Osnovni principi kvantnog računanja

Ivica Friščić, Zoran Rukelj, Petar Žugec, Mihael S. Grbić, Ivan Kupčić[1]

Uvod

Sigurno ste se već susreli s pojmom *kvantno računalo*, tj. s novim tipom računala koje bi u odnosu na klasično računalo trebalo biti superiorno u obavljanju specifičnih zadataka kao što su dešifriranje kriptiranih podataka, simulacija kvantnih procesa u fizici čvrstoga stanja i kemiji, u strojnom učenju, itd. Sam koncept kvantnog računala počeo se razvijati tijekom 80-tih godina te su do danas uspješno formulirani različiti algoritmi koji se temelje na principima kvantne mehanike. Međutim, razvoj uređaja na kojima bi se ti algoritimi trebali izvršavati ne teče baš tako glatko. Za razliku od klasičnih računala koja podatke spremaju u bitove s dobro definiranim stanjima 0 i 1, kvantna računala koriste *qubitove* koji mogu biti i u stanju između 0 i 1. Pokazalo se da je tehnički vrlo zahtjevno napraviti veliki broj qubitova i držati ih u stanjima superpozicije tijekom izvođenja algoritma. Kvantni procesor radi na vrlo niskim temperaturama, a stanja superpozicije vrlo lako mogu uništiti različiti tipovi šumova kao što su termičke vibracije, elektromagnetske smetnje, kozmičke zrake i slično. U praksi veliki broj qubitova mora biti rezerviran za ispravljanje grešaka uzrokovanih šumom, pa ih malo ostaje za same izračune, tako da jedan od sugovornika u članku iz časopisa Nature iz 2023. godine pesimistično kaže da kvantna računala trenutno nisu korisna ni za što [1]. Naravno, uz odgovarajuće inovacije i tehnički napredak kvantna računala bi mogla odjednom postati vrlo korisna. Nemojte zaboraviti da kvantne algoritme već imamo.

U ovom članku nećemo se baviti tehničkim detaljima rada takvog uređaja, nego ćemo se koncentrirati na principe kvante mehanike i kako iz njih slijedi ideja za *kvantno računanje*. Započet ćemo s osnovama linarne algebre, povezati sve s qubitovima i superpozicijom stanja te u drugom dijelu pogledati kvantna vrata koja u specijalnim slučajevima imaju analogone u klasičnim logičkim vratima i spomenuti neka koja nemaju. Pritom ćemo u nekim dijelovima slijediti udžbenik *Introduction to Quantum Computing* autora H. Y. Wong-a [2].

Malo linearne algebre i analogija s kvantnom mehanikom

Svoje razmatranje započet ćemo s vektorima u dvodimenzionalnom prostoru:

$$\vec{v}_1 = a \cdot \hat{x} + b \cdot \hat{y} = \begin{pmatrix} a \\ b \end{pmatrix}, \qquad \vec{v}_2 = c \cdot \hat{x} + d \cdot \hat{y} = \begin{pmatrix} c \\ d \end{pmatrix}. \tag{1}$$

Vektore $\vec{v}_1$ i $\vec{v}_2$ smo zapisali kao linearne kombinacije jediničnih vektora $\hat{x}$ i $\hat{y}$, s koeficijentima a, b, c i d. Jedinični vektori su međusobno ortogonalni i imaju normu (duljinu) jednaku 1 te čine ortonormiranu bazu 2D vektorskog prostora. Alternativno, vektore $\vec{v}_1$ i $\vec{v}_2$ možemo zapisati samo pomoću koeficijenata tako da ih organiziramo u stupac gdje prvi redak u stupcu odgovara onom koji stoji uz jednični vektor $\hat{x}$, a drugi redak uz jednični

[1] Autori su s Fizičkog odsjeka Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu.

vektor $\hat{y}$. U takvom zapisu *skalarni* ili *unutarnji produkt* možemo zapisati kao umnožak retka i stupca matrice:

$$\vec{v}_1 \cdot \vec{v}_2 = (a^* \; b^*) \begin{pmatrix} c \\ d \end{pmatrix} = a^* \cdot c + b^* \cdot d. \tag{2}$$

U općenitom slučaju koeficijenti mogu biti i kompleksni brojevi pa zvjezdica "*" označava konjugirano kompleksni broj. Ako uzmemo skalarni produkt vektora samog sa sobom, dobit ćemo kvadrat duljine tog vektora L^2:

$$\vec{v}_1 \cdot \vec{v}_1 = (a^* \; b^*) \begin{pmatrix} a \\ b \end{pmatrix} = a^* \cdot a + b^* \cdot b = |a|^2 + |b|^2 = L^2. \tag{3}$$

Pogledajmo sada analogni primjer u kvantnoj mehanici. Pretpostavimo da imamo qubit reprezentiran elektronom koji je čestica sa spinom $1/2$ pa ima dvije projekcije, spin gore $|1/2, 1/2\rangle$ i spin dolje $|1/2, -1/2\rangle$ [3]. Primijetite da smo ovo mogli označiti i sa $|1/2, 1/2\rangle = |\uparrow\rangle$ i $|1/2, -1/2\rangle = |\downarrow\rangle$. Međutim, mi ćemo izabrati oznake $|1/2, 1/2\rangle = |0\rangle$ i $|1/2, -1/2\rangle = |1\rangle$. Općenito se qubit može nalaziti u bilo kojem stanju između te dvije projekcije pa to prikazujemo valnom funkcijom $|\psi\rangle$ koja je linearna kombinacija ta dva stanja:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,. \tag{4}$$

Ako sada jednadžbu (4) usporedimo s izrazom (1), vidimo da valna funkcija $|\psi\rangle$ odgovara vektoru $\vec{v}$, a projekcije spina $|0\rangle$ i $|1\rangle$ nam čine bazu slično kao i jedinični vektori $\hat{x}$ i $\hat{y}$ u 2D vektorskom prostoru, a linearnu kombinaciju sada zovemo *superpozicijom*. Za stanja baze i dalje vrijedi svojstvo ortonormiranosti pa će za skalarni produkt vrijediti

$$\hat{\imath} \cdot \hat{\jmath} = \langle i|j\rangle = \begin{cases} 1 & i = j \\ 0 & i \neq j. \end{cases}$$

Za kvantna računala također želimo da i sama valna funkcija bude normirana:

$$\langle \psi|\psi\rangle = (\alpha^* \; \beta^*) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = |\alpha|^2 + |\beta|^2 = 1. \tag{5}$$

