math.e

Hrvatski matematički elektronički časopis

Kvantni logički sklopovi

Aleksandar Hatzivelkos,
Veleučilište Velika Gorica, Velika Gorica

1 Uvod

Ideja o kvantom računalu pojavila se prije četrdesetak godina kada je u osamdesetim godinama prošlog stoljeća fizičar Richard Feynman održao seriju predavanja te objavio dva ključna članka o mogućnostima izgradnje računala temeljenog na kvantnoj mehanici. Sljedeći velik korak je objava članka Davida Deutscha 1985. godine o „univerzalnom kvantom računalu", nakon čega je u devedesetim godinama objavljen niz članaka o algoritmima kreiranima za rad na kvantnim računalima (Shorov algoritam, Groverov algoritam pretraživanja, Loydov algoritam ...). [5, 11]

Godine 2001. IBM i Stanford University provode prvu primjenu Shorovog algoritma na 7-*qbitnom* kvantom računalu. Godine 2010. bilježimo pojavu prvog komercijalnog kvantnog računala, *D-Wave One*. Devet godina kasnije Google proglašava postizanje „kvantne nadmoći". Riječ je o terminu kojeg je skovao John Preskill 2012. godine i koji opisuje trenutak u kojemu kvantni sustavi mogu obavljati zadatke koji nadmašuju mogućnost klasičnih računala. Posljednjih deset godina bilježimo ubrzan razvoj kvantnih računala, kako softvera, tako i hardvera. Primjerice, posljednje konstruirano kvantno računalo radi s više od 1000 *qbita*. [10]

Razvoj kvantnih računala, prirodno, otvara nova područja istraživanja, kako u razvoju hardvera (dakle, samih kvantnih računala), softvera (algoritama konstruiranih za rad na kvantnim računalima), tako i u matematičkoj (logičkoj) formalizaciji rada kvantnih računala. Početkom te formalizacije smatra se von Neumannova aksiomatizacija kojom su kvantni sustavi opisani pomoću kompleksnog separabilnog Hilbertovog prostora. [8]

Unatoč ubrzanom razvoju i bogatom prostoru istraživanja, kvantno računarstvo je još uvijek relativno slabo poznato u široj javnosti, pa čak i široj akademskoj zajednici. Dok se, recimo, Booleova algebra i binarni brojevi kao temelj rada klasičnih računala smatraju općom kulturom, malo tko bi znao iznijeti osnovnu ideju rada kvantnih računala ili pak matematičkih koncepata kojima se ono služi. Smatramo da je stoga korisno na jednom mjestu dati pregled osnova rada i računanja s kvantnim računalima, što je osnovni cilj ovog članka.

2 Što je *qbit*?

Opis kvantne logike iz perspektive primjene kreće od definicije osnovne informacijske jedinice, kvantnog bita, odnosno *qbita*. Za usporedbu, osnovna informacijska jedinica u primjeni klasične logike, *bit*, može pohraniti dvije brojčane vrijednosti, 1 i 0. U kvantnom slučaju, osnovna informacijska jedinica *qbit* može se izmjeriti u dva stanja, koja se u standardnoj Diracovoj notaciji obilježavaju s $|0\rangle$ i $|1\rangle$. Fizičku realizaciju kvantnog bita moguće je ostvariti spinom elektrona (spin gore i spin dolje), stanjem polarizacije fotona ili spinom jezgre atoma.

Osnovna razlika između *bita* i *qbita* je u tome što *qbit* može biti u superpoziciji stanja prije mjerenja, dok *bit* može biti u samo jednom od dva stanja, 0 ili 1. Pored toga, *qbite* možemo mjeriti na više načina, no nakon prvog mjerenja i kolapsa valne funkcije, svako sljedeće mjerenje dati će isti (bazni) rezultat. To znači da *qbit* ne ostaje u stanju superpozicije nakon provedenog mjerenja te se informacija iz stanja superpozicije može dobiti samo jednom.

Kvantni bit, *qbit*, u svakom kvantno-mehaničkom sustavu možemo reprezentirati dvodimenzionalnim kompleksnim vektorom, uz uvjet da pripadni vektorski prostor ima $|0\rangle$ i $|1\rangle$ za kanonske vektore baze, pri čemu zapisujemo $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Kažemo da je kvantno stanje $|\psi\rangle$ superpozicija baznih stanja $|1\rangle$ i $|0\rangle$ ako je netrivijalna linearna kompozicija vektora baze, odnosno ako vrijedi:

$$|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle, \qquad \alpha, \beta \neq 0, \quad \alpha, \beta \in \mathbb{C}.$$

Definicija 1. *Skup kvantnih bitova, qbita, je skup vektora $\vec{v} \in \mathbb{C}^2$ norme 1. Svaki qbit se može zapisati u obliku $|\psi\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix} \in \mathbb{C}^2$ pri čemu je $|\alpha|^2 + |\beta|^2 = 1$, i obrnuto, svaki element $\begin{bmatrix} \alpha \\ \beta \end{bmatrix} \in \mathbb{C}^2$ koji zadovoljava $|\alpha|^2 + |\beta|^2 = 1$ je qbit. Vrijednosti $\alpha, \beta \in \mathbb{C}$ nazivamo amplitudama qbita.*

Pokazuje se da navedeni skup opisan u Definiciji 1 čini vektorski prostor, a skup $\{|0\rangle, |1\rangle\}$ čini bazu tog vektorskog prostora. [1] Ta se baza naziva standardnom (ortonormiranom) bazom, no kao što znamo (beskonačni) vektorski prostori imaju po volji mnogo (ortonormiranih) baza, pa stoga i vektorski prostor $\mathbb{C}^2$ norme 1 ima po volji mnogo baza koje zadovoljavaju Definiciju 1.[1] U sljedećoj definiciji navodimo još dvije često korištene baze.

Definicija 2. *Neka je* $\{|0\rangle, |1\rangle\}$ *baza prostora qbita. Hadamardovom bazom nazivamo skup* $\{|+\rangle, |-\rangle\}$ *pri čemu je*

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Također, skup $\{|i\rangle, |-i\rangle\}$ *predstavlja bazu prostora qbita, pri čemu je*

$$|i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i \cdot |1\rangle), \qquad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i \cdot |1\rangle).$$

Notacija koju koristimo za zapisivanje *qbita* naziva se *Diracovom notacijom*, a često je u primjeni i naziv *bra-ket notacija*. U njoj kao oznaku za *qbite* (vektore) koristimo grčko slovo ψ, pa se zapis qbita $|\psi\rangle$, čita „ket-psi". U paru s *ket*-notacijom u koristimo *bra*-notaciju: za vektor *ket-psi* $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle = \begin{bmatrix} \alpha \\ \beta \end{bmatrix}$ definiramo *bra-psi* $\langle\psi| = \begin{bmatrix} \overline{\alpha} & \overline{\beta} \end{bmatrix}$. Vidimo kako je *bra-psi* vektor redak čiji su elementi konjugirane amplitude vektora *ket-psi*. Posebno, za *ket* vektore baze vrijedi $\langle 0| = \begin{bmatrix} 1 & 0 \end{bmatrix}, \langle 1| = \begin{bmatrix} 0 & 1 \end{bmatrix}$.

Takva notacija omogućava nam interpretaciju *bra-ket* zapisa $\langle\psi_1|\psi_2\rangle$ kao skalarnog produkta vektora $\langle\psi_1| \cdot |\psi_2\rangle$ gdje je $\cdot$ oznaka za matrično množenje vektora retka i vektora stupca. Dakle, za $|\psi_1\rangle = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}$ i $|\psi_2\rangle = \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix}$ vrijedi:

$$\langle\psi_1|\psi_2\rangle = \begin{bmatrix} \overline{\alpha}_1 & \overline{\beta}_1 \end{bmatrix} \cdot \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix} = \overline{\alpha}_1\alpha_2 + \overline{\beta}_1\beta_2$$

Specijalno imamo $\langle 0|0\rangle = 1 \cdot 1 + 0 \cdot 0 = 1$ i $\langle 1|1\rangle = 0 \cdot 0 + 1 \cdot 1 = 1$ što nam potvrđuje normiranost vektora $|0\rangle$ i $|1\rangle$. Također, lako je provjeriti da vrijedi $\langle 0|1\rangle = \langle 1|0\rangle = 0$, što potvrđuje ortogonalnost baze. Čitatelju predlažemo da na sličan način provjeri ortonormiranost baza $\{|+\rangle, |-\rangle\}$ i $\{|i\rangle, |-i\rangle\}$.

