k \in \mathbb{Z}$. Na slici 15 dan je simbol za logička vrata operator faznog pomaka \mathbf{P}_ρ u kvantnom logičkom sklopu.



Slika 15: \mathbf{P}_ρ vrata

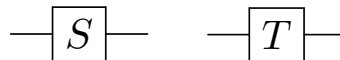
Matrični zapis operatora \mathbf{P}_ρ dan je s

$$\mathbf{P}_\rho = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\rho} \end{bmatrix}.$$

S operatorom faznog pomaka susreli smo se ranije, primijetimo kako za $\rho = \pi$ vrijedi $\mathbf{P}_\pi = \mathbf{Z}$. Ako na operator faznog pomaka stavimo uvjet unitarnosti, slijedi

$$\begin{aligned} \mathbf{P}_\rho^\dagger &= \mathbf{P}_\rho \\ \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\rho} \end{bmatrix} &= \begin{bmatrix} 1 & 0 \\ 0 & e^{i\rho} \end{bmatrix} \\ e^{-i\rho} &= e^{i\rho} \\ \sin(-\rho) + i\cos(-\rho) &= \sin(\rho) + i\cos(\rho) \\ \sin(\rho) &= 0 \\ \rho &= k \cdot \frac{\pi}{2}, k \in \mathbb{Z} \end{aligned}$$

Zaključujemo da je operator faznog pomaka unitaran, odnosno hermitski ako i samo ako je $\rho = k \cdot \frac{\pi}{2}, k \in \mathbb{Z}$. Za $\rho = \frac{\pi}{2}$ dolazimo do **S** vrata (Slika 16. lijevo), a za $\rho = \frac{\pi}{4}$ dolazimo do **T** vrata (Slika 16. desno).



Slika 16: **S** i **T** vrata

3.2.4 Kvadratni korijen iz NOT vrata

Pokušajmo konstruirati bijektivnu Booleovu funkciju $f : \{0, 1\} \rightarrow \{0, 1\}$ tako da vrijedi $(f \circ f)(x) = \neg x, x, \neg x \in \{0, 1\}$. Ako postoji takvo preslikavanje, mora vrijediti

$$\begin{aligned} (f \circ f)(0) &= \neg 0 = 1 & (f \circ f)(1) &= \neg 1 = 0 \\ f(f(0)) &= 1, & f(f(1)) &= 0. \end{aligned}$$

Pretpostavimo da takva funkcija postoji. Nadalje pretpostavimo da je $f(0) = 0$ pa je tada $f(f(0)) = f(0) = 0$. Slično, pretpostavimo li da je $f(0) = 1$ tada je $f(f(0)) = f(1)$, no kako zahtijevamo da je funkcija i bijekcija, to slijedi $f(1) = 0$, odnosno $f(f(0)) = f(1) = 0$. Dolazimo do kontradikcije. U kvantnom slučaju takvo rješenje je moguće naći, odnosno postoji unitaran operator (15) kvadratnog korijena iz **NOT**.

$$\sqrt{\mathbf{NOT}} = \frac{1}{2} ((1 + i) |0\rangle \langle 0| + (1 - i) |1\rangle \langle 0| + (1 - i) |0\rangle \langle 1| + (1 + i) |1\rangle \langle 1|) \quad (15)$$

Djelovanje kompozicije operatora $\sqrt{\mathbf{NOT}}$ na qubit $|0\rangle$ dano je s

$$\begin{aligned} \sqrt{\mathbf{NOT}}\sqrt{\mathbf{NOT}} |0\rangle &= \sqrt{\mathbf{NOT}} \left(\frac{1}{2} ((1 + i)(|0\rangle \langle 0|0\rangle + |1\rangle \langle 1|0\rangle) + (1 - i)(|1\rangle \langle 0|0\rangle + |0\rangle \langle 1|0\rangle)) \right) \\ &= \sqrt{\mathbf{NOT}} \left(\frac{1}{2} ((1 + i) |0\rangle + (1 - i) |1\rangle) \right) \\ &= \left(\frac{1}{2} \right)^2 ((1 + 2i + i^2 + 1 - 2i + i^2) |0\rangle + (1 - i^2 + 1 - i^2) |1\rangle) \\ &= \frac{1}{4} 4 |1\rangle, \end{aligned}$$

što nakon sređivanja daje rezultat

$$\sqrt{\mathbf{NOT}}\sqrt{\mathbf{NOT}} |0\rangle = |1\rangle$$

Slično se pokaže kako vrijedi

$$\sqrt{\mathbf{NOT}}\sqrt{\mathbf{NOT}} |1\rangle = |0\rangle.$$

Na slici 17 dan je simbol za kvantna logička vrata kvadratni korijen iz **NOT** u kvantnom logičkom sklopu.

$$\boxed{\sqrt{\mathbf{NOT}}}$$

Slika 17: $\sqrt{\mathbf{NOT}}$ vrata

3.2.5 C_{NOT} vrata

Do sada spomenuta logička vrata djeluju na jedan qubit, odnosno to su operatori na jednodimenzionalnom Hilbertovom prostoru. Također, postoje i logička vrata koja djeluju na

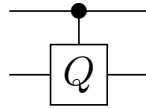
višedimenzionalnim Hilbertovim prostorima. U Hilbertovom prostoru $V_1 \otimes V_2$ valja izdvojiti skup kontrolnih vrata, od kojih su najistaknutija \mathbf{C}_{NOT} vrata. U standardnoj bazi, unitarna operacija (16) se definira tako da unitaran operator \mathbf{Q} djeluje na drugi qubit ako i samo ako je prvi qubit $|1\rangle$, inače djeluje jedinični operator \mathbf{I} , odnosno stanje se ne mijenja.

$$\bigwedge \mathbf{Q} = |0\rangle \langle 0| \otimes \mathbf{I} + |1\rangle \langle 1| \otimes \mathbf{Q} \quad (16)$$

Operator je moguće prikazati u obliku blok-dijagonalne matrice dimenzije 4×4

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q_1 & q_2 \\ 0 & 0 & q_3 & q_4 \end{bmatrix} = \begin{bmatrix} I & 0 \\ 0 & Q \end{bmatrix}$$

Simbolički zapis $\bigwedge \mathbf{Q}$ vrata dan je na slici 18. Puni kružić je kontrolni qubiti, a linija koja spaja puni kružić s kvadratićem uvjetno djelovanje operatora \mathbf{Q} na drugi qubit.



Slika 18: $\bigwedge \mathbf{Q}$ vrata

C_{NOT} vrata: \mathbf{C}_{NOT} vrata definirana su tako da Paulijeva vrata \mathbf{X} djeluju na drugi qubit ako i samo ako je prvi qubit $|1\rangle$, inače djeluje jedinični operator \mathbf{I} , što je transformacija (17). Drugim riječima, dolazi do negacije drugog qubita ako i samo ako je prvi qubit $|1\rangle$.

$$\mathbf{C}_{\text{NOT}} = |0\rangle \langle 0| \otimes \mathbf{I} + |1\rangle \langle 1| \otimes \mathbf{X} \quad (17)$$

Djelovanje na stanja standardne baze time je dano s

$$\begin{aligned} |00\rangle &\mapsto |00\rangle & |10\rangle &\mapsto |11\rangle \\ |01\rangle &\mapsto |01\rangle & |11\rangle &\mapsto |10\rangle, \end{aligned}$$

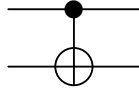
a matricni zapis s

$$\mathbf{C}_{\text{NOT}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Primijetimo, \mathbf{C}_{NOT} možemo zapisati i kao

$$\mathbf{C}_{\text{NOT}} = |00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 11| + |11\rangle \langle 10|.$$

Simbolički zapis \mathbf{C}_{NOT} vrata dan je na slici 19. Puni kružić je kontrolni qubit, linija koja spaja puni kružić sa šupljim kružićem uvjetna negacija drugog qubita.



Slika 19: \mathbf{C}_{NOT} vrata

Generalizacija da \mathbf{C}_{NOT} vrata, odnosno kontrolna vrata općenito, djeluju tako da uzmu prvi qubit za kontrolni je pogrešna. U Hadamardovoj bazi je tako drugi qubit na mjestu kontrolnog.

$$\begin{aligned} \mathbf{C}_{\text{NOT}} |++\rangle &= (|00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 11| + |11\rangle \langle 10|) \left(\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \right) \\ &= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \\ &= |++\rangle \end{aligned}$$

$$\begin{aligned} \mathbf{C}_{\text{NOT}} |+-\rangle &= (|00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 11| + |11\rangle \langle 10|) \left(\frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \right) \\ &= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \\ &= |--\rangle \end{aligned}$$

$$\begin{aligned} \mathbf{C}_{\text{NOT}} |-+\rangle &= (|00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 11| + |11\rangle \langle 10|) \left(\frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) \right) \\ &= \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle) \\ &= |-+\rangle \end{aligned}$$

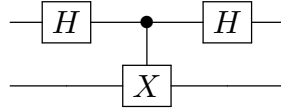
$$\begin{aligned} \mathbf{C}_{\text{NOT}} |--\rangle &= (|00\rangle \langle 00| + |01\rangle \langle 01| + |10\rangle \langle 11| + |11\rangle \langle 10|) \left(\frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \right) \\ &= \frac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle) \\ &= |--\rangle \end{aligned}$$

Primijetimo ako je drugi qubit u stanju $|+\rangle$, stanje prvog qubita se ne mijenja. Općenito, kontrolna vrata mijenjaju spregnutost dvaju qubita što se može pokazati primjerom gdje nespregnuto stanje $|-\rangle \otimes |1\rangle$ postaje spregnuto.