Ovaj izraz znači da kada napravimo mjerenje, vjerojatnost da qubit nađemo u stanju $|0\rangle$ iznosi $|\alpha|^2$, dok vjerojatnost da qubit nađemo u stanju $|1\rangle$ iznosi $|\beta|^2$. Primijetite da se skalarni produkt (5) ne mijenja ako bi uz neki od koeficijenata α i β dodali *fazni faktor* $e^{i\theta}$ jer bismo imali $(e^{i\theta})^* e^{i\theta} = e^{-i\theta} e^{i\theta} = 1$. U kvantnom računarstvu fazni faktor je vrlo važan i koristi se za postizanje *interferencije*. Ovdje smo se počeli koristiti takozvanom *bra-ket* notacijom koja dolazi od engleske riječi "bracket" što znači zagrada, tako da svaki ket-vektor $|\cdot\rangle$ također ima svoji dualni bra-vektor $\langle\cdot|$ i obrnuto:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \iff \langle\psi| = \alpha^*\,\langle 0| + \beta^*\,\langle 1|\,. \tag{6}$$

Ako želimo izmjeriti koliko iznosi pojedini koeficijent $|\alpha|$ ili $|\beta|$, prvo na valnu funkciju trebamo djelovati *operatorom projekcije*, tj. trebamo je projicirati na potprostor stanja koje nas zanima. Operator projekcije P_i možemo vrlo lako konstruirati pomoću *tenzors-*

kog produkta:

$$P_i = |i\rangle\,\langle i|\,. \tag{7}$$

Recimo da nas zanima projekcija na stanje $|1\rangle$. Pripadni projektor bio bi:

$$P_1 = |1\rangle\,\langle 1| = \begin{pmatrix} 0 \\ 1 \end{pmatrix}(0^*\ 1^*) = \begin{pmatrix} 0\ 0 \\ 0\ 1 \end{pmatrix}. \tag{8}$$

A mjerenje koeficijenta β bi onda odgovaralo:

$$\langle\,\psi|P_1|\psi\rangle = (\alpha^*\ \beta^*)\begin{pmatrix} 0\ 0 \\ 0\ 1 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = (\alpha^*\ \beta^*)\begin{pmatrix} 0 \\ \beta \end{pmatrix} = \alpha^*\cdot 0 + \beta^*\cdot\beta = |\beta|^2. \tag{9}$$

U gornjem redu prvo smo projektorom P_1 djelovali na ket-vektor $|\psi\rangle$ kako bismo ga projicirali na potprostor vektora $|1\rangle$ te smo ga zatim skalarno pomnožili bra-vektorom $\langle\,\psi|$ te dobili, odnosno izmjerili $|\beta|^2$.

Pogledajmo što se događa ako na projekcije spina $|0\rangle$ i $|1\rangle$ djelujemo operatorom $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$:

$$\sigma_z\,|0\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = 1\cdot|0\rangle\,, \tag{10}$$

$$\sigma_z\,|1\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -\begin{pmatrix} 0 \\ 1 \end{pmatrix} = -1\cdot|1\rangle\,. \tag{11}$$

Kao što vidimo, operator σ_z ne mijenja stanja $|0\rangle$ i $|1\rangle$ kada djeluje na njih, već ih samo skalira za faktor 1, odnosno -1. Dakle, kažemo da su $|0\rangle$ i $|1\rangle$ *svojstvena stanja* operatora σ_z sa svojstvenim spinovima 1 i -1. Ekvivalentno možemo reći da su $|0\rangle$ i $|1\rangle$ *svojstveni vektori* matrice σ_z sa *svojstvenim vrijednostima* 1 i -1.

Što će se dogoditi ako operator σ_z djeluje na sljedeća stanja:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}? \tag{12}$$

Računamo:

$$\sigma_z\,|+\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = |-\rangle\,, \tag{13}$$

$$\sigma_z\,|-\rangle = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |+\rangle\,. \tag{14}$$

Vidimo da rezultat djelovanja operatora σ_z više nije skalar puta originalni vektor, nego da operator σ_z rotira stanje $|+\rangle$ u $|-\rangle$, i obrnuto. Dakle, stanja $|+\rangle$ i $|-\rangle$ nisu svojstvena stanja operatora σ_z. Ono što možemo pokazati je da su $|+\rangle$ i $|-\rangle$ svojstvena stanja operatora $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$:

$$\sigma_x\,|+\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = 1\cdot|+\rangle\,, \tag{15}$$

$$\sigma_x\,|-\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} -1 \\ 1 \end{pmatrix} = -1\cdot\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} = -1\,|-\rangle\,. \tag{16}$$

Ovdje smo vektore $|+\rangle$ i $|-\rangle$ zapisali preko ortonormirane baze koju čine vektori $|0\rangle$ i $|1\rangle$. Također možemo promijeniti bazu te napraviti obrnuto, tj. zapisati vektore $|0\rangle$ i $|1\rangle$

u bazi $|+\rangle$ i $|-\rangle$:

$$|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle), \qquad |1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle). \tag{17}$$

Važno je zapamtiti da koju god bazu izabrali, promijenit ćemo samo matričnu i vektorsku reprezentaciju, no svojstvene vrijednosti ostat će nepromijenjene.

Ako dodamo još i operator $\sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$, matrice σ_x, σ_y i σ_z čine skup *Paulijevih matrica*, koje su vrlo važne u kvantnom računarstvu. Kada želimo mjeriti spin, potrebno je primijeniti vanjsko magnetsko polje, koje može biti u $\hat{x}$, $\hat{y}$ i $\hat{z}$ smjeru. Svaki od postava i mjerenja odgovara matrici u matričnoj reperezentaciji kvantne mehanike.

Ranije smo spomenuli da svaki vektor u ket-prostoru ima odgovarajući vektor u bra-prostoru, vidi izraz (6). Isto tako svaki oprator koji djeluje na vektor u ket-prostoru ima i odgovarajući operator koji djeluje na vektor u bra-prostoru:

$$A|\psi\rangle = |\psi'\rangle \iff \langle\psi|A^\dagger = \langle\psi'|. \tag{18}$$

Ovdje je $A^\dagger$ *adjungirana matrica* matrice A, koju dobivamo tako da matricu A transponiramo i konjugiramo elemente matrice a_{ij}:

$$A^\dagger = (A^*)^T, \qquad a^\dagger_{ji} = a^*_{ij}. \tag{19}$$

Ako dva puta ajdungiramo istu matricu, opet ćemo dobiti početnu, tj. $(A^\dagger)^\dagger = A$. Postoji posebna vrsta matrica koje su jednake svojoj adjungiranoj matrici, a zovemo ih *samoadjungiranim* ili *hermitskim matricama*:

$$A^\dagger = A, \qquad a^\dagger_{ji} = a_{ij}. \tag{20}$$

Hermitske matrice su važne u kvantnoj mehanici jer predstavljaju operatore koji imaju realne svojstvene vrijednosti, tako da sve observable odgovaraju operatorima reprezentiranima hermitskim matricama.