Diracova kotacija omogućava nam i interpretaciju zapisa *ket-bra*, $|\psi_1\rangle\langle\psi_2|$. Kao što zapis *bra-ket* opisuje skalarni (unutarnji) produkt, tako *ket-bra* zapis opisuje tenzorski (vanjski) produkt vektora. Tako za vektore $|\psi_1\rangle = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix}$ i $|\psi_2\rangle = \begin{bmatrix} \alpha_2 \\ \beta_2 \end{bmatrix}$ vrijedi:

$$|\psi_1\rangle\langle\psi_2| = \begin{bmatrix} \alpha_1 \\ \beta_1 \end{bmatrix} \cdot \begin{bmatrix} \overline{\alpha}_2 & \overline{\beta}_2 \end{bmatrix} = \begin{bmatrix} \alpha_1\overline{\alpha}_2 & \alpha_1\overline{\beta}_2 \\ \overline{\alpha}_2\beta_1 & \beta_1\overline{\beta}_2 \end{bmatrix}.$$

Dakle, *ket-bra* zapis opisuje linearni operator prikazan gornjom matricom. *Bra-ket* i *ket-bra* zapisi međusobno se nadopunjuju u računu s *qbitima*. [4]

2.1 Mjerenje *qbita*

Mjerenje u kvantnoj mehanici je fizički proces u kojem kvantni sustav dolazi u interakciju s klasičnim mjernim aparatom, što dovodi do kolapsa valne funkcije. U slučaju kubita, koji je osnovna jedinica kvantne informacije i može biti u stanju:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \text{gdje su } \alpha, \beta \in \mathbb{C} \text{ i } |\alpha|^2 + |\beta|^2 = 1.$$

Mjerenje može biti provedeno u različitim bazama, ali najčešće se provodi u bazi $\{|0\rangle, |1\rangle\}$. Opisuje se pomoću skupa hermitskih operatora $\{\widehat{O}_i\}$, koji djeluju na vektore stanja i imaju svojstva:[2]

- Svojstvene vrijednosti operatora $\widehat{O}_i$ predstavljaju moguće ishode mjerenja.
- Svojstveni vektori operatora $\widehat{O}_i$, $|o_i\rangle$ formiraju ortonormiranu bazu Hilbertovog prostora.

Ako je kvantno stanje $|\psi\rangle$ izraženo u bazi svojstvenih vektora operatora $\{\widehat{O}_i\}$, tada je vjerojatnost da će mjerenje dati rezultat o_i (koji odgovara svojstvenom vektoru $|o_i\rangle$) određena pomoću kvadrata apsolutne vrijednosti projekcije:[3]

$$P(o_i) = |\langle o_i|\psi\rangle|^2$$

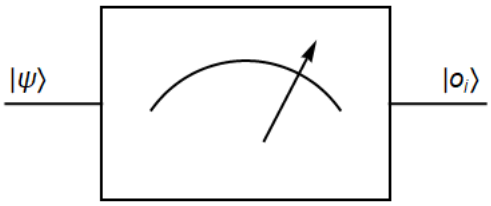
Nakon mjerenja, prema postulatima kvantne mehanike, sustav kolabira u odgovarajuće svojstveno stanje $|o_i\rangle$.

Mjerenje uzrokuje kolaps kvantnog stanja. To znači da ako je *qbit* bio u superpoziciji prije mjerenja, nakon mjerenja ostaje samo u jednom od stanja baze u kojoj se provodi mjerenje. Na primjer, ako je *qbit* prije mjerenja bio u stanju $|\psi\rangle = \frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle$ mjerenje će proizvesti $|0\rangle$ s vjerojatnošću $P(0) = 0.25$ ili $|1\rangle$ s vjerojatnošću $P(1) = 0.75$, a nakon mjerenja *qbit* više neće biti u superpoziciji. Ako odmah nakon mjerenja ponovno mjerimo (isti *qbit*) u istoj bazi, dobit ćemo isti rezultat kao i u prvom mjerenju sa 100 % vjerojatnosti. Dakle, mjerenje je nepovratno i eliminira superpoziciju, ostavljajući sustav u određenom svojstvenom stanju operatora kojim je provedeno mjerenje. [6]

Kao što smo spomenuli, mjerenja se najčešće izvode u bazi $\{|0\rangle, |1\rangle\}$. Postupak mjerenja zapisujemo na sljedeći način. Mjerenje *qbita* $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ je sljedeća operacija:

$$|\psi\rangle \overset{\text{mjerenje}}{\longrightarrow} \begin{cases} \text{ishod je } 0 \text{ s vjerojatnošću } |\alpha|^2, \ |\psi\rangle \text{ kolabira na } |1\rangle. \\ \text{ishod je } 1 \text{ s vjerojatnošću } |\beta|^2, \ |\psi\rangle \text{ kolabira na } |0\rangle. \end{cases}$$

Dakle, mjerenje stanja $|\psi\rangle$ daje vrijednost 0 ili 1 s vjerojatnošću ovisnom o amplitudama *qbita*. Potom stanje *qbita* kolabira na bazno stanje koje ovisi o rezultatu mjerenja. Na Slici 1 dan je simbolički prikaz za operaciju mjerenja koji koristimo u shematskom prikazu kvantnih logičkih sklopova.



Slika 1: Simbolički prikaz u logičkom sklopu za operaciju mjerenja *qbita*

Iako je *qbit* definiran kao vektor s kompleksnim amplitudama, tj. kao što smo vidjeli ranije, struktura koja pohranjuje dva stupnja slobode, konačan ishod je prilično mršava informacija u formi jednog bita. No prava snaga kvantnog računala dolazi iz rada s više *qbita*.

Za razumijevanje rada s *qbitima* važan nam je još jedan interesantan fenomen, tzv. *globalna faza qbita*. Ako je $|\psi\rangle$ neki vektor stanja *qbita*, a za vektor stanja $|\psi'\rangle$ vrijedi

$$|\psi'\rangle = e^{i\varphi}\,|\psi\rangle,$$

gdje je $\varphi \in \mathbb{R}$, tada realni broj φ nazivamo *globalnom fazom*.[4] *Qbiti* $|\psi\rangle$ i $|\psi'\rangle$ predstavljaju isto fizičko stanje jer globalna faza ne utječe na rezultat mjerenja. Uistinu, ako stanje $|\psi\rangle$ transformiramo u stanje $|\psi'\rangle$, vjerojatnost mjerenja ostaje ista:

$$P(o_i) = |\langle o_i|\psi'\rangle|^2 = |\langle o_i|e^{i\varphi}\,\psi\rangle|^2 = |e^{i\varphi}\,\langle o_i|\psi\rangle|^2 = |e^{i\varphi}|\cdot|\langle o_i|\psi\rangle|^2 = |\langle o_i|\psi\rangle|^2.$$

Ukratko, globalna faza u matematičkoj reprezentaciji kvantnog stanja predstavlja stupanj slobode koji nema fizički značaj jer ne utječe na ishode mjerenja.

2.2 Rad s *qbitima*

Operacije na *qbitima* provodimo pomoću unitarnih operatora koje zapisujemo pomoću unitarnih matrica.[5] Prisjetimo se, za matricu $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, gdje su $a, b, c, d \in \mathbb{C}$, kažemo da je *unitarna* ako za njoj konjugirano transponiranu matricu $U^* = \begin{bmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{bmatrix}$ vrijedi

$$U \cdot U^* = U^* \cdot U = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Može se pokazati kako je matrica U unitarna ako za njezine vektore stupce $\begin{bmatrix} a \\ b \end{bmatrix}$ i $\begin{bmatrix} c \\ d \end{bmatrix}$ vrijedi da su vektori norme 1 ($|a|^2 + |c|^2 = |b|^2 + |d|^2 = 1$), te da su međusobno okomiti ($ab + cd = 0$).

Vidjet ćemo da su unitarni operatori ključni za konstrukciju logičkih sklopova na *qbitima*. Kako bi objasnili njihov rad, uvodimo sljedeće

pravilo.

Definicija 3. *Primjenom unitarne matrice* $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *na qbit* $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$*. dobivamo qbit* $U|\psi\rangle$ *provođenjem standardnog množenja matrice* U *i vektora* $|\psi\rangle$*:*

$$U \cdot |\psi\rangle = (\alpha\, a + \beta\, b) \cdot |0\rangle + (\alpha\, c + \beta\, d) \cdot |1\rangle\,.$$

Qbit predstavlja kvantni sustav koji može biti u superpoziciji dva fizička stanja koja označavamo s $|0\rangle$ i $|1\rangle$. Dva *qbita* predstavljaju dva takva sustava koja su ekvivalentna sustavu s četiri fizička stanja, koja ćemo označiti s $|00\rangle$, $|01\rangle$, $|10\rangle$. i $|11\rangle$. (za detalje ekvivalencije vidi [1]).

Definicija 4. *Stanje* $|\psi\rangle$ *sustava s dva qbita je element vektorskog prostora* $\mathbb{C}^4$ *s normom* 1*. Zapisujemo ga u obliku:*

$$|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle,$$

pri čemu vrijedi $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$ *te*

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

Unitarni operator na sustavu s dva *qbita* prikazujemo unitarnom kompleksnom matricom U s četiri retka i četiri stupca za koju vrijedi $U \cdot U^* = U^* \cdot U = I_4$. Na analogan način definiramo sustave s više od dva *qbita*. Tako sustav s n *qbita* prikazujemo kao linearnu kombinaciju 2^n baznih vektora u prostoru $\mathbb{C}^{2^n}$ s normom 1. Sada možemo definirati tenzorski produkt dva *qbita*.

