Kvantno računanje

Matija Kazalicki

Sadržaj

1 Uvod

Krajem listopada 2019. u popularnim medijima odjeknula je vijest da je Googleovo kvantno računalo Sycamore (na hrvatskom javor) demonstriralo kvantnu premoć – za 200 sekundi izračunalo je nešto za što bi

najboljem klasičnom superračunalu trebalo 10 000 godina [ea19].[1] Iako program koji je Googlovo računalo izvršilo ne radi ništa korisno ni zanimljivo – uzorkuje slučajnu vjerojatnosnu distribuciju – ipak možemo reći da je to bio važan trenutak u četrdesetogodišnjoj povijesti kvantnog računarstva jer je svima postalo jasno da taj teorijski koncept funkcionira i da se u (ne tako skoroj) budućnosti možemo nadati velikim stvarima.

Iako se ideja o računanju baziranom na zakonima kvantne mehanike pojavila još u sedamdesetima, tek desetljeće kasnije, popularizirana fizičarima kao što su Benioff, Feynman i Deutsch, počinje se ozbiljnije proučavati. Tako je, na primjer, Deutsch 1985., u analogiji s Turingovim strojem definirao univerzalno kvantno računalo i time formalizirao koncept kvantnog računanja. Zanimalo ga je (u analogiji s jakom Church-Turingovom tezom) može li takav "uređaj" efikasno simulirati proizvoljan fizikalni sustav. To pitanje do danas je ostalo otvoreno. Osim toga, zanimalo ga je i mogu li kvantna računala efikasno riješiti neki problem za koji ne postoji efikasno rješenje pomoću vjerojatnosnih Turingovih strojeva (te tako oboriti jaku Church-Turingovu tezu). On sam konstruirao je neke (ne baš praktične) algoritme koji sugeriraju da bi to moglo biti tako, no pravo iznenađenje dogodilo se 1994. kada je Peter Shor na sveopće zaprepaštenje pokazao da se dva problema na kojima počiva sigurnost moderne kriptografije mogu efikasno riješiti na kvantnom računalu. To su problem faktorizacije prirodnih brojeva i problem diskretnog logaritma. Danas je općeprihvaćeno da se ti problemi ne mogu efikasno riješiti na klasičnom računalu, ali to nije dokazano.

No što je to kvantno računalo?

Najkraće rečeno, kvantno je računalo kvantno-mehanički sustav koji efikasno uzorkuje vjerojatnosnu distribuciju koja je opisana programom koji računalo izvodi. Slikovito rečeno, zamislimo da želimo simulirati milijun bacanja neke nesimetrične igraće kocke s bilijardu stranica. Na klasičnim računalima to bi bilo vrlo neefikasno jer bi nam već i za sam opis kocke (odnosno vjerojatnosti s kojima se pojedina stranica

[1] Nekoliko dana nakon toga Googleovo "slavlje" malo je poremetio njihov najveći takmac na tom polju, IBM, koji je ustvrdio da bi njihovom (klasičnom) superračunalu Summit za tu zadaću trebalo dva i pol dana [PG19].

kod bacanja kocke pojavljuje) trebalo oko petabajt memorije, što je jedva dostupno na najvećim svjetskim superračunalima. S druge strane, kvantno računalo, uređaj baziran na čudesnim zakonima kvantne mehanike, takvu kocku može simulirati s eksponencijalno manjih 50-ak qubita. No dobro, zašto bi netko želio simulirati bacanje kocke? Jedan odgovor je zato što se pomoću kvantnih algoritama mogu konstruirati "kocke" čije stranice odgovaraju mogućim rješenjima nekog teškog problema (kao što je npr. problem faktorizacije velikih brojeva – problem na čijoj se težini temelji moderna kriptografija). Ono što je najvažnije jest da pritom stranica koja odgovara točnom rješenju (a priori se ne zna koja je to stranica) ima veliku vjerojatnost pojavljivanja pri bacanju. Tada jednostavnim bacanjem kocke (simuliranjem) možemo vrlo brzo saznati koje je to rješenje.

Cilj je ovih predavanja izložiti matematički model kvantnog računanja (koji je opisan jezikom linearne algebre), objasniti vezu tog modela i kvantne mehanike i nakon toga opisati neke kvantne algoritme. Studenti te algoritme mogu implementirati na IBM-ovim kvantnim računalima koji se nalaze na oblaku (IBM Q Experience).

2 Osnovni pojmovi kvantnog računanja

Osnovne pojmove uvest ćemo koristeći analogiju s klasičnim računarstvom.

2.1 Kvantni bit

Kvantni bit ili *qubit* osnovna je jedinica informacije u kvantnom računarstvu. Za razliku od klasičnog bita koji se može nalaziti u jednom od dva stanja – 0 ili 1 – stanje qubita opisuje se *vektorom stanja* – vektorom norme 1 u dvodimenzionalnom unitarnom vektorskom prostoru $(V, \langle \cdot \,|\, \cdot \rangle)$ nad poljem kompleksnih brojeva s ortonormiranom bazom čiji se elementi tradicionalno označavaju s $|0\rangle$ i $|1\rangle$. Prostor V naziva se *prostor stanja*. Za zapisivanje vektora stanja (i funkcionala koji djeluju na njih) upotrebljavamo standardnu Diracovu (ili bra-ket) notaciju. Vektore ćemo označavati ket simbolima, $|\Psi\rangle$, dok ćemo bra simbolom

$\langle\Phi|$ označavati funkcional, pridružen vektoru $|\Phi\rangle$, koji djeluje na vektor $|\Psi\rangle$ preko skalarnog produkta, tj. $\langle\Phi|\,|\Psi\rangle = \langle\Phi|\Psi\rangle$.[2] Ako je U operator na V, onda s $\langle\Phi|U|\Psi\rangle$ označavamo djelovanje funkcionala $\langle\Psi|$ na vektor $U\,|\Psi\rangle$. Osnovne informacije o unitarnim vektorskim prostorima možete pronaći u Dodatku A.

Primjer. Jedan vektor stanja prostora V je

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle\,.$$

Uočimo da je $\langle\Psi|\Psi\rangle = \frac{1}{2} + \frac{1}{2} = 1$.

Ako na klasičnom računalu pristupamo nekom bitu (na primjer u stanju 1) pohranjenom na tvrdom disku, uvijek ćemo očitati (izmjeriti) 1 (osim ako je slučajno neka kozmička zraka baš udarila u taj dio memorije i promijenila ga) – dakle klasično zapravo nema smisla govoriti o mjerenju bitova jer se to što izmjerimo uvijek poklapa sa stanjem.

