Specifičnosti kvantnog računanja sa primenom na kvantnu teleportaciju

*SVETOMIR I. SIMONOVIĆ***,** Akademija tehničkih strukovnih studija, Beograd

Pregledni rad
UDC: 004.2:510.683
DOI: 10.5937/tehnika2305567S

U radu je objašnjen teoretsko-fizički osnov kvantnog računanja iz kojeg su izvedene specifične osobine kvantne obrade informacija. Potom je data logička reprezentacija kvantne obrade informacija kroz paradigmu kvantnih kola, definisane su neke teoretski važne kvantne kapije i dat poseban osvrt na postojanje univerzalnog skupa kvantnih kapija. Na kraju je dat primer primene paradigme kvantnih kola na generisanje zapletenih stanja kvantnih sistema i ostvarivanje kvantne teleportacije

Ključne reči: *kvantna kola, univerzalni skup kvantnih kapija, zapletena stanja, teleportacija*

1. UVOD

Kvantno računanje zasniva se na pojavama da se nosioci kvantnih jedinica informacija (kubitovi) mogu istovremeno nalaziti u više kvantnih stanja (superpozicija), da se ta stanja mogu preklapati i sabirati (interferencija) i da mogu biti međusobno zavisna (zapletenost) i to tako da se promena stanja jednog nosioca može trenutno odraziti na promenu stanja drugih nosilaca bez obzira na prostorni raspored nosilaca (kvantna teleportacija).

Kvantno računanje se obavlja paralelnim transformacijama početnih kvantnih stanja kvantnih nosilaca korišćenjem gore navedenih fenomena pri čemu se te transformacije mogu predstaviti kvantnim kapijama, a sam proces računanja organizacijom kvantnih kapija u kvantna kola. Na kraju procesa kvatnog računanja dobija se superpozicija rešenja (završnih kvantnih stanja) i vrši se očitavanje jednog od tako dobijenih kvantnih stanja.

Klasična jedinica informacija – bit na logičkom nivou se pretstavlja ili stanjem 0 ili stanjem 1. Bit se može fizički implementirati bilo čime što ima dva fizička stanja koja ne mogu postojati istovremeno.

Kao i bit, kubit može imati dva logička stanja koje se, analogno stanjima bita, standardno označavaju u Dirakovoj notaciji kao ketovi $|0\rangle$ i $|1\rangle$. Ali, za razliku od klasičnih bitova, kubitovi mogu istovremeno biti i u stanju $|0\rangle$ i stanju $|1\rangle$, preciznije, mogu biti u stanju proizvoljne linearne kombinacija stanja $|0\rangle$ i stanja$|1\rangle$.

Kubit se može fizički implementirati bilo čime što ima dva fizička stanja koja mogu postojati istovremeno.

Kubit se može na logičkom nivou predstaviti kao jedinični ket $|\psi>$ u dvodimenzionalnom Hilbertovom vektorskom prostoru čiji bazni ketovi formiraju otronormalnu bazu $\{|0\rangle,|1\rangle\}$, [1], odnoso kao linearna kombinacija baznih vektora stanja Hilbertovog vektorskog prostora - ketova $|0\rangle$ i $|1\rangle$, u vidu izraza

$$|\psi >= a\,|0\rangle + b \qquad (1)$$

gde su a, b kompleksni brojevi.

Za bazne vektore se usvajaju sledeće matrice kolone, [2, 3] :

$$|0\rangle = \binom{1}{0};\ |1\rangle = \binom{0}{1} \qquad (2)$$

Proizvoljni kubit $|\psi>$ se može predstaviti i geometrijski kao na slici 1, pri čemu se može pokazati da važi sledeća identičnost, u kojoj su oznake objašnjene slikom 1, [4] :

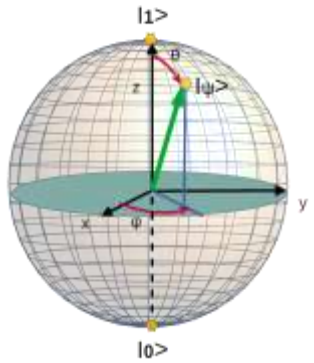
$$|\psi>=a|0\rangle + b|1\rangle \equiv cos(\theta/2)|0\rangle + e^{i\varphi}sin(\theta/2)|1\rangle \qquad (3)$$

gde

$$0 \le \theta \le \pi \quad i \quad 0 \le \varphi \le 2\pi$$

Pošto kubit može da bude bilo koji jedinični ket i pošto postoji beskonačno mnogo jediničnih ketova, to kubit može imati beskončno mnogo vrednosti. To je mnogo drugačije u poređenju sa klasičnim računanjem koje je zasnovano na samo dve moguće vrednosti bita.

