

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 69420

Simulacija kvantnog računala

Dominik Matić

Zagreb, svibanj 2021.

SADRŽAJ

1. Uvod	1
2. Kvantno računalo	3
2.1. Polarizacija svjetlosti	3
2.2. Kvantni bit	4
2.2.1. Definicija	4
2.2.2. Diracova notacija	5
2.2.3. Svojstva Hilbertovog prostora	5
2.2.4. Amplituda vjerojatnosti i vjerojatnost	6
2.2.5. Vektorski prikaz	6
2.3. Sustav kvantnih bitova i spregnutost	7
2.4. Kvantni operatori	7
2.5. Kvantni paralelizam	7
2.6. Kvantni logički kurg	7
3. Kvantni algoritmi	8
3.1. Groverov algoritam	8
3.2. Deutschov algoritam	8
3.3. Shorov algoritam	8
4. Simulacija kvantnog računala	9
4.1. Postojeći simulatori kvantnog računala	9
4.2. Izrada simulatora kvantnog računala	9
4.3. Primjeri simulacije kvantnih logičkih krugova	9
4.4. Prednosti i mane simulatora kvantnog računala	9
5. Zaključak	10
Literatura	11

1. Uvod

Neprestanim razvojem znanosti i tehnologije, kvantna računala postaju sve bitnijim dijelom računarstva. Predstavljaju sasvim drugačiji način računanja koji otvara vrata rješavanju mnogih problema koje klasično računalo, zbog same prirode problema, ili rješava znatno sporije ili uopće ne može riješiti u razumnom vremenu. Takvi problemi javljaju se u područjima kriptografije, umjetne inteligencije i strojnog učenja, računalne biologije, financija, simulacije kvantnih sustava kao i u ostalim područjima računarstva kao što su algoritmi pretraživanja.

Područje kriptografije je posebno zanimljivo jer se većina današnjih sigurnosnih mehanizama interneta temelji na matematičkim problemima za koje se smatra da su teško izračunljivi. To su primarno problem faktORIZACIJE velikih brojeva te problem diskretnog logaritma. Kvantno računalo efikasno rješava takve probleme, što je još devedesetih godina demonstrirao Peter Shor[2]. Naravno, iz toga slijedi da će kvantna računala biti velika prijetnja sigurnosti na internetu, no već su se počeli razvijati mehanizmi koji će biti otporni na napade kvantnim računalom[citati?] što samo govori o tome koliko je kvantno računalo blizu da postane veliki dio računarstva.

Potencijal kvantnog računala poznat je desetljećima te su već smišljeni i detaljno opisani mnogi od algoritama prikladni za takav način računanja. Sve što je preostalo je izgraditi računalo koja će moći provoditi te algoritme. Danas, IBM posjeduje kvantno računalo s najvećim brojem kvantnih bitova, njih čak 65, no ni to još nije dovoljno da bude korisno. Naime, problem nastaje s pojavom kvantne dekoherencije. Dekoherencija predstavlja gubitak informacije kvantnog sustava zbog interakcije s okolinom što onemogućava precizno ili čak bilo kakvo računanje. No, kvantno računarstvo je trenutno veliki predmet istraživanja te se napretci ostvaruju skoro svaki dan. Mogućnost izgradnje kvantnog računala sa dovoljno velikim brojem kvantnih bitova je sve izglednija, kao primjer, IBM obećava do 2023. godine izgraditi kvantno računalo sa 1000 kvantnih bitova[1].

S ciljem demonstracije nekih od mogućnosti kvantnog računala, ovaj rad se u prvom dijelu bavi osnovnim načelima kvantnog računala, tj. matematičkim modelom

kojim opisujemo kvantnomehaničke pojave koje nam omogućuju drugačiji način računanja. Nakon toga rad opisuje neke od algoritama namijenjenih za kvantno računalo te ćemo zatim neke od njih implementirati i demonstrirati u samostalno izgrađenom simulatoru.