Primjer 3.1.

$$\begin{aligned} \mathbf{C}_{\text{NOT}} |-\rangle \otimes |1\rangle &= \mathbf{C}_{\text{NOT}} \frac{1}{\sqrt{2}}(|01\rangle - |11\rangle) \\ &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned}$$

Primjer 3.2. Kako je Hadamardov operator involucija, nespretnim čitanjem kvantnog logičkog sklopa kao sa slike 20 moglo bi se zaključiti da njegovo uzastopno djelovanje u kvantnom logičkom sklopu na sustav jednog qubita možemo zamijeniti operatorom identiteta.



Slika 20: Kvantni logički sklop sastavljen od jednih CNOT vrata i dvoje Hadamardovih vrata

Neka je stanje prvog qubita dano s $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, $|\alpha|^2 + |\beta|^2 = 1$, a stanje drugog qubita je $|0\rangle$. Promatramo djelovanje kvantnog logičkog sklopa na sistem dva qubita:

$$|\Psi\rangle \otimes |0\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle.$$

Prolaskom kroz prva Hadamardova vrata sustav prelazi u stanje

$$\frac{1}{\sqrt{2}}[\alpha(|0\rangle + |1\rangle) + \beta(|0\rangle - |1\rangle)] \otimes |0\rangle$$

Prolaskom kroz \mathbf{C}_{NOT} vrata stanje sustava je

$$\begin{aligned} & \frac{1}{\sqrt{2}}\mathbf{C}_{\text{NOT}}[\alpha(|00\rangle + |10\rangle) + \beta(|00\rangle - |10\rangle)] = \\ & \frac{1}{\sqrt{2}}[(\alpha + \beta)|00\rangle + (\alpha - \beta)|11\rangle] \end{aligned}$$

Primijetimo kako je dobiveno stanje spregnuto. Prolaskom kroz druga Hadamardova vrata, stanje sustava postaje

$$\begin{aligned} & \frac{1}{\sqrt{2}}\mathbf{H}[(\alpha + \beta)|0\rangle \otimes |0\rangle + (\alpha - \beta)|1\rangle \otimes |1\rangle] = \\ & \frac{1}{2}[(\alpha + \beta)(|0\rangle + |1\rangle) \otimes |0\rangle + (\alpha - \beta)(|0\rangle - |1\rangle) \otimes |1\rangle] = \\ & \frac{1}{2}[(\alpha + \beta)|00\rangle + (\alpha - \beta)|01\rangle + (\alpha + \beta)|10\rangle + (\alpha - \beta)|11\rangle] \end{aligned}$$

Vrata kontrolirane faze: Vrata kontrolirane faze mogu mijenjati relativnu fazu stanja. Djelovanje vrata $\wedge e^{i\theta}$ na stanja standardne baze dano je s:

$$\begin{aligned} |00\rangle & \mapsto |00\rangle & |10\rangle & \mapsto e^{i\theta}|10\rangle \\ |01\rangle & \mapsto |01\rangle & |11\rangle & \mapsto e^{i\theta}|11\rangle, \end{aligned}$$

Primjer 3.3. $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ prelazi u stanje $\frac{1}{\sqrt{2}}(|00\rangle + e^{i\theta}|11\rangle)$. Kako faktor $e^{i\theta}$ nije moguće izlučiti ispred zgrade, to je relativna faza stanja promijenjena u odnosu na početnu.

Toffolijeva (CCNOT) vrata: U Hilbertovom prostoru $V_1 \otimes V_2 \otimes V_3$ postoje i tri qubitna kontrolna vrata, Toffolijeva (CCNOT) vrata, dana s:

$$\begin{array}{ll} |000\rangle \mapsto |000\rangle & |101\rangle \mapsto |101\rangle \\ |001\rangle \mapsto |001\rangle & |011\rangle \mapsto |001\rangle \\ |010\rangle \mapsto |010\rangle & |110\rangle \mapsto |111\rangle \\ |100\rangle \mapsto |100\rangle & |111\rangle \mapsto |110\rangle . \end{array}$$

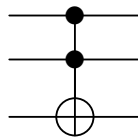
Matrični zapis Toffolijevog operatora dan je s

$$\text{CCNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix} .$$

Kod Toffolijevog operatora, dolazi do negacije trećeg qubita ako i samo ako su stanja prvog i drugog qubita $|1\rangle$. Simbolički zapis Toffolijevih vrata dan je na slici 21. Puni kružići su kontrolni qubiti, a linija koja spaja pune kružiće sa šupljim kružićem uvjetna negacija trećeg qubita. Primijetimo, Toffolijev operator možemo shvatiti kao preslikavanje (18)

$$|a\rangle \otimes |b\rangle \otimes |c\rangle \mapsto |a\rangle \otimes |b\rangle \otimes |c \leftrightarrow (a \wedge b)\rangle , \quad (18)$$

čime je on povezan s klasičnim logičkim operacijama **ekskluzivno ILI** i **I**.



Slika 21: Toffolijeva vrata

3.2.6 SWAP vrata

Unitarna transformacija (19) koja mijenja stanje $|a\rangle \otimes |b\rangle$ dva qubita ako i samo ako je $a \neq b$, $a, b \in \{0, 1\}$ zove se SWAP, odnosno **SWAP** vrata (Slika 22).

$$\text{SWAP} = |0\rangle \langle 0| \otimes \mathbf{I} + |1\rangle \langle 1| \otimes \mathbf{Q}. \quad (19)$$

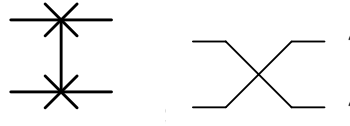
Matrični zapis operatora **SWAP** dan je s

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

Primjer 3.4. Neka su $|\psi\rangle, |\tau\rangle$ dva stanja sistema od jednog qubita. Tada djelovanjem **SWAP** operatora stanje $|\psi\rangle \otimes |\tau\rangle$ prelazi u stanje $|\tau\rangle \otimes |\psi\rangle$.

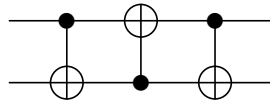
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |\tau\rangle = \gamma|0\rangle + \delta|1\rangle$$

$$\begin{aligned} \mathbf{SWAP}[|\psi\rangle \otimes |\tau\rangle] &= \mathbf{SWAP}[\alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle] \\ &= \alpha\gamma|00\rangle + \alpha\delta|10\rangle + \beta\gamma|01\rangle + \beta\delta|11\rangle \\ &= (\gamma|0\rangle + \delta|1\rangle) \otimes \alpha|0\rangle + (\gamma|0\rangle + \delta|1\rangle) \otimes \beta|1\rangle \\ &= (\gamma|0\rangle + \delta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= |\tau\rangle \otimes |\psi\rangle \end{aligned}$$



Slika 22: **SWAP** vrata

Primjer 3.5. **SWAP** vrata mogu se konstruirati kvantnim logičkim sklopom sastavljenim od tri **C_{NOT}** vrata (slika 23).



Slika 23: **SWAP** vrata konstruirana pomoću **C_{NOT}** vrata.

Prolaskom kroz prva **C_{NOT}** vrata, stanje sustava prelazi u stanje

$$\begin{aligned} \mathbf{C}_{\mathbf{NOT}}[|\psi\rangle \otimes |\tau\rangle] &= \mathbf{C}_{\mathbf{NOT}}[\alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle] \\ &= \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle. \end{aligned}$$

Primijetimo kako kod drugih **C_{NOT}** ulogu kontrolnog qubita ima drugi qubit. Nakon prolaska kroz druga **C_{NOT}** vrata stanje sustava prelazi u

$$\mathbf{C}'_{\mathbf{NOT}}[\alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|11\rangle + \beta\delta|10\rangle] = [\alpha\gamma|00\rangle + \alpha\delta|11\rangle + \beta\gamma|01\rangle + \beta\delta|10\rangle].$$

Prolaskom kroz treća \mathbf{C}_{NOT} vrata, stanje sustava prelazi u stanje

$$\begin{aligned} \mathbf{C}_{\text{NOT}}[\alpha\gamma|00\rangle + \alpha\delta|11\rangle + \beta\gamma|01\rangle + \beta\delta|10\rangle] &= [\alpha\gamma|00\rangle + \alpha\delta|10\rangle + \beta\gamma|01\rangle + \beta\delta|11\rangle] \\ &= (\gamma|0\rangle + \delta|1\rangle) \otimes (\alpha|0\rangle + \beta|1\rangle) \\ &= |\tau\rangle \otimes |\psi\rangle. \end{aligned}$$

SWAP operator je također involucija, odnosno unitarni i hermitski operator

$$\mathbf{SWAP} \cdot \mathbf{SWAP}^\dagger = \mathbf{I}.$$

3.3 Univerzalnost kvantnog računala

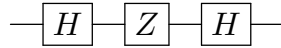
3.3.1 Cliffordova grupa

Definicija 3.1. Cliffordova grupa \mathfrak{C} je grupa unitarnih transformacija koje normaliziraju Paulijevu grupu, odnosno za svaku Paulijevu transformaciju $\mathcal{P}, \mathcal{P}'$ vrijedi

$$\mathcal{U} \cdot \mathcal{P} \cdot \mathcal{U}^\dagger = \mathcal{P}', \mathcal{C} \in \mathfrak{C}.$$

Cliffordova grupa generirana je Hadamardovim operatorom, \mathbf{H} , operatorom faznog pomaka za $\frac{\pi}{2}$, \mathbf{S} i kontrolno negiranim vratima, \mathbf{C}_{NOT} vratima. Svaki element Cliffordove grupe može se dobiti konačnim umnoškom spomenutih unitarnih operatora.