Definicija 5. *Neka su* $\alpha\,|0\rangle + \beta\,|1\rangle$ *i* $\alpha'\,|0\rangle + \beta'\,|1\rangle$ *dva qbita. Stanje sustava kojeg tvore ta dva qbita opisujemo pomoću tenzorskog produkta* $\otimes$ *te vrijedi:*

$$(\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\alpha'\,|0\rangle + \beta'\,|1\rangle) = \alpha\alpha'\,|00\rangle + \alpha\beta'\,|01\rangle + \beta\alpha'\,|10\rangle + \beta\beta'\,|11\rangle.$$

Tenzorski produkt dva *qbita* u stvarnosti predstavlja konkatenaciju dva fizička sustava. Stoga ne čudi da se i u zapisu često izostavlja oznaka $\otimes$ te se tenzorski produkt $|x\rangle \otimes |y\rangle$ piše u skraćenom obliku $|x\rangle|y\rangle$, $|x, y\rangle$ ili $|xy\rangle$. Na isti se način bazna stanja $|00\rangle$, $|01\rangle$, $|10\rangle$ i $|11\rangle$ mogu promatrati kao tenzorski produkti $|0\rangle \otimes |0\rangle$, $|0\rangle \otimes |1\rangle$, $|1\rangle \otimes |0\rangle$ i $|1\rangle \otimes |1\rangle$.

Promotrimo što se događa ukoliko tenzorski pomnožimo *qbite* Hadamardove baze (vidi Definiciju 2). Tada imamo:

$$\begin{aligned} |+-\rangle = |+\rangle \otimes |-\rangle \quad &= \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\ &= \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \end{aligned} \tag{1}$$

Tako smo dobili prikaz (jednog) tenzorskog produkta vektora Hadamardove baze pomoću vektora kanonske baze, što će nam koristiti kasnije u analizi djelovanja kvantnih algoritama.

Za tenzorski produkt operatora (koje prikazujemo matrično) koristimo standardnu definiciju Kroneckerovog produkta. Za matrice $A = [a_{ij}]$ i $B = [b_{ij}]$, gdje su $A, B \in M_n$ na sljedeći način definiramo produkt $A \otimes B$ (naravno, nad poljem $\mathbb{C}$):

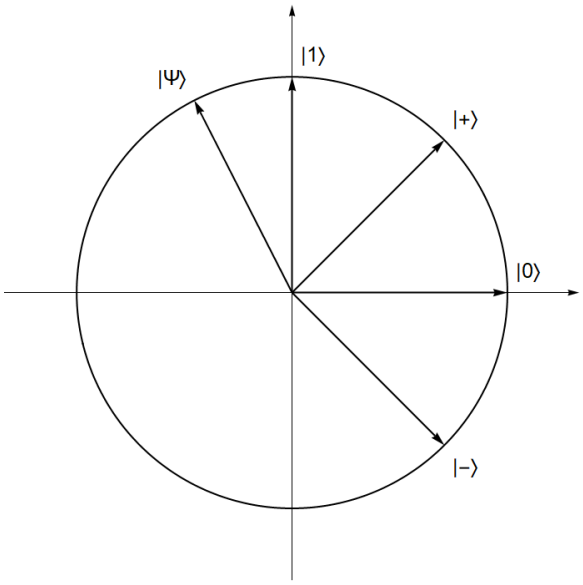
$$A \otimes B = \begin{bmatrix} a_{11} \cdot B & \cdots & a_{1n} \cdot B \\ \vdots & \ddots & \vdots \\ a_{n1} \cdot B & \cdots & a_{nn} \cdot B \end{bmatrix}.$$

Ilustracije radi, recimo da trebamo odrediti tenzorski produkt matrica $A = \begin{bmatrix} 1 & -1 \\ 0 & 2 \end{bmatrix}$ i $B = \begin{bmatrix} 1 & 2 \\ 3 & 4 \end{bmatrix}$.

$$A \otimes B = \begin{bmatrix} 1 \cdot B & -1 \cdot B \\ 0 \cdot B & 2 \cdot B \end{bmatrix} = \begin{bmatrix} 1 & 2 & -1 & -2 \\ 3 & 4 & -3 & -4 \\ 0 & 0 & 2 & 4 \\ 0 & 0 & 6 & 8 \end{bmatrix}$$

3 Vizualni prikaz *qbita*

Prostor *qbita* često se prikazuje vizualno. Za početak, na Slici 2 nalazi se vizualni prikaz potprostora qbita s realnim amplitudama.



Slika 2: Prikaz potprostora *qbita* s realnim amplitudama

Kao što se vidi u Definicijama 1 i 2, standardna i Hadamardova baza imaju realne amplitude pa se mogu ovako prikazati. S druge strane baza $\{|i\rangle, |-i\rangle\}$ nema realne amplitude, što onemogućuje njezin prikaz na ovaj način. Istaknimo na toj kružnici mogu prikazati svi *qbiti* $|\psi\rangle$ s realnim amplitudama.

Kako je na taj način prikaz prostora *qbita* nepotpun, standardni način vizualnog prikaza prostora *qbita* je *Blochova sfera*, nazvana prema švicarskom fizičaru i nobelovcu Felixu Blochu. Već samo ime govori kako se radi o dvodimenzionalnoj reprezentaciji u prostoru. No kako su *qbiti* definirani kao dvodimenzionalni vektori nad poljem kompleksnih brojeva, na prvi pogled radi se o strukturi s četiri stupnja slobode.

Jedan stupanj slobode gubi se kroz invarijantnost *qbita* na globalnu fazu. Naime, jedine mjerljive vrijednosti *qbita* $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ gdje su α i β kompleksni brojevi različiti od nule su $|\alpha|^2$ i $|\beta|^2$. Stoga množenje kvantnog stanja proizvoljnim faktorom oblika $e^{i\varphi}$ (globalnom fazom) ne proizvodi mjerljive posljedice, budući da vrijedi:

$$\left|e^{i\varphi}\,\alpha\right|^2 = \overline{(e^{i\varphi}\,\alpha)} \cdot \left(e^{i\varphi}\,\alpha\right) = e^{-i\varphi}\,\bar{\alpha} \cdot\; e^{i\varphi}\,\alpha = \bar{\alpha} \cdot \alpha = |\alpha|^2\,.$$

Ukoliko kompleksne brojeve α i β zapišemo u polarnom obliku, $\alpha = r_\alpha \cdot e^{\phi_\alpha i}$, $\beta = r_\beta \cdot e^{\phi_\beta i}$, *qbit* $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ možemo pomnožiti globalnom fazom $e^{-\phi_\alpha i}$ (pri čemu *qbit* zbog invarijantnosti na množenje globalnom fazom, ostaje isti u odnosu na fizičko mjerenje), nakon čega on prelazi u oblik:

$$|\psi\rangle = r_\alpha \cdot |0\rangle + r_\beta \cdot e^{(\phi_\beta - \phi_\alpha)i} \cdot |1\rangle. \qquad (2)$$

Sada je jasno kako u zapisu *qbita* danog u jednadžbi (2) imamo tri stupnja slobode, realne vrijednosti r_α, r_β i $\phi = \phi_\beta - \phi_\alpha$.

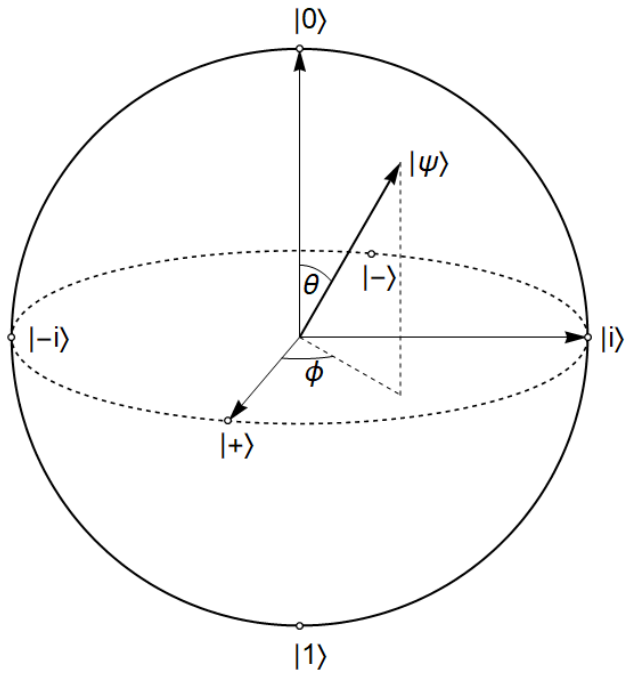
Drugi stupanj slobode gubi se ispunjavanjem uvjeta normalizacije iz Definicije 1, $|\alpha|^2 + |\beta|^2 = 1$.