Sljedeći tip operatora koji će nam biti važan reprezentiran je *unitarnom matricom*. Unitarna matrica ima svojstvo da ne mijenja skalarni produkt dva vektora koji su transformirani istim unitarnim operatorom. Dakle, ne mijenja duljinu vektora, tj. normu stanja. Ovo svojstvo je vrlo važno u kvantnom računarstvu jer se čuva norma vjerojatnosti stanja koja je jednaka 1. Prema definiciji kažemo da je matrica U unitarna ako je adjungirana matrica $U^\dagger$ jednaka inverznoj matrici U^{-1}:

$$U^\dagger = U^{-1}. \tag{21}$$

Ako gornji izraz pomnožimo ili slijeva ili zdesna unitarnom matricom U, dobivamo jediničnu matricu I koja nema nikakav efekt ako djeluje na neki vektor:

$$U^\dagger U = I, \qquad UU^\dagger = I. \tag{22}$$

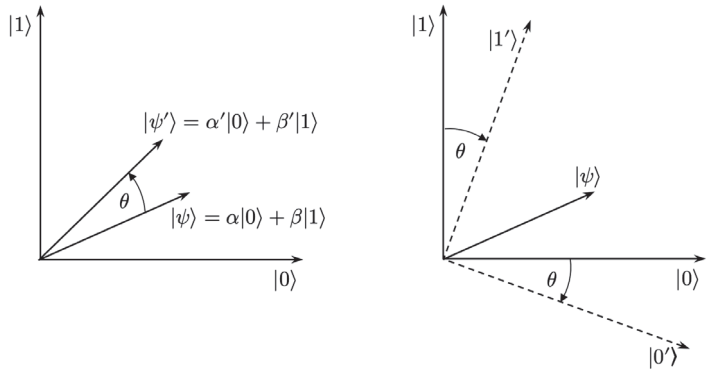
odnosno ako takvim operatorom djelujemo na stanja:

$$\langle f|\, U^\dagger U\, |i\rangle = \langle f|\, I\, |i\rangle = \langle f|i\rangle\ . \tag{23}$$

Vidimo da je skalarni produkt nepromijenjen ako je rotacijska matrica unitarna. Također, ako imamo ortonormirani skup vektora baze, nakon transformacije unitarnom matricom rotirani skup vektora baze će i dalje biti ortonormiran. U kvantnom računarstvu, kada radimo operacije na qubitu, moramo osigurati da je matrica operacije unitarna. Napomenimo još da unitarna matrica služi za opis evolucije kvantnog stanja u vremenu.

Nešto ranije smo spomenuli da kada operator A djeluje na stanje $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, koje nije svojstveno stanje operatora A, dobit ćemo rotirano stanje $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$, kao što je prikazano na lijevoj slici 1. U tom slučaju stanje $|\psi\rangle$ je rotirano za neki kut θ

suprotno od smjera kazaljke na satu. Vektori baze ostaju nepromijenjeni, a mijenjaju se samo koeficijenti α i β u α' i β'. Potpuno istu stvar dobivamo ako vektore baze $|0\rangle$ i $|1\rangle$ rotiramo u smjeru kazaljke na satu za kut θ u nove vektore baze $|0'\rangle$ i $|1'\rangle$, kao što je ilustrirano na desnoj slici 1. To ćemo napraviti pomoću unitarne transformacije koja je, naravno, reprezenirana unitarnom matricom U. Takav način promjene baze često se koristi u kvantnom računarstvu.



Slika 1. Općenito, operator A, koji djeluje na stanje $|\psi\rangle$, rotirat će to stanje za neki kut θ suprotno od smjera kazaljke na satu u rotirano stanje $|\psi'\rangle$ (lijevo). Dobivamo potpuno isti rezultat ako unitarnom transformacijom rotiramo vektore baze za taj isti kut θ u smjeru kazaljke na satu, tj. promijenimo bazu (desno).

Uz uvjet ortonormiranosti važno je da je baza *kompletna*. Drugim riječima, da vektori baze razapinju cijeli postor koji nas zanima. Ortonormirana baza je kompletna ako vrijedi

$$\sum_{i=0}^{n-1} |i\rangle \langle i| = I. \tag{24}$$

Ovdje je I jedinična matrica. Sami se možete uvjeriti da vektori $|0\rangle$ i $|1\rangle$ te $|+\rangle$ i $|-\rangle$ tvore baze koje su kompletne.

U matematičkoj formulaciji kvantne mehanike stanja se nalaze u prostoru koji nazivamo *Hilbertov prostor*. Hilbertov prostor je potpuni linearni prostor s definiranim skalarnim produktom te može imati konačan ili beskonačan broj dimenzija. Svaki par vektora $|\psi_1\rangle$ i $|\psi_2\rangle$ iz tog prostora, te kompleksni broj a imaju sljedeća svojstva:

$$\langle \psi_1|\psi_1\rangle \geq 0, \tag{25}$$

$$\langle a\psi_1|\psi_2\rangle = a^* \langle \psi_1|\psi_2\rangle , \tag{26}$$

$$\langle \psi_1|a\psi_2\rangle = a \langle \psi_1|\psi_2\rangle , \tag{27}$$

$$\langle \psi_1|\psi_2\rangle = \langle \psi_2|\psi_1\rangle ^* , \tag{28}$$

$$\langle \psi_1 + \psi_2|\psi_3\rangle = \langle \psi_1|\psi_3\rangle + \langle \psi_2|\psi_3\rangle . \tag{29}$$

U našem slučaju jedan qubit ima svojstvena stanja $|0\rangle$ i $|1\rangle$ koja čine kompletnu ortnormiranu bazu dvodimenzionalnog Hilbertovog prostora, što označavamo s $\mathbb{C}^2$. Ako želimo raditi s dva qubita, onda trebamo povećati dimenziju prostora i to ćemo napraviti pomoću

tenzorskog produkta, $\mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$:

$$\begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} \otimes \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} = \begin{pmatrix} |0\rangle \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} \\ |1\rangle \begin{pmatrix} |0\rangle \\ |1\rangle \end{pmatrix} \end{pmatrix} = \begin{pmatrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{pmatrix}. \tag{30}$$

U zadnjem stupcu izraza (30) dobili smo četiri nova vektora baze. Kako smo se ranije odlučili označavati stanje spin gore s $|0\rangle$, a stanje spin dolje s $|1\rangle$, uočite da novi vektori baze sustava s 2 qubita odgovaraju binarnom zapisu brojeva od 0 do 3. Potpuno isto kao i kod klasičnih računala. Kad bismo imali n-qubitova, pripadni Hilbertov prostor imao bi 2^n dimenzija, $\mathbb{C}^{2^n}$, a vektori baze odgovarali bi binarnim brojevima od 0 do $2^n - 1$.