Primjer 3.6. Kvantni logički sklop \mathbf{HZH} ekvivalentan je kvantnim logičkim vratima \mathbf{X} .

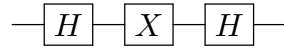


Slika 24: \mathbf{HZH} kvantni logički sklop

Tako djelovanje operatora \mathbf{HZH} na stanje $|0\rangle$ rezultira stanjem $|1\rangle$ i obratno, djelovanje operatora \mathbf{HZH} na stanje $|1\rangle$ rezultira stanjem $|0\rangle$.

$$\begin{aligned} \mathbf{HZH}|0\rangle &= \mathbf{HZ} \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) & \mathbf{HZH}|1\rangle &= \mathbf{HZ} \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \\ &= \frac{1}{\sqrt{2}} \mathbf{H} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} & &= \frac{1}{\sqrt{2}} \mathbf{H} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ -1 \end{bmatrix} \\ &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ -1 \end{bmatrix} & &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} \\ &= \frac{1}{2} \cdot \begin{bmatrix} 0 \\ 2 \end{bmatrix} & &= \frac{1}{2} \cdot \begin{bmatrix} 2 \\ 0 \end{bmatrix} \\ &= |1\rangle & &= |0\rangle \end{aligned}$$

Primjer 3.7. Kvantni logički sklop **HXH** ekvivalentan je kvantnim logičkim vratima **Z**.



Slika 25: **HXH** kvantni logički sklop

$$\begin{aligned}
 \mathbf{HXH} |0\rangle &= \mathbf{HX} \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right) & \mathbf{HXH} |1\rangle &= \mathbf{HX} \left(\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right) \\
 &= \frac{1}{\sqrt{2}} \mathbf{H} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} & &= \frac{1}{\sqrt{2}} \mathbf{H} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ -1 \end{bmatrix} \\
 &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix} & &= \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \cdot \begin{bmatrix} -1 \\ 1 \end{bmatrix} \\
 &= \frac{1}{2} \cdot \begin{bmatrix} 2 \\ 0 \end{bmatrix} & &= \frac{1}{2} \cdot \begin{bmatrix} 0 \\ -2 \end{bmatrix} \\
 &= |0\rangle & &= -|1\rangle
 \end{aligned}$$

Cliffordova grupa zanimljiva je radi rezultata [10] Daniela Gottesmana, prezentiranog na simpoziju 1999. godine, gdje dokazuje teorem Emanuela Knilla, poznatog pod nazivom **Gottesman - Knillov teorem**.

Teorem 3.2. Kvantno računalo koje koristi samo sljedeće elemente:

1. unitarne transformacije Cliffordove grupe,
2. mjerenja operatora Paulijeve grupe i
3. Cliffordove grupne operacije uvjetovane klasičnim bitovima, koje mogu biti rezultati ranijih mjerenja

moguće je učinkovito simulirati na klasičnom (probabilističkom) računalu u polinomnom vremenu.

Prema **Gottesman - Knillovom teoremu**, moć kvantnog računala nad klasičnim računalom izražena je prilikom korištenja logičkih vrata koja nisu sadržana u Cliffordovoj grupi. Zaključujemo kako Cliffordova grupa nije univerzalni skup kvantnih logičkih vrata, jer nije moguće svaku unitarnu transformaciju prikazati kao konačnu kompoziciju elemenata Cliffordove grupe. Standardno, za univerzalni skup kvantnih logičkih vrata, Cliffordovu grupu proširujemo s **S** vratima. Može se pokazati kako **T** vrata nisu normalizator Paulijeve grupe transformacija, odnosno da za sve Paulijeve transformacije $\mathcal{P}, \mathcal{P}'$ ne vrijedi

$$\mathbf{T} \cdot \mathcal{P} \cdot \mathbf{T}^\dagger = \mathcal{P}'.$$

U slučaju kvantnih logičkih vrata koja djeluju na jedan qubit, vrijedi sljedeći teorem.

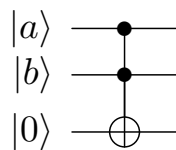
Teorem 3.3. Skup univerzalnih kvantnih logičkih vrata za unitarne operatore koje djeluju na jedan qubit sadrži Hadamardova vrata, **H** i vrata faznog pomaka **T**.

3.3.2 Kvantno izvođenje klasičnih logičkih operacija

1980. godine, američki fizičar Paul Anthony Benioff u svome radu *The computer as a physical system: A microscopic QM Hamiltonian model of computers as represented by Turing machines*, [12], dolazi do zaključka kako je kvantno računalo moćno barem kao i klasično računalo. David Deutsch, nadahnut Richardom Feynmanom, pitao se može li kvantno računalo nadići efikasnost izvođenja operacija klasičnog računala. Univerzalnost kvantnog računala podrazumijeva da se logičke operacije koje izvodi klasično računalo, mogu izvesti i na kvantnom računalu. Kako su jedino klasična **NE** vrata povratna, odnosno, ako su poznate izlazne vrijednosti, mogu se odrediti ulazne vrijednosti, postavlja se pitanje kako izvesti kvantni logički sklop koji izvodi nepovratne logičke operacije **I** i **ILI** pomoću povratnih kvantnih logičkih vrata, odnosno unitarnih operacija.

Logička vrata I, AND Kako bismo izveli klasičnu logičku operaciju **I**, odnosno **AND** koristimo Toffolijev operator, [13], tako da prva dva qubita, $|a\rangle$ i $|b\rangle$, predstavljaju binarne vrijednosti 0 ili 1, a treći qubit pripremimo u stanju $|0\rangle$. Raspišemo li tablicu istinitosti, primijetimo kako su dobiveni rezultati jednaki onima u slučaju $a \wedge b$.

| a | b | c | $a \wedge b$ | $c \leftrightarrow (a \wedge b)$ |
|-----|-----|-----|--------------|----------------------------------|
| 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 |
| 0 | 1 | 0 | 0 | 0 |
| 0 | 0 | 0 | 0 | 0 |



Slika 26: Kvantni logički sklop koji izvodi klasičnu operaciju **I** (**AND**).

Logička vrata ILI, OR Prema logici sudova, sljedeće dvije formule su ekvivalentne:

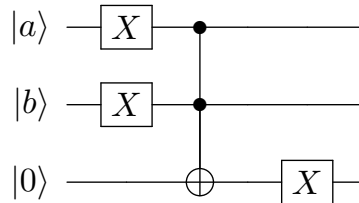
$$\neg(A \vee B) \Leftrightarrow \neg A \wedge \neg B,$$

iz čega slijedi ekvivalentnost formula:

$$A \vee B \Leftrightarrow \neg(\neg A \wedge \neg B).$$

Kako bismo izveli klasičnu logičku operaciju **ILI**, odnosno **OR** također koristimo Toffolijev operator kako bismo izveli operaciju **I**, **AND**, a negaciju ostvarujemo pomoću Paulijevog **X** operator. Postavimo prva dva qubita, $|a\rangle$ i $|b\rangle$, tako da predstavljaju binarne vrijednosti 0 ili 1, a treći qubit pripremimo u stanju $|0\rangle$. Raspišemo li tablicu istinitosti, primijetimo kako su dobiveni rezultati jednaki onima u slučaju $a \vee b$.

| a | b | c | $\neg a$ | $\neg b$ | $c \leftrightarrow (\neg a \wedge \neg b)$ | $\neg(c \leftrightarrow (\neg a \wedge \neg b))$ |
|-----|-----|-----|----------|----------|--|--|
| 1 | 1 | 0 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 0 | 1 | 0 | 1 |
| 0 | 1 | 0 | 1 | 0 | 0 | 1 |
| 0 | 0 | 0 | 1 | 1 | 1 | 0 |



Slika 27: Kvantni logički sklop koji izvodi klasičnu operaciju **ILI** (**OR**).

3.4 Kvantna teleportacija i *No-cloning* teorem

3.4.1 *No-cloning* teorem

1982. godine dvojica fizičara, William K. Wootters i Wojciech H. Zurek objavljuju rad *A single quantum cannot be cloned* [14] u kojem dokazuju kako niti jedan uređaj ne može amplificirati, odnosno klonirati, proizvoljnu polarizaciju. Formalno je taj rezultat dobio naziv *No-cloning* teorem [15].

Teorem 3.4. U Hilbertovom prostoru $\mathcal{H}_1 \otimes \mathcal{H}_2$ ne postoji unitaran kvantnomehanički operator koji može klonirati proizvoljno kvantno stanje $|\Psi\rangle$.

Dokaz. Pretpostavimo da postoji unitaran operator \mathcal{U} za koji vrijedi

$$|\Psi\rangle_1 \otimes |\theta\rangle_2 \mapsto e^{i\tau} |\Psi\rangle_1 \otimes |\Psi\rangle_2,$$

gdje je $|\theta\rangle \in \mathcal{H}_2$ normalizirano stanje na koje se klonira proizvoljno normalizirano stanje $|\Psi\rangle$ iz \mathcal{H}_1 , a $e^{i\tau}$ globalna faza. Neka je $|\psi\rangle$ normalizirano stanje iz prostora \mathcal{H}_1 , različito od $|\Psi\rangle$.

