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.

[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].

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 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.

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

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 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:

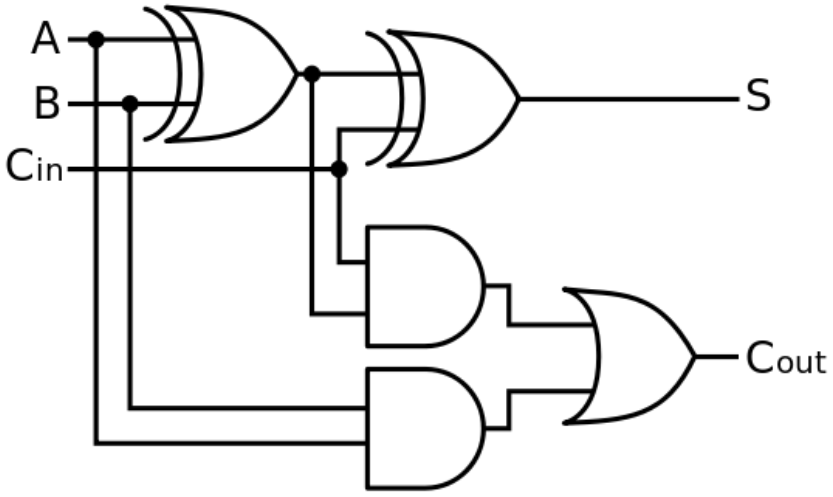
$$|\Psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}.$$

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.

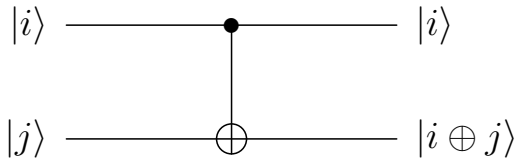
Što su to kvantna vrata? Općenito, kvantna vrata proizvoljni su unitarni operatori na prostoru stanja (prisjetimo se da unitarni operatori

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 $H^2 = I$.

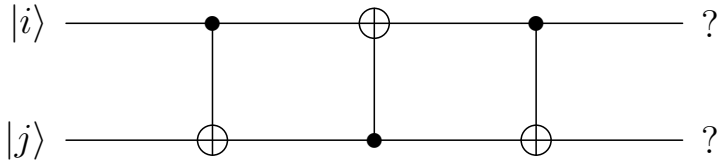
Od vrata koja djeluju na dva qubita trebat će nam kontrolirana NOT ili CNOT vrata. Ona djeluju na dva qubita, kontrolni qubit $|i\rangle$ i qubit $|j\rangle$. Kontrolni qubit se ne mijenja, dok se na drugi qubit primjenjuju NOT ili X vrata ako je kontrolni qubit jednak $|1\rangle$, inače se ništa ne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



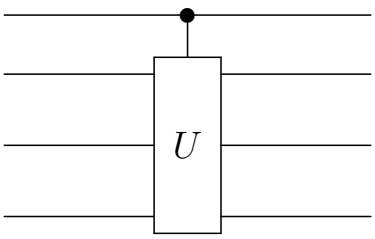
Slika 2: CNOT vrata

- 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?



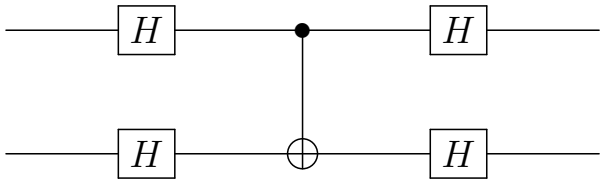
Neka su U bilo koja vrata (unitaran operator). Na sličan način možemo definirati kontrolirana U ili CU vrata (vidi Sliku 3).



Slika 3: CU vrata

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

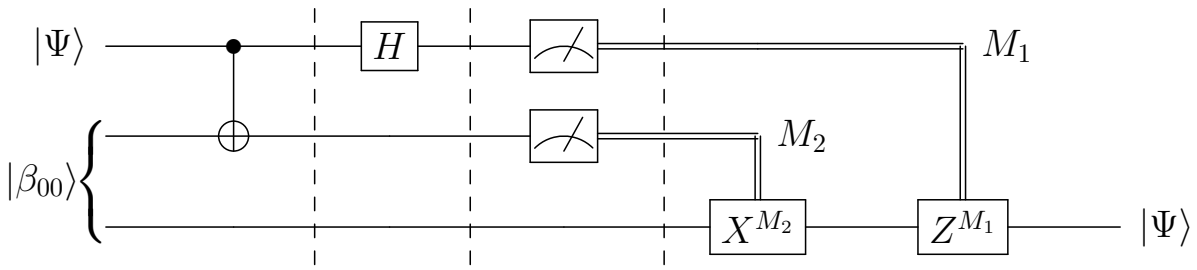
Zadatak 2.3. Što radi ovaj program?