U klasičnom računalu, *klasični registar* čini skup bitova u koje zapisujemo podatke u binarnom obliku. Recimo, u 8-bitni registar ukupno možemo upisati 256 brojeva u binarnom obliku, to su brojevi od 0 do 255. Npr. binarni broj $(11110000)_2$ odgovara broju 240 u dekadskom sustavu. *Kvantni registar* možemo zamisliti kao grupirane qubitove, ali ne nužno kao memoriju u klasičnom računalu, nego kao prirodno proširenje koncepta klasičnog registra. U n-bitni klasični registar pohranjuje se n-bitna informacija, dok se u n-qubitni registar pohranjuje n-qubitna informacija. Kako klasični registar može pohraniti samo jednu kombinaciju nula i jedinica, kvantni registar će biti jednak klasičnom samo u slučaju ako je u njemu pohranjen samo jedan od vektora baze. Općenito u kvantni registar možemo zapisati stanje koje odgovara superpoziciji svih vektora baze, tj. možemo istovremeno pohraniti sve kombinacije nula i jedinica istovremeno te istovremeno raditi račune na svim brojevima od 0 do $2^n - 1$. To se naziva *kvantna usporednost* ili *kvantni paralelizam*. Potrebno je napomenuti da iako kvantno računalo dopušta istovremeno pohranjivanje 2^n koeficijenata i izvođenje 2^n operacija, rezultat je teško očitati zbog kolapsa valne funkcije prilikom samo jednog mjerenja. U praksi kvantni algoritmi koriste interferenciju između stanja baze da bi se dobio željeni rezultat.

Vratimo se na slučaj s 2 qubita. Općenito ćemo sada stanje 2 qubita $|\psi\rangle_{(2)}$ zapisati kao superpoziciju, tj. linearnu kombinaciju vektora baze $|00\rangle$, $|01\rangle$, $|10\rangle$ i $|11\rangle$:

$$|\psi\rangle_{(2)} = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle\ . \tag{31}$$

Index (2) je oznaka da se radi o stanju 2 qubita. Isti smo rezultat mogli dobiti da smo tenzorski pomnožili dva općenita stanja $|\psi_1\rangle_{(1)}$ i $|\psi_2\rangle_{(1)}$ koja opisuju jedan qubit:

$$|\psi\rangle_{(2)} = |\psi_1\rangle_{(1)} \otimes |\psi_2\rangle_{(1)} = (\alpha_1\,|0\rangle + \beta_1\,|1\rangle\,) \otimes (\alpha_2\,|0\rangle + \beta_2\,|1\rangle\,). \tag{32}$$

Ovakva stanja su *neprepletena*, odnosno zovu se *separabilna* ili *produktna* stanja. Postoje linearne kombinacije stanja 2 qubita u $\mathbb{C}^4$ prostoru koje se ne mogu konstruirati kao tenzorski produkt dva 1-qubita stanja iz $\mathbb{C}^2$ prostora pa kažemo da su *prepletena*, a zovu se *Bellova stanja*. U $\mathbb{C}^4$ Hilbertovom prostoru imamo ih četiri:

$$|\psi^+\rangle_{(2)} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle\,) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix},$$

$$|\psi^-\rangle_{(2)} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle\,) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}, \tag{33}$$

$$|\Phi^+\rangle_{(2)} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\1\\0\end{pmatrix},$$

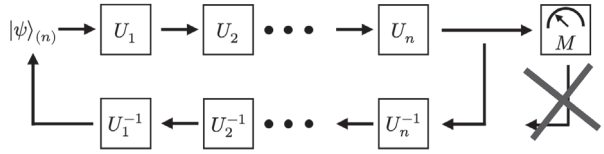
$$|\Phi^-\rangle_{(2)} = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix}0\\1\\-1\\0\end{pmatrix}. \tag{34}$$

Moguće je pokazati da Bellova stanja ostaju i dalje potpuno prepletena ako ih se rotira ili ako promijenimo reprezentaciju baze. Primijetite da jednadžba (31) predstavlja *polupreplepteno* stanje jer sadrži primjese prepletenih stanja.

Da izbjegnemo zabunu, nadalje ćemo s indeksom (n) označavati od koliko qubitova se sastoji superpozicija $|\psi\rangle$ koju razmatramo, pa ćemo stoga pisati $|\psi\rangle_{(n)}$.

Kvantna vrata i kvantni sklopovi

Najkraće rečeno, kvantno računanje možemo opisati kao seriju rotacija višedimenzionalnog vektora u višedimenzionalnom prostoru, koji je tenzorski produkt prostora nižih dimenzija. Na primjer, kod 5-bitnog kvantnog algoritma bitan nam je 32-dimenzionalni vektor u $\mathbb{C}^{32}$ prostoru koji, recimo, možemo ostvariti grupiranjem spinova 5 elektrona. Spin pojedinog elektrona opisan je 2D vektorom u $\mathbb{C}^2$ Hilbertovom prostoru, a tenzorskim produktom dobivamo 32-dimenzionalni prostor $\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2\otimes\mathbb{C}^2 = \mathbb{C}^{2^5} = \mathbb{C}^{32}$. Na kraju rotacija napravimo mjerenje da dobijemo rezultat koji nas zanima, kako je i ilustriano na slici 2.



Slika 2. Ilustracija kvantnog računanja. U i U^{-1} su unitarna kvantna vrata. U gornjem redu, na kraju rotacija početnog stanja $|\psi\rangle_{(n)}$ n-qubitova napravimo mjerenje koje daje rezultat kvantnog računanja. U donjem redu, na konačno rotirano stanje, ali prije mjerenja, možemo djelovati odgovarajućim inverznim operatorima U^{-1} i vratiti se do početnog stanja $|\psi\rangle_{(n)}$. Jednom kad smo napravili mjerenje, takav povratak do počentnog stanja više nije moguć.

Kako su operatori U koji rotiraju vektor unitarni, uvijek postoji i inverzni operator $U^{-1} = U^\dagger$. To znači da ako prije mjerenja na konačno rotirano stanje djelujemo inverznom serijom operatora, vratit ćemo se na stanje od kojeg smo počeli (slika 2). Ovo svojstvo proizlazi iz zahtjeva da je u kvantnoj mehanici evolucija (rotacija) valne funkcije *reverzibilna*. *Kvantna vrata* su dakle vrata koja izvode unitarnu operaciju nad nekim vektorom, odnosno stanjem.

