UDK: 004.3 Stručni rad

KVANTNI RAČUNARI: POTENCIJAL I PRIMENA

QUANTUM COMPUTERS: POTENTIAL AND APPLICATION

Jasmina Dj. Novakovic[1], Vladimir Veljovic[2]
[1]*Belgrade Business School, Higher Education Institution for Applied Studies*
[2]*Techical Faculty Cacak, University of Kragujevac*
[1]jnovakovic@sbb.rs, [2]veljo09@gmail.com

Abstrakt: *U radu su dati osnovni pojmovi i koncepti kvantnog računarstva. Oblast kvantnog računarstva bavi se proučavanjem računara zasnovanih na principima kvantne mehanike. Ostvarena su značajna dostignuća u ovoj oblasti i konstruisani prvi kvantni računari. Iako još uvek ne pokazuju svu snagu upotrebe kvantne mehanike, ovakav pomak u njihovom razvoju je evidentan, zbog čega možemo svrstati kvantne računare u obećavajuće tehnologije naslednike trenutne silicijumske arhitekture. U radu se razmatra i programiranje kvantnog računara koje se razlikuje od programiranja tradicionalnog računara. Radi adekvatnog opisivanja kvantnih algoritama javlja se potreba za razvijanjem jezika za kvantno programiranje. Uporedo sa razvojem kvantnih računara nameće se i potreba za odgovarajućom notacijom i kontrolnom strukturom koja omogućava rad sa kvantnim i drugim tipovima podataka. Takođe, u radu su prikazane mogućnosti korišćenja kvantnih računara u rešavanju praktičnih problema.*
Ključne reči: *kvantni računari, kubit, kvantno kolo.*

Abstract: *The paper presents the basic terms and concepts of quantum computing. Quantum computing is the study of computers based on the principles of quantum mechanics. There have been significant achievements in this field and constructed the first quantum computers. Although there still do not show all the power use of quantum mechanics, such a progress in their development is evidence, and it can be classified into promising successors of current silicon technology architecture. The paper considers the quantum computer programming that differs from traditional computer programming. For adequate describe quantum algorithms, there is a need to develop a language of quantum programming. Along with the development of quantum computers there is a need for an appropriate notation and control structure that enables work with quantum and other data types. Also, paper presents possibility of using quantum computers in solving practical problems.*
Key words: *quantum computers, qubit, quantum circuit.*

1. UVOD

Teorijska i praktična istraživanja razmatraju „Murov zakon“ i granicu do koje je moguće povećavati gustinu komponenata mikroprocesora, smanjujući im veličinu. Postoje istraživanja po kojima će ova granica biti dostignuta već za jednu deceniju, kako zbog veličine atoma, tako i zbog termodinamičkih svojstava sistema [1]. Razvoj novih tehnologija treba da omogući dalje ubrzanje rada računara kako bi se prevazišla ova ograničenja. Jedna od tehnologija koja najviše obećava je kvantno računarstvo. Da bi se kvantni računari koristili, neophodni su i odgovarajući programski jezici zasnovani na arhitekturi kvantnog računara.

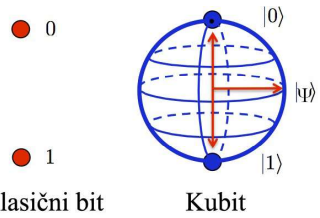
2. KONCEPTI KVANTNOG RAČUNARSTVA

Najvažniji koncepti kvantnog računarstva su u stvari dva osnovna pojma kvantne fizike: superpozicija i isprepletenost čestica. Osobina čestice da se nalazi u svim mogućim stanjima, dokle god ne dođe do njenog posmatranja, odnosno merenja predstavlja superpoziciju. Često navođen primer principa superpozicije je Šredingerova mačka koja bi istovremeno bila u oba stanja - i živa i mrtva, dok ne otvorimo kutiju, čime smo odredili njeno konačno stanje. Hajzenbergov princip neodređenosti takođe na ovo ukazuje, jer objašnjava da je nemoguće istovremeno precizno odrediti položaj i impuls čestice, što se odnosi i na druge zavisne parove veličina. Isprepletanost podrazumeva pojavu čestica u parovima ili grupama, gde promena na jednoj čestici utiče i na ostale, iako ne postoji direktan uticaj i na nju.