Zapišemo li kompleksni broj $r_\beta \cdot e^{(\phi_\beta - \phi_\alpha)i}$ u Kartezijevim koordinatama, jednadžba (2) prelazi u $|\psi\rangle = r_\alpha \cdot |0\rangle + (x + y\,i) \cdot |1\rangle$, pa zbog uvjeta normalizacije iz Definicije 1 vrijedi:

$$\begin{aligned} 1 = |r_\alpha|^2 + |x + y\,i|^2 \quad &= r_\alpha^2 + (x + y\,i) \cdot \overline{(x + y\,i)} \\ &= r_\alpha^2 + (x + y\,i) \cdot (x - y\,i) \\ &= r_\alpha^2 + x^2 + y^2, \end{aligned}$$

što je jednadžba sfere u realnom trodimenzionalnom prostoru s Kartezijevim koordinatama (x, y, r_α). Ta sfera naziva se **Blochovom sferom**.[6] Uvođenjem sfernih koordinata u zapis *qbita*, jednadžba (2) prelazi u zapis:

$$|\psi\rangle = \cos\frac{\theta}{2} \cdot |0\rangle + e^{\phi i} \sin\frac{\theta}{2} \cdot |1\rangle, \quad \theta \in [0, \pi]\,,\ \phi \in [0, 2\pi] \qquad (3)$$



Slika 3: Blochova sfera

Istaknute točke na Blochovoj sferi su sjeverni i južni pol, odnosno presjecišta sfere s osi z, koja reprezentiraju vektore $|0\rangle$. i $|1\rangle$. Presjecišta sfere s osi x reprezentiraju vektore Hadamardove baze $|+\rangle$ i $|-\rangle$ te presjecišta sfere s osi y koja reprezentiraju vektore baze $|i\rangle$ i $|-i\rangle$. Te istaknute točke nam sugeriraju jedno korisno svojstvo Blochove sfere.

Propozicija 6. *Suprotne točke na Blochovoj sferi reprezentiraju ortogonalne qbite.*

Dokaz: Neka je s $|\psi\rangle = \cos\frac{\theta}{2}\cdot|0\rangle + e^{\phi i}\sin\frac{\theta}{2}\cdot|1\rangle$ dan *qbit*. *Qbit* $|\xi\rangle$ reprezentiran njemu suprotnom točkom na Blochovoj sferi tada ima sljedeći zapis.

$$\begin{aligned}|\xi\rangle &= \cos\tfrac{\pi-\theta}{2}\cdot|0\rangle + e^{(\phi+\pi)i}\sin\tfrac{\pi-\theta}{2}\cdot|1\rangle \\ &= \cos\tfrac{\pi-\theta}{2}\cdot|0\rangle + e^{\phi i}\sin\tfrac{\pi-\theta}{2}\cdot|1\rangle\end{aligned}$$

Sada je (zbog $\langle 0|0\rangle = \langle 1|1\rangle = 1$ i $\langle 0|1\rangle = \langle 1|0\rangle = 0$):

$$\langle\xi|\psi\rangle = \cos\frac{\theta}{2}\cos\frac{\pi-\theta}{2} - \sin\frac{\theta}{2}\sin\frac{\pi-\theta}{2}.$$

Po trigonometrijskom identitetu za kosinus zbroja, slijedi $\langle\xi|\psi\rangle = \cos\frac{\pi}{2} = 0$. Kako je skalarni produkt jednak nuli, slijedi da su *qbiti* $|\psi\rangle$ i $|\xi\rangle$ okomiti. Na sličan se način pokazuje kako je $\langle\xi|\xi\rangle = 1$ te $\langle\psi|\psi\rangle = 1$, što pokazuje da svaki par suprotnih točaka na Blochovoj sferi čini ortonormiranu bazu za prostor *qbita*. U nastavku teksta vidjeti ćemo kako se djelovanje logičkih sklopova na *qbite* interpretira na Blochovoj sferi.

4 Kvantni logički sklopovi

Prva grupa logičkih sklopova koju ćemo obraditi su logički sklopovi koji se odnose na transformacije jednog *qbita*.

Paulijeva logička vrata

Paulijeva logička vrata predstavljaju skup od četiri unitarna operatora:

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

Jednostavno se vidi da skup Paulijevih vrata $\{X,\ Y,\ Z,\ I\}$ čini bazu vektorskog prostora linearnih operatora s $\mathbb{C}^2$ u $\mathbb{C}^2$. Paulijeva logička vrata su izuzetno praktična za računanje promjene spina pojedinog elektrona, a upravo su spinovi elektrona najčešće korišteni za formiranje *qbita* u današnjim kvantnim računalima. [7]

Logička vrata X u literaturi se naziva i *bit flip* (eng. promjena bita) vratima. Ona na *qbit* (zapisan u standardnoj bazi) djeluju tako da mu zamijene amplitude, odnosno vrijedi $X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$. Na Blochovoj sferi, dana transformacija označava rotaciju za π oko osi x. Logička vrata X mogu se interpretirati i kao generalizaciju logičkih vrata NE (NOT) u klasičnoj logici, ukoliko se preslikavanje vektora baze $|0\rangle \to |1\rangle$ i $|1\rangle \to |0\rangle$ interpretira negacijom. *Bit flip* vrata zamijene vjerojatnosti da *qbit* poprimi vrijednost $|0\rangle$ ili $|1\rangle$.

Logička vrata X u Diracovoj notaciji zapisujemo:
$X = |1\rangle\langle 0| + |0\rangle\langle 1|$. Lako je provjeriti da taj zapis odgovara matričnom zapisu logičkih vrata X.

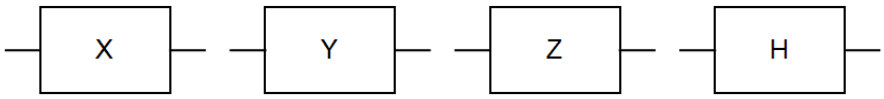
$$|1\rangle\langle 0| + |0\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

Logička vrata Z u literaturi se nazivaju i *phase-flip* (eng. promjena faze) vratima. Ona na *qbit* (zapisan u standardnoj bazi) djeluju tako da amplitudi uz vektor $|1\rangle$ (u zapisu u bazi $\{|0\rangle, |1\rangle\}$) promijene predznak. Logička vrata Z predstavljaju promjenu faze *qbita*, odnosno rotaciju za π oko osi z na Blochovoj sferi. [2] Zapis vrata Z u Diracovoj notaciji glasi $Z = |0\rangle\langle 0| - |1\rangle\langle 1|$.

Logička vrata Y djelovanjem na standardne vektore baze dobivamo $Y|0\rangle = i|1\rangle$ te $Y|1\rangle = -i|0\rangle$. Na Blochovoj sferi, dana transformacija označava rotaciju za π oko osi y, pri čemu se provodi i promjena bita i promjena faze na *qbitu*. [??] Zapis vrata Y u Diracovoj notaciji glasi:

$$Y = -i\,|0\rangle\langle 1| + i\,|1\rangle\langle 0|.$$

Logička vrata I predstavljaju operator identiteta, i na ovom mjestu ih navodimo radi potpunosti Paulijeve baze za vektorski prostor logičkih vrata koja djeluju na jednom *qbitu*. Paulijeva logička vrata X, Y i Z simbolički su prikazana na Slici 4.



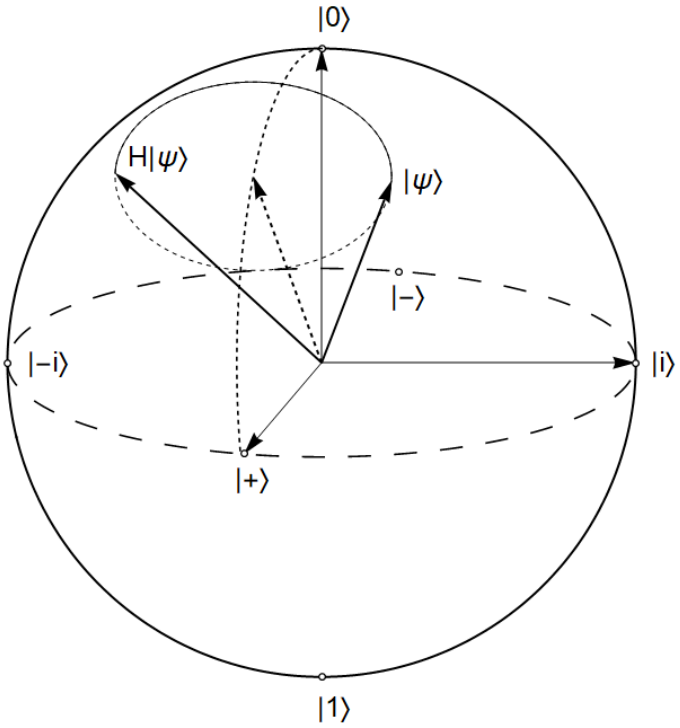
Slika 4: Simbolički prikazi Paulijevih logičkih vrata i Hadamardovih logičkih vrata