Kod klasičnih računala i klasičnih logičkih vrata nemamo svojstvo reverzibilnosti, tj. iz rezultata izlaza logičkih vrata ne možemo rekonstruirati što je bilo na ulazu. Ako se

sjetimo klasičnih logičkih OR-vrata (or = ili), jedino ako je na izlazu logičkih OR-vrata rezultat 0, znamo da smo na ulazu imali $(0,0)$. Međutim, ako je na izlazu logičkih OR-vrata rezultat 1, nikako se iz toga ne može odrediti je li na ulazu bila kombinacija $(0,1)$, $(1,0)$ ili $(1,1)$.

A. NOT- ili X-vrata

Prva kvantna vrata koja ćemo pogledati se zovu NOT-vrata (not = ne) ili X-vrata zbog razloga koji će vrlo brzo postati očit. Definirana su na sljedeći način:

$$U_{\text{NOT}}\,|0\rangle = |1\rangle\,, \qquad U_{\text{NOT}}\,|1\rangle = |0\rangle\,. \tag{35}$$

Primijetite da bismo isti rezultat dobili i u slučaju klasičnih NOT-vrata ako bismo stanja baze tretirali kao klasične vrijednosti, što je i u skladu s činjenicom da se kvantni registar ponaša kao klasični registar ako je u njemu pohranjen samo jedan vektor baze. Matrica, tj. operator kvantnih NOT-vrata dana je s

$$U_{\text{NOT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{36}$$

Vidimo da je U_{NOT} matrica jednaka Paulijevoj σ_x matrici pa odatle dolazi i naziv X-vrata. Vektore baze možemo zapisati kao $|0\rangle$ i $|1\rangle$ pa dobivamo

$$\begin{aligned} U_{\text{NOT}}\,|0\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle\,, \\ U_{\text{NOT}}\,|1\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle\,. \end{aligned} \tag{37}$$

Kada U_{NOT} djeluje na superpoziciju $|\psi\rangle_{(1)} = \alpha\,|0\rangle + \beta\,|1\rangle$, dobivamo

$$U_{\text{NOT}}\,|\psi\rangle_{(1)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} = \beta\,|0\rangle + \alpha\,|1\rangle = |\psi'\rangle_{(1)}\,. \tag{38}$$

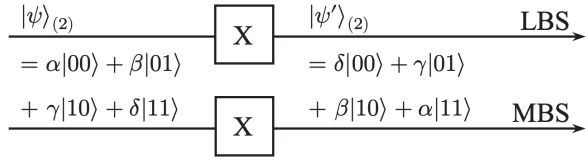
Dakle, NOT-vrata možemo shvatiti kao vrata koje zamijene koeficijente vektora baze (α postaje β i obrnuto).

Pogledajmo sada što se događa kada kvantna NOT-vrata djeluju na stanje s 2 qubita $|\psi\rangle_{(2)} = \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + \delta\,|11\rangle$. Prvo moramo povećati dimenziju operatora U_{NOT} koji je za jedan qubit djelovao na prostor $\mathbb{C}^2$, tako da za 2 qubita djeluje na prostor $\mathbb{C}^4$, tj. trebamo napraviti tenzorski produkt:

$$\begin{aligned} U_{\text{NOT}_2} = U_{\text{NOT}} \otimes U_{\text{NOT}} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 0\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ 1\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & 0\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}. \end{aligned} \tag{39}$$

Djelujemo s U_{NOT_2} na $|\psi\rangle$:

$$U_{\mathrm{NOT}_2}\,|\psi\rangle_{(2)} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \delta \\ \gamma \\ \beta \\ \alpha \end{pmatrix} = |\psi'\rangle_{(2)}\,. \tag{40}$$



Slika 3. Dijagram 2-qubitnih kvantnih NOT- ili X-vrata pomoću kvantnog sklopa. Imamo dvije linije za 2 qubita, gdje donja linija predstavlja najznačajniji bit MBS.

Vidimo da je poredak koeficijenata obrnut. Kada želimo dizajnirati kvantni algoritam, važno je da znamo kakav rezultat dobivamo kad neka kvantna vrata djeluju na stanje pohranjeno u kvantnom registru.

Ovaj primjer možemo prikazati i pomoću *kvantnog sklopa* (analogno logičkim sklopovima). Pri tome ćemo se koristiti konvencijom da najmanje značajan bit LBS (s krajnje desne strane u binarnom zapisu) prikažemo u prvom retku, a najznačajniji bit MBS (s krajnje lijeve strane u binarnom zapisu) u zadnjem retku, vidi sliku 3. Moguća je i obrnuta konvencija. U dijagramu kvantnog sklopa evolucija stanja iz $|\psi\rangle_{(2)}$ u $|\psi'\rangle_{(2)}$ ide slijeva na desno, a kada radimo preko zapisa s operatorima (recimo izraz (40)) evolucija stanja iz $|\psi\rangle_{(2)}$ u $|\psi'\rangle_{(2)}$ ide zdesna na lijevo.

B. XOR- ili CNOT-vrata

Klasična XOR (exclusive-or = isključivo-ili) logička vrata imaju 2 ulaza pa će i kvantna verzija tih vrata biti vrata za 2 qubita. XOR-vrata nazivaju se još i CNOT-vrata (controlled-not = kontrolirana-ne), a definicija glasi

$$U_{\mathrm{XOR}}\,|ab\rangle = |a, a \oplus b\rangle\,. \tag{41}$$

$|ab\rangle$ je vektor u $\mathbb{C}^4$ prostoru, dok a i b mogu poprimiti vrijednosti 0 i 1. $\oplus$ je oznaka za klasičnu XOR logičku operaciju. XOR-vrata djeluju na vektore baze tako da prvu znamenku ne mijenjaju, a drugu znamenku promijene prema logičkoj tablici XOR-vrata. Primijetite da smo desnu stranu izraza (41) mogli zapisati i kao $|a, a \oplus b\rangle = |a\rangle \otimes |a \oplus b\rangle$. Imamo:

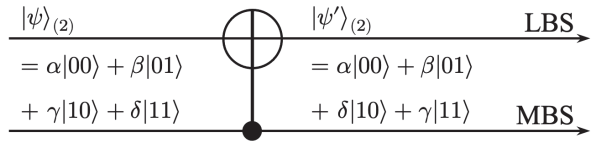
$$\begin{aligned} U_{\mathrm{XOR}}\,|00\rangle &= |0, 0 \oplus 0\rangle = |00\rangle\,, & U_{\mathrm{XOR}}\,|10\rangle &= |1, 1 \oplus 0\rangle = |11\rangle\,, \\ U_{\mathrm{XOR}}\,|01\rangle &= |0, 0 \oplus 1\rangle = |01\rangle\,, & U_{\mathrm{XOR}}\,|11\rangle &= |1, 1 \oplus 1\rangle = |10\rangle\,. \end{aligned} \tag{42}$$