Tada vrijedi:

$$\begin{aligned}
\langle \Psi | \psi \rangle \langle \theta | \theta \rangle &= (\langle \Psi |_1 \otimes \langle \theta |_2) (| \psi \rangle_1 \otimes | \theta \rangle_2) \\
&= (\langle \Psi |_1 \otimes \langle \theta |_2) \mathcal{U}^\dagger \mathcal{U} (| \psi \rangle_1 \otimes | \theta \rangle_2) \\
&= (\langle \Psi |_1 \otimes \langle \theta |_2) \mathcal{U}^\dagger e^{i\tau_1} | \psi \rangle_1 \otimes | \psi \rangle_2 \\
&= (e^{i\tau_2} | \Psi \rangle_1 \otimes | \Psi \rangle_2) (e^{i\tau_1} | \psi \rangle_1 \otimes | \psi \rangle_2) \\
&= e^{i(\tau_1 + \tau_2)} \langle \Psi | \psi \rangle^2
\end{aligned}$$

Dolazimo do uvjeta:

$$\begin{aligned}
| \langle \Psi | \psi \rangle | &= | \langle \Psi | \psi \rangle |^2 \\
\implies | \langle \Psi | \psi \rangle | &= 1 \vee | \langle \Psi | \psi \rangle | = 0.
\end{aligned}$$

Primijetimo kako oba uvjeta općenito nisu zadovoljena, osim u slučaju kada su stanja $|\Psi\rangle$ i $|\psi\rangle$ odabrana tako da su ortogonalna ili jednaka do na fazu, dakle nisu proizvoljna. Time zaključujemo kako strogo gledano *No-cloning* teorem ipak dozvoljava mogućnost kloniranja istog stanja ili ortogonalnog stanja. \square

Teorem isključuje mogućnost savršenog kloniranja nepoznatog kvantnog stanja. Ipak, pokazalo se kako je moguće konstruirati nesavršeni klon. V. Bužek i M. Hiller u radu *Quantum copying: Beyond the no-cloning theorem*, [16], dolaze do transformacije koja daje nesavršeni klon u nespregnutom stanju s originalom. Takvi nesavršeni klonovi predstavljaju potencijalne sigurnosne rizike za informacijske protokole. I više, prema *No cloning* teoremu, ukoliko je poznato da su stanja koja mjerimo ili paralelna⁷ ili ortogonalna s poznatim kvantnim stanje, može se kreirati potreban broj kopija svakog stanja. Kako bi se to izbjeglo, u kvantnoj kriptografiji koriste se dvije različite orijentacije linearne polarizacije⁸.

3.4.2 Kvantna teleportacija

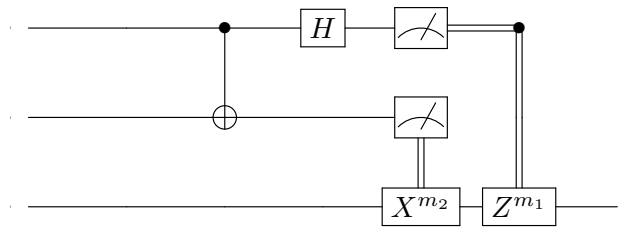
Iako *No-cloning* teorem ne dozvoljava savršeno kloniranje nepoznatog kvantnog stanja, ono može biti teleportirano, pri čemu originalno stanje kolapsira u jedno od dozvoljenih stanja. Neka Alice i Bob posjeduju parove spregnutih qubita u stanju $|\beta_{00}\rangle$, gdje je

$$\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}} (|00\rangle + |11\rangle), \\
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}} (|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B).
\end{aligned}$$

Alice želi poslati Bobu qubit nepoznatog stanja $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$. Pripremi se kvantni logički sklop [17] shematski dan na slici 28. Neka Alice posjeduje prvi qubit, a Bob drugi qubit.

⁷Normalizirana paralelna stanja su isto kvantno stanje.

⁸U slučaju kada kao qubite koristimo polarizirane fotone.



Slika 28: Kvantni logički sklop za teleportaciju - m_1 i m_2 predstavljaju ishode mjerenja prvog i drugog qubita, $m_1, m_2 \in \{0, 1\}$.

Ukupno stanje sustava tri qubita pri ulasku u kvantni logički sklop glasi:

$$|\Psi\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B),$$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle).$$

Prolaskom kroz C_{NOT} vrata stanje postaje:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle).$$

Prolaskom kroz Hadamardova vrata \mathbf{H} ono je:

$$|\Psi\rangle = \left(\frac{1}{\sqrt{2}}\right)^2 (\alpha(|0\rangle + |1\rangle) \otimes |00\rangle + \alpha(|0\rangle + |1\rangle) \otimes |11\rangle + \beta(|0\rangle - |1\rangle) \otimes |10\rangle + \beta(|0\rangle - |1\rangle) \otimes |01\rangle),$$

$$|\Psi\rangle = \frac{1}{2}(|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + |01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + |10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + |11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)).$$

Sada Alice može izmjeriti prva dva qubita u jednom od dopuštenih stanja $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$.

Mjerenjem, valna funkcija originala $|\psi\rangle$ kolapsira u $|m_1\rangle$, $m_1 \in \{0, 1\}$. Moguća su sljedeća četiri slučaja, od kojih svaki odgovara mogućem ishodu mjerenja koje obavi Alice:

1. Alice izmjeri stanje $|m_1 m_2\rangle = |00\rangle$. Tada Bob na stanje svoga qubita djeluje transformacijama $\mathbf{X}^0 = \mathbf{I}$ te $\mathbf{Z}^0 = \mathbf{I}$. Vrijedi:

$$\mathbf{I} \cdot \mathbf{I} \cdot \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

te je stanje Bobova qubita $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$.

2. Alice izmjeri stanje $|m_1 m_2\rangle = |01\rangle$. Tada Bob na stanje svoga qubita djeluje transformacijama $\mathbf{X}^1 = \mathbf{X}$ te $\mathbf{Z}^0 = \mathbf{I}$. Vrijedi:

$$\mathbf{I} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

te je stanje Bobova qubita $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha|0\rangle + \beta|1\rangle$.

3. Alice izmjeri stanje $|m_1 m_2\rangle = |10\rangle$. Tada **Bob** na stanje svoga qubita djeluje transformacijama $\mathbf{X}^0 = \mathbf{I}$ te $\mathbf{Z}^1 = \mathbf{Z}$. Vrijedi:

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \mathbf{I} \cdot \begin{bmatrix} \alpha \\ -\beta \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

te je stanje **Bobova** qubita $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha |0\rangle + \beta |1\rangle$.

4. Alice izmjeri stanje $|m_1 m_2\rangle = |11\rangle$. Tada **Bob** na stanje svoga qubita djeluje transformacijama $\mathbf{X}^1 = \mathbf{X}$ te $\mathbf{Z}^1 = \mathbf{Z}$. Vrijedi:

$$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -\beta \\ \alpha \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \cdot \begin{bmatrix} -\beta \\ \alpha \end{bmatrix} = \begin{bmatrix} \alpha \\ \beta \end{bmatrix},$$

te je stanje **Bobova** qubita $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \alpha |0\rangle + \beta |1\rangle$.

U svakom od četiri slučaj, stanje **Bobova** qubita jednako je stanju originalnog qubita od Alice prije teleportacije. Eksperimentalno, kvantna teleportacija potvrđena je na mikroskopskim objektima poput fotona. Problem opažanja kvantnih fenomena na makroskopskim, ali i mikroskopskim objektima, može se objasniti, iako ne isključivo, kvantnom dekoherencijom ⁹ Također, svako međudjelovanje sustava s okolinom je zapravo mjerenje toga sustava. [18] Kako bi se ti problemi što bolje nadišli, eksperimentalni fizičari koriste se uvjetima niske temperature ($T \approx 0$ K) ili ultrabrzim laserima pomoću kojih je moguće detektirati koherenciju kratkoživućih kvantnih stanja. U radu *Quantum teleportation from light beams to vibrational states of a macroscopic diamond* [19] korištenjem procesa kvantne tomografije ¹⁰ ostvarena je kvantna teleportacija s uspješnosti $(90,6 + 1,0)\%$ korištenjem titanijevog lasera valne duljine $\lambda = 706,5$ nm. Svakako, valja naglasiti razliku između *Science Fiction* teleportacije složenih objekata od kvantne teleportacije kvantnog stanja.

⁹Kvantna dekoherencija ireverzibilan je gubitak koherencije sustava.

¹⁰Kvantna tomografija služi za rekonstrukciju stanja sustava prije mjerenja uzastopnim mjerenjem na ansamblu identičnih, izlaznih, kvantnih stanja.

4 Kvantna računala i algoritmi

Cilj druge kvantne revolucije je izrada efikasnog i pouzdanog kvantnog računala. Ingeniozna ideja Paula Anthony Benioffa o kreiranju kvantne verzije Turingova stroja, kao i članak *Simulating physics with computers* Richarda Feynmana, unazad dvadesetak godina bude pažnju znanstvenika i šire publike zbog potencijalno brže i efikasnije obrade informacija. Od 2019. godine, kada je IBM predstavio svoju verziju kvantnog računala, *IBM Quantum System One*, novčana sredstva koja su usmjerena prema *Start-Up* tvrtkama povezanih s implementacijom kvantnih tehnologija, prema procjeni konzultantske tvrtke *McKnissey & Co.*, iznosila su 1,4 milijarde dolara 2021. godine, što je povećanje od gotovo 100% u odnosu na 2020. godinu. Prema istom izvoru, među državama, Narodna Republika Kina ima najveća javna ulaganja u kvantne tehnologije u odnosu na ostale. Ove godine, Kineska tehnološka kompanija Baidu Inc. objavila je kako su izradili kvantno računalo *Qian-Shi* s procesorom od 10 qubita, a nedugo nakon toga, unaprijeđeno kvantno računalo s procesorom od 36 qubita. S druge strane, računalo *IBM Quantum System One* podržava tri IBM-ova procesora, 27 qubitni *Falcon* procesor, 65 qubitni *Hummingbird* procesor te najnoviji 127 qubitni *Eagle* procesor. Korištenje kvantnih računala podrazumijeva implementaciju kvantnih algoritama. Algoritam ¹¹ označava skup svih simbola i postupaka za rješavanje problema, a potječe od latiniziranog imena iranskog matematičara i astronoma Abu Džafar Muhamad ibn Musa-al-Hvarizmi.