U kvantnom svijetu to nije tako. Neka je $\{|\Phi_0\rangle\,, |\Phi_1\rangle\}$ proizvoljna ortonormirana baza prostora V. Ako mjerimo qubit opisan vektorom stanja $|\Psi\rangle$ u toj bazi, kao rezultat mjerenja dobit ćemo $|\Phi_0\rangle$ s vjerojatnošću $|\langle\Psi|\Phi_0\rangle|^2$ i $|\Phi_1\rangle$ s vjerojatnošću $|\langle\Psi|\Phi_1\rangle|^2$. Ako $|\Psi\rangle$ iz primjera izmjerimo u bazi $\{|0\rangle\,, |1\rangle\}$ (gotovo uvijek ćemo mjeriti u toj bazi tako da ako kod mjerenja ne specificiramo bazu u kojoj mjerimo, na tu bazu mislimo), dobit ćemo $|0\rangle$ s vjerojatnošću $\frac{1}{2}$ te $|1\rangle$ s vjerojatnošću $\frac{1}{2}$. Primijetimo da isto vrijedi i za stanje $\left|\tilde{\Psi}\right\rangle = \frac{i}{\sqrt{2}}\,|0\rangle + \frac{1}{\sqrt{2}}\,|1\rangle$ iako su ta dva stanja različita.

Sada je jasno zašto zahtijevamo da je vektor stanja vektor norme 1 – zato što zbroj vjerojatnosti mora biti jednak jedan, tj. ako je $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, mora vrijediti da je $|\alpha|^2 + |\beta|^2 = 1$.

Važno je naglasiti da se nakon mjerenja qubit nalazi u stanju koje smo izmjerili. Slikovito se još kaže da mjerenje uništava kvantno stanje.

Fizikalno se qubit može implementirati na puno načina. Npr. možemo zamisliti da je qubit elektron čiji spin mjerimo duž neke osi (ovisno o

[2]Prema Rieszovom teoremu svaki funkcional koji djeluje na prostoru stanja je oblika $\langle\Phi|$ za neki vektor stanja $|\Phi\rangle$.

tome u kojem "smjeru" se elektron zakreće u magnetskom polju kažemo da je spin prema gore ili prema dolje).

2.2 Kvantni bitovi i kvantno sprezanje

S jednim qubitom ne možemo puno toga izračunati – kako onda opisujemo veći broj qubita?

Stanje sustava od n qubita opisuje se normiranim vektorom u tenzorskom produktu vektorskih prostora $V^{\otimes n} = V \otimes V \otimes \cdots \otimes V$. Bez ulaženja u preveliku teoriju, opisat ćemo osnovna svojstva tog vektorskog prostora koja će nam omogućiti da s njime računamo.

Prostor stanja $V^{\otimes n}$ unitaran je vektorski prostor dimenzije 2^n s istaknutom ortonormiranom bazom

$$\{|00\cdots00\rangle, |00\cdots01\rangle, |00\cdots10\rangle, \ldots, |11\cdots11\rangle\}.$$

Ponekad, na primjer za $n = 3$, umjesto $|010\rangle$ možemo pisati $|0\rangle|1\rangle|0\rangle$ ili još matematički najpravilnije $|0\rangle \otimes |1\rangle \otimes |0\rangle$. Kako su elementi te baze indeksirani binomnim razvojem brojeva od 0 do $2^n - 1$, nekada elemente te baze označavamo i ovako: $\{|0\rangle, |1\rangle, \ldots, |2^n - 1\rangle\}$.

Ono što razlikuje tenzorski produkt od ostalih unitarnih vektorskih dimenzije 2^n jest operacija $\otimes$ – tenzorsko množenje. Ta operacija definirana je multilinearnim preslikavanjem $V \times V \times \cdots \times V \to V^{\otimes n}$ koje uređenu n-torku vektora $(|i_1\rangle, |i_2\rangle, \ldots, |i_n\rangle)$ preslikava u $|i_1 i_2 \ldots i_n\rangle$, gdje su $i_1, i_2, \ldots, i_n$ proizvoljni elementi skupa $\{0, 1\}$.

Ako imamo n qubita s vektorima stanja $|\Psi_1\rangle, |\Psi_2\rangle, \ldots, |\Psi_n\rangle$, onda cijeli taj sustav opisujemo vektorom $|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes \ldots \otimes |\Psi_n\rangle \in V^{\otimes n}$.

Na primjer, ako je $\Psi_1 = \alpha|0\rangle + \beta|1\rangle$ i $\Psi_2 = \gamma|0\rangle + \delta|1\rangle$, onda je

$$|\Psi_1\rangle \otimes |\Psi_2\rangle = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle.$$

Uočimo da se ne mogu svi vektori iz $V^{\otimes n}$ "faktorizirati". Stanje $\frac{1}{\sqrt{34}}(|00\rangle + 2|01\rangle + 2|10\rangle + 5|11\rangle)$ jedan je takav primjer. U tom slučaju kažemo da su qubiti koje to stanje opisuje *kvantno spregnuti* (eng. quantum entanglement). To nadalje znači da mjereći stanje jednog qubita

"mijenjamo" stanja drugih qubita – qubiti u tom stanju nisu nezavisni. Naravno, kod običnih bitova taj fenomen ne postoji. Takva spregnuta stanja osobito je teško kvalitetno implementirati (problem je što se u interakciji s okolinom brzo "raspadaju") i to je razlog zašto danas najbolja kvantna računala raspolažu s manje od sto qubita.

Objasnimo još mjerenja u sustavu s n qubita. Radi jednostavnosti pretpostavimo da je $n = 2$ i da Alice i Bob posjeduju svatko po jedan qubit (npr. elektron kojem mjere spin duž neke osi) čije je stanje opisano vektorom

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

gdje su $\alpha_{ij} \in \mathbb{C}$ takvi da je $|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1$. Ako Alice mjeri svoj (recimo prvi) qubit, dobit će rezultat $|0\rangle$ s vjerojatnošću $|\alpha_{00}|^2 + |\alpha_{01}|^2$ te rezultat $|1\rangle$ s vjerojatnošću $|\alpha_{10}|^2 + |\alpha_{11}|^2$. U prvom slučaju, tj. ako je Alice izmjerila $|0\rangle$, sustav prelazi u stanje $\frac{\alpha_{00}|00\rangle+\alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2+|\alpha_{01}|^2}}$, dok u drugom slučaju stanje prelazi u $\frac{\alpha_{10}|10\rangle+\alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2+|\alpha_{11}|^2}}$.