Vidimo da operator U_{XOR} zamijeni mjesta trećeg i četvrtog vektora baze, a ostale ne mijenja. Isto tako, kada operator U_{XOR} djeluje na stanje 2 qubita $|\psi\rangle_{(2)}$, zamijenit će zadnji

i predzadnji koeficijent. U matričnom zapisu to je

$$U_{\mathrm{XOR}}\,|\psi\rangle_{(2)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \delta \\ \gamma \end{pmatrix}$$
$$= \alpha\,|00\rangle + \beta\,|01\rangle + \delta\,|10\rangle + \gamma\,|11\rangle = |\psi'\rangle_{(2)}\,. \tag{43}$$

Ukoliko je vrijednost qubita $a = 0$, vrijednost qubita b se ne mijenja. Međutim, ako je vrijednost qubita $a = 1$, dolazi do negacije qubita b (NOT-b). Odatle dolazi ime "kontrolirana-ne" vrata. U izrazu $a \otimes b$ prvi qubit naziva se *kontrolni qubit*, dok se drugi qubit naziva *ciljani qubit*. Na slici 4 prikazan je kvantni sklop sa XOR-vratima za stanje 2 qubita.



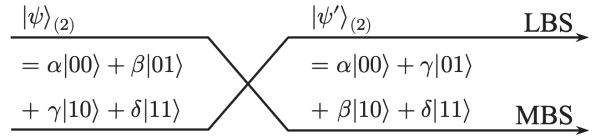
Slika 4. Dijagram kvantnog sklopa s XOR-vratima za stanje 2 qubita.

C. SWAP-vrata

Kvantna SWAP-vrata (swap = izmjena) mijenjaju poredak bitova u vektoru baze

$$U_{\mathrm{SWAP}}\,|ab\rangle = |ba\rangle\,. \tag{44}$$

U matričnom zapisu kada operator U_{SWAP} djeluje na stanje 2 qubita $|\psi\rangle_{(2)}$, zamijenit će koeficijente drugog i trećeg vektora baze, a dijagram pripadnog kvantnog sklopa prikazan je na slici 5.



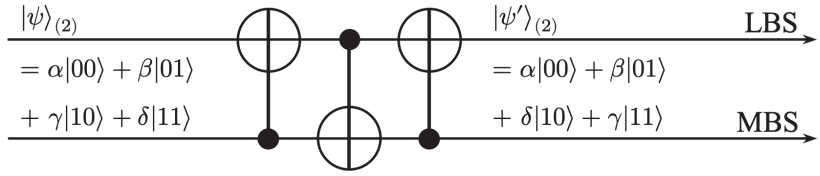
Slika 5. Dijagram kvantnog sklopa sa SWAP-vratima za stanje 2 qubita.

$$U_{\mathrm{SWAP}}\,|\psi\rangle_{(2)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \gamma \\ \beta \\ \delta \end{pmatrix}$$
$$= \alpha\,|00\rangle + \gamma\,|01\rangle + \beta\,|10\rangle + \delta\,|11\rangle = |\psi'\rangle_{(2)}\,. \tag{45}$$

Zanimljivo je spomenuti da se SWAP-vrata mogu izvesti pomoći triju CNOT-vrata (slika 6), s time da je za prva i treća vrata kontrolni qubit prvi qubit (prva i treća matrica),

a za druga vrata kontrolni qubit je drugi qubit (srednja matrica) [4].

$$U_{\text{SWAP}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{46}$$



Slika 6. Izvedba kvantnih SWAP-vrata preko triju CNOT-vrata te odgovarajući dijagram kvantnog sklopa za stanje 2 qubita.

D. Vrata faznog pomaka, Z-vrata i kontrolirana vrata faznog pomaka

Vrata faznog pomaka (fazna ili P-vrata) su kvantna vrata za jedan qubit koja pomiču relativnu fazu između dva vektora baze. Definicija je:

$$U_{\text{PS},\phi}\,|0\rangle = |0\rangle\,, \qquad U_{\text{PS},\phi}\,|1\rangle = e^{i\phi}\,|1\rangle\,. \tag{47}$$

ovdje je ϕ faza, a $e^{i\phi}$ zovemo fazni faktor. Vrata faznog pomaka nemaju nikakav utjecaj na vektor baze $|0\rangle$, dok kod vektora baze $|1\rangle$ dobivamo dodatni faktor $e^{i\phi}$ koji množi vektor $|1\rangle$. Općenito, kada ta vrata djeluju na stanje jednog qubita $|\psi\rangle_{(1)} = \alpha\,|0\rangle + \beta\,|1\rangle$, imamo

$$U_{\text{PS},\phi}\,|\psi\rangle_{(1)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha \\ e^{i\phi}\beta \end{pmatrix} = \alpha\,|0\rangle + e^{i\phi}\beta\,|1\rangle = |\psi'\rangle_{(1)}\,. \tag{48}$$

U početnom vektoru $|\psi\rangle$ koeficijenti α i β su općenito kompleksni brojevi, koji se mogu zapisati kao umnožak apsolutne vrijednosti i faznog faktora. Dakle, $\alpha = |\alpha|e^{i\theta_1}$ i $\beta = |\beta|e^{i\theta_2}$. Ovdje su $|\alpha|$ i $|\beta|$ apsolutne vrijednosti kompleksnih brojeva, θ_1 i θ_2 su faze pa je $\theta_1 - \theta_2$ je razlika faza. Vrata faznog pomaka ne mijenjaju fazu od α dok se faza od β promijeni za $\phi + \theta_2$ pa će se i relativna faza promijeniti za ϕ. Ovo objašnjava zašto ima smisla da se fazni pomak primjenjuje samo na drugi vektor baze. Ako bi se primjenio na oba vektora baze, ne bi došlo do faznog pomaka.

Primijetite da je za fazni pomak $\phi = \pi$ matrica $U_{\text{PS},\phi=\pi}$ jednaka Paulijevoj σ_z matrici. Stoga $U_{\text{PS},\phi=\pi}$ zovemo Z-vrata. Ova vrata imaju specijalno svojstvo da kada djeluju na $|+\rangle\ /\ |-\rangle$ bazu, ponašaju se kao NOT-vrata za tu bazu. Dakle, operator $U_{\text{PS},\phi=\pi}$ pro-

mijenit će $|+\rangle$ u $|-\rangle$ i obrnuto

$$U_{\mathrm{PS},\phi=\pi}\,|+\rangle = U_{\mathrm{PS},\phi=\pi}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |-\rangle\ . \tag{49}$$