4.1 Deutschov algoritam

Deutschov algoritam [3] određuje je li nepoznata funkcija $f : \{0, 1\} \rightarrow \{0, 1\}$ konstantna, $f(0) = f(1)$, ili je balansirana, $f(0) \neq f(1)$. Klasični algoritam zahtijeva izvrednjavanje funkcije f dva puta, za ulazne vrijednosti 0 i 1. Potrebno je pripremiti dva qubita u stanju $|0\rangle \otimes |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |0\rangle \otimes |1\rangle)$. Operator U_f dan je s djelovanjem:

$$|a\rangle \otimes |b\rangle \mapsto |a\rangle \otimes |(b + f(a)) \pmod{2}\rangle, a, b \in \{0, 1\}. \quad (20)$$

Kako bismo pokazali da je operator U_f unitaran, treba provjeriti svaki od četiri slučaja:

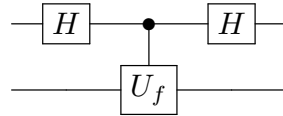
- | | |
|----------------------|-------------------------------|
| 1. $f(0) = f(1) = 0$ | 3. $f(0) = 0 \wedge f(1) = 1$ |
| 2. $f(0) = f(1) = 1$ | 4. $f(0) = 1 \wedge f(1) = 0$ |

¹¹algoritam - Hrvatska enciklopedija, mrežno izdanje. Leksikografski zavod Miroslav Krleža, 2021. (26.10.2022.)

Uzmimo za primjer slučaj 3., $f(0) = 0 \wedge f(1) = 1$. Tada je djelovanje operatora \mathbf{U}_f dano s:

$$\begin{aligned} |0\rangle \otimes |0\rangle &\mapsto |0\rangle \otimes |(0 + f(0)) \pmod{2}\rangle = |0\rangle \otimes |0\rangle, \\ |0\rangle \otimes |1\rangle &\mapsto |0\rangle \otimes |(1 + f(0)) \pmod{2}\rangle = |0\rangle \otimes |1\rangle, \\ |1\rangle \otimes |0\rangle &\mapsto |0\rangle \otimes |(0 + f(1)) \pmod{2}\rangle = |1\rangle \otimes |1\rangle, \\ |1\rangle \otimes |1\rangle &\mapsto |1\rangle \otimes |(1 + f(1)) \pmod{2}\rangle = |1\rangle \otimes |0\rangle, \end{aligned} \quad \mathbf{U}_f^\dagger = \mathbf{U}_f = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Slično se pokaže i za preostale slučaje. Koristimo kvantni logički sklop sa slike 29.



Slika 29: Logički sklop za Deutschov algoritam

Prolaskom kroz Hadamardova vrata, stanje je:

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

Prolaskom kroz kontrolna \mathbf{U}_f vrata stanje je dano s:

$$\begin{aligned} &\frac{1}{2} [|0\rangle \otimes |(0 + f(0)) \pmod{2}\rangle - |0\rangle \otimes |(1 + f(0)) \pmod{2}\rangle + \\ &\quad |1\rangle \otimes |(0 + f(1)) \pmod{2}\rangle - |1\rangle \otimes |(1 + f(1)) \pmod{2}\rangle], \end{aligned}$$

odnosno

$$\begin{aligned} &\frac{1}{2} [|0\rangle \otimes (|(0 + f(0)) \pmod{2}\rangle - |(1 + f(0)) \pmod{2}\rangle) + \\ &\quad |1\rangle \otimes (|(0 + f(1)) \pmod{2}\rangle - |(1 + f(1)) \pmod{2}\rangle)]. \end{aligned}$$

Možemo primjetiti sljedeće:

1. $f(0) = 0$

$$|(0 + f(0)) \pmod{2}\rangle - |(1 + f(0)) \pmod{2}\rangle = (-1)^{f(0)} (|0\rangle + |1\rangle),$$

2. $f(0) = 1$

$$|(0 + f(0)) \pmod{2}\rangle - |(1 + f(0)) \pmod{2}\rangle = (-1)^{f(0)} (|0\rangle + |1\rangle),$$

3. $f(1) = 0$

$$|(0 + f(1)) \pmod{2}\rangle - |(1 + f(1)) \pmod{2}\rangle = (-1)^{f(1)} (|0\rangle - |1\rangle),$$

4. $f(1) = 1$

$$|(0 + f(1)) \pmod{2}\rangle - |(1 + f(1)) \pmod{2}\rangle = (-1)^{f(1)}(|0\rangle - |1\rangle).$$

Sada prethodno dobiveno stanje možemo zapisati kao:

$$\frac{1}{2} [|0\rangle \otimes (-1)^{f(0)}(|0\rangle + |1\rangle) + |1\rangle \otimes (-1)^{f(1)}(|0\rangle - |1\rangle)].$$

Prolaskom kroz druga Hadamardova vrata, konačno stanje glasi:

$$\frac{1}{2} \left[\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes (-1)^{f(0)}(|0\rangle + |1\rangle) + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \otimes (-1)^{f(1)}(|0\rangle - |1\rangle) \right],$$

što sređivanjem daje

$$\frac{\sqrt{2}}{4} \{ |0\rangle \otimes [(-1)^{f(0)} + (-1)^{f(1)}] (|0\rangle - |1\rangle) + |1\rangle \otimes [(-1)^{f(0)} - (-1)^{f(1)}] (|0\rangle - |1\rangle) \}.$$

Ako je:

1. funkcija konstantna, $f(0) = f(1)$, tada je

$$[(-1)^{f(0)} - (-1)^{f(1)}] = 0,$$

a stanje prvog qubita je $|0\rangle$.

2. funkcija balansirana, $f(0) \neq f(1)$, tada je

$$[(-1)^{f(0)} + (-1)^{f(1)}] = 0,$$

a stanje prvog qubita je $|1\rangle$.

Time je pokazano kako je jednim mjerenjem moguće ustanoviti je li polazna nepoznata funkcija konstantna ili balansirana.

4.2 Shorov algoritam

Jedan od najpoznatijih kvantnih algoritama koji pokazuje nadmoć nad najefikasnijim klasičnim algoritmom faktoriziranja je Shorov algoritam. Peter Shor 1994. godine objavljuje rad *Algorithms for quantum computation: discrete logarithms and factoring* u kojem daje kvantni algoritam za rješavanje problema faktorizacije i diskretnog logaritma. Već iduće godine, doraduje prvi rad, ispravljajući manju pogrešku u algoritmu za rješavanje diskretnog logaritma i objavljuje *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*. U srcu Shorovog algoritma nalazi se kvantni Fourierov transformat. Potreba za korištenje kvantnog Fourierovog transformata proizašla je iz ideje Petra Shora kako spojiti problem traženja perioda funkcije s poznatim tehnikama u fizici.

4.2.1 Kvantni Fourierov transformat

Neka je $|j\rangle$ element ortonormirane baze $\{|0\rangle, |1\rangle, \dots, |q-1\rangle\}$, gdje je $q = 2^n$.

Definicija 4.1. Kvantni Fourierov transformat je unitarna transformacija ¹² koja $|j\rangle$ preslika u uniformnu linearnu kombinaciju vektora Fourierove baze:

$$|j\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{k=0}^{2^n-1} \exp\left\{\frac{2 \cdot \pi \cdot \mathbf{i}}{q} \cdot j \cdot k\right\} |k\rangle \quad (21)$$

Uobičajeno je $k \in \mathbb{N}$ zapisati u obliku binarnog razvoja kao, [17]:

$$k = 2^{n-1}k_1 + 2^{n-2}k_2 + \dots + 2^0k_n = \sum_{l=1}^n 2^{n-l}k_l, \quad (22)$$

$$|k\rangle = |k_1k_2 \dots k_n\rangle \quad (23)$$

Tada je kvantni Fourierov transformat uobičajeno pisati kao

$$|j\rangle \mapsto \frac{1}{\sqrt{q}} \sum_{k_1=0}^1 \sum_{k_2=0}^1 \dots \sum_{k_n=0}^1 \exp\left\{2 \cdot \pi \cdot \mathbf{i} \cdot \sum_{l=1}^n 2^{-l} \cdot k_l \cdot j\right\} |k_1 \dots k_n\rangle, \quad (24)$$

što je u preglednijem obliku dano pomoću tenzorskog produkta

$$|j\rangle \mapsto \frac{1}{\sqrt{q}} \left(|0\rangle + \exp\left\{\frac{2 \cdot \pi \cdot \mathbf{i} \cdot j}{2^1}\right\} |1\rangle \right) \otimes \dots \otimes \left(|0\rangle + \exp\left\{\frac{2 \cdot \pi \cdot \mathbf{i} \cdot j}{2^n}\right\} |1\rangle \right) \quad (25)$$

Za izvođenje kvantnog Fourierovog transformata, [20], koriste se Hadamardova vrata, vrata operator faznog pomaka i SWAP vrata. Neka su i i m i -ti i m -ti bitovi. Definiraju se kvantna logička vrata R_i

$$R_i = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},$$

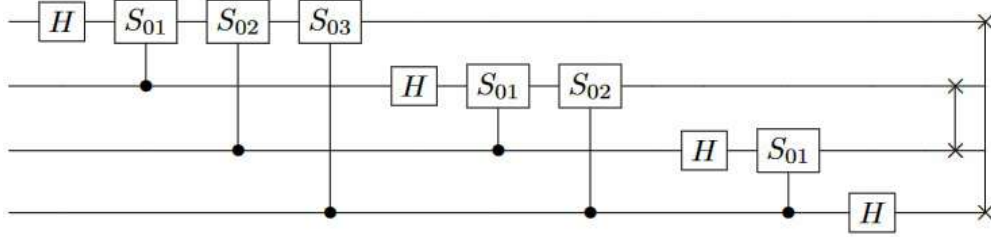
koja su zapravo Hadamardov operator koji djeluje na i -ti bit te kvantna logička vrata S_{im}

$$S_{im} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \omega \end{bmatrix}, \omega = \exp\left\{\mathbf{i} \cdot \frac{\pi}{2^{m+1-i}}\right\}$$

koja djeluju na bitove s pozicijama i i m kada je $i < m$.