Hadamardova logička vrata

Hadamardova logička vrata zapisujemo pomoću unitarnog operatora

$$H = \frac{1}{\sqrt{2}} \cdot \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} = \frac{1}{\sqrt{2}} \big(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1| \big).$$

Kada se *spin-up* ili *spin-down* elektron pošalje kroz Hadamardova logička vrata, njegov novi „položaj" možemo opisati kao novčić koji smo postavili na njegov rub te ima 50 % šanse da padne na glavu (*spin-up*) ili pismo (*spin-down*). Zbog toga se Hadamardova vrata često koriste na početku izvođenja kvantnog algoritma, jer se na taj način prethodno postavljeni, ili inicijalizirani, *qbiti* iz definitivnog stanja prebacuju u stanje superpozicije, što omogućava korištenje njihove pune snage. [4] Dakle, osnovna primjena Hadamardovih logički vrata je promjena baze iz baze $\{|0\rangle, |1\rangle\}$ u bazu $\{|+\rangle, |-\rangle\}$. [7]



Slika 5: Prikaz djelovanja Hadamardovih logičkih vrata na Blochovoj sferi

Simbolički prikaz Hadamardovih logičkih vrata prikazan je na Slici 4 (posljednji simbol u nizu). Na Blochovoj sferi Hadamardova vrata se često opisuju kao kompoziciju rotacije oko osi y za $\frac{\pi}{2}$ i rotacije oko osi x za π. No takav opis zapravo predstavlja dekompoziciju operacije na Eulerove rotacije, koja se umjesto toga može prikazati kao jedna rotacija. Radi se o rotaciji za kut π oko simetrale ravnine xz, kao što je prikazano na Slici 5.

Logička vrata faznog pomaka

Sva prethodno opisana logička vrata pripadaju klasi logičkih vrata koja se nazivaju *Cliffordovim vratima*. Za tu klasu je karakteristično da koordinatne osi prostora preslikavaju opet u koordinatne osi. No, kako bi bili u mogućnosti opisati univerzalne transformacije, potrebno je koristiti i logička vrata koja ne pripadaju klasi Cliffordovih vrata. [2] Jedna takva klasa kvantnih logičkih vrata su logička vrata faznog pomaka:

$$P_\phi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\cdot\phi} \end{bmatrix} = |0\rangle\langle 0| + e^{i\cdot\phi}\,|1\rangle\langle 1|$$

Prikazana logička vrata na Blochovoj sferi opisuju rotaciju za kut ϕ oko osi z. Među logičkim vratima faznog pomaka ističe se upotreba tzv. vrata T i vrata S. Vrata T su logička vrata faznog pomaka za $\phi = \frac{\pi}{4}$, dok su vrata S logička vrata faznog pomaka za $\phi = \frac{\pi}{2}$. Pokazuje se da za ta vrata vrijedi $T^4 = S^2 = Z$, gdje su Z Paulijeva logička vrata Z.

Logička vrata $\sqrt{NOT}$

Brojnost logičkih vrata koja djeluju na jedan *qbit* je velika, i ovaj tekst je prekratak da bismo istaknuli sva. Širinu prostora konstrukcije novih logičkih vrata zorno opisuju logička vrata $\sqrt{NOT}$. Radi se o logičkim vratima koja opisuju djelovanje (invertibilnog) operatora čijom uzastopnom kompozicijom dobivamo logički NOT operator, odnosno Paulijeva vrata X. Radi jednostavnosti zapisa za logička vrata $\sqrt{NOT}$ koristiti ćemo oznaku vrata V, kao što je uobičajeno u literaturi (vidi [2]).

Istaknimo na početku kako je u klasičnoj Booleovoj algebri navedena konstrukcija nemoguća. Ni za koju funkciju $f : \{0,1\} \to \{0,1\}$ ne vrijedi $f(f(x)) = 1 - x$ za svaki $x \in \{0,1\}$.

S druge strane u kvantnoj logici možemo konstruirati operator V za koji vrijedi $V \circ V = X$:

$$V = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} = \frac{1+i}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) + \frac{1-i}{2}(|0\rangle\langle 1| + |1\rangle\langle 0|)$$

Uistinu vrijedi:

$$V \circ V = \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix} \cdot \frac{1}{2}\begin{bmatrix} 1+i & 1-i \\ 1-i & 1+i \end{bmatrix}$$

$$= \frac{1}{4}\begin{bmatrix} (1+i)^2 + (1-i)^2 & 2(1+i)(1-i) \\ 2(1+i)(1-i) & (1+i)^2 + (1-i)^2 \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 0 & 4 \\ 4 & 0 \end{bmatrix} = X.$$

Logička vrata $\sqrt{NOT}$ na Blochovoj sferi *qbit* rotiraju za $\frac{\pi}{2}$ oko osi x, što je upravo pola rotacije koju na Blochovoj sferi provode Paulijeva vrata X. Može se pokazati kako se vrata $\sqrt{NOT}$ mogu zapisati pomoću vrata H i S , tj. da vrijedi $\sqrt{NOT} = H \circ S \circ H$.[7]

4.1 Logička vrata za dva *qbita*

Logički sklopovi koji djeluju na dva qbita reprezentiraju se kompleksnom unitarnom matricom reda 4. Najznačajniji među takvim sklopovima su tzv. *controlled* Q sklopovi. Radi se o sklopovima kod kojih (arbitrarni) unitarni operator Q djeluje na drugi *qbit* ako i samo ako je prvi *qbit* $|1\rangle$, inače na drugi *qbit* djeluje jedinični operator I. U Diracovoj notaciji takve je operatore (u oznaci C_Q, kao *control*-Q) moguće zapisati na sljedeći način:

$$C_Q = (|0\rangle\langle 0|) \otimes I + (|1\rangle\langle 1|) \otimes Q.$$

Prelaskom u matrični zapis dobivamo dijagonalnu blok matricu koja za prvi blok ima jediničnu matricu $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, a za drugi blok matricu operatora $Q = \begin{bmatrix} q_1 & q_2 \\ q_3 & q_4 \end{bmatrix}$:

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

Logička vrata *CNOT* (kontrolirani *NOT*)

Prema prethodno opisanom, operator *CNOT* matrično zapisujemo na sljedeći način:

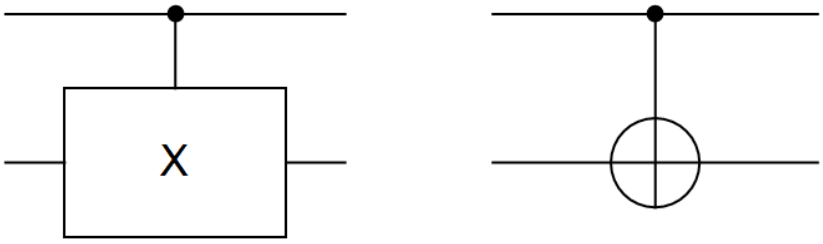
$$C_{NOT} = \begin{bmatrix} I & 0 \\ 0 & X \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$$

Drugi, eksplicitni način za zapis vrata *CNOT* u Diracovoj notaciji u kojem ne koristimo druge unitarne operatore poput Paulijevih vrata X ili identiteta I, glasi:

$$C_{NOT} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 11| + |11\rangle\langle 10|$$

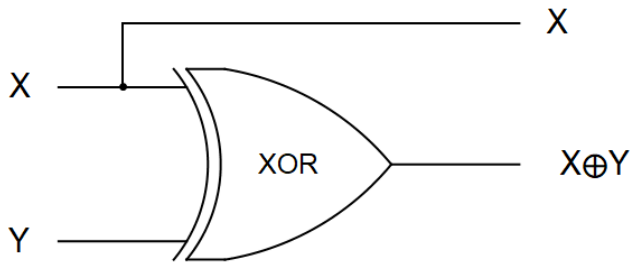
Lako se vidi kako *CNOT* djeluje na vektorima kanonske baze:

$$C_{NOT}|00\rangle = |00\rangle,\ C_{NOT}|01\rangle = |01\rangle,\ C_{NOT}|10\rangle = |11\rangle,\ C_{NOT}|11\rangle = |10\rangle.$$



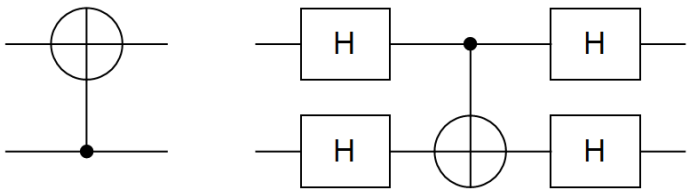
Slika 6: Simbolički prikazi logičkih vrata *CNOT*

Nije teško provjeriti da se logička vrata *CNOT* na vektorima standardne baze ponašaju kao klasična reverzibilna logička vrata *XOR* (logička vrata *isključivo ili*). Reverzibilnost u klasičnoj digitalnoj paradigmi ostvarujemo čuvanjem informacije o vrijednosti prvog bita, kao što je prikazano na Slici 7. Pri tome se rezultat logičkih vrata *XOR*, $X \oplus Y$, može interpretirati i kao binarno zbrajanje modulo 2.