Za vježbu, po analogiji, sami formulirajte pravilo mjerenja u sustavu od n qubita.

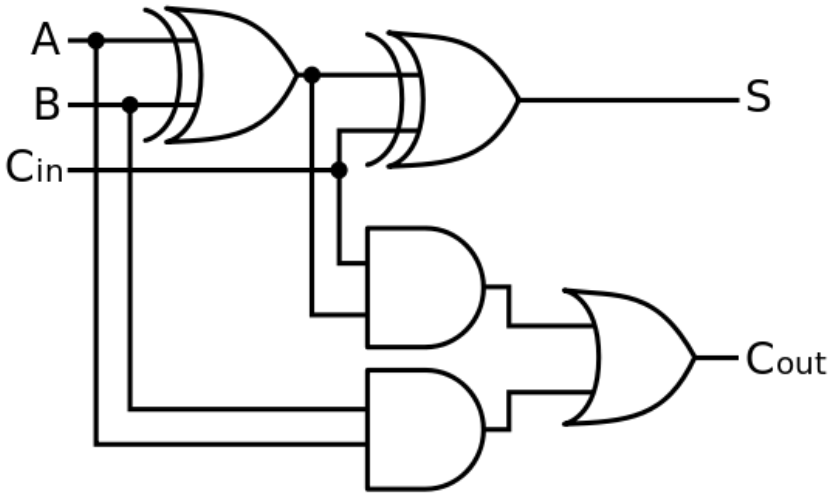
Primjer (EPR paradoks). Promotrimo takozvano Bellovo stanje:

$$|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

Možemo opet zamisliti Alice i Boba na različitim krajevima svijeta koji su u posjedu tih qubita (Alice može pristupiti prvom, a Bob drugom qubitu). Ako Alice mjeri svoj qubit, dobit će $|0\rangle$ s vjerojatnošću $1/2$ i u tom slučaju sustav prelazi u stanje $|00\rangle$. Ako sada Bob izmjeri svoj qubit dobit će $|0\rangle$ s vjerojatnošću 1! To je malo zbunjujuće, je li došlo do prijenosa informacije brzinom većom od brzine svjetlosti? Taj paradoks zbunjivao je i poznate fizičare (EPR = Einstein, Podolsky i Rosen).

2.3 Kvantna vrata

Svi programi koji se izvršavaju na klasičnim računalima mogu se opisati pomoću logičkih krugova koji se sastoje od logičkih vrata (AND, OR, XOR, NOT,...) koja djeluju na bitove. (To gotovo nikada ne radimo jer bi tako naš kod bio vrlo nepregledan.) Na primjer, na Slici 1 nalazi se sklop koji računa zbroj dva jednobitna broja.



Slika 1: Zbrajalo

Izvor: Cburnett, CC BY-SA 3.0, via Wikimedia Commons

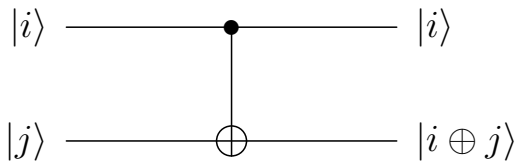
Kao i u klasičnom računarstvu, programi koji se izvršavaju na kvantnim računalima mogu se opisati preko kvantnih krugova u kojima kvantna vrata djeluju na qubite.

Što su to kvantna vrata? Općenito, kvantna vrata proizvoljni su unitarni operatori na prostoru stanja (prisjetimo se da unitarni operatori čuvaju normu vektora na koji djeluju pa tako preslikavaju vektor stanja u vektor stanja). Slično kao u klasičnom slučaju, istaknut ćemo mali broj kvantnih vrata pomoću kojih možemo "simulirati" proizvoljan unitaran operator.

Krenimo s vratima koja djeluju na jedan qubit.

- NOT ili X vrata: $X|0\rangle = |1\rangle$, $X|1\rangle = |0\rangle$, tj. $X(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$. Matrično, $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.
- Z vrata: $Z|0\rangle = |0\rangle$, $Z|1\rangle = -|1\rangle$. Matrično, $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.
- Hadamardova vrata H: $H|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $H|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Matrično, $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. Uočimo da je $H^2 = I$.

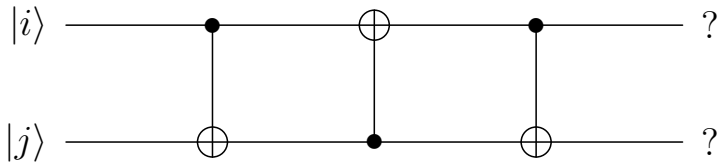
Od vrata koja djeluju na dva qubita trebat će nam kontrolirana NOT ili CNOT vrata. Ona djeluju na dva qubita, kontrolni qubit $|i\rangle$ i qubit $|j\rangle$. Kontrolni qubit se ne mijenja, dok se na drugi qubit primjenjuju NOT ili X vrata ako je kontrolni qubit jednak $|1\rangle$, inače se ništa ne događa. Ako sa $\oplus$ označimo operaciju XOR (odnosno zbrajanje modulo dva), onda CNOT vrata opisujemo sljedećim dijagramom.



Slika 2: CNOT vrata

- CNOT vrata: $|00\rangle \mapsto |00\rangle, |01\rangle \mapsto |01\rangle, |10\rangle \mapsto |11\rangle, |11\rangle \mapsto |10\rangle$.

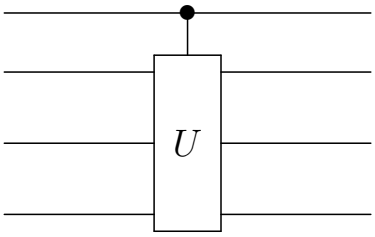
Zadatak 2.1. Što radi ovaj program?



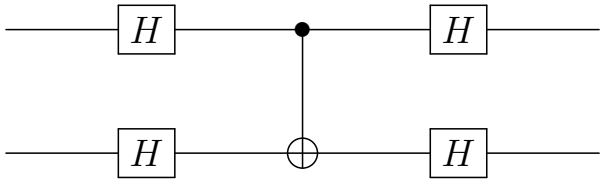
Neka su U bilo koja vrata (unitaran operator). Na sličan način možemo definirati kontrolirana U ili CU vrata (vidi Sliku 3).

Zadatak 2.2. Simulirajte kontrolirana Z vrata pomoću CNOT i Hadamardovih vrata.

Zadatak 2.3. Što radi ovaj program?