2. Kvantno računalo

2.1. Polarizacija svjetlosti

Klasična fizika shvaća svjetlost kao transversalni elektromagnetski val koji može biti poraliziran na različite načine. Polarizacija svjetlosti određena je njenom električnom komponentom te je svjetlost koju emitiraju prirodni izvori svjetlosti uglavnom nepolarizirana. Tek kada se snop svjetlosti pusti kroz polarizator dobije se linearno polariziran val svjetlosti — val koji ima stalni smjer širenja okomit na smjer titranja. Njegova električna komponenta dana je jednadžbom:

$$E = E_0 \hat{p} e^{i\omega t} \quad (2.1)$$

gdje je \hat{p} jedinični vektor u smjeru polarizacije vala. Intenzitet ovako polariziranog vala biti će upola manji od intenziteta početnog nepolariziranog vala jer će točno toliko intenziteta polarizator apsorbirati. Kada ovakav val pustimo kroz još jedan polarizator (tzv. analizator), val koji ćemo dobiti jest:

$$E' = (E \cdot \hat{n}) \hat{n} = E_0 (\hat{p} \cdot \hat{n}) \hat{n} e^{i\omega t} = E_0 \cos \alpha \quad (2.2)$$

gdje je \hat{n} jedinični vektor u smjeru polarizacije analizatora, a α kut između vektora \hat{p} i \hat{n} . Intenzitet novog vala dobivamo po Malusovom zakonu:

$$I' = I \cos^2 \alpha \quad (2.3)$$

gdje je I intenzitet prethodno polariziranog vala. Drugim riječima, polarizacijom vala dobivamo njegovu projekciju na ravninu određenu kutom polarizatora.

U kvantnoj mehanici, svjetlost je definirana drugačije — kao niz fotona, nedjeljivih elementarnih čestica. Kod takve interpretacije postavlja se pitanje što se događa kada individualni fotoni prolaze kroz polarizator. Ako polarizator propušta projekciju, koja je uvijek manja ili jednaka ulaznom valu, što će se dogoditi fotonu, ako je on nedjeljiv? Eksperimenti su pokazali da će foton sa točno određenom šansom ili cijeli proći kroz

polarizator sa novim smjerom polarizacije ili biti apsorbiran. Ključan element takvih eksperimenata je činjenica da je nemoguće *niti u načelu* odrediti što će se dogoditi sa fotonom. To znači da čak uz poznavanje svih varijabli nekog sustava, nemoguće je deterministički odrediti ishod.

Prijelaze kvantnih sustava iz jednog stanja u drugo modeliramo takozvanom amplitudom vjerojatnosti:

$$a(\Phi \rightarrow \Psi) \quad (2.4)$$

koja je element skupa kompleksnih brojeva, a vjerojatnost da neki sustav koji je u stanju Φ bude izmjeren u stanju Ψ dobivamo na način:

$$p(\Phi \rightarrow \Psi) = |a(\Phi \rightarrow \Psi)|^2 \quad (2.5)$$

U slučaju polarizatora, vjerojatnost smo mogli izračunati pomoću Malusovog zakona što nam daje vjerojatnost prolaska fotona kroz polarizator jednaku

$$p(\Phi \rightarrow \Psi) = \cos^2 \alpha \quad (2.6)$$

iz čega je vidljiva amplituda vjerojatnosti:

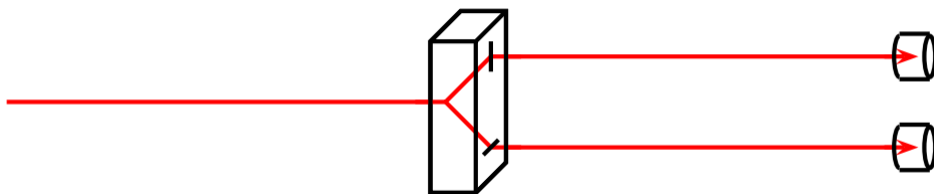
$$|a(\Phi \rightarrow \Psi)|^2 = \cos^2 \alpha \Rightarrow a(\Phi \rightarrow \Psi) = \cos \alpha \quad (2.7)$$

gdje je α kut koji zatvaraju vektori polarizacije fotona i polarizatora, Φ stanje fotona prije prolaska kroz polarizator, a Ψ stanje u kojemu foton nije apsorbiran.