Osamdesetih godina prošlog veka počeo je razvoj kvantnog računarstva. Šor je 1994. godine objavio kvantni algoritam za faktorizaciju celih brojeva u polinomijalnom vremenu. Potom slede nova otkrića kvantnih algoritama. Do danas su ostvarena značajna dostignuća u ovoj oblasti i konstruisani prvi kvantni računari. Ovi računari još ne pokazuju svu snagu upotrebe kvantne mehanike, a zahtevaju i posebne uslove izolacije i temperaturu blizu apsolutne nule. Ali, ovakav pomak predstavlja dokaz da je kvantni računar moguće konstruisati, i da ga možemo svrstati u obećavajuće tehnologije naslednike trenutne silicijumske arhitekture, što potvrđuju i vodeći stručnjaci u oblasti arhitekture kvantnih računara.

3. MODEL KVANTNOG RAČUNARA

Kvantni računar predstavlja vrstu računara koji koriste mogućnost kvantnog sistema da bude u više stanja odjednom, omogućavajući time izvršenje velikog broja paralelnih operacija [2]. Možemo reći i da je kvantni računar onaj računar koji koristi osobine superpozicije u kvantnoj mehanici kako bi omogućio da se jedna operacija izvrši na velikom broju podataka [3].



Slika 1: Klasični bit i kubit

Prednost kvantnog računara, u odnosu na klasični je mogućnost paralelizacije izvršavanja programa, koja se postiže korišćenjem ranije pomenutih svojstava superpozicije i isprepletenosti.

Jedan od osnovnih koncepata kvantnog računarstva - kubit ili kvantni bit (Slika 1). Kubit predstavlja izolovan sistem sa dva stanja, kao ona kod klasičnog posmatranja bita, s tim što za takav izolovan sistem važe zakoni kvantne fizike. Takav sistem može biti i u stanju superpozicije, što kvantni algoritmi koriste kako bi ubrzali izračunavanje. Model kvantnog kola je uobičajen model koji se koristi, a sačinjen je od kvantnih registara i kvantnih logičkih kola, koja predstavljaju implementaciju standardnih logičkih operacija nad kubitima. Kvantna memorija i operacije nad njom predstavljaju osnovu rada kvantnog računara. U nastavku teksta dajemo opis najbitnijih segmenata na kojima se zasniva rad kvantnih računara.

Kod kvantnog računarstva osnovni nosilac informacije je kvantni bit ili **kubit**. Kubit predstavlja kvantni sistem čije se stanje može opisati kao linearna superpozicija $|\phi\rangle$ dva ortonormalna stanja zapisana kao $|0\rangle$ i $|1\rangle$. Superpozicija stanja se može zapisati na sledeći način: $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$, pri čemu su α , $\beta \in C$. Takođe, α i β se nazivaju amplitudama kvantnog stanja [4]. Stanja kvantnog sistema čine bazu N-dimenzionog Hilbertovog prostora, u kome je kvantno stanje vektor. Uobičajeno se posmatra sistem koji ima 2 stanja, iako teorijski mogu postojati sistemi sa N klasičnih stanja i u kom slučaju se superpozicija zapisuje kao:

$$|\phi\rangle = \alpha_1|1\rangle + \alpha_2|2\rangle + \alpha_3|3\rangle + \ldots + \alpha_N|N\rangle \qquad (1)$$

Kvanti registar čini skup, odnosno sekvenca kvantnih bitova. Kvantni registar sačinjen od n kvantnih bitova ima 2^n osnovnih stanja. U n-bitni kvantni registar moguće je upisati 2^n stanja dok je kod klasičnih računara to samo n bita.

U kvantnom stanju osnovna operacija je **merenje** i nju je najjednostavnije opisati kao pokušaj da se posmatranjem kvantnog bita dobije klasična vrednost. Ako posmatramo kvantno stanje kubita $|\phi\rangle$, mi ne možemo „videti" njegovu superpoziciju, već za normalizovani sistem kod kojeg je $|\propto|^2 + |\beta|^2 = 1$, mi možemo dobiti vrednost 0 sa verovatnoćom $|\propto|^2$ ili vrednost 1 sa verovatnoćom $|\beta|^2$. To znači da merenjem dolazi do zamene kvantnog stanja jednom od klasičnih vrednosti. U slučaju

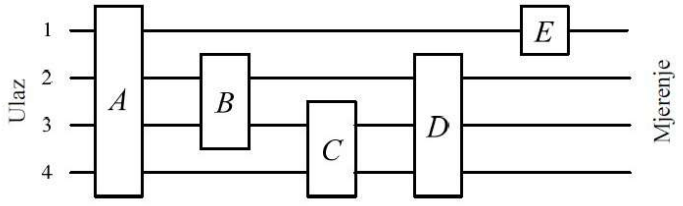
dvodimenzionalnog sistema, za merenje 1 kubita, to će biti 0 ili 1. Znatno složeniji slučaj predstavlja merenje stanja 2 ili više kubita [4].