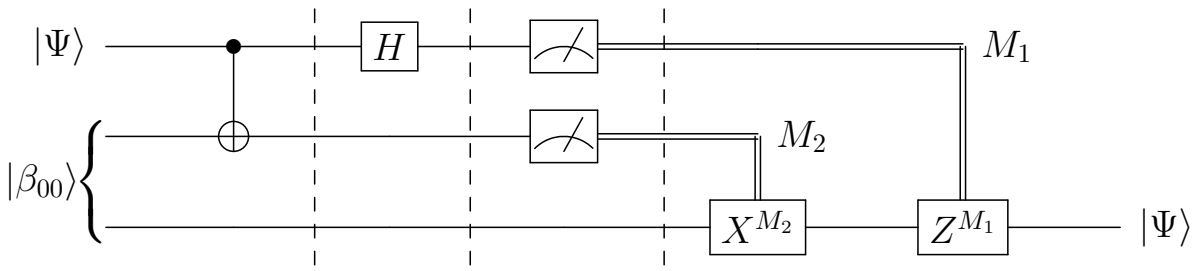
Slika 3: CU vrata



2.4 Primjer – Kvantna teleportacija

Pretpostavimo da Alice i Bob dijele Bellovo stanje $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ – Alice je u posjedu prvog qubita, a Bob drugog. Alice želi prenijeti (teleportirati) qubit $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ Bobu. Problem je što ni sama ne zna koeficijente α i β (ima samo pristup qubitu u stanju $|\Psi\rangle$), a budući da je Bob na Marsu taj qubit ne može ni fizički njemu poslati. Na raspolaganju još imaju klasični komunikacijski kanal (npr. Alice može telefonirati Bobu). Je li to moguće izvesti?

Iako se intuitivno čini da je to nemoguće, sljedeći dijagram opisuje protokol koji omogućava kvantnu teleportaciju (Alice ima pristup qubitu $|\Psi\rangle$).



Slika 4: Kvantna teleportacija

Brojevi M_1 i M_2 iz skupa $\{0, 1\}$ označavaju ishode mjerenja  prva dva qubita, koji se onda klasičnim kanalom (koji se označava dvostrukom crtom) komuniciraju Bobu. Operatori X^{M_2} i Z^{M_1} redom su potencije operatora X i Z.

Sada ćemo ovaj algoritam analizirati korak po korak. Izračunat ćemo međustanja u kojima se nalazi ovaj sustav od tri qubita na svakoj od barijera . Početno stanje je jednako

$$\begin{aligned}|\Psi_0\rangle = |\Psi\rangle \otimes |\beta_{00}\rangle &= \frac{1}{\sqrt{2}} (\alpha |0\rangle + \beta |1\rangle) \otimes (|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|00\rangle + |11\rangle)] .\end{aligned}$$

Nakon primjene CNOT vrata na prvoj barijeri dobivamo stanje

$$|\Psi_1\rangle = \frac{1}{\sqrt{2}} [\alpha |0\rangle (|00\rangle + |11\rangle) + \beta |1\rangle (|10\rangle + |01\rangle)] .$$

Primjenom Hadamardovih vrata na prvi qubit na drugoj barijeri dobivamo stanje

$$\begin{aligned}|\Psi_2\rangle &= \frac{1}{2} [\alpha(|0\rangle + |1\rangle)(|00\rangle + |11\rangle) + \beta(|0\rangle - |1\rangle)(|10\rangle + |01\rangle)] \\ &= \frac{1}{2}[|00\rangle (\alpha |0\rangle + \beta |1\rangle) + |01\rangle (\alpha |1\rangle + \beta |0\rangle) + \\ &\quad + |10\rangle (\alpha |0\rangle - \beta |1\rangle) + |11\rangle (\alpha |1\rangle - \beta |0\rangle)].\end{aligned}$$

Primijetimo da smo u drugoj jednakosti promijenili način označavanja qubita (npr. $|0\rangle |01\rangle \mapsto |00\rangle |1\rangle$) kako bismo naglasili da prva dva qubita pripadaju Alice. Ako Alice sada izmjeri svoje qubite (označimo rezultate mjerenja s M_1 i M_2), ovisno o tome što je izmjerila stanje Bobovog qubita $|\Psi_B\rangle$ bit će sljedeće:

$$\begin{aligned}|M_1 M_2\rangle = |00\rangle &\mapsto |\Psi_B\rangle = \alpha |0\rangle + \beta |1\rangle \\ |M_1 M_2\rangle = |01\rangle &\mapsto |\Psi_B\rangle = \alpha |1\rangle + \beta |0\rangle \\ |M_1 M_2\rangle = |10\rangle &\mapsto |\Psi_B\rangle = \alpha |0\rangle - \beta |1\rangle \\ |M_1 M_2\rangle = |11\rangle &\mapsto |\Psi_B\rangle = \alpha |1\rangle - \beta |0\rangle ,\end{aligned}$$

dok će stanje cijelog sustava biti jednako $|\Psi_3\rangle = |M_1 M_2\rangle\,|\Psi_B\rangle$.

Nakon što je izmjerila svoje qubite, Alice telefonira Bobu rezultate svog mjerenja, bitove M_1 i M_2. Kad je primio tu informaciju, Bob na svoj qubit primjenjuje prvo vrata X^{M_2} (odnosno ako je $M_2 = 1$, primijeni vrata X, inače ništa ne napravi), a onda vrata Z^{M_1}. Tvrdimo da se Bobov qubit na kraju nalazi u stanju $|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$.

Za dokaz bi trebalo provjeriti sva četiri slučaja. Pretpostavimo da je Alice izmjerila $(M_1, M_2) = (0, 1)$. Tada se Bobov qubit nalazi u stanju $|\Psi_B\rangle = \alpha\,|1\rangle + \beta\,|0\rangle$ pa ako na njega djelujemo X vratima, dobit ćemo stanje $|\Psi\rangle$. Preostali slučajevi dokazuju se na sličan način.

Nekoliko komentara za kraj. Uočimo da je Alicina kopija stanja $|\Psi\rangle$ uništena u ovom procesu (stanje prvog qubita nakon mjerenja je $|M_1\rangle$). To nije slučajno, nije teško dokazati da se kvantna informacija ne može kopirati. Također, budući da je Alice klasičnim kanalom javila rezultate svog mjerenja, kod teleportacije nije došlo do prijenosa informacije brzinom većom od brzine svjetlosti. Bez rezultata Alicinog mjerenja Bob ne zna u kojem se od četiri moguća stanja nalazi njegov qubit i zato iz njega ne može "izvući" nikakvu klasičnu informaciju.