2.2. Kvantni bit

2.2.1. Definicija

Dvolomac je vrsta polarizatora koji dijeli svjetlost na dva ortogonalno polarizirana snopa. Kombinirajući dvolomac sa dva detektora uvijek je moguće odrediti u koje je stanje prešao foton pušten kroz dvolomac.



Slika 2.1: Dvolomac s dva detektora

Nakon detekcije, foton je apsorbiran i ne može se više mjeriti. Takav kvantnomehanički sustav, koji je moguće samo jednom izmjeriti u samo jednom od dva moguća stanja nazivamo **kvantnim bitom** ili **qubitom**. Kvantni bit prije mjerenja može biti u beskonačno mnogo različitih stanja te općenito jedno takvo stanje zovemo **superpozicijom** dvaju stanja. Ta dva stanja se odnose na stanja baze mjerenja koja mogu biti proizvoljna, ali su uvijek međusobno ortogonalna. Pojam superpozicije se može primijeniti i u klasičnom smislu. U slučaju svjetlosti, uzimajući dva linearno polarizirana vala s okomitim smjerovima polarizacije kao bazu sustava, općenito stanje polarizacije vala možemo prikazati kao:

$$E = E_x \hat{x} e^{i(\omega t + \phi_x)} + E_y \hat{y} e^{i(\omega t + \phi_y)} = E_0 (\lambda \hat{x} + \mu \hat{y}) e^{i\omega t} \quad (2.8)$$

gdje vrijedi:

$$E_0 = \sqrt{(E_x^2 + E_y^2)} \quad \lambda = \frac{E_x}{E_0} e^{i\phi_x} \quad \mu = \frac{E_y}{E_0} e^{i\phi_y} \quad |\lambda|^2 + |\mu|^2 = 1 \quad (2.9)$$

Bitno je uočiti da su λ i μ kompleksni brojevi kao i da dio izraza $\lambda \hat{x} + \mu \hat{y}$ sadrži informaciju o stanju polarizacije vala te da takvih stanja ima beskonačno mnogo.

2.2.2. Diracova notacija

Stanja kvantnih bitova u praksi se prikazuje ket simbolima koji su dio Diracove ili bra-ket notacije:

$$\text{bra:} \quad \langle \Phi |$$

$$\text{ket:} \quad | \Phi \rangle$$

$$\text{braket:} \quad \langle \Phi | \Phi \rangle$$

S pretpostavkom da su $|x\rangle$ i $|y\rangle$ dva stanja baze mjerenja sustava, kao npr. stanje fotona polariziranog u smjeru x i stanje fotona polariziranog u smjeru y , općenito stanje polarizacije fotona možemo prikazati superpozicijom ta dva stanja:

$$| \Phi \rangle = \lambda |x\rangle + \mu |y\rangle$$

gdje su λ i μ kompleksni brojevi te vrijedi $|\lambda|^2 + |\mu|^2 = 1$.

2.2.3. Svojstva Hilbertovog prostora

U matematičkom smislu, stanja kvantnih bitova prikazanih ketovima su zapravo vektori dvodimenzionalnog kompleksnog Hilbertovog prostora. Za takav prostor vrijede sljedeća svojstva.

Skalarni umnožak:

$$\langle \Phi | \Psi \rangle = \langle \Psi | \Phi \rangle^* \in \mathbb{C}$$

$$\langle \Phi | \Phi \rangle \geq 0$$

Norma vektora $|\Phi\rangle$:

$$||\Phi|| = \sqrt{\langle \Phi | \Phi \rangle}$$

Vektori stanja baze moraju biti ortonormirani što znači da mora vrijediti:

$$\langle x | y \rangle = 0 \quad \langle x | x \rangle = \langle y | y \rangle = 1$$

