SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

ZAVRŠNI RAD br. 69420

Simulacija kvantnog računala

Dominik Matić

Zagreb, svibanj 2021.

SADRŽAJ

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 kvantog 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 provm 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

2.2. Kvantni bit i Diracova notacija

3. Simulacija kvantnog računala

3.1. Postojeći simulatori kvantnog računala

4. Kvantni algoritmi

4.1. Groverov algoritam

4.2. Deutschov algoritam

4.3. Shorov algoritam

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.