Teleportacija nije samo teorijski koncept: kineski su znanstvenici 2017. godine uspjeli teleportirati fotone sa stanice Ngari u Tibetu do satelita Micius koji kruži u niskoj orbiti oko Zemlje. Malo više o tome možete pročitati u ovom popularnom članku:

`https://www.technologyreview.com/2017/07/10/150547/first-object-teleported-from-earth-to-orbit/`.

2.5 Primjer – Deutsch-Jozsa algoritam

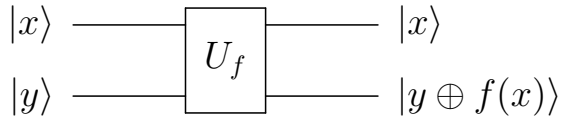
Pretpostavimo da nam je dana funkcija $f : \{0,1\}^n \to \{0,1\}$ za koju se zna da je ili konstanta ili balansirana (tj. $\#f^{-1}(\{0\}) = \#f^{-1}(\{1\}) = 2^{n-1}$, gdje $\#S$ označava broj elemenata skupa S). Problem je koristeći što manje poziva funkcije f odrediti je li funkcija konstantna ili balansirana. Klasično, u najgorem slučaju potreban nam je $2^{n-1} + 1$ poziv funkcije f.

Deutsch-Jozsa algoritam deterministički je kvantni algoritam (deter-

ministički ovdje znači da u teoriji uvijek daje točan rezultat za razliku od vjerojatnosnog, koji daje točan rezultat s nekom vjerojatnošću) koji rješava ovaj problem sa samo jednim pozivom funkcije f. To je bio jedan od prvih algoritama koji je pokazao da kvantni algoritmi mogu neke probleme riješiti eksponencijalno brže od klasičnih determinističkih algoritama.

Radi jednostavnosti, opisat ćemo samo specijalan slučaj algoritma kad je $n = 1$. Opći slučaj ostavljamo zainteresiranom čitatelju za domaću zadaću.

Pretpostavimo da su nam dana kvantna vrata U_f (potprogram) koja proizvoljan element baze $|x\rangle\,|y\rangle$ preslikavaju u $|x\rangle\,|y \oplus f(x)\rangle$ (ovdje je $\oplus$ zbrajanje mod 2). Ova vrata još se nazivaju kvantna proročica (eng. quantum oracle) ili crna kutija.



Slika 5: Kvantna proročica

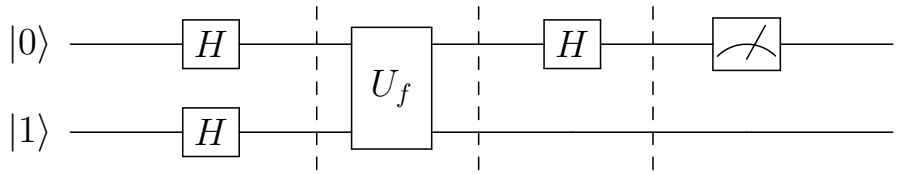
Primijetimo da je U_f uistinu unitaran operator pa predstavlja neka kvantna vrata. Inače, nismo mogli definirati funkciju na samo jednom qubitu, npr. preko pravila $|x\rangle \mapsto |f(x)\rangle$, jer f ne mora biti injekcija, dok sva naša vrata moraju biti unitarni operatori pa specijalno moraju biti invertibilna.

Pokazat ćemo da problem možemo riješiti sa samo jednim pozivom proročice U_f (za razliku od dva poziva funkcije f u klasičnom slučaju) tako što ćemo izračunati $f(0) \oplus f(1)$ izvršavanjem sljedećeg programa.

Za analizu će nam trebati sljedeća lema (koja se lako generalizira i za slučaj kad je $n > 1$).

Lema 2.4. *Za $x \in \{0, 1\}$ vrijedi*

$$U_f\left(|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = (-1)^{f(x)}\,|x\rangle \frac{|0\rangle - |1\rangle}{\sqrt{2}}.$$



Slika 6: Deutschov algoritam

Dokaz. Računamo

$$\begin{aligned} U_f\left(\frac{|x\rangle|0\rangle}{\sqrt{2}} - \frac{|x\rangle|1\rangle}{\sqrt{2}}\right) &= \frac{1}{\sqrt{2}}|x\rangle|f(x)\oplus 0\rangle - \frac{1}{\sqrt{2}}|x\rangle|f(x)\oplus 1\rangle \\ &= \frac{1}{\sqrt{2}}|x\rangle\left(|f(x)\rangle - |f(x)\oplus 1\rangle\right), \end{aligned}$$

iz čega tvrdnja direktno slijedi. □

Računamo međustanja nakon svake barijere.

- Početno stanje je $|\Psi_0\rangle = |01\rangle$.
- Nakon primjene Hadamardovih operatora sustav prelazi u stanje $|\Psi_1\rangle = \left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$.
- Primjenom vrata U_f na stanje $|\Psi_1\rangle$ dobivamo stanje

$$\begin{aligned} |\Psi_2\rangle = U_f|\Psi_1\rangle &= U_f\left(\frac{1}{\sqrt{2}}|0\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) + U_f\left(\frac{1}{\sqrt{2}}|1\rangle\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right) \\ &= \frac{1}{2}\left((-1)^{f(0)}|0\rangle\left(|0\rangle-|1\rangle\right) + (-1)^{f(1)}|1\rangle\left(|0\rangle-|1\rangle\right)\right) \\ &= \begin{cases} \pm\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{ako je } f(0) = f(1) \\ \pm\frac{|0\rangle-|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{ako je } f(0) \neq f(1). \end{cases} \end{aligned}$$

- Primjenom Hadamardovog operatora na prvi qubit (sjetimo se $H^{-1} = H$) dobivamo

$$|\Psi_3\rangle = \begin{cases} \pm|0\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{ako je } f(0) = f(1) \\ \pm|1\rangle \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} & \text{ako je } f(0) \neq f(1). \end{cases}$$

Mjerenjem prvog qubita dobit ćemo $|0\rangle$ ako je $f(0) = f(1)$, odnosno $|1\rangle$ ako je $f(0) \neq f(1)$, tj. jednim mjerenjem dobivamo $|f(0) \oplus f(1)\rangle$ i utvrđujemo je li funkcija f balansirana ili konstantna.

Zadatak 2.5. Poopćite ovaj algoritam tako da radi za proizvoljan n.