Primjer 4.1. Na slici 30 dan je kvantni logički sklop koji izvodi 4-qubitni kvantni Fourierov transformat.

¹²Unitarnost se pokazuje u obliku propozicije, ali kako je to kvantni operator, ona se nužno zahtjeva.



Slika 30: Kvantni logički sklop koji izvodi 4-qubitni kvantni Fourierov transformat.

Broj 15 ima binarni zapis 1111. Djelovanje kvantnog Fourierovog transformata na $|15\rangle = |1111\rangle$, za $q = 2^n = 16$, je

$$\begin{aligned} |\widetilde{15}\rangle = \frac{1}{\sqrt{16}} & \left(|0\rangle + \exp\left\{\frac{2 \cdot \pi \cdot i \cdot 15}{2^1}\right\} |1\rangle \right) \otimes \left(|0\rangle + \exp\left\{\frac{2 \cdot \pi \cdot i \cdot 15}{2^2}\right\} |1\rangle \right) \otimes \\ & \left(|0\rangle + \exp\left\{\frac{2 \cdot \pi \cdot i \cdot 15}{2^3}\right\} |1\rangle \right) \otimes \left(|0\rangle + \exp\left\{\frac{2 \cdot \pi \cdot i \cdot 15}{2^4}\right\} |1\rangle \right) \quad (26) \end{aligned}$$

Primijetimo faktor $\frac{1}{\sqrt{q}}$ koji je dobiven korištenjem Hadamardovih vrata. U slučaju $q = 2^4$ rezultira faktorom $\frac{1}{\sqrt{2^4}} = \frac{1}{4}$. Djelovanjem kvantnog Fourierovog transformata na prvi qubit, on prolazi kroz Hadamardova vrata i troje S vrata. Hadamardov operator djeluje na $|1\rangle$ i daje rezultat

$$\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left\{2 \cdot \pi \cdot i \cdot \frac{1}{2}\right\} |1\rangle \right)$$

Sada troje S vrata doprinose relativnoj fazi s $\exp\{2 \cdot \pi \cdot i \cdot \frac{1}{4}\} \cdot \exp\{2 \cdot \pi \cdot i \cdot \frac{1}{8}\} \cdot \exp\{2 \cdot \pi \cdot i \cdot \frac{1}{16}\}$,

$$\begin{aligned} \frac{1}{\sqrt{2}} & \left(|0\rangle + \exp\left\{2 \cdot \pi \cdot i \cdot \left(\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16}\right)\right\} |1\rangle \right) = \\ & \frac{1}{\sqrt{2}} \left(|0\rangle + \exp\left\{2 \cdot \pi \cdot i \cdot \frac{15}{16}\right\} |1\rangle \right), \end{aligned}$$

djelovanjem **SWAP** vrata¹³, dolazimo do rezultata.

Cliffordova grupa ne sadrži sva S_{im} vrata te je time onemogućena efikasna implementacija kvantnog Fourierovog transformata na klasičnom računalu. Ipak, danas postoje računalni programi koji dobro izvode kvantni Fourierov transformat za manji broj qubita.

4.2.2 Shorov algoritam za faktorizaciju

Pokazat ćemo primjenu Shorova algoritma [20] za faktorizaciju broja $N = 21$.

Primjer 4.2. Faktorizacija broja $N = 21$.

¹³Dobiveni rezultat za prvi qubit dolazi kao zadnji član tenzorskog produkta u 26.

1. Odaberemo $q = 2^n$ tako da vrijedi $N^2 \leq q \leq 2N^2$.

$$\begin{aligned} 21^2 &= 441 \\ 2 \cdot 21^2 &= 882 \\ \implies q &= 2^9 = 512 \end{aligned}$$

2. Odaberemo prirodan broj y koji je relativno prost s brojem $N = 21$. Bez smanjenja općenitosti, odaberemo $y = 2$.

$$\text{NZD}(2, 21) = 1$$

3. Stvorimo dva međusobno spregnuta kvantna registra, ulazni i izlazni. Ulazni registar mora sadržavati dovoljno qubita kako bi se prikazao broj do $q - 1$, što u slučaju $q - 1 = 440$ iznosi $n = 9$ qubita. Izlazni registar mora biti dovoljno velik da prikažemo broj do $N - 1$, što u slučaju $N - 1 = 20$, gdje je 21 u binarnom zapisu 10101 iznosi 5 qubita. Izlazne registre postavimo na nulu.

$$\frac{1}{\sqrt{2^9}} \sum_{a=0}^{2^9-1} |a, 0\rangle$$

4. Djelujemo transformacijom $y^a \pmod{N}$ na svaki broj u prvom registru i te vrijednosti pohranimo u drugi registar.

| ulazni (a) | izlazni (i) |
|----------------|----------------------|
| 0 | $2^0 \pmod{21} = 1$ |
| 1 | $2^1 \pmod{21} = 2$ |
| 2 | $2^2 \pmod{21} = 4$ |
| 3 | $2^3 \pmod{21} = 8$ |
| 4 | $2^4 \pmod{21} = 16$ |
| 5 | $2^5 \pmod{21} = 11$ |
| 6 | $2^6 \pmod{21} = 1$ |

$$\frac{1}{\sqrt{2^9}} \{ |0, 1\rangle + |1, 2\rangle + |2, 4\rangle + \dots + |255, 2^{440} \pmod{21}\rangle \}$$

5. Mjerimo drugi registar [21]. Pretpostavimo da smo mjerenjem dobili rezultat 4 i neka je M broj elemenata drugog registra, Tada je:

$$\begin{aligned} &\frac{1}{\sqrt{M}} \{ |2, 4\rangle + |8, 4\rangle + |14, 4\rangle + \dots + \dots \} = \\ &\frac{1}{\sqrt{M}} \{ |2, 4\rangle + |2 + 6 \cdot 1, 4\rangle + |2 + 6 \cdot 2, 4\rangle + \dots \}. \end{aligned}$$

Za $a_0 + r \cdot (M - 1) < N$, općenito vrijedi:

$$\frac{1}{\sqrt{2^9}} \{ |a_0, 4\rangle + |a_0 + r \cdot 1, 4\rangle + |a_0 + r \cdot 2, 4\rangle + \dots + |a_0 + r \cdot (M - 1), 4\rangle \},$$

6. Primijenimo inverzni kvantni Fourierov transformat na ulazni registar [11]:

$$\frac{1}{\sqrt{M \cdot 2^9}} \sum_{s=0}^{255} \sum_{k=0}^{M-1} \exp \left\{ -2 \cdot \pi \cdot i \cdot \frac{s \cdot (a_0 + k \cdot r)}{2^9} \right\} |s, 4\rangle$$

7. Računamo vjerojatnost da mjerenjem dođemo do stanja $|s, 4\rangle$.

$$p(s) = \frac{1}{M \cdot 2^9} \left| \sum_{k=0}^{M-1} \exp \left\{ -2 \cdot \pi \cdot i \cdot \frac{s \cdot k \cdot r}{2^9} \right\} \right|^2,$$

gdje je izlučeni član $\exp \left\{ \frac{2 \cdot \pi \cdot i \cdot s \cdot a_0}{2^9} \right\}$ jer je njegov iznos jednak 1.

8. Izmjerimo s . Maksimalne vrijednosti amplitude vjerojatnosti bit će ostvarene za

$$\begin{aligned} \frac{s \cdot r}{q} &\approx p \in \mathbb{N} \\ \implies \frac{s}{q} &\approx \frac{p}{r} \end{aligned}$$

Za $s = 427$ vrijedi, koristeći metodu kontinuiranih razlomaka

$$\frac{s}{q} = \frac{427}{512} = 0 + \frac{1}{1 + \frac{1}{5 + \frac{1}{42 + \frac{1}{2}}}}$$

Zaključujemo da je $r = 6$. Ako je dobiveni r jednak nuli ili je neparan, potrebno je ponoviti algoritam s drugom bazom y . Za paran r vrijedi $(y^r - 1) = (y^{\frac{r}{2}} - 1) \cdot (y^{\frac{r}{2}} + 1)$. [22] Kako je dobiveni r paran broj, vrijedi $2^{\frac{6}{2}} \pmod{21} = \alpha$, što je u ovom slučaju $\alpha = 8$. Ako je $\alpha + 1 \not\equiv 0 \pmod{21}$, onda su faktori broja $N = n_1 \cdot n_2$ najveći zajednički djelitelji brojeva $(\alpha - 1) = 7$ i 21 te $(\alpha + 1) = 9$ i 15 , odnosno $n_1 = 7$ i $n_2 = 3$.