Adresa autora: Svetomir Simonović, Akademija tehničkih strukovnih studija, Beograd, Katarine Ambrozić 3
e-mail: svetomir.simonovic@visokatehnicka.edu.rs
Rad primljen: 13.02.2023.
Rad prihvaćen: 16.10.2023.



Slika 1 - Geometrijska reprezentacija kubita u bazi $\{\ |0\rangle, |1\rangle\}$

Najnaprednija fizička implementacija kvantnog računanja danas zasnovana je na tehnologijama superprovodljivih kubita i kubita u jonskim zamkama. Najveće kvantno računanje do danas izvršio je Google u eksperimentu sa 53 kubitova radi dokazivanja „kvantne računske superiornosti", pri čemu je obavljen komplikovan (i prilično beskoristan) zadatak uzorkovanja koji, kako izgleda, ne može više da se simulira u razumnom vremenskom intervalu ni na najvećim postojećim superračunarima,[2, 5].

Postoje dva modela kvantnog računanja: model kvantne Turingove mašine, [6, 7], i model kvantnih kola, [8, 9]. Ova dva modela su ekvivalentna u smislu da mogu simulirati jedan drugog za polinomijalno vreme. Ovde će se u razmatranjima koristiti samo model kvantnih kola

2. O SUPERPOZICIJI I ZAPLETENOSTI QUBITOVA

Kvantna superpozicija je netrivijalna linearna kombinacija baznih vektora stanja koja daje jedinični vektor u Hilbertovom prostoru stanja. Stanje koje predstavljaju ovako dobijeni vektori se naziva čisto stanje,[1].

Stanje superpozicije kubita zavisi od izbora baznih stanja (baza). Sva stanja su u superpoziciji u odnosu na neke baze, a nisu u odnosu na druge, [10].

Kod kvantne superpozicije nije reč o sabiranju (dodavanju) u klasičnom smislu već o postojanju jednog kvantno-mehaničkog objekta ili skupa objekata u istovremenoj kombinaciji više kvantnih stanja, [11].

Sistem više kubita (registar) može postojati u separabilnoj ili zapletenoj superpoziciji stanja. Separabilna superpozicija stanja sistema je superpozicije stanja koja se može predstaviti tenzorskim proizvodom stanja svojih podsistema koji se nalaze u čistom stanju, [1].

Stanja sistema koja se ne mogu izraziti kao tenzorski proizvod stanja svojih komponentnih sistema u čistom stanju nazivaju se zapletena stanja. Postojanje zapletenih stanja je fizička činjenica koja ima važne konsekvence za kvantno računanje. Naime, bez postojanja takvih stanja kvantni računari ne bi bili moćniji od svojih klasičnih parnjaka,[12].

Dok klasičan registar, sastavljen od *n* binarnih bitova, može sadržati samo jedan od 2^n mogućih brojeva, odgovarajući kvantni registar, sastavljen od n kubitova, može sadržavati 2^n brojeva istovremeno, (slika 2). Na taj način, kvantni kopjuter sa registrom od 30 kubitova se može uporediti sa digitalnim kompjuterom koji je sposoban da izvrši 10^{13} (trillion) operacija u pokretnom zarezu po sekundi (TFLOPS) što je uporedivo sa trenutno najbržim računarima, [13].

Slika 2 – Poređenje klasičnog i kvantnog registra

Neka su $(|i_0\rangle, |i_1\rangle)$ i $(|j_0\rangle, |j_1\rangle)$ ortonormalne baze Hilbertovog vektorskog prostora. Posmatra se sistem od dva kubita u respektivnim stanjima $|\Phi\rangle = a\ |i_0\rangle\ + b\ |i_1\rangle$ i $|\Psi\rangle = c\ |j_0\rangle\ + d\ |j_1\rangle$.

Superpozicija navedenih stanja je njihov tenzorski proizvod:

$$\begin{aligned} |\Phi\rangle \otimes |\Phi\rangle &= (a|i_0\rangle +\ b|i_1\rangle) \otimes (c|j_0\rangle + d|j_1\rangle) = \\ &= ac|i_0\rangle\otimes|j_0\rangle + ad|i_0\rangle\otimes|j_1\rangle + \\ &\quad +bc|i_0\rangle\otimes|j_1\rangle + bd|i_1\rangle \otimes |j_1\rangle \qquad (4) \end{aligned}$$

Notacija se može uprostiti definisanjem $|i_x\rangle \otimes |i_y\rangle\ \equiv |i_x i_y\rangle$, pa prethodni izraz prelazi u

$$\begin{aligned} |\Phi\rangle|\Phi\rangle &= (a|i_0\rangle +\ b|i_1\rangle)(c|j_0\rangle + d|j_1\rangle) = \\ &= ac|i_0 j_0\rangle\rangle + ad|i_0 j_1\rangle\rangle + bc|i_0 j_1\rangle + \\ &\quad +bd|i_1 j_1\rangle \qquad (5) \end{aligned}$$