U kvantnoj mehanici osim merenja kvantnog stanja $|\phi\rangle$, na njemu se mogu vršiti i operacije. Kvantna mehanika dozvoljava samo primenu linearnih operacija nad kvantnim stanjem. Ako npr. želimo naše stanje promeniti u neko $|\phi\rangle = \beta_1 |1\rangle + \beta_2 |2\rangle + \beta_3 |3\rangle + ... + \beta_N |N\rangle$, to bi podrazumevalo množenje matricom *U* dimenzija *NxN*. Navedena operacija morala bi očuvati formu vektora i mora biti unitarna. Operacija koja zadovoljava ovakve uslove, mora imati i svoju inverznu operaciju, što dovodi do prednosti **unitarnih transformacija** nad merenjem, jer se posmatranjem dobijenog klasičnog stanja ne može rekonstruisati stanje $|\phi\rangle$.

Kvantno kolo generalizuje ideju klasičnih logičkih kola, menjajući ih kvantnim kapijama, gde kvantna kapija predstavlja unitarnu operaciju na malom broju kubita, obično 1-3. Često se koristi Hadamardova transformacija (H), kao jednostavan primer kvantne kapije [4]. Hadamardova transformacija se matematički predstavlja kao:

$$|H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{2}$$

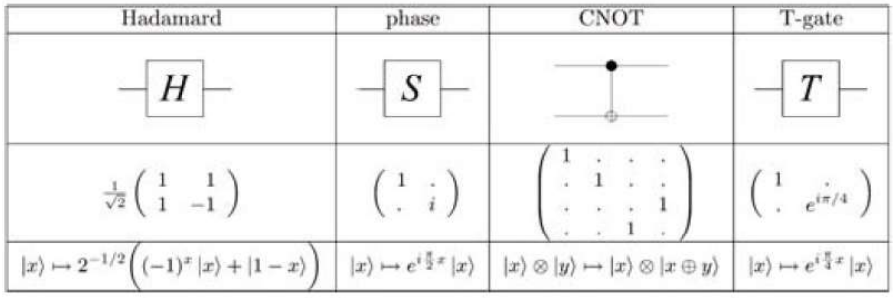
$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{3}$$



$$U = (E_1 \otimes \mathbb{1} \otimes \mathbb{1} \otimes \mathbb{1})(\mathbb{1} \otimes D_{234})(\mathbb{1} \otimes \mathbb{1} \otimes C_{34})(\otimes \mathbb{1} \otimes B_{23} \otimes \mathbb{1})(A_{1234})$$

Slika 2. Primer kvantnog kola

U slučaju da primenimo *H* na inicijalno stanje $|0\rangle$ ili na inicijalno stanje $|1\rangle$, verovatnoća da na izlazu dobijemo $|0\rangle$ ili $|1\rangle$ posmatranjem je jednaka. Ako primenimo *H* na superpoziciju $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$, sigurno dobijamo stanje $|0\rangle$, jer se pozitivna i negativna amplituda za $|1\rangle$ međusobno isključuju.



Slika 3. Najčešće korišćene kvantne kapije

Navedena pojava se naziva inteferencija, i analogna je inteferenciji kod svetlosnih ili zvučnih talasa. Kvantno kolo može biti sastavljeno iz više unitarnih transformacija, ali je broj unitarnih transformacija koje čine kolo konačan. Slika 2. prikazuje kvantno kolo koje je sastavljeno iz više unitarnih transformacija.

Najčešće korišćene kvantne kapije pored kapije za već pomenutu Hadamardovu transformaciju, su još i phase, CNOT (XOR) i T-gate kapija, što je prikazano na slici 3.

4. PROGRAMSKI JEZICI ZA KVANTNE RAČUNARE

Programiranje kvantnog računara se razlikuje od programiranja tradicionalnog računara. Kvantni računar je više zasnovan na verovatnoći, daje npr. i do 10.000 odgovora u sekundi, kao i više alternativa. Korisnik koristeći kvantni računar mapira problem na jednačinu čiji je cilj da vrati optimalno rešenje. Potrebno je obezbediti dve vrednosti: "težina" kubita i "jačina" u interakciji između njih. Pri tome, vrednosti se dostavljaju sistemu koji izvršava jednu kvantnu mašinsku instrukciju i vraća određeni broj rezultata korisniku.