Za računanje skalarnog umnoška potrebno je izračunati bra nekog stanja koji se dobiva kompleksnom konjugacijom keta. Općenito, izračun $\langle \Psi | \Phi \rangle$ dobiva se:

$$|\Phi\rangle = \lambda |x\rangle + \mu |y\rangle$$

$$|\Psi\rangle = \nu |x\rangle + \sigma |y\rangle \Rightarrow \langle \Psi | = \nu^* \langle x | + \sigma^* \langle y |$$

$$\langle \Psi | \Phi \rangle = \nu^* \lambda \langle x | x \rangle + \nu^* \mu \langle x | y \rangle + \sigma^* \lambda \langle y | x \rangle + \sigma^* \mu \langle y | y \rangle = \nu^* \lambda + \sigma^* \mu = \langle \Phi | \Psi \rangle^*$$

Norma vektora se računa na analogan način.

2.2.4. Amplituda vjerojatnosti i vjerojatnost

Amplituda vjerojatnosti modelira prijelaz jednog kvantnog stanja u drugo kojeg računamo skalarnim umnoškom vektora stanja.

$$a(\Phi \rightarrow \Psi) = \langle \Psi | \Phi \rangle$$

Odgovarajuća vjerojatnost mjerenja kvantnog bita u stanju Ψ ako se prethodno nalazio u stanju Φ računa se:

$$p(\Phi \rightarrow \Psi) = |a(\Phi \rightarrow \Psi)|^2 = |\langle \Psi | \Phi \rangle|^2$$

2.2.5. Vektorski prikaz

Za lakšu implementaciju kvantnog bita na klasičnom računalu, korisno je prikazati kvantne bitove vektorski. Klasična nula i jedinica bi imale vektorski oblik:

$$0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \quad 1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Ti vektori odgovaraju ujedno i vektorima stanja baze mjerenja nekog sustava koji se mogu označiti kao $|0\rangle$ i $|1\rangle$. Sva ostala stanja mogu se dobiti superpozicijom tih vektora:

$$|\Phi\rangle = \lambda |0\rangle + \mu |1\rangle = \lambda \begin{bmatrix} 1 \\ 0 \end{bmatrix} + \mu \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} \lambda \\ \mu \end{bmatrix}$$

Bra dobivamo kompleksnim konjugiranjem i transponiranjem keta:

$$\langle\Psi| = \begin{bmatrix} \nu \\ \sigma \end{bmatrix}^\dagger = \begin{bmatrix} \nu^* & \sigma^* \end{bmatrix}$$

Računanje amplitude vjerojatnosti se tada svodi na jednostavno matrično množenje:

$$\langle\Psi|\Phi\rangle = \begin{bmatrix} \nu^* & \sigma^* \end{bmatrix} \begin{bmatrix} \lambda \\ \mu \end{bmatrix} = \nu^* \lambda + \sigma^* \mu$$

2.3. Sustav kvantnih bitova i spregnutost

2.4. Kvantni operatori

2.5. Kvantni paralelizam

2.6. Kvantni logički kurg

3. Kvantni algoritmi

3.1. Groverov algoritam

3.2. Deutschov algoritam

3.3. Shorov algoritam

4. Simulacija kvantnog računala

- 4.1. Postojeći simulatori kvantnog računala**
- 4.2. Izrada simulatora kvantnog računala**
- 4.3. Primjeri simulacije kvantnih logičkih krugova**
- 4.4. Prednosti i mane simulatora kvantnog računala**

5. Zaključak

LITERATURA

- [1] Adrian Cho. IBM promises 1000-qubit quantum computer—a milestone—by 2023, September 2020. URL <https://www.sciencemag.org/news/2020/09/ibm-promises-1000-qubit-quantum-computer-milestone-2023>.
- [2] Peter W. Shor. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Sci. Statist. Comput.*, 26:1484, 1997. doi: 10.1137/S0097539795293172.

Simulacija kvantnog računala

Sažetak

Sažetak na hrvatskom jeziku.

Ključne riječi: Ključne riječi, odvojene zarezima.

Title

Abstract

Abstract.

Keywords: Keywords.