Tenzorski proizvodi $|i_0 j_0\rangle$, $|i_0 j_1\rangle$ $|i_1 j_0\rangle$ i $|i_1 j_1\rangle$ predstavljaju ortonormalnu bazu sistema $|\Phi\rangle|\Psi\rangle$, to jest svaki od navdenih tenzorskih proizvoda je jedinični vektor i svi proizvodi su međusobno ortogonalni. ac, ad, bc i bd su amplitude verovatnoće predmetnog sistema, a $(ac)^2$, $(ad)^2$, $(bc)^2$ i $(bd)^2$ su verovatnoće da će biti izmerene, respektivno, vrednosti 00, 01, 10 i 11.

Ako je stanje sistema od dva kubita

$$p\,|i_0 j_0\rangle + q\,|i_0 j_1\rangle + r\,|i_1 j_0\rangle + s\,|i_1 j_1\rangle \qquad (6)$$

tako da važi

$$p^2 + q^2 + r^2 + s^2 = 1 \;\; i \;\; ps \neq qr, \qquad (7)$$

ovo stanje se definiše kao zapleteno.

Ako se članovi vektora stanja napišu tako da prate subskripte u redosledu 00, 01, 10 i 11, onda predmetni kubiti nisu zapleteni ako je proizvod spoljašnjih amplituda verovatnoća jednak proizvodu unutrašnjih, u suprotnom su zapleteni, [14].

3. KVANTNO RAČUNANJE

Fundamentalna ideja kvantnog računanja je da se informacija uskladištena u kubitovima obrađuje putem kvantnih logičkih kapija. Ovo se može postići modifikovanjem Hamiltonovog operatora sistema putem primene dodatnih kontrolnih polja na osnovni Hamiltonov operator sistema, [15].

Kao i svaka druga evolucija kvantnog stanja, evolucija kvantnog stanja kubita ili sistema kubitova $|\psi\rangle$ definisana je rešenjem Šredingerove jednačine (8), što znači Hamiltonovim operatorom H te jednačine. Hamiltonov operator uzima u obzir ukupnu energiju sistema i specifični raspored atoma, molekula i naelektrisanja koji sačinjavaju računar. O Hamiltonovom operatoru se može razmišljati analogno modelu hardvera klasičnog računara a o početnom stanju kvantnog registra analogno podacima kojima je nahranjen klasični računar. Vremenski zavisna Šredingerova jednačina

$$i\hbar\, \partial/\partial t\, |\psi\rangle = H|\psi\rangle \qquad (8)$$

ima rešenje

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \qquad (9)$$

gde su $U(t)$ operator evolucije stanja, a $\psi(0)$ početno stanje sistema.

Ako je Hamiltonov operator vremenski nezavisan,

$$U(t) = exp(-i(H/\hbar)t \qquad (10)$$

Tada se evolucija kvantnog stanja kubita može opisati u kompaktnoj notaciji kao

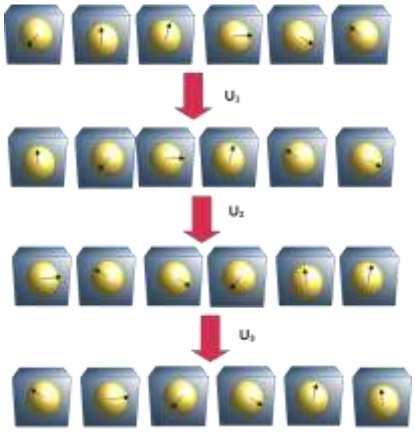
$$|\psi\rangle \xrightarrow{Ht} U|\psi\rangle \qquad (11)$$

Pošto je H hermitski operator, operator evolucije stanja U, koji se obično zove propagator, mora biti unitaran.

U mnogim slučajevima Hamiltonov operator je konstantan po konačnim vremenskim deonicama, pa se jedan konstantni Hamiltonov operator na kraju svoje vremenske deonice može zameniti drugim konstantnim Hamiltonovim operatorom za narednu konačnu vremensku deonicu. U tom slučaju se evolucija stanja može predstaviti nizom propagatora

$$|\psi\rangle \xrightarrow{H_1 t_1} \xrightarrow{H_2 t_2} \xrightarrow{H_3 t_3} U_3 U_2 U_1 |\psi\rangle \qquad (12)$$

gde je $U_1 = \exp[-i(H_1/\hbar)t_1]$ itd, (slika 3), [6].