Godine 2019. objavljen je rad *An Experimental Study of Shor's Factoring Algorithm on IBM Q* u kojem se Shorov algoritam primijenio na kvantnom računalu, [22]. U radu navode kako su dobiveni rezultati u skladu s teorijom za brojeve $N = 15$ i $N = 21$, ali veća odstupanja su primijećena za $N = 35$. Točnost je veća što je potrebno manje qubita u izlaznom registru, radi izraženijeg utjecaja kvantne dekoherencije na sustave s više qubita.

4.3 Budućnost kvantnih računala

U današnje vrijeme, efikasnost i pouzdanost kvantnih računala i dalje nije zadovoljavajuća, odnosno njihova primjena za probleme koje uspješno rješavaju, poput faktorizacije manjih brojeva, nije isplativa. Rad kvantnih računala ovisi o preciznim mjerenjima, mogućnosti ispravljanja grešaka te komunikacijskim protokolima.

Precizna mjerenja Precizna mjerenja (eng. *Quantum metrology*) ostvaruju se korištenjem spregnutih čestica u *NOON* stanju, predloženih u članku [23] *A Quantum Rosetta Stone for Interferometry* trojca Hwang Lee, Pieter Kok i Jonathan P. Dowlinga, u **Mach – Zenderovom** interferometru. *NOON* stanje N spregnutih čestica dano je s

$$|\Psi_N\rangle = |N, 0\rangle + e^{i \cdot N \cdot \rho} |0, N\rangle,$$

gdje se prisustvo relativne faza $e^{i \cdot N \cdot \rho}$ koristi za pohranu odgovarajuće informacije [24].

Mogućnost ispravljanja grešaka Mogućnost ispravljanja grešaka (eng. *Quantum Control*) odnosi se na optimizaciju kvantnih procesa poput unaprijeđenih laserskih tehnika za željena pobuđenja atoma. Finim laserskim manipulacijama nad atomima, moguće je kreirati qubite za korištenje u prijenosu i obradi informacija.

Komunikacijski protokoli Komunikacijski protokoli (eng. *Quantum protocols*) poput **BB84** protokola predloženog od strane Charles H. Bennetta i Gilles Brassarda, omogućuju siguran prijenos informacije putem javnog kanala između dva subjekta. **BB84** protokol koristi polarizaciju fotona i njime se može odrediti je li prilikom prijenosa informacije kvantnim kanalom došlo do prisluškivanja od treće strane. Postoje i drugi komunikacijski protokoli, poput **E91** protokola Artura Ekerta.

BB84 protokol [11], [25]

1. Alice konstruira stanje sustava on n qubita

$$|\Psi\rangle = \bigotimes_{i=1}^n \Psi_{a_i b_i},$$

gdje su a i b stringovi duljine n , a a_i i b_i i -ti bitovi stringa a , odnosno stringa b . Svaki qubit $\Psi_{a_i b_i}$ element je ili standardne baze $\{|0\rangle, |1\rangle\}$ ili Hadamardove baze $\{|+\rangle, |-\rangle\}$. Vrijedi:

$$\begin{aligned} \Psi_{00} &= |0\rangle & \Psi_{01} &= |+\rangle \\ \Psi_{10} &= |1\rangle & \Psi_{11} &= |-\rangle. \end{aligned}$$

2. Putem javnog kvantnog komunikacijskog kanala Alice pošalje n qubita Bobu. Svaki primljeni qubit Bob izmjeri u jednoj od dvije baze, proizvoljno. Proizvoljni odabir baze realizira tako što odabere string b' duljine n . Ako je Alice pripremila k -ti qubit u stanju $|+\rangle$, odnosno $b_k = 1$, tada Bob izmjeri taj qubit u stanju $|+\rangle$ ako je izabrao Hadamardovu bazu. Ako je Bob izabranu standardnu bazu, odnosno vrijedi $b'_k = 0$, tada on izmjeri stanje $|0\rangle$, odnosno $|1\rangle$ s vjerojatnošću 50%. Nakon obavljenog mjerenja Bob bilježi vrijednost a_i u string a' , gdje je $a'_i = 0$ ako on izmjeri i -ti qubit u stanju $|0\rangle$ ili $|+\rangle$, odnosno $a'_i = 1$ u stanju $|1\rangle$ ili $|-\rangle$.

3. Alice i Bob putem klasičnog javnog kanala objave svoje stringove b i b' te iz poruke izbace svaki a_i, a'_i za koji vrijedi $b_i \neq b'_i$. Za $b_i = b'_i$ nužno vrijedi $a_i = a'_i$. Bez smanjenja općenitosti, neka je $b_i = b'_i = 0$, tada je Bob mjerio i -ti qubit u standardnoj bazi, a Alice je kreirala i -ti qubit u stanju $|0\rangle$ ili $|1\rangle$. Ako je Alice poslala i -ti qubit u stanju $|0\rangle$, tada Bob sa sigurnošću izmjeri i -ti qubit u stanju $|0\rangle$ te vrijedi $a_i = a'_i = 0$. Slično se pokaže i za ostale slučajeve.
4. Kako Alice i Bob koriste javne komunikacijske kanale, oni su podložni prisluškivanju. Neka treća osoba, Eva prisluškuje i -ti qubit koji je poslala Alice. Tada ona, ne znajući bazu u kojoj je Alice pripremila taj qubit, odabire krivu, odnosno točnu bazu mjerenja u 50% slučajeva. Eva će proći neprimijećeno, odnosno saznat će točno stanje u kojem je Alice pripremila svoj i -ti qubit bez njihova saznanja, ako ga pošalje Bobu koji će ga zatim izmjeriti u stanju kojem ga je pripremila Alice, odnosno ako Alice i Bob izaberu istu bazu. U 25% slučajeva, Eva će odabrati pogrešnu bazu i rezultat Bobova mjerenja će biti različit od stanja koje je pripremila Alice. Kako bi odredili jesu li prisluškivani, Alice i Bob usporede dio stringa a i a' te ovisno o rezultatu ponove postupak.

4.4 Životni vijek qubita

Vrijeme koje je qubit sposoban pohraniti neku informaciju ovisi o podložnosti materijala od kojeg je qubit sastavljen na dekoherenciju, odnosno koliko vremena prođe do kada interakcija s okolinom ne degenerira pohranjenu informaciju na qubit. Vrijeme dekoherencije [26] varira između 10^4 sekundi, za qubite napravljene pomoću nuklearnog spina jezgre, i 10^{-9} sekundi, za qubite od kvantnih točaka¹⁴. Za elektron, ono iznosi otprilike 10^{-5} sekundi. Idući veliki iskorak u izradi kvantnih računala je mogućnost rada pri sobnoj temperaturi. Zasad proizvedena kvantna računala, poput IBM-ova *Quantum System One*, rade na temperaturama bliskim $T = 0$ K¹⁵. Zanimljivi rezultat objavljen je u radu *Room-Temperature Quantum Bit Storage Exceeding 39 Minutes Using Ionized Donors in Silicon-28*, gdje je ostvarena koherentnost qubita od nuklearnog spina ioniziranih fosforovih iona u izotopno pročišćenom siliciju-28 od 39 minuta do čak 50 minuta pri sobnoj temperaturi, $T = 298$ K. Uklanjanjem elektrona, produljuje se vrijeme koherencije sustava, što daje prednost korištenju ioniziranih donora. Općenito, šum uzorkovan nabojem u donor materijalu uzrokuje dekoherenciju sustava qubita i time degeneraciju pohranjene informacije.

¹⁴Kvantni sustav u kojemu su elektron ili šupljina u poluvodiču zarobljeni u trodimenzionalnoj potencijalnoj jami dimenzija manjih od pripadne de Broglieove valne duljine. Izvor: <http://struna.ihj.hr/naziv/kvantna-tocka/18991/> (15.11.2022.)

¹⁵Područje niskotemperaturne fizike - *kriofizike*.

5 Zaključak

1935. godine, rad *Einstein - Podolsky - Rosen* potaknuo je raspravu o konzistentnosti fenomena spregnutosti u kvantnoj mehanici s teorijom relativnosti. Tek tridesetak godina kasnije, **John S. Bell** odbacuje tezu **Alberta Einsteina** o intrinzično sadržanim skrivenim varijablama kod spregnutih čestica, što je neformalno označilo kraj doba prve te početak doba druge kvantne revolucije. 80-tih godina prošlog stoljeća, fizičari, okupljeni oko **Richarda Feynmana**, krenuli su s izgradnjom formalizma kvantnog računanja - kvantnih logičkih vrata i sklopova. Osnovni pojam kvantnog računanja, qubit, počiva na principu superpozicije stanja prije mjerenja, što je revolucionarni odmak od determinističkog stanja klasičnih bitova. Unitarnim transformacijama nad qubitima, mijenja se njihovo stanje, što se opisuje prolaskom qubita kroz kvantna logička vrata. Implementacijom više kvantnih logičkih vrata, omogućeno je pokretanje kvantnih algoritama. Prvi kvantnomehanički algoritmi napravljeni su gotovo 30 godina prije pojave prototipa kvantnog računala. Rezultatom **Gottesman - Knillova teorema**, naglašena je premoć kvantnih algoritama koji koriste kvantna logička vrata van Cliffordove grupe, poput Shorova algoritma za faktorizaciju. Iako su pojedine kompanije uspjele proizvesti kvantna računala, njihova učinkovitost nije na razini kojom bi mogli zamijeniti klasična računala pri obavljanju zadataka. Očekivana efikasnost i nadmoć kvantnih računala još nisu realnost, jer njihov rad ovisi o mogućnosti savladavanja kvantnih fenomena, poput kvantne dekoherencije, a iako mogu izvoditi sve operacije kao i klasična, njihovo korištenje nije isplativo. U budućnosti, ako se savladaju poteškoće uzrokovane kvantnim fenomenima, očekuje se, ovisno o danom problemu, korištenje kombinacije kvantnih i klasičnih računala.