Slika 7: Klasična reverzibilna logička vrata *XOR*

Djelovanje *CNOT* logičkih vrata nije simetrično, tj. nije svejedno koristimo li prvi ili drugi *qbit* kao kontrolni *qbit*. Štoviše, pogrešno je generalizirati i da je prvi *qbit* kontrolni *qbit* u svim upotrebama kontrolnih logičkih vrata. Primjerice, može se pokazati da se kod primjene logičkih vrata *CNOT* na vektore Hadamardove baze $|+\rangle$ i $|-\rangle$, drugi *qbit* ponaša kao kontrolni *qbit*. [2] Upravo taj rezultat vodi do logičkih vrata *CNOT* s drugim *qbitom* kao kontrolnim *qbitom*, kao kompozicije Hadamardovih vrata na oba *qbita* prije i nakon klasičnih logičkih vrata *CNOT*, kao što je prikazano na Slici 8.

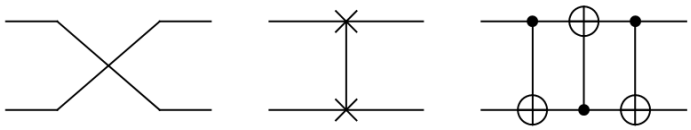


Slika 8: Simbolički prikazi logičkih vrata *CNOT* s drugim kontrolnim qbitom

U upotrebi je velik broj kontroliranih Q vrata čija brojnost nadilazi okvire ovog članka. Čitatelje zaineresirane za taj segment kvantnih logičkih sklopova upućujemo na [2].

Logička vrata *SWAP*

Još jedna logička vrata koja djeluju na dva *qbita*, a čija je upotreba česta su logička vrata *SWAP*, čiji se simbolički prikaz nalazi na Slici 9. Kao što je prikazano na slici, vrata *SWAP* se mogu prikazati i kao djelovanje triju uzastopnih vrata *CNOT* s različitim kontrolnim *qbitima*.



Slika 9: Simbolički prikazi logičkih vrata *SWAP*

U matričnoj, odnosno Diracovoj, notaciji vrata *SWAP* zapisujemo na sljedeći način:

$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} = |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|.$$

Vrata *SWAP* su posebno korisna u fizičkoj izvedbi kvantnog računala, jer omo\-gu\-ća\-va\-ju dovođenje željenih *qbita* u fizičku blizinu i potreban položaj kao ulaze u pojedina logička vrata, bez presijecanja nositelja *qbita*.

4.2 Logička vrata za tri i više *qbita*

Jedan od prvih logičkih sklopova formiranih da djeluje na tri *qbita* je tzv. *CCNOT*, odnosno *Controlled controlled NOT* sklop.

Logička vrata *CCNOT*

Logička vrata *CCNOT* nazivaju se još i *Toffolijevim logičkim vratima*. Radi se o logičkim vratima koja djeluju na tri *qbita*, od čega su prva dva *qbita* kontrolni *qbiti*. Logička vrata *CCNOT* negiraju posljednji *qbit* ako su oba kontrolna *qbita* u stanju $|1\rangle$. Matricu koja opisuje djelovanje logičkih vrata *CCNOT* zapisat ćemo pomoću dijagonalne blok matrice, u kojoj su I_2 i X matrični zapisi odgovarajućih Paulijevih logičkih vrata:

$$CCNOT = \begin{bmatrix} I_2 & 0 & 0 & 0 \\ 0 & I_2 & 0 & 0 \\ 0 & 0 & I_2 & 0 \\ 0 & 0 & 0 & X \end{bmatrix}$$

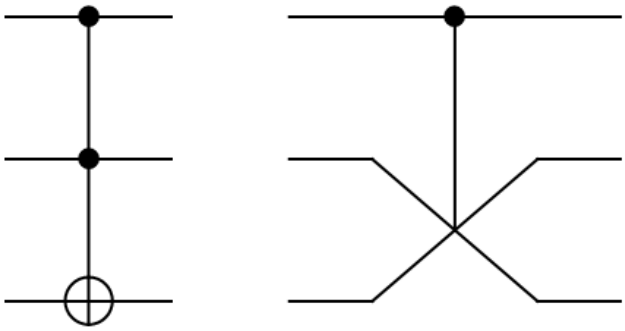
$$= (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I_2 + |11\rangle\langle 11| \otimes X.$$

Simbolički prikaz logičkih vrata *CCNOT* dan je na Slici 10. Naziv Toffolijeva logička vrata duguju radu talijanskog profesora računalnih znanosti Tommasa Toffolija, koji je dokazao njihovu univerzalnost. To znači da se svi logički sklopovi klasične logike mogu realizirati pomoću kvantnih logičkih vrata, štoviše, korištenjem jedino logičkih vrata *CCNOT*.[8] Logička vrata *AND* ($\wedge$) klasične logike realiziraju se pomoću

$$CCNOT \begin{bmatrix} x \\ y \\ 0 \end{bmatrix} = \begin{bmatrix} x \\ y \\ x \wedge y \end{bmatrix},$$

dok se logička vrata *NOT* ($\neg$) klasične logike realiziraju pomoću

$$CCNOT \begin{bmatrix} 1 \\ 1 \\ z \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ \neg z \end{bmatrix}.$$



Slika 10: Simbolički prikazi Toffolijevih (*CCNOT*) i Fredkinovih (*CSWAP*) logičkih vrata

Logička vrata *CSWAP*

Još jedna interesantna logička vrata koja se primjenjuju na sustavu od tri *qbita* su logička vrata *CSWAP* (*kontrolirani SWAP*). Ta se logička vrata često nazivaju i *Fredkinovim logičkim vratima*, prema njihovu tvorcu Edwardu Fredkinu. Simbolički prikaz *CSWAP* logičkih vrata dan je na Slici 10.

Kao i logička vrata *CCNOT*, logička vrata *CSWAP* su univerzalna, budući pomoću njih možemo generirati klasične logičke veznike *AND* i *NOT*:

$$CSWAP \begin{bmatrix} x \\ 0 \\ z \end{bmatrix} = \begin{bmatrix} x \\ x \wedge z \\ \neg x \wedge z \end{bmatrix}, \qquad CSWAP \begin{bmatrix} x \\ 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x \\ \neg x \\ x \end{bmatrix}.$$

Matrično logička vrata *CSWAP* možemo zapisati u obliku dijagonalne blok matrice oblika:

$$CSWAP = \begin{bmatrix} I_2 & 0 & 0 \\ 0 & I_2 & 0 \\ 0 & 0 & SWAP \end{bmatrix},$$

gdje je I_2 matrični zapis Paulijevog operatora identiteta, a *SWAP* matrični zapis logičkih vrata *SWAP*.

Ovime se ne iscrpljuje pregled kvantnih logičkih vrata, štoviše navedeno treba promatrati kao kratki uvod u tu bogatu temu. Pored brojnih nespomenutih kvantnih logičkih vrata, treba istaknuti kako je dobro izučavana tema i različiti načini faktorizacije, odnosno zapisa kvantnih logičkih vrata pomoću kompozicije nekog skupa logičkih vrata. Čitatelje zainteresirane za tu temu upućujemo primjerice na [1, 2].

5 Kvantni logički algoritmi

Kvantna logička vrata, kao i logička vrata u klasičnoj logici, koristimo za izgradnju kvantnih logičkih algoritama.[9] Kako smo pokazali da postoje univerzalna kvantna logička vrata (Toffolijeva i Fredkinova kvantna logička vrata) pomoću kojih je moguće formati klasične logičke veznike *AND* i *NOT*, teoretski, svaki se klasični logički algoritam koji je moguće implementirati pomoću klasičnih logičkih vrata, može implementirati i pomoću kvantnih logičkih vrata. Usprkos tome, takva implementacija nije cilj niti osnovna prednost kvantne logike, u prvom redu zbog hardverskih pretpostavki koje zahtjeva izgradnja i upotreba kvantnih računala.

Umjesto toga, cilj kvantne logike je konstrukcija algoritama koji su značajno efikasniji od algoritama koje provodimo pomoću klasične logike. Istaknimo odmah kako su takvi algoritmi (još uvijek) vrlo specifični i vezani uz točno određen tip problema. No i takvi pokazuju velik potencijal za daljnji razvoj, te ne čude velika ulaganja vodećih računalnih kompanija u razvoj kvantnih računala. [9]

5.1 Deutschov algoritam

U ovom ćemo članku objasniti jedan od prvih formuliranih kvantnih algoritama, *Deutschov algoritam*. Iako je problem koji algoritam rješava jednostavan, već se i kod njega vidi komparativna prednost koju kvantni algoritam može ostvariti u usporedbi s algoritmima klasične logike.