Slika 3 - Kvantno računanje

Iz činjenice da je svaki propagator U koji opisuje evoluciju kvantnog sistema unitaran, odnosno da važi

$$U^{-1} = U^{\dagger} \qquad (13)$$

gde je $U^{\dagger}$ kompleksno konjugovana i transponovana matrica U, slede dve važne posledice.

Prva posledica je da svaki propagator ima svoj inverzni propagator, odnosno kvantna evolucija je povratna. To znači da nema gubitaka informacija (izuzetak od ovog opšteg principa je merenje), [15].

Druga posledica je da ove unitarne transformacije čuvaju intenzitet vektora stanja, pa evolucija izolovanog kubita pod dejstvom Hamiltonovog operatora odgovara rotaciji vektora na Blochovoj sferi, [15].

Model kvantnog računanja poseduje urođeni računski paralelizam, što sledi iz činjenice da se proizvoljna unitarna transformacija U može primeniti tako da istovremeno transformiše sva stanja u superpoziciji. Na primer, ako je dato stanje dvokubitnog registra

$$|\psi\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle \qquad (14)$$

onda

$$U|\psi\rangle = aU|00\rangle + bU|01\rangle + cU|10\rangle + dU|11\rangle \qquad (15)$$

i sve četiri računske operacije su izvršene u jednom računskom koraku, [17].

Kvantna informacija se ne može kopirati. Drugim rečima nemoguće je kopirati superpoziciju stanja jednog kvantnog registra u drugi kvantni registar. Može se pokazati da, ako je stanje u proizvoljnom dvokubitnom kvantnom registru $|P\rangle$ i ako je $|Q\rangle$ stanje u drugom dvokubitnom kvantnom registru, ond ne postoji unitarna transformacija U takva da

$$U\,|P\rangle\,|Q\rangle \rightarrow |P\rangle\,|P\rangle \qquad (16)$$

za bilo koje stanje $|P\rangle$. Ovo je tzv. Teorema nekloniranja, [17, 23].

4. MERENJE (OČITAVANJE)

Pre obavljenog merenja kvantni registar od n kubitova se nalazi u stanju superpozicije $|\mathbf{\Psi}\rangle$ svojih baznih stanja $|\mathbf{\Psi}\rangle_{\boldsymbol{k}}$ (izraz 11),

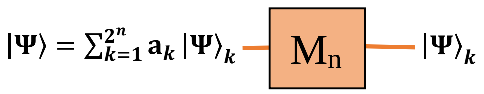
$$|\Psi\rangle = \sum_{k=1}^{2^n} a_k \, |\Psi\rangle_k \tag{17}$$

gde su koeficijenti a_k kompleksni brojevi, koji se nazivju amplitudr verovatnoće, za koje važi

$$\sum a_k^2 = 1 \tag{18}$$

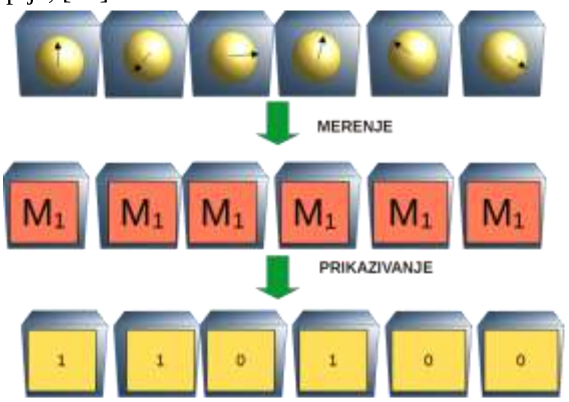
i koji su determinisani mernim instrumentom, [2]. Posle izvršenog merenja vektor stanja će preći u isključivo jedno od stanja $|\Psi\rangle_k$, sa verovatnoćom a_k^2, Ponovljeno merenje istim instrumentom daje poslednji rezultat merenja sa verovatnoćom 1. To znači da su sva stanja koja su bila u superpoziciji sa očitanim stanjem uništena, odnosno da je Kvantno-mehaničko merenje nepovratan proces,[17].

Proces merenja (očitavanja) obavlja se delom hardvera sa digitalnim displejom koji je poznat pod nazivom n-kubitna merna kapija M_n (koja je šematski prikazana na na slikama 4 i 5)



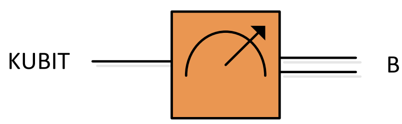
Slika 4 – Merenje

Može se pokazati da se n-kubitna merna kapija može realizovati primenom n 1-bitnih mernih kapija na svaki od ulaznih n kubitova (slika 5). Proces merenja se tako može redukovati na primenu više kopija jednog, elementarnog, dela hardvera: 1-kubitne merne kapije, [18].