A Metodički dodatak

Predložak nastavnog sata Kvantne mehanike

Nastavna jedinica: **Primjena kvantne mehanike u informatici**

Ishodi na kraju nastavne jedinice:

1. Zadovoljavajuća
 - (a) Definira qubit i prikazuje ga na Blochovoj sferi.
 - (b) Definira osnova kvantna logička vrata i povezuje ih s rotacijama na Blochovoj sferi.
2. Dobra
 - (a) Određuje bazu Hilbertovog prostora korištenjem antipodalnih točaka.
 - (b) Tumači posljedice Gottesman-Knillova teorema.
3. Vrlo dobra
 - (a) Analizira djelovanje kvantnog logičkog sklopa na qubite.
 - (b) Argumentira prednost korištenja kvantnih algoritama.
4. Iznimna
 - (a) Procjenjuje korisnost korištenja kvantnih računala.
 - (b) Izvodi Bellovu nejednakost.

Postupci vrednovanja ishoda:

1. Zadovoljavajuća

Student točno određuje parove antipodalnih točaka na Blochovoj sferi. Student računa djelovanje kvantnih logičkih vrata na elemente baze. *Kako geometrijski opisujemo djelovanjem Paulijevih vrata X na elemente standardne baze?*
2. Dobra

Pokažite da parovi antipodalnih točaka Blochove sfere čine ortonormiranu bazu Hilbertovog prostora. Zašto nije moguće vjerno prikazati Shorov algoritam na klasičnom računalu? Jesu li sva vrata potrebna za izvođenje kvantnog Fourierovog transformata elementi Cliffordove grupe?
3. Vrlo dobra

Student temeljem kvantnog logičkog sklopa rješava dani problem. *Odredite djelovanje kvantnog logičkog sklopa sa slike - npr. za kvantnu teleportaciju. Student elaborira prednost kvantnih algoritama nad klasičnim. Objasnite razliku određivanja je li funkcija konstanta ili balansirana na klasičnom i kvantnom računalu.*

4. Iznimna

Student temeljeno na rezultatima pročitanih znanstvenih članaka argumentira koje su prednosti, a koji su nedostaci kvantnih računala danas. Student objašnjava utjecaj dekoherencije na vjernost rezultata. Student izvodi Bellovu nejednakost i njenu posljedicu na teoriju skrivenih varijabli u kvantnoj mehanici.

Nastavne metode:

1. Višesmjerna metoda rasprave

Profesor potiče studente na međusobnu komunikaciju prilikom iznošenja ideja. Metodom heurističkog razgovora, profesor vodi studente prema točnom odgovoru.

2. Metoda usmenog izlaganja

Profesore usmeno izlaže gradivo studentima, odgovara na pitanja i daje upute za rješavanje zadataka.

3. Metoda pisanja

Profesor piše na ploči, studenti prave bilješke.

Sociološki oblici rada:

1. Frontalni.

2. Individualni.

Nastavna sredstva i pomagala:

1. Prezentacija, stručna literatura, internet.

2. Ploča, kreda, računalo s projektorom.

Popis slika

| | | |
|----|---|----|
| 1 | Filteri međusobno okomite polarizacije | 3 |
| 2 | 3 polarizacijska filtera | 4 |
| 3 | Stereografska projekcija | 5 |
| 4 | Blochova sfera | 6 |
| 5 | Emisija para elektron - pozitron iz nestabilne jezgre | 9 |
| 6 | Grafički prikaz nejednadžbe 9 | 11 |
| 7 | Tablica istinitosti i simbol za logička vrata I (AND) | 13 |
| 8 | Tablica istinitosti i simbol za logička vrata ILI (OR) | 13 |
| 9 | Tablica istinitosti i simbol za logička vrata NE (NOT) | 14 |
| 10 | Tablica istinitosti i simbol za logička vrata ekskluzivno ILI (XOR) | 14 |
| 11 | X vrata | 15 |
| 12 | Y vrata | 16 |
| 13 | Z vrata | 16 |
| 14 | H vrata | 17 |
| 15 | P_ρ vrata | 18 |
| 16 | S i T vrata | 18 |
| 17 | $\sqrt{\text{NOT}}$ vrata | 19 |
| 18 | $\wedge \mathbf{Q}$ vrata | 20 |
| 19 | C_{NOT} vrata | 21 |
| 20 | Kvantni logički sklop | 22 |
| 21 | Toffolijeva vrata | 23 |
| 22 | SWAP vrata | 24 |
| 23 | SWAP vrata konstruirana pomoću C_{NOT} vrata. | 24 |
| 24 | HZH kvantni logički sklop | 25 |
| 25 | HXH kvantni logički sklop | 26 |
| 26 | Kvantni logički sklop koji izvodi klasičnu operaciju I (AND). | 27 |
| 27 | Kvantni logički sklop koji izvodi klasičnu operaciju ILI (OR). | 28 |
| 28 | Kvantni logički sklop za teleportaciju | 30 |
| 29 | Logički sklop za Deutschov algoritam | 33 |
| 30 | 4-qubitni Fourierov transformat | 36 |

Literatura

- [1] J. P. Dowling, G. J. Milburn, Quantum technology: the second quantum revolution, The Royal Society, vol. 361, 2003.
- [2] D. J. Griffiths, Introduction to Quantum Mechanics, Upper Saddle River, NJ: Pearson Prentice Hall, 2005.
- [3] E. Rieffe, W. Polak, Quantum computing – A Gentle Introduction, The MIT Press, Cambridge Massachusetts, 2011.
- [4] A. Einstein, B. Podolsky, N. Rosen, Can Quantum – Mechanical Description of Physical Reality Be Considered Complete?, Physical Review, vol. 47, 1935.
- [5] J.J. Biney, University of Oxford, „Einstein-Podolski-Rosen Experiment and Bell’s Inequality“, www.youtube.com/watch?v=uef_qN7VFuY, 2011.
- [6] L. Smolin, Einstein’s Unfinished Revolution, Penguin Books, 2020.
- [7] J. S. Bell, On The Einstein Podolsky Rosen Paradox, Physics 1, 1964.
- [8] B. Hensen, H. Bernien, A. Dréau, et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, Nature, 2015.
- [9] K. Horvatić: Linearna algebra, deveto izdanje, Golden marketing - Tehnička knjiga, Zagreb, 2004.
- [10] D. Gottesman, ”The Heisenberg Representation of Quantum Computers,” Group22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics, eds. S. P. Corney, R. Delbourgo, and P. D. Jarvis, pp. 32-43 (Cambridge, MA, International Press), 1999.
- [11] M. Kazalicki, Kvantno računanje - skripta, Sveučilište u Zagrebu, PMF - Matematički odsjek, 2022.
- [12] P. A. Benioff, ”The Computer as a Physical System: A Microscopic Quantum Mechanical Hamiltonian Model of Computers as Represented by Turing Machines”, Journal of Statistical Physics, 22, 563, 1980.
- [13] T. Toffoli, Reversible computing, Lecture Notes in Computer Science, vol 85., Springer, Berlin, Heidelberg., 1980.
- [14] W. Wootters, W. Zurek, A single quantum cannot be cloned, Nature 299, 802–803, 1982.

- [15] J. Hammoud, Kvantni aspekti crnih rupa, - Diplomski rad, Sveučilište u Zagrebu, PMF - Fizički odsjek, 2020.
- [16] V. Bužek, M. Hillery, "Quantum Copying: Beyond the No-Cloning Theorem". *Phys. Rev. A.* 54 (3): 1844–1852., 1996.
- [17] M. Nielsen, I. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Pres, 2010.
- [18] A. Dundović, Dekoherencija i problem mjerenja u kvantnoj mehanici - Diplomski rad, Sveučilište u Zagrebu, PMF - Fizički odsjek, 2013.
- [19] Y. P. Hou. et al., Quantum teleportation from light beams to vibrational states of a macroscopic diamond, *Nature Communications*, 2016.
- [20] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, *SIAM Journal on Computing*, vol. 26, nr. 5, 1484-1509, 1997.
- [21] G. E. Moorhouse, Shor's Algorithm for Factorizing Large Integers, University of Wyoming , University of Wyoming , 2000.
- [22] M. Amico, Z. H. Saleem, M. Kumph, An Experimental Study of Shor's Factoring Algorithm on IBM Q, *Physical Review A*, vol. 100, nr. 1, 2019.
- [23] H. Lee, P. Kook, J. P. Dowling, A Quantum Rosetta Stone for Interferometry, *Journal of Modern Optics*, vol 49., nr. 14/15, 2002.
- [24] Grün, D.S., K. Wittmann W., L.H. Ymai et al., Protocol designs for NOON states, *Communiation Physics* 5, 36, 2022.
- [25] J. A. Bergou, M. Hillery, *Introduction to the Theory of Quantum Information Processing*, Springer, 2013.
- [26] D. C. Marinescu, G. M. Marinescu, *Classical and Quantum Information*, Academic Press, 2012.