Radi adekvatnog opisivanja kvantnih algoritama javlja se potreba za razvijanjem jezika za kvantno programiranje. Uporedo sa razvojem kvantnih računara nameće se i potreba za odgovarajućom notacijom i kontrolnom strukturom koja omogućava rad sa kvantnim i drugim tipovima podataka. Često se kvantni algoritmi opisuju pseudokodom ili u obliku kvantnih logičkih kola, pri čemu oba pristupa imaju ozbiljne nedostatke:

- pseudokodu nedostaje egzaktnost formalnih jezika,
- logička kola imaju veoma malu izražajnost [5].

Neki od zahteva koje jezik za kvantno programiranje mora da zadovoljava su [6]: potpunost, proširivost, separabilnost, izražajnost i nezavisnost. Zahtev za potpunošću podrazumeva da se jezikom može izraziti bilo koje kvantno logičko kolo i da time obezbedi programeru da napiše validan kvantni program. Proširivost kao zahtev podrazumeva da jezik mora uključivati kao svoj sastavni deo jezik koji implementira neku od klasičnih vodećih paradigmi. Pomenuti zahtev je važan jer neki kvantni algoritmi zahtevaju netrivijalno klasično računanje. Separabilnost kao uslov podrazumeva da kvantni i klasični delovi jezika bi trebalo da budu razdvojeni, čime se obezbeđuje da se klasična izračunavanja mogu izvršavati na klasičnoj mašini bez

kvantnih resursa. Uslov izražajnosti podrazumeva da jezik mora da obezbedi elemente za programiranje kvantnih algoritama. Nezavisnost kao uslov obezbeđuje da jezik mora biti nezavisan od fizičke implementacije kvantne mašine.
Za potrebe kvantnih računara razvili su se funkcionalni i imperativni jezici za kvantno programiranje. Funkcionalni jezici za kvantno programiranje zasnovani su na lambda računu i pokušavaju da spoje koncepte funkcionalnog programiranja sa kvantnom mehanikom. Prilikom razvijanja kvantnog lambda računa bitna stavka je da li se funkcije mogu smatrati kao klasični podaci ili kao kvantni podaci. Imperativni jezici za kvantno programiranje su naslednici kvantnog pseudokoda. I pored toga što su funkcionalni jezici zasnovani na čvršćoj formalnoj podlozi i lakši za analizu, imperativni jezici imaju praktičniju upotrebu i lakši su programerima za korišćenje jer su zasnovani na jezicima kao što su C i C++.

5. ZAKLJUČAK

Kvantno računarstvo će omogućiti raznim sferama privrede i nauke rešavanje problema koji su isuviše složeni za današnje računarske sisteme. Kvantno računarstvo ima ogromnu moć u obradi podataka takođe, rešavaju probleme mnogo brže nego klasični računari. Zbog toga se očekuje značajna civilna, tržišna i poslovna upotreba kvantnih računara. Što se tiče interneta očekuje se primena u: prepoznavanju slika i paterna, mašinskom učenju, komunikaciji i naprednoj pretragi. U laboratoriji kvantno računarstvo će se koristiti za: probleme optimizacije, probleme teorije grafova i nauku o materijalima.

Za univerzitetske potrebe kvantno računarstvo će se koristiti za: klimatsko modeliranje, bioinformatiku, vremensko predviđanje i istraživanje kvantnog računarstva. Za potrebe ekonomije u: modeliranju rizika, strategiji trgovine i finansijskom predviđanju. U oblasti energetike za: istraživanje energije, istraživanje seizmičke optimizacije, rezerve i optimizaciju trgovanja i optimizaciju skladištenja. U odbrani za: planiranje i logistiku misija, validaciju sistema i verifikaciju, prepoznavanje šablona i anomalija detekcije, nauku o mrežama i primeni teorije grafova. Treba ipak napomenutu i da postoje neki problemi koje kvantni računari ne mogu da reše koji su takođe nerešivi i od strane klasičnih računara.

LITERATURA

[1] Suhas Kumar. (2012). *Fundamental limits to moore's law*. Fundamental Limits to Moore's Law. Stanford University, 9.

[2] Collins english dictionary - complete and unabridged 10th edition. Apr 2016.

[3] The american heritage science dictionary. Apr 2016.

[4] S. Gay. (Januar 1999). *Quantum computation and Shor's factoring algorithm.* University of Amsterdam.

[5] Dominique Unruh. (2006). *Quantum programming languages*. Inform., Forsch. Entwickl., 21(1-2):55-63.

[6] Jaroslaw Adam Miszczak. (2010). *Introduction to models of quantum computation and quantum programming languages*. CoRR, abs/1012.6035.