Slika 5 - Očitavanje kvantnog registra

Jednolubitna merna kapija se simbolički prikazuje u notaciji kvantnih kola kao na slici 6.



Slika 6 – Jednokubitna merna kapija u notaciji kvantnih kola

Kvantno računanje je probabilističko, postoji urođena neizvesnost prilikom merenja na superponiranim stanjima. Kada se stanje n-kubitnog kvantnog registra nalazi u superpoziciji od 2^n stanja, operacija čitanja tog registra izazvaće kolaps te superpozicije stanja u jedno klasično stanje, na slučajan način. To jest merenje stanja n-kubitnog registra na slučajan način daje kao rezultat stanje n-bitnog registra (slike 5 i 7), [17]. Posebno nije tačna tvrdnja da je stanje posmatranog kvantnog sistema, u stvari, uvek samo jedno od stanja $|\Psi\rangle_k$, a da se radi samo o tome da se ne zna koje je to stanje. Radije, reč je o potpuno određenom stanju koje, kada se meri u jednoj bazi, daje deterministički rezultat, a kada se meri u drugoj daje probabilistički rezultat, [10]).

5. INTERFERENCIJA

Da bi se sračunao efekat višestrukih alternativa koje su na raspolaganju kvantnom sistemu moraju se prvo superponirati vektori stanja svih alternativa, a onda sračunati neto verovatnoća odgovarajućeg ishoda preko kvadrata modula amplituda verovatnoća kompozitnog vektora stanja. Na primer, posmatra se događaj sa mogućim ishodima označenim sa „0“ i „1“.

Neka su verovatnoće ishoda „0“ tog događaja sračunate metodama A i B respektivno $P_{A0} \equiv \omega_{A0}^2 = 7/20$ i $P_{B0} \equiv \omega_{B0}^2 = 4/5$ (verovatnoće alternativnog ishoda „1“ se označavaju respektivno $P_{A1} \equiv \omega_{A1}^2 = 13/20$ i $P_{B10} \equiv \omega_{B1}^2 = 1/5$). Ako klasični računar, da bi sračunao verovatnoću ishoda „0“, bira metod A sa verovatnoćom $\cos^2(\alpha)$ onda je verovatnoća ishoda „0“ u klasičnom režimu:

$$P_{kl} = \frac{23 - 9\cos(2\alpha)}{40} \tag{19}$$

Kvantna analogija slučajnog izbora metoda određivanja verovatnoća je kvantno stanje

$$|\psi\rangle = \cos(\alpha)|A\rangle + \sin(\alpha)\,|B\rangle \tag{20}$$

a kvantne analogije metoda A i B su kvantna stanja

$$|A\rangle = \omega_{A0}|0\rangle + \omega_{A1}|1\rangle \tag{21}$$

$$|B\rangle = \omega_{B0}|0\rangle + \omega_{B1}|1\rangle \tag{22}$$

odakle, posle formiranja kompozitnog vektora stanja, sledi verovatnoća ishoda „0“ u kvantnom režimu:

$$P_{kv} = \frac{|\cos(\alpha)\omega_{A0} + \sin(\alpha)\omega_{B0}|^2}{|\cos(\alpha)\omega_{A0} + \sin(\alpha)\omega_{B0}|^2 + |\cos(\alpha)\omega_{A1} + \sin(\alpha)\omega_{B1}|^2} \tag{23}$$

odnosno, posle zamena i sređivanja:

$$P_{kv} = \frac{23 - 9\cos(2\alpha) - 8\sqrt{7}\sin(2\alpha)}{40 - (8\sqrt{7} - 4\sqrt{13})\sin(2\alpha)} \tag{24}$$

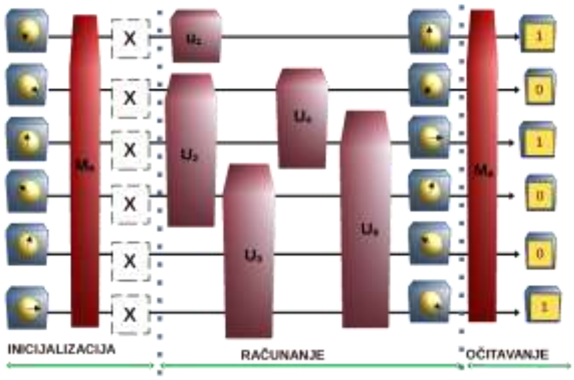
Poređenjem izraza (19) i (24) sledi da kvantna verovatnoća u zavisnosti od α može biti manja, veća ili jednaka klasičnoj verovatnoći, što je glavno obeležje interferencije, [16].