Vidjeli smo da su Z-vrata zapravo NOT-vrata ako smo u bazi $|+\rangle\ /\ |-\rangle$. Stoga možemo pretpostaviti da postoje "kontrolirana-Z-vrata" koja se ponašaju kao CNOT-vrata u bazi $|+\rangle\ /\ |-\rangle$ pa za 2 qubita definiramo

$$U_{\mathrm{CPS},\phi}\,|ab\rangle = e^{i(a\cdot b)\phi}\,|ab\rangle\ . \tag{50}$$

a i b su prvi i drugi qubit baze, dok $(a\cdot b)$ označavaju klasična logička AND-vrata (and = i), što znači da su jednaka 1 samo ako su i a i b jednaki 1:

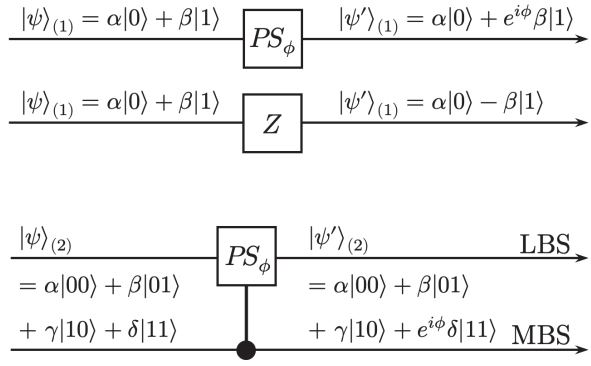
$$\begin{aligned} U_{\mathrm{CPS},\phi}\,|00\rangle &= e^{i(0\cdot 0)\phi}\,|00\rangle = |00\rangle\ , \qquad & U_{\mathrm{CPS},\phi}\,|10\rangle &= e^{i(1\cdot 0)\phi}\,|10\rangle = |10\rangle\ , \\ U_{\mathrm{CPS},\phi}\,|01\rangle &= e^{i(0\cdot 1)\phi}\,|01\rangle = |01\rangle\ , \qquad & U_{\mathrm{CPS},\phi}\,|11\rangle &= e^{i(1\cdot 1)\phi}\,|11\rangle = e^{i\phi}\,|11\rangle\ . \end{aligned} \tag{51}$$

Vidimo da samo vektor $|11\rangle$ dobiva dodatnu fazu. Ako je prvi qubit 0 ($|00\rangle$ ili $|01\rangle$), nema utjecaja na drugi qubit. Međutim, ako je prvi qubit 1, primjenjuje se fazni pomak na drugi qubit, i to samo ako je i drugi qubit jednak 1. Drugim riječima, prvi qubit se ponaša kao *kontrolni qubit*, a drugi kako *ciljani qubit*. Odatle i naziv kontrolirana vrata faznog pomaka.

Kada operator kontroliranog faznog pomaka $U_{\mathrm{CPS},\phi}$ djeluje na stanje 2 qubita $|\psi\rangle_{(2)}$, dobit ćemo fazni pomak samo kod vektora baze $|11\rangle$

$$\begin{aligned} U_{\mathrm{CPS},\phi}\,|\psi\rangle_{(2)} &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ \delta \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \\ \gamma \\ e^{i\phi}\delta \end{pmatrix} \\ &= \alpha\,|00\rangle + \beta\,|01\rangle + \gamma\,|10\rangle + e^{i\phi}\delta\,|11\rangle = |\psi'\rangle_{(2)}\,. \end{aligned} \tag{52}$$

Dijagrami sklopova za operatore faznog pomaka koje smo ovdje spominjali dani su na slici 7.



Slika 7. Sklopovi s vratima faznog pomaka. Od vrha prema dolje redom imamo P-vrata za jedan qubit, Z-vrata te kontrolirana vrata faznog pomaka za stanje 2 qubita.

Toffoli vrata su vrata za 3 qubita, a zovemo ih još i "kontrolirana-kontrolirana-NOT" vrata (CCNOT). Slično kao što CNOT-vrata djeluju na vektor baze $\mathbb{C}^4$ prostora i daju negaciju drugog qubita ako je prvi qubit jednak 1, tako i CCNOT-vrata daju negaciju trećeg qubita ako su u vektoru baze $\mathbb{C}^8$ prostora prva dva qubita jednaka 1. Definicija

$$T\,|abc\rangle \;= T\,|a\rangle \otimes |b\rangle \otimes |c\rangle \;= |a, b, (a \cdot b) \oplus c\rangle \;. \tag{53}$$

T je oznaka za Toffoli vrata, $|abc\rangle$ je vektor baze 3 qubita u $\mathbb{C}^8$ prostoru, a, b i c mogu poprimiti vrijednosti 0 i 1. Nakon djelovanja Toffoli vrata prva dva qubita su nepromijenjena. $(a \cdot b)$ je oznaka za klasičnu logičku AND-operaciju, a $\oplus$ je oznaka za klasičnu XOR-operaciju pa imamo:

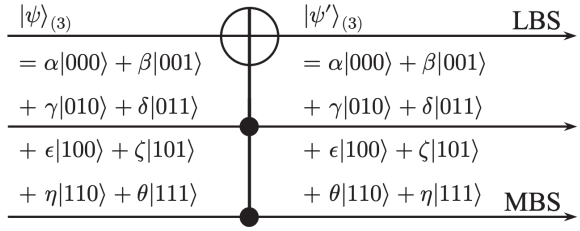
$$\begin{aligned}
T\,|000\rangle &= |0,0,(0\cdot 0)\oplus 0\rangle = |000\rangle\;, & T\,|100\rangle &= |1,0,(1\cdot 0)\oplus 0\rangle = |100\rangle\;,\\
T\,|001\rangle &= |0,0,(0\cdot 0)\oplus 1\rangle = |001\rangle\;, & T\,|101\rangle &= |1,0,(1\cdot 0)\oplus 1\rangle = |101\rangle\;,\\
T\,|010\rangle &= |0,1,(0\cdot 1)\oplus 0\rangle = |010\rangle\;, & T\,|110\rangle &= |1,1,(1\cdot 1)\oplus 0\rangle = |111\rangle\;,\\
T\,|011\rangle &= |0,1,(0\cdot 1)\oplus 1\rangle = |011\rangle\;, & T\,|111\rangle &= |1,1,(1\cdot 1)\oplus 1\rangle = |110\rangle\;.
\end{aligned} \tag{54}$$