3 Zadaci

3.1 Zadaci

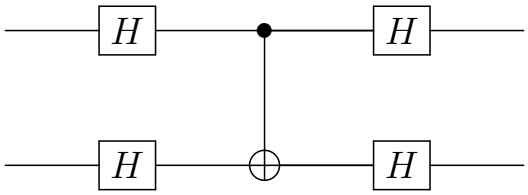
Na internetu je slobodno dostupan velik broj skripti sa zadacima iz kolegija vezanih uz kvantno računanje [Aar17, Pre13, Vaz04]. Ovdje navodimo neke zadatke koji mogu poslužiti studentima za vježbu.

1. Jesu li dva qubita opisana stanjem

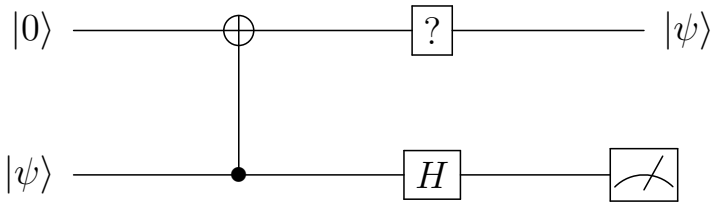
$$|\Psi\rangle = \frac{1}{\sqrt{34}} \left(|00\rangle + 2\,|01\rangle + 2\,|10\rangle + 5\,|11\rangle\right)$$

   kvantno spregnuta?

2. Što radi ovaj program?



3. Promotrite sljedeći kvantni krug. Ovisno o rezultatu mjerenja dru-



   gog qubita $M \in \{|0\rangle, |1\rangle\}$, što trebate napraviti s prvim qubitom da biste dobili vektor $|\psi\rangle$?

4. Neka su V i W konačno dimenzionalni vektorski prostori nad $\mathbb{C}$, te $A \in L(V)$ i $B \in L(W)$ linearni operatori definirani na njima. Dokažite da postoji jedinstven linearan operator $A \otimes B \in L(V \otimes W)$ takav da za sve $v \in V$ i $w \in W$ vrijedi $(A \otimes B)(v \otimes w) = A(v) \otimes B(w)$. Dokažite da je $Tr(A \otimes B) = Tr(A)Tr(B)$, gdje $Tr(C)$ označava trag linearnog operatora C.

5. Konstruirajte kvantni krug (koji prima dva qubita), a sastoji se samo od vrata koja djeluju na jedan qubit i CNOT vrata te preslikava $|00\rangle \mapsto \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ i $|11\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

6. Simulirajte kontrolirana Z vrata pomoću CNOT i Hadamardovih vrata.

7. Konstruirajte kvantni krug, koristeći samo CNOT i Toffoli vrata, koji zbraja dva dvobitna broja x i y modulo 4, tj. koji implementira transformaciju $|x, y\rangle \mapsto |x, x + y \bmod 4\rangle$ (možete koristiti dodatne qubite).

8. Pretpostavimo da Alice zna dva bita x i y i da Bobu želi poslati jedan nespregnuti qubit tako da Bob iz toga qubita s vjerojatnošću od $\cos^2(\pi/8) \approx 85\%$ može saznati vrijednost jednog bita x ili y po njegovom izboru. Osmislite protokol koji će riješiti ovaj problem. Hint: možete korisiti sljedeća stanja

$$\cos(\pi/8)|0\rangle + \sin(\pi/8)|1\rangle, \quad \sin(\pi/8)|0\rangle + \cos(\pi/8)|1\rangle,$$
$$\cos(\pi/8)|0\rangle - \sin(\pi/8)|1\rangle, \quad \sin(\pi/8)|0\rangle - \cos(\pi/8)|1\rangle.$$

9. Alice i Bob igraju sljedeću igru. Alice dobije bit x, a Bob bit y (x i y su slučajno odabrani i nezavisni). Oni trebaju, bez komuniciranja, generirati dva bita a i b tako da je $a + b \equiv xy \pmod 2$. Klasično optimalna strategija daje vjerojatnost uspjeha od 75%. No pretpostavimo da Alice i Bob dijele spregnuto stanje

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

(Alice ima pristup jednom qubitu dok Bob ima pristup drugom qubitu). Osmislite strategiju koja će za Alice i Boba biti pobjednička s vjerojatnošću $\cos^2 \frac{\pi}{8}$.

10. Tri igrača, Alice, Bob i Charlie, igraju sljedeću igru. Dana su im tri bita, redom x, y i z, takva da je $x + y + z \equiv 0 \pmod 2$. Oni trebaju, bez dogovaranja i komuniciranja, generirati tri bita a, b i c tako da vrijedi $a+b+c \equiv OR(x, y, z) \pmod 2$. Drugim riječima, parnost zbroja bitova koje generiraju treba biti neparna ako i samo ako je barem jedan od bitova x, y i z različit od nule.

    a) Dokažite da u klasičnom svijetu ne postoji pobjednička strategija (koja uvijek radi).

    b) Pretpostavimo da svaki od igrača na raspolaganju ima qubit takav da je (spregnuto) stanje sva tri qubita jednako:
    $$\frac{|000\rangle - |011\rangle - |101\rangle - |110\rangle}{2}.$$
    Pokažite da sada Alice, Bob i Charlie imaju pobjedničku strategiju. Hint: Svaki od igrača može mjeriti svoj qubit u jednoj od baza $\{|0\rangle, |1\rangle\}$ i $\{|+\rangle, |-\rangle\}$, gdje je $|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ i $|-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.

    c) Možete li osmisliti strategiju u slučaju da igrači dijele stanje
    $$\frac{|000\rangle + |111\rangle}{\sqrt{2}}?$$

11. Opišite varijantu Simonovog algoritma koja u polinomijalnom vremenu u n nalazi stringove s, t i $s \oplus t$, $s \neq t$, sa svojstvom da je $f(x) = f(x \oplus t) = f(x \oplus s) = f(x \oplus s \oplus t)$ za sve x. Kao i u Simonovom problemu dana je funkcija $f : \{0,1\}^n \to \{0,1\}^n$, a stringovi nula i jedinica s i t su jedinstveni.

12. Pretpostavimo da vam je dano jedno od dva stanja
$$|\Psi_1\rangle = \frac{1}{\sqrt{10}} (3|0\rangle + |1\rangle) \text{ i } |\Psi_2\rangle = \frac{1}{\sqrt{10}} (3|0\rangle - |1\rangle).$$

a) Koje mjerenje trebate izvršiti kako biste pogodili o kojem se stanju radi sa što većom vjerojatnošću? Koja je to vjerojatnost?

b) Ako za pogodak dobijete jednu kunu, a za promašaj izgubite tri kune, koja je vaša optimalna strategija?

13. Dan je neusmjereni graf G s n vrhova preko kvantne proročice koja element baze $|i, j, a\rangle$ (gdje su $i, j \in \{1, \ldots, n\}$ i $a \in \{0, 1\}$) preslika u $|i, j, NOT(a)\rangle$ ako G sadrži brid koji povezuje vrhove i i j, a u $|i, j, a\rangle$ inače. Problem je utvrditi je li G povezan. Osmislite kvantni algoritam koji rješava ovaj problem s velikom vjerojatnošću u $O(n^{3/2} \log n)$ koraka. Hint: možete koristiti Groverov algoritam zajedno s nekim klasičnim algoritmom za pretraživanje grafa.

14. a) Konstruirajte reverzibilni krug koji za dana dva bita x i y "ispisuje" $(x, y, c, x \oplus y)$, gdje je c carry bit.

b) Konstruirajte reverzibilni krug pomoću Fredkinovih vrata (potražite definiciju na web-u) koji simulira Toffolijeva vrata.

c) Konstruirajte kvantni krug koji zbraja dva dvobitna broja x i y modulo 4, tj. koji implementira transformaciju $|x, y\rangle \mapsto |x, x + y \bmod 4\rangle$.

15. Konstruirajte kvantni krug koji izvršava sljedeću unitarnu transformaciju:

$$|z\rangle |0\rangle \mapsto |z\rangle |w(z)\rangle ,$$

gdje $w(z)$ označava Hammingovu težinu od z (tj. broj jedinica u binarnom zapisu broja z). Broj z je reprezentiran s n qubita (tj. z ima n bitova).

16. Konstruirajte kvantni krug koji koristeći Fredkinova vrata (potražite definiciju na web-u) simulira kontrolirana U vrata gdje je U unitarni operator koji je dan kao crna kutija. Uz to poznat je svojstven vektor $|u\rangle$ od U sa svojstvenom vrijednošću 1 koji se također može koristiti u konstrukciji.

17. Pretpostavimo da je dana crna kutija koja evaluira funkciju

$$f : \{0,1\}^n \to \{0,1\}^{n-1},$$

za koju znamo da je 2:1 (praslika svakog elementa kodomene ima dva elementa). Potrebno je pronaći koliziju – vrijednosti x i y za koje je $f(x) = f(y)$.

a) Opišite vjerojatnosni klasični algoritam koji zahtjeva $O(\sqrt{N})$ memorije i koji rješava problem s velikom vjerojatnošću s $O(\sqrt{N})$ pozivanja crne kutije.

b) Pretpostavimo sad da imamo $O(N^{1/3})$ memorije na raspolaganju. Opišite klasični vjerojatnosni algoritam koji rješava problem s velikom vjerojatnosti u $O(N^{2/3})$ poziva funkcije.

c) Pokažite da Groverov algoritam može pronaći koliziju u $O(\sqrt{N})$ kvantnih poziva crne kutije koristeći $O(1)$ memorije.

d) Opišite kvantni algoritam koji koristeći $O(M)$ memorije nalazi koliziju u $O(M) + O(\sqrt{N/M})$ koraka. (Hint: Prvo spremite vrijednosti funkcije u točkama $\{x_1, x_2, \ldots, x_M\}$), a zatim potražite y tako da je $f(y) = f(x_i)$ za neki x_i.)

3.2 Qiskit projekt

Qiskit je open source okruženje (bazirano na Pythonu) za rad s IBM Q Experience kvantnim računalima. Na službenom web-u `https://qiskit.org/textbook/preface.html` mogu se pronaći implementacije osnovnih algoritama (kvantna teleportacija, Deutschov algoritam, Simonov algoritam, Shorov algoritam, Groverov algoritam, kvantne šetnje...) koje se onda mogu izvršiti na simulatoru ili na stvarnom kvantnom računalu. Za vježbu implementirajte i izvršite algoritam po izboru.

4 Literatura

[Aara] Scott Aaronson. Quantum randomness. *American Scientist*, 102(4).

[Aarb] Scott Aaronson. The quest for randomness. *American Scientist*, 102(3).

[Aar13] Scott Aaronson. *Quantum Computing since Democritus*. Cambridge University Press, 2013.

[Aar17] Scott Aaronson. *Introduction to Quantum Information Science*. 2017. https://www.scottaaronson.com/blog/?p=3943.

[Ana18] Anil Ananthaswamy. *Through Two Doors at Once: the elegant experiment that captures the enigma of our quantum reality*. Dutton, 2018.

[Duj20] Andrej Dujella. *Teorija brojeva*. Školska knjiga, 2020.

[ea19] Frank Arute et al. Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779):505–510, October 2019.

[FLSL66] Richard P. Feynman, Robert B. Leighton, Matthew Sands, and R. Bruce Lindsay. The Feynman Lectures on Physics, Vol. 3: Quantum Mechanics. *Physics Today*, 19(11):80–83, November 1966.

[GNTZ11] Sheldon Goldstein, Travis Norsen, Daniel Tausk, and Nino Zanghi. Bell's theorem. *Scholarpedia*, 6(10):8378, 2011.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing - STOC '96*. ACM Press, 1996.

[GS18] David J. Griffiths and Darrell F. Schroeter. *Introduction to Quantum Mechanics*. Cambridge University Press, August 2018.

[KS75] Simon Kochen and E. P. Specker. The problem of hidden variables in quantum mechanics. In *The Logico-Algebraic Approach to Quantum Mechanics*, pages 293–328. Springer Netherlands, 1975.

[NC09] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2009.

[PG19] Edwin Pednault and John Gunnels. On "quantum supremacy". 2019.

[Pre13] John Preskill. *Quantum computing*. 2013. http://theory.caltech.edu/ preskill/ph219.

[RL09] William E. Ryan and Shu Lin. *Channel Codes*. Cambridge University Press, 2009.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[Vaz04] Umesh Vazirani. *Quantum computation*. 2004. https://people.eecs.berkeley.edu/ vazirani/f04quantum/quantum.html.

A Unitarni prostori

U ovom dodatku ćemo navesti osnovne pojmove i teoreme teorije unitarnih operatora koje koristimo u ovoj skripti.

Neka je V vektorski prostor nad $\mathbb{C}$. Preslikavanje $\langle\cdot|\cdot\rangle : V \times V \to \mathbb{C}$ zovemo skalarni produkt na vektorskom prostoru V ako je

a) linearno u drugoj varijabli

$$\langle v| \sum_i \lambda_i |w_i\rangle = \sum_i \lambda_i \langle v|w_i\rangle ,$$

za sve $|v\rangle , |w_i\rangle \in V$ i $\lambda_i \in \mathbb{C}$,

b) konjugirano simetrično

$$\langle v|w\rangle = \overline{\langle w|v\rangle},$$

za sve $|v\rangle , |w\rangle \in V$,

c) pozitivno

$$\langle v|v\rangle \geq 0,$$

za sve $|v\rangle \in V$ gdje jednakost vrijedi ako i samo ako je $|v\rangle = 0$.

Uočimo da iz a) i b) slijedi da je preslikavanje anti-linearno u prvoj varijabli

$$\left\langle \sum_i \lambda_i w_i \middle| v \right\rangle = \sum_i \overline{\lambda_i} \langle w_i|v\rangle ,$$

za sve $|v\rangle , |w_i\rangle \in V$ i $\lambda_i \in \mathbb{C}$.

Definicija A.1. *Vektorski prostor V nad $\mathbb{C}$ sa skalarnim produktom $\langle\cdot|\cdot\rangle$ se naziva unitaran prostor. Potpun unitaran prostor se naziva Hilbertov prostor.*

Napomena A.2. Svaki konačno dimenzionalan unitaran prostor V je potpun (tj. svaki Cauchyev niz u V je konvergentan) jer je $\mathbb{C}$ potpun.

Unitarnost nam omogućava da definiramo normu vektora $|v\rangle$

$$\| |v\rangle \| := \sqrt{\langle v|v\rangle},$$

i kut ϕ između vektora $|u\rangle$ i $|v\rangle$

$$\cos\phi = \frac{\langle u|v\rangle}{\| \, |u\rangle \, \| \cdot \| \, |v\rangle \, \|}.$$

Kažemo da je baza vektorskog prostora V ortonormirana, ako je svaki vektor te baze norme jedan i ako su svaka dva različita vektora međusobno okomita. Gram-Schmidtovim postupkom ortogonalizacije iz proizvoljne baze dobivamo ortonormiranu bazu. Ako je $\{|i\rangle\}_{i\in I}$ neka ortonormirana baza, onda za vektore $|w\rangle = \sum_i w_i \, |i\rangle$ i $|v\rangle \sum_i v_i \, |i\rangle$ gdje su $w_i, v_i \in \mathbb{C}$ vrijedi

$$\langle v|w\rangle = \sum_i \overline{v_i} w_i.$$

Napomena A.3. a) Svaki $|\Psi\rangle \in V$ u ortonormiranoj bazi $\{|i\rangle\}_{i\in I}$ možemo zapisati kao

$$|\Psi\rangle = \sum_{i\in I} \langle i|\Psi\rangle \, |i\rangle \, .$$

b) Za sve $|v\rangle \, , |w\rangle \in V$ vrijedi Cauchy-Schwarzova nejednakost

$$| \, \langle v|w\rangle \, |^2 \leq \langle v|v\rangle \, \langle w|w\rangle \, .$$

Definicija A.4. *Svojstveni vektor linearnog operatora $A : V \to V$ je vektor $v \in V$ za koji vrijedi $Av = \lambda v$ za neki $\lambda \in \mathbb{C}$. Broj λ zovemo svojstvena vrijednost operatora A.*

Napomena A.5. Svojstvene vrijednosti su nultočke karakterističnog polinoma operatora A, $c(\lambda) = \det |A - \lambda I|$.

Definicija A.6. *Linearni operator $A : V \to V$ na unitarnom vektorskom prostoru V je unitaran ako vrijedi*

$$\langle u|v\rangle = \langle Au|Av\rangle \, ,$$

za sve $|u\rangle \, , |v\rangle \in V$. Kažemo da A čuva skalarni produkt.

Napomena A.7. Unitarni operatori čuvaju norme vektora (jer za svaki $|u\rangle \in V$ vrijedi $\| |u\rangle \|^2 = \langle u|u\rangle = \langle Au|Au\rangle = \|Au\|$) i kutove između vektora. Specijalno, A ima trivijalnu jezgru pa je invertibilan.

Definicija A.8. *Za svaki linearan operator $A : V \to V$ postoji jedinstveni linearan operator $A^\dagger \in L(V)$ takav da za sve $|u\rangle, |v\rangle \in V$ vrijedi*

$$\langle v|A|w\rangle = \left\langle A^\dagger v \middle| w \right\rangle.$$

Za taj operator kažemo da je adjungiran operatoru A.

Uočimo da za unitaran operator A vrijedi $AA^\dagger = A^\dagger A = I$, odnosno $A^\dagger$ je inverz od A. Naime, za sve $v, w \in V$ vrijedi

$$\langle Av|w\rangle = \left\langle Av \middle| AA^{-1}w \right\rangle = \left\langle v \middle| A^{-1}w \right\rangle.$$

Napomena A.9. a) Za sve $A, B \in L(v)$ vrijedi $(AB)^\dagger = B^\dagger A^\dagger$.

b) Za vektor $|v\rangle \in V$ definiramo funkcional $|v\rangle^\dagger := \langle v|$. Lako se provjeri da vrijedi $(A|v\rangle)^\dagger = \langle v| A^\dagger$.

Ako sa $\mathcal{A}$ označimo matrični prikaz operatora A u nekoj ortonormiranoj bazi, onda je $(\overline{\mathcal{A}})^T$ matrični prikaz operatora $A^\dagger$ u toj istoj bazi.

Definicija A.10. *Operator $A \in L(V)$ se zove hermitski ako je $A^\dagger = A$.*

Važan primjer hermitskih operatora su *projektori*. Neka je $W \subset V$ potprostor vektorskog prostora V i neka je $\{|1\rangle, |2\rangle, \ldots, |k\rangle\}$ ortonormirana baza od V takva da je $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ baza za W (dakle $\dim V = k$ i $\dim W = d$). Operator

$$P = \sum_{i=1}^{d} |i\rangle\langle i|$$

zovemo projektor na potprostor W.

Za operator A kažemo da je *normalan* ako vrijedi $AA^\dagger = A^\dagger A$. Unitarni operatori su normalni jer za njih vrijedi $AA^\dagger = A^\dagger A = I$. Isto vrijedi i za hermitske operatore.

Normalni operatori imaju jednostavnu spektralnu dekompoziciju.

Teorem A.11. *Operator $A \in L(V)$ normalan je ako i samo ako se može dijagonalizirati u ortonormiranoj bazi (odnosno ako postoji ortonormirana baza prostora V koja se sastoji od svojstvenih vektora operatora A).*