6. KVANTNE KAPIJE I KOLA

Analogno klasičnom modelu kola, kod kvantno-mehaničkog modela kola postoje logički kubitovi koji se prenose duž „žica“ i kvantne kapije koje dejstvuju na kubitove.

Kvantna kola se obično prikazuju šematski onako kako je to prikazano na slici 7 . Žice su prikazane kao horizontalne linije, i zamišlja se da se kubitovi kreću duž tih žica sa leva na desno u vremenu. Kapije su prikazane kao pravougaoni „U“ blokovi. Kapije pripadaju određenim konačnim klasama kapija, primaju informacije duž ulaznih žica i predajuju informacije duž izlaznih žica, [19].

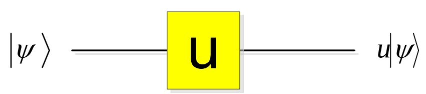
Kada se kvantni računar prvi put pokrene, njegov kvantni registar može imati proizvoljno stanje koje je nemoguće odrediti. Zbog toga se kvantni registar, po uključivanju računara, inicijalizuje u nulto stanje koje se realizuje kriogenim hlađenjem ili, najčešće, kombinacijom merne i, ako se pri merenju dobije stanje |1>, X kapije (slika 7), [18].



Slika 7 – Model kvantnog računara

U notaciji kvantnih kola, unitarni operator **u** koji dejstvuje na jednom kubitu predstavlja 1-kubitnu kvantnu kapiju. Isti operator se u dvodimenzionalnom Hilbertovom prostoru pojedinačnog kubita može pretstaviti i kao matrica dimenzija 2x2. U produžetku su definisane neke teoretski važne kvantne kapije u matričnoj i notaciji kvantnih kola, [19].

Opšti oblik jednokubitne kvantne kapije u notaciji kvantnih kola prikazan je na slici 8, [18].



Slika 8 – Jednokubitna kvantna kapija

pri čemu je u jedna od kapija iz skupa

{H, I. X, Y, Z, T, ... }

gde su

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \textit{- Hadamardova kapija}$$

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \textit{- jedinična kapija}$$

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \textit{- kapija X}$$

$$Y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \quad \textit{- kapija Y}$$

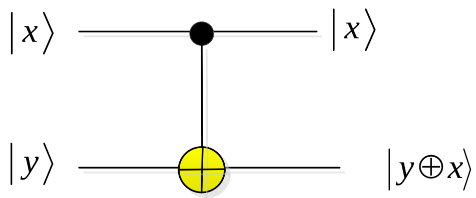
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \textit{- kapija Z}$$

$$T = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{pmatrix} \quad \textit{- kapija T}$$

Kapija CNOT predstavlja unitarni operator nad dva kubita koji se definiše u matričnoj notaciji kao

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

i notacijom kola kao na slici 9.



Slika 9 - Kapija CNOT

Gornja linija na slici 9 predstavlja kontrolni kubit $|x\rangle$, dok donja linija predstavlja ciljni kubit $|y\rangle$. $|x\rangle$,$|y\rangle$ mogu uzimati vredosti iz skupa $\{|0\rangle, |1\rangle\}$. Operator $\oplus$ je isključivo ILI, [4].

Za skup kapija se kaže da je univerzalan u odnosu na kvantno računanje ako bilo koja unitarna operacija može biti aproksimirana do proizvoljne tačnosti putem kvantnog kola koje sadrži samo te kapije, [20, 21].

Proizvoljna unitarna matrica na n-dimenzionalnom Hilbertovom vektorskom prostoru može se predstaviti kao proizvod od najviše $2^{n-1}(2^n -1)$ dvonivoiskih unitarnih matrica, gde se pod dvonivoiskom unitarnom matricom podrazumeva matrica koja netrivijalno dejstvuje samo na dve ili manje komponenti vektora datog Hilbertovog prostora, [20].

Kvantno kolo sastavljeno od CNOT kapija i jednokubitnih kapija može se upotrebiti za formiranje proizvoljne dvonivojske unitarne operacije na prostoru stanja od n kubitova, [20].

Iz prethodnih rezultata sledi da je skup koji se sastoji od svih jednokubitnih kapija i CNOT kapije univerzalan u odnosu na kvantno računanje, [2, 20].

Diskretan (konačan) skup kapija se ne može upotrebiti za tačnu implementaciju proizvoljne unitarne operacije jer je skup unitarnih operacija kontinualan i njihova praktična realizacija se ne može izvršiti sa beskonačnom preciznošću, [2, 20].