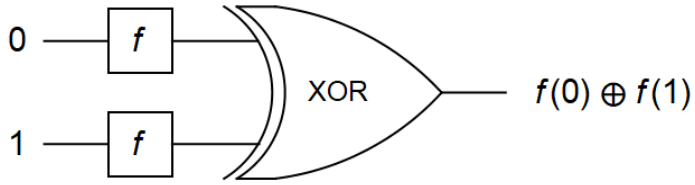
Deutschov problem pripada skupu tzv. *problema upita*. Radi se o problemima u kojima nam je cilj postaviti što manje upita (eng. *query*) kako bismo odredili odgovor na postavljeno pitanje. U tu skupinu problema spadaju i neki drugi složeniji kvantni algoritmi poput Deutsch–Jozsina ili Simonova algoritama (vidi [4, 9]).

U Deutschovu problemu dana nam je funkcija $f : \{0, 1\} \to 0, 1$, dakle funkcija koja vrijednosti jednog bita preslikava u drugi bit. Upitima ovdje smatramo računanja pojedinih vrijednosti funkcije f. Stoga nam je cilj odgovoriti na postavljeno pitanje sa što manjim brojem izvršenih upita, odnosno što manjim brojem računanja vrijednosti

funkcije f.

Pitanje na koje tražimo odgovor glasi: je li funkcija f *balansirana* ili *konstantna*? Funkcija je *konstantna* ako su obje njezine vrijednosti jednake, odnosno ako sve elemente domene preslikava u broj 0 ili ih sve preslikava u broj 1. S druge strane, funkcija je *balansirana* ako jednu vrijednost preslika u broj 0, a drugu u broj 1, ili drugim riječima, ako je bijekcija. Dakle, traženi algoritam treba vratiti vrijednost 1 ako je funkcija balansirana, odnosno 0 ako nije.

Algoritam klasične logike za rješavanje Deutschovog problema mora postaviti dva upita o vrijednosti funkcije f: mora postaviti upit koliko iznosi $f(0)$ te koliko iznosi $f(1)$. Odgovor na postavljeno pitanje daje primjena logičkog *XOR* (*isključivo ili*) veznika na vrijednosti funkcija $f(0)$ i $f(1)$, kao što je prikazano na Slici 11.[10]



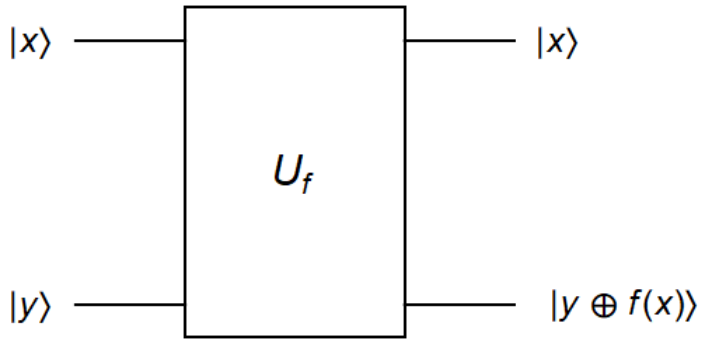
Slika 11: Simbolički prikaz algoritma klasične logike za Deutschov problem

S druge strane, kvantni Deutschov algoritam za rješavanje istog problema postavlja samo jedan upit, odnosno samo jednom računa vrijednost funkcije f. No prije nego li promotrimo sam Deutschov algoritam moramo objasniti kako kvantno računalo postavlja upite funkciji f.

Naime, kvantni logički algoritmi rade isključivo pomoću unitarnih (reverzibilnih) transformacija. Djelovanje funkcije f ne mora biti reverzibilno, budući da funkcija ne mora biti bijekcija. Stoga ćemo (u Diracovoj notaciji) prvo definirati unitarni operator U_f kojim ćemo implementirati djelovanje funkcije f, na sljedeći način:

$$U_f(|xy\rangle) = U_f(|x\rangle \otimes |y\rangle) = |x\rangle \otimes |y \oplus f(x)\rangle \qquad (4)$$

gdje je $\oplus$ zbrajanje modulo 2. Primijetimo kako $y \oplus f(x)$ ostavlja bit y na miru ako je $f(x) = 0$, te ga okreće ako je $f(x) = 1$. Zainteresiranog čitatelja upućujemo na literaturu [8,10] kako bi se uvjerili da je tako definiran operator uistinu unitaran. Simbolički prikaz djelovanja operatora U_f prikazan je na Slici 12. Gornji *qbit* zovemo ulaznim, a donji izlaznim *qbitom*.[11]

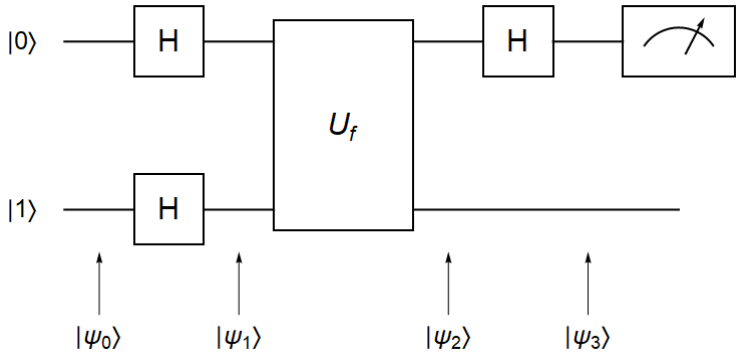


Slika 12: Simbolički prikaz kvantne implementacije funkcije f

Snaga kvantnog računa proizlazi iz djelovanja funkcije na superpoziciju ortogonalnih stanja (baze), čime se jednim pozivom funkcije (na opće kvantno stanje) dobiva informacija o djelovanju funkcije na sva ortogonalna bazna stanja. Pametnom konstrukcijom unitarnog operatora U_f tako možemo dobiti informacije koje simuliraju paralelno djelovanje kvantnog algoritma na svim stanjima baze, usprkos ograničenju o jednom mjerenju dobivenog rezultata.

Upravo zbog toga kvantni algoritmi značajno (eksponencijalno) dobivaju na efikasnosti pri upotrebi većeg broja *qbita* (odnosno baznih stanja). Deutschov algoritam prikazuje tu prednost pri upotrebi (samo) dva *qbita*, no upravo ga to čini dovoljno jednostavnim za razumijevanje procesa koji se odvijaju iza kvantnih algoritama.

Na Slici 13 dan je simbolički prikaz kvantnog Deutschovog algoritma. Na prikazu su posebno označenja stanja sustava dva *qbita*, $|\psi_0\rangle$, $|\psi_1\rangle$, $|\psi_2\rangle$ i $|\psi_3\rangle$, kroz koja ćemo analizirati rad samog algoritma. Pri tome stanje sustava $|\psi_0\rangle$ označava ulazno stanje i vrijedi $|\psi_0\rangle = |01\rangle$.



Slika 13: Simbolički prikaz kvantnog Deutschovog algoritma

Prođimo računski kroz prikazani algoritam. Ulaz u algoritam je stanje $|\psi_0\rangle = |01\rangle$, na koje potom primjenjujemo unitarni operator $H \otimes H$. Za taj operator vrijedi:

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

Sada računamo kvantno stanje $|\psi_1\rangle$ (prisjetimo se vektorskog zapisa za $|01\rangle$ iz Definicije 4):

$$|\psi_1\rangle = H \otimes H|01\rangle = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix},$$

tj. u Diracovoj notaciji

$$|\psi_1\rangle = \frac{1}{2}\big(|00\rangle - |01\rangle + |10\rangle - |11\rangle\big).$$

Prisjetimo li se kako izgleda tenzorski produkt vektora Hadamardove baze (??), vidimo da vrijedi $|\psi_1\rangle = |+-\rangle$. Kvantno stanje $|\psi_1\rangle$ zapisati ćemo u malo drugačijem obliku:

$$|\psi_1\rangle = \frac{1}{2}|0\rangle\big(|0\rangle - |1\rangle\big) + \frac{1}{2}|1\rangle\big(|0\rangle - |1\rangle\big) \qquad (5)$$

Na to kvantno stanje potom primjenjujemo operator U_f. Kako je $U_f|xy\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$, raspisivanjem djelovanja operatora U_f na (??) dobivamo:

$$|\psi_2\rangle = U_f|\psi_1\rangle = \frac{1}{2}|0\rangle\big(|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle\big) + \frac{1}{2}|1\rangle\big(|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle\big),$$

gdje je $\oplus$ zbrajanje modulo 2. Taj izraz možemo pojednostavniti, budući je

$$|0 \oplus a\rangle - |1 \oplus a\rangle = (-1)^a\big(|0\rangle - |1\rangle\big),$$

gdje je a bilo $f(0)$ ili $f(1)$, tj. poprima vrijednost 0 ili 1. Sada je:

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}(-1)^{f(0)}\big(|0\rangle - |1\rangle\big) + \frac{1}{2}(-1)^{f(1)}\big(|0\rangle - |1\rangle\big) \\ &= \left(\frac{(-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle}{\sqrt{2}}\right)|-\rangle \end{aligned}$$

jer je $|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$.