Kada Toffoli vrata djeluju na stanje 3 qubita $|\psi\rangle_{(3)} = \alpha\,|000\rangle + \beta\,|001\rangle + \gamma\,|010\rangle + \delta\,|011\rangle + \epsilon\,|100\rangle + \zeta\,|101\rangle + \eta\,|110\rangle + \theta\,|111\rangle$, dobivamo:

$$T\,|\psi\rangle_{(3)} = \begin{pmatrix} 1&0&0&0&0&0&0&0\\ 0&1&0&0&0&0&0&0\\ 0&0&1&0&0&0&0&0\\ 0&0&0&1&0&0&0&0\\ 0&0&0&0&1&0&0&0\\ 0&0&0&0&0&1&0&0\\ 0&0&0&0&0&0&0&1\\ 0&0&0&0&0&0&1&0 \end{pmatrix} \begin{pmatrix} \alpha\\ \beta\\ \gamma\\ \delta\\ \epsilon\\ \zeta\\ \eta\\ \theta \end{pmatrix} = \begin{pmatrix} \alpha\\ \beta\\ \gamma\\ \delta\\ \epsilon\\ \zeta\\ \theta\\ \eta \end{pmatrix}$$

$$\begin{aligned}
&= \alpha\,|000\rangle + \beta\,|001\rangle + \gamma\,|010\rangle + \delta\,|011\rangle + \epsilon\,|100\rangle + \zeta\,|101\rangle + \theta\,|110\rangle + \eta\,|111\rangle\\
&= |\psi'\rangle_{(3)}\,.
\end{aligned} \tag{55}$$

Vidimo da su dva zadnja koeficijenta baze zamijenila mjesto. Slika 8 prikazuje dijagram kvantnog sklopa s Toffoli vratima za stanje 3 qubita, gdje se dva najznačajnija qubita ponašaju kao kontrolni qubitovi.



Slika 8. Sklop s Toffoli vratima, gdje zadnja dva koeficijenta zamijene mjesta.

Toffoli vrata imaju specijalno svojstvo da se ponašaju kao univerzalna vrata klasične logike. Na primjer, Toffoli vrata ponašaju se kao klasična AND-vrata kada je treći qubit jednak 0 pa onda prva dva qubita možemo shvatiti kao ulaz, a treći kao izlaz klasičnih logičkih AND-vrata:

$$T\,|ab0\rangle \;=|a,b,(a\cdot b)\oplus 0\rangle \;=|a,b,a\cdot b\rangle\;. \tag{56}$$

Slično, ako su prva dva qubita jednaka 1 i shvatimo ih kao ulazne qubitove, Toffoli vrata ponašaju se kao klasična logička NOT-vrata za treći izlazni qubit jer vrijedi $1\oplus c=\bar{c}$:

$$T\,|11c\rangle \;=|1,1,(1\cdot 1)\oplus c\rangle \;=|1,1,1\oplus c\rangle \;=|1,1,\vec{c}\rangle\;. \tag{57}$$

Kako se bilo koja klasična logika može implementirati kombinacijom AND- i NOT-vrata, slijedi da su Toffoli vrata univerzalna vrata za klasičnu logiku.

Primijetite da ako u kvantni registar spremimo samo jedan vektor baze, onda se ovdje spomenuta kvantna vrata ponašaju analogno klasičnim logičkim vratima. Međutim, postoje i kvantna vrata koja nemaju klasični analogon. Ovdje ćemo ukratko spomenuti samo jedna takva vrata, *Walsh-Hadamardova vrata*. Ta vrata se obično koriste kao početna vrata mnogih kvantnih algoritama. Prvo se u kvantni registar n-qubita pohranjuje nul-vektor baze $|0\rangle_{(n)}=|00\cdots 0\rangle$ (imamo n nula). Nakon što Walsh-Hadamardova vrata djeluju na nul-vektor baze, dobit ćemo superpoziciju svih vektora baze s jednakim koeficijentima. Stoga ta vrata služe za inicijalizaciju kvantnog registra:

$$\begin{aligned} H^{\otimes n}\,|0\rangle_{(n)} &= \frac{1}{\sqrt{2^n}}\Big(\,|00\cdots 00\rangle\,+|00\cdots 01\rangle\,+|00\cdots 10\rangle\,+|00\cdots 11\rangle \\ &\quad +\cdots+|11\cdots 10\rangle\,+|11\cdots 11\rangle\,\Big) \\ &= \frac{1}{\sqrt{2^n}}\Big(\,|0\rangle\,+|1\rangle\,+|2\rangle\,+|3\rangle\,+\cdots+|2^n-2\rangle\,+|2^n-1\rangle\,\Big) \\ &= \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2n-1}|x\rangle\;. \end{aligned} \tag{58}$$

Vidimo da smo pomoću Walsh-Hadamardovih vrata u kvantni registar pohranili sve brojeve od 0 do 2^n-1, i to s jednakom amplitudom (svi imaju jednake koeficijente). Računanje na kvantnom računalu bilo bi zatim djelovanje kombinacije različitih kvantnih vrata (unitarnih operatora) na tako inicijalizirano stanje, sve dok se ne dođe do valne funkcije čije koeficijente želimo očitati mjerenjem.

Zaključak

Samu ideju koja stoji iza kvantnog računanja, a proizlazi iz zakona kvantne mehanike, vrlo je lako razumijeti uz poznavanje osnova linearne algebre, što smo i pokušali dočarati ovim člankom. Za produbljivanje znanja preporučujemo udžbenik *Introduction to Quantum Computing* autora H. Y. Wong-a [2] koji pokriva i složenije teme iz kvantnog računarstva.

Prednost kvantnih računala u odnosu na klasična proizlazi iz činjenice da je kvantni algoritam skup kvantnih vrata koja su unitarna pa ako na određeno stanje u nekoj fazi kvantnog algoritma djelujemo inverznim operatorima, možemo se vratiti u inicijalno stanje, što kod klasičnih logičkih vrata ne možemo. Isto tako, u n-qubitni kvantni registar možemo pohraniti sve brojeve od 0 do 2^n-1 te istovremeno vršiti operacije na svim brojevima,

dok kod klasičnog registra možemo istovremeno pohraniti samo jedan broj. Mane leže u činjenici da je još uvijek tehnički nemoguće napraviti kvantna računala s velikim brojem n-qubitova koja će **dugotrajno** održavati superpoziciju tijekom izvođenja kvantnog algoritma. Iako danas postoje kvantna računala s preko 1000 qubitova, veliki dio qubitova se mora rezervirati za korekciju grešaka pa trenutno uistinu nema neke velike koristi od takvih uređaja. Stoga danas velik dio istraživanja u području kvantnog računarstva otpada na rješavanje različitih tehničkih problema. Što će budućnost donijeti – vidjet ćemo.

Literatura

[1] M. Brooks, *Quantum computers: what are they good for?*, Nature 617, S1–S3, 2023., 10.1038/d41586-023-01692-9

[2] H. Y. Wong, *Introduction to Quantum Computing*, Springer Cham, 2023., 10.1007/978-3-031-36985-8

[3] W. Gerlach, O. Stern, *Der experimentelle Nachweis der Richtungsquantelung im Magnetfeld*, Z. Physik 9, 349–352, 1922., 0.1007/BF01326983

[4] R. P. Feynman, *Quantum Mechanical Computers*, Found. Phys. 16, 507–531, 1986., 10.1007/BF01886518