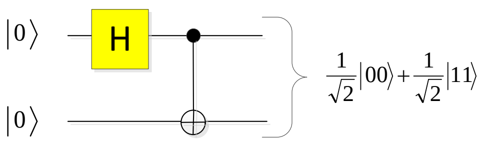
Ali se pokazuje da postoji mali, konačni skup jednokubitnih kapija kojim se mogu efikasno aproksimirati sve druge jednokubitne kapije, [2, 20].

Skup koji se sastoji od CNOT, Hadamardove i fazne kapije $T = R_{\frac{\pi}{4}}$ je univerzalan u smislu aproksimacije, što znači da se svaka druga unitarna kapija može przivoljno dobro aproksimirati tim kapijama. Dokazana je velika efikasnost ove aproksimacije: bilo koja jednokubitna ili dvokubitna kapija se može aproksimirati do greške ε korišćenjem broja kapija (iz ovog malog skupa) koji je jednak polilog (1/ ε), odnosno koji je polinomijalan po logaritmu 1/ ε; simuliranje proizvoljne kapije do eksponencijalno male greške plaća se samo polinomijalnim brojem ovih kapija, [2, 20].

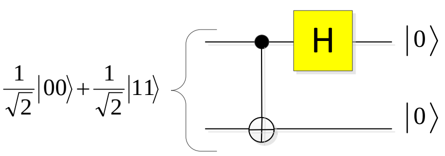
Takođe, skup od Hadamardovih i Toffoli (CCNOT) kapija je univerzalan u smislu aproksimacije za sve unitarne kapije sa samo realnim unosima, što znači da se bilo koja unitarna kapija sa samo realnih unosima može do proizvoljne tačnosti aproksimirati kolima sastavljenim od samo ovih kapijja, [2, 20].

7. GENERISANJE ZAPLETENIH STANJA I KVANTNA TELEPORTACIJA

Osnovna karakteristika Belovih kola je da nezapleten ulaz mogu transforisati u zapleten izlaz (slika 10) i zapleten ulaz u nezapleten izlaz (inverzno Belovo kolo na slici 11).

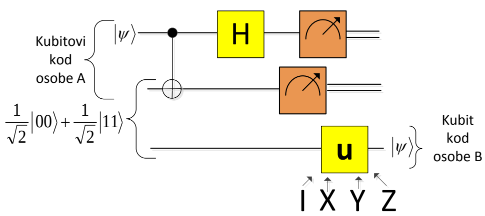


Slika 10 - Belovo kolo



Slika 11 - Inverzno Belovo kolo

Belova kola zajedno sa kapijama I, X, Y i Z se mogu koristiti za izgradnju kola koje daje efekat kvantne teleportacije, kao na slici 12:



Slika 12 - Kvantna teleportacija

Kako je prikazano na slici 12, dva kubita su kod osobe A, a jedan kod osobe B koja može biti proizvoljno udaljena od osobe A. Želi se kvantna teleportacija proizvoljnog kubita $|\psi\rangle = a|0\rangle + b|1\rangle$ od osobe A do osobe B. Kubitovi se nalaze u početnom stanju zapletene superpozicije prikazanom na slici 12 i izrazom 25, u kojem prva dva člana tenzorskog proizvoda odgovaraju stanjima kubitova koji pripadaju osobi A, a treći član odgovara stanju kubita osobe B.

$$\frac{1}{2}|00\rangle(a|0\rangle + b|1\rangle) + \frac{1}{2}|01\rangle(a|1\rangle + b|0\rangle) + \frac{1}{2}|10\rangle(a|0\rangle - b|1\rangle) + \frac{1}{2}|11\rangle(a|1\rangle - b|0\rangle) \qquad (25)$$

Kada osoba A izvrši merenje na ciljom kubitu kapije CNOT, stanje kubita kod osobe B se usled zapletenosti trenutno menja. Osoba A klasičnim putem šalje osobi B rezultate merenja nad svojim kubitovima, koji mogu biti 00, 01, 10 i 11, a osoba B na osnovu istih respektivno primenjuje jednu od kapija I, X, Y ili Z na svoj kubit i na taj način rekonstruiše stanje kubita $|\psi\rangle$, [2, 14, 22] .

8. ZAKLJUČAK

U radu je dat opis procesa kvantnog računanja primenom paradigme kvantnih kola kojima se kvantno mehanički fenomeni kao što su superpozicija, zapletenost i interferencija objedinjuju i prikazuju na način koji odgovara procesu obrade informacija. Ovo može ukazivati na to da se samo funkcionisanje prirode može shvatiti kao proces kvantno-mehaničkog računanja.

Prenos informacija u okviru ove računarske paradigme obavlja se kvantnom teleportacijom koja je zasnovana na kvantno-mehaničkom fenomenu zapletenosti stanja kvantnih nosioca informacija i koja se može modelovati putem Belovih kola. Uočljivo je da se kvantnom teleportacijom ne vrši transfer nosioca informacija nego njihovih kvantnih stanja. Iako je ovaj transfer trenutan on zahteva prethodno prostorno razmeštanje nosioca informacija koje sa svoje strane podleže vremensko-prostornim ograničenjima klasične, odnosno relativističke mehanike.