Vidimo kako u stanju $|\psi_2\rangle$ drugi *qbit* ima vrijednost $|-\rangle$ bez obzira na to kakva je funkcija f. No zato su u vrijednosti prvog *qbita* sadržane informacije o vrijednostima funkcije f i u 0 i u 1. Još je potrebno te informacije očitati na domišljat način. U tu svrhu izlučimo vrijednost $(-1)^{f(0)}$, pri čemu ćemo iskoristiti činjenicu da je $(-1)^{f(1)-f(0)} = (-1)^{f(0)\oplus f(1)}$.

Navedeni identitet vrijedi jer $f(0)$ i $f(1)$ mogu poprimiti samo dvije vrijednosti, 0 i 1. Stoga i njihova razlika može poprimiti samo vrijednosti -1, 0 i 1. Ako su vrijednosti $f(0)$ i $f(1)$ jednake (tj. ako je funkcija konstantna), razlika je jednaka nuli, a ako nisu (tj. ako je

funkcija balansirana), razlika je jednaka 1 ili -1. U oba slučaja, uvrštavanjem lako provjeravamo istinitost navedenog identiteta. Dakle, vrijedi:

$$|\psi_2\rangle = (-1)^{f(0)} \left(\frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}} \right) |-\rangle$$

Promotrimo li izraz u zagradi vidimo da vrijedi:

$$\begin{cases} \frac{|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}} = \frac{|0\rangle+|1\rangle}{\sqrt{2}} = |+\rangle, \ \text{ako je funkcija konstantna} \\ \\ \frac{|0\rangle+(-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}} = \frac{|0\rangle-|1\rangle}{\sqrt{2}} = |-\rangle, \ \text{ako je funkcija balansirana} \end{cases}$$

odnosno

$$|\psi_2\rangle = \begin{cases} (-1)^{f(0)}|+-\rangle, \ \text{ako je funkcija konstantna} \\ \\ (-1)^{f(0)}|-\rangle, \ \text{ako je funkcija balansirana} \end{cases}$$

Dakle, informacija o tome je li funkcija konstantna ili balansirana pohranjena je u prvom *qbitu* (pri čemu drugi *qbit* uvijek ima istu vrijednost). Posljednji korak je primjena Hadamardovih logičkih vrata na prvi *qbit*, što nam daje kvantno stanje $|\psi_3\rangle$.

$$|\psi_3\rangle = \begin{cases} (-1)^{f(0)}|0-\rangle, \ \text{ako je funkcija konstantna} \\ \\ (-1)^{f(0)}|1-\rangle, \ \text{ako je funkcija balansirana} \end{cases}$$

Konačno mjerenjem prvog *qbita* dobivamo vrijednost 0 ako je funkcija konstantna, odnosno 1 ako je balansirana. Istaknimo i kako se primjenom algoritma ispred stanja sustava pojavio faktor $(-1)^{f(0)}$. No tu se radi o globalnoj fazi koju i tako ne možemo mjeriti pa ne utječe na provođenje algoritma i njegov rezultat.[12]

6 Zaključak

Cilj ovog teksta bio je opisati temeljne pojmove i procese u radu kvantnog računala i u izgradnji algoritama kojima se isto služi. Naravno, tema je opsežna i ovim smo člankom tek otvorili vrata zainteresiranim čitateljima. Mnoge su teme ostale neobrađene: od teorijske formalizacije kvantne logike, do načina rada složenijih kvantnih algoritama. No vjerujemo kako će, nakon ovog uvoda te teme biti lakše pronaći, pratiti i razumjeti.

Bibliografija

[1] Chailloux, A. „Quantum Circuits and Logic Gates“, nastavni materijali Sorbonne Université (2023)

[2] Crooks, G.E. „Quantum Gates“, unpublished (2024) \url{https://threeplusone.com/gates} (pristupljeno: 6. kolovoza 2024)

[3] Glendinning, I. „The Bloch sphere,”, QIA Meeting. Vienna, (2005)

[4] Ilijić, S. „Kvantna računala“, nastavni materijali, Fakultet elektotehnike i računarstva, Sveučilište u Zagrebu (2022), http://sail.zpf.fer.hr/labs/kvarac/slides/ (pristupljeno: 10. kolovoza 2024)

[5] Krupansky, J., „Feynman's Three Papers Related to Quantum Computing", Medium, (2023) https://jackkrupansky.medium.com/feynmans-three-papers-related-to-quantu... (pristupljeno: 25. kolovoz 2024)

[6] McDonald, K.T., „Physics of Quantum Computation", nastavni materijal, Princeton University (2022)

[7] Roel, J. „Demystifying Quantum Gates – One Qubit At A Time", Towards Data Science (2018)

[8] de Ronde, C., Domenech, G., Freytes, H. „Quantum Logic in Historical and Philosophical Perspective", The Internet Encyclopedia of Philosophy, (2016) https://iep.utm.edu/qu-logic/ (pristupljeno: 26. studeni 2024)

[9] Watrous, J., „Fundamentals of Quantum Algorithms", IBM Quantum Learning, https://learning.quantum.ibm.com/course/fundamentals-of-quantum-algorithms (pristupljeno: 19. kolovoza 2024)

[10] Wilkins, A., „Record-breaking quantum computer has more than 1000 qubits", New Scientist, (2023) https://www.newscientist.com/article/2399246-record-breaking-quantum-com... (pristupljeno: 26. studeni 2024)

[11] „The History of Quantum Computing You Need to Know", Quantum Insider, (2024) https://thequantuminsider.com/2020/05/26/history-of-quantum-computing/ (pristupljeno 26. studeni 2024)

---

[1]Zbog opsežnosti članka, na ovom mjestu pretpostavljamo osnovno znanje čitatelja o vektorskim prostorima, poput poznavanja pojmova (i svojstava) baze vektorskog prostora, standardno definiranog skalarnog (unutarnjeg) produkta i ortogonalnosti.
[2]Za svojstvene vrijednosti hermitskih operatora vrijedi da su realne vrijednosti, dok za njihove svojstvene vektore vrijedi da su međusobno okomiti.
[3]Za detaljniji izvod, zainteresirane čitatelje upućujemo na [4].
[4]Prisjetimo se, po definiciji djelovanja eksponencijalne funkcije na kompleksne brojeve vrijedi $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Odavde jednostavno slijedi $|e^{i\varphi}| = 1$
[5]Za početak, unitarne operatore definiramo pomoću dvodimenzionalnih matrica, no kako ćemo kasnije opisati rad na sustavima s više od jednog *qbita*, tako će se mijenjati i veličina unitarne matrice koja djeluje na takvim sustavima.
[6]Potpune preciznosti radi, kroz opisani postupak se svi *qbiti* mogu jedinstveno prikazati kao točke na (gornjoj) polovici opisane sfere (zato jer je realna vrijednost r_α iz polarnog zapisa kompleksnog broja α pozitivan broj). Zbog toga se uvodi korekcija dvostrukim kutom, odnosno vrijednost kuta θ se množi s 2. Pri tome se pokazuje kako se tim procesom ne gubi jedinstvenost zapisa, iako se sve točke „ekvatora" preslikavaju na „južni pol" Blochove sfere, što ne utječe na mogućnost reprezentacije *qbita*. [3]
[7]Vrata $\sqrt{NOT}$ znaju se zapisivati i na sljedeći način: $\sqrt{NOT} = \frac{1}{\sqrt{2}i}\begin{bmatrix} 1 & i \\ i & 1 \end{bmatrix}$.
Navedeni zapisi operatora jednaki su do na globalnu fazu.
[8]Prisjetimo se, u klasičnoj logici skup veznika $\wedge, \neg$ je potpun, što znači da je pomoću ta dva logička veznika moguće iskazati sve ostale logičke veznike.
[9]Napomenimo kako pojam "algoritam" u ovom kontekstu ne promatramo kao niz (iterativnih) naredbi, već kao matematički koncept koji opisuje rješenje problema koristeći kvantno računanje. Pri tome kvantne algoritme implementiramo pomoću kvantnih logičkih sklopova, što znači da je sklop fizička realizacija algoritma.
[10]Na Slici 11 simbol $\oplus$ označava zbrajanje modulo 2, koje primijenjeno na ulazima iz skupa $\{0,1\}$ daje rezultat ekvivalentan primjeni *XOR* logičkih vrata.
[11]Uloga gornjeg i donjeg *qbita* može biti obrnuta, ovisno o prikazu kvantnog logičkog sklopa.
[12]Faktor $(-1)^{f(0)}$ može poprimiti vrijednosti -1 ili 1. U oba slučaja radi se o globalnoj fazi oblika $e^{i\,\varphi}$, u prvom slučaju za $\varphi = \pi$, a u drugom za $\varphi = 0$.

ISSN 1334-6083