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:

$$\begin{aligned}
|M_1M_2\rangle = |00\rangle &\mapsto |\Psi_B\rangle = \alpha|0\rangle + \beta|1\rangle \\
|M_1M_2\rangle = |01\rangle &\mapsto |\Psi_B\rangle = \alpha|1\rangle + \beta|0\rangle \\
|M_1M_2\rangle = |10\rangle &\mapsto |\Psi_B\rangle = \alpha|0\rangle - \beta|1\rangle \\
|M_1M_2\rangle = |11\rangle &\mapsto |\Psi_B\rangle = \alpha|1\rangle - \beta|0\rangle,
\end{aligned}$$

dok će stanje cijelog sustava biti jednako $|\Psi_3\rangle = |M_1M_2\rangle|\Psi_B\rangle$.

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/`.

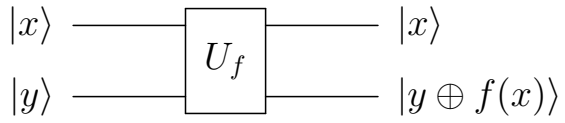
2.5 Primjer – Deutsch-Jozsa algoritam

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 (deterministički 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 deterističkih 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.

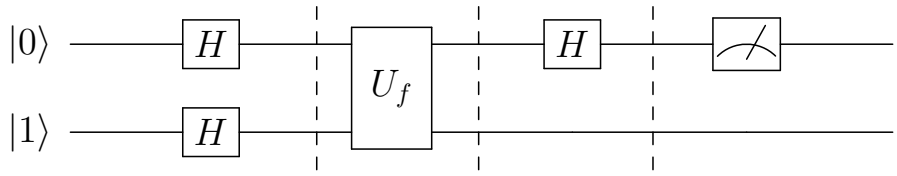


Slika 5: Kvantna proročica

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.



Slika 6: Deutschov algoritam

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*

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

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

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

- 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 Postulati kvantne mehanike

U prethodnom smo odjeljku matematički opisali kvantni model računanja (qubit, kvantna vrata, mjerenje ...) i pokazali smo kako s njime možemo raditi zanimljive stvari. U ovom odjeljku motivirat ćemo definiciju tog modela, odnosno, opisat ćemo fizikalnu osnovu na kojoj se bazira konstrukcija kvantnog računala – govorit ćemo o kvantnoj mehanici. Krenimo s opisom njezinih postulata. Pratimo izlaganje iz [NC09]. Za više detalja pogledajte standardni udžbenik za kvantnu mehaniku [GS18].

3.1 Stanja kvantnog sustava

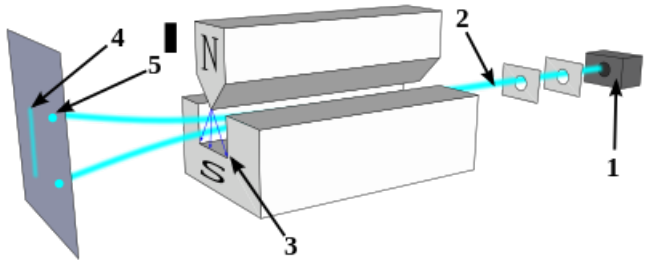
Postulat 1. *Svakom izoliranom fizikalnom sustavu pridružujemo (kompleksan) Hilbertov prostor $\mathcal{H}$ koji zovemo prostor stanja sustava. Sustav*

je u potpunosti opisan svojim vektorom stanja $|\Psi\rangle$, što je jedinični vektor u prostoru stanja.

Prisjetimo se, Hilbertov prostor potpun je unitaran vektorski prostor. Napomenimo da je svaki konačno dimenzionalan kompleksan vektorski prostor potpun (jer je $\mathbb{C}$ potpuno polje), pa je onda i Hilbertov. Mi ćemo promatrati samo sustave čiji je prostor stanja konačno dimenzionalan, pa nam je jedini zahtjev na taj vektorski prostor unitarnost. Kratak podsjetnik na definicije i tvrdnje iz teorije unitarnih prostora koje ćemo koristiti u skripti nalazi se u Dodatku A.

Najjednostavniji primjer (apstraktnog) kvantnog sustava (s dvodimenzionalnim prostorom stanja) je qubit. Kažemo još da je qubit kvantnomehanički sustav s dva stanja (eng. two-state quantum-mechanical system). Može se fizikalno realizirati na različite načine. Jedna od realizacija koju je najjednostavnije objasniti (ali nije praktična, ne upotrebljava se u izradi kvantnih računala) jest preko čestica sa spinom $\frac{1}{2}$, npr. elektrona. Spin je fundamentalno svojstvo subatomskih čestica koje opisuje kako se čestice gibaju u magnetskom polju. Na Slici 7 nalazi se prikaz poznatog Stern-Gerlachovog eksperimenta (u kojem se umjesto elektrona upotrebljavaju atomi srebra).

Vidimo da nehomogeno magnetsko polje zakreće snop atoma srebra prema gore ili dolje (tj. u smjeru z osi) kao da svaki atom posjeduje vlastiti magnetski moment. Stern i