Na kraju kvantnomehaničkog računanja u opštem slučaju se dobija superpozicija završnih stanja registara računara (rešenja) koja se ukida očitavanjem koje nepovratno daje samo jedno od tih rešenja i to na inherentno stohasitčki način, što predstavlja problem koji bi trebao biti predmet budućih istraživanja.

LITERATURA

[1] Chubb J, Harizanov V. A (very) brief tour of quantum mechanics, computation, and category theory**,** In *Logic and Algebraic Structures in Quantum Computing, pp. 8-22*, Cambridge University Press, United Kingdom, 2016 .

[2] De Wolf, R. *Quantum Computing:Lecture Notes*, QuSoft, CWI and University of Amsterdam, Amsterdam, 2022

[3] Pathak A. *Quantum Computation and Quantum Communication,* Taylor & Francis Group, Boca Raton, USA, 2014.

[4] Wong T. G. *Introduction to Classical and Quantum Computing*, Published by Rooted Grove, Omaha, Nebraska, 2022.

[5] Arute, F. et al. Quantum supremacy using a programmable superconducting processor, *Nature,* No. 574, pp. 505–510, 2019.

[6] Deutsch D. Quantum Theory, the Church-Turing Principle, and the Universal Quantum Computer, In Proceedings of the Royal Society of London, Vol. A400, pp. 97-117, 1985.

[7] Bernstein, E. and Vazirani, U. Quantum complexity theory. *SIAM Journal on Computing*, No. 26(5), pp.1411–1473, 1997

[8] Deutsch, D. Quantum computational networks. In Proc. of the Royal Society of London, London, Great Britain, Volume 425, Issue 1868, pp. 73-90, 1989.

[9] Yao, A. C. C. Quantum circuit complexity. In *Proceedings of 34th IEEE FOCS*, Palo Alto, CA, United States of America, pp. 352–360, November 1993.

[10] Rieffel E, Polak W. *Quantum computing: a gentle introduction*, The MIT Press Cambridge, Massachusetts London, England, 2011.

[11] Hughes C, et al. *Quantum Computing for the Quantum Curious*, Springer, https://doi.org/10.1007-/978-3-030-61601-4, 2021

[12] Abhijith J. et al. Quantum Algorithm Implementations for Beginners, In *ACM Transactions on Quantum Computing,* Vol. 3, No. 4, Article 18, pp. 1-92, 2022.

[13] Amoroso R. L. *Universal quantum computing: supervening decoherence — surmounting uncertainty*. World Scientific, Hackensack, 2017.

[14] Bernhardt C. *Quantum computing for everyone*, The MIT Press, Cambridge, Massachusetts, 2019.

[15] Jones J. A, Jaksch, D. *Quantum information, computation and communication*. Cambridge University Press, New York, 2012.

[16] Williams C. P, Clearwater SH. *Explorations in quantum computing*, Springer-Verlag, New York, 1998.

[17] Lanzagorta M, Uhlmann J. *Synthesis lectures on quantum computing* #2, Morgan & Claypool, San Rafael, California, USA 2009. DOI 10.2200/-S00159ED1V01Y200810QMC002, 2009.

[18] Mermin, N. D. *Quantum computer Science-An Introduction,* Cambridge University Press, New York, 2007.

[19] Kaye P. R, Laflamme R, Mosca M. *An Introduction to Quantum Computing*, Oxford University Press, New York, 2007.

[20] Nielsen M, Chuang I. *Quantum Computation and Quantum Information*. Cambridge University Press, New York, 2010.

[21] Gruska J. *Quantum Computing*, McGraw-Hill, London, 1999.

[22] Bennett, C. et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, No. 70, pp. 1895–1899, 1993.

[23] Wootters W. K. and Zurek W. H. A single quantum cannot be copied. *Nature*, No. 299, pp. 802–803, 1982.

SUMMARY

QUANTUM COMPUTING SPECIFICITIES WITH THE APPLICATION TO QUANTUM TELEPORTATION

The work explains quantum computing theoretical-physical basis from where quantum information processing specific features are deduced. Thereupon, quantum information processing logical representation is laid down through quantum circuits paradigm, some quantum gates of theoretical importance are defined and special attention is dedicated to existence of universal quantum gates set. Finally, an example of quantum circuits paradigm application to entangled states generation and quantum teleportation realization is exposed.

Key Words: *Quantum circuits, Universal quantum gates set, Entangled states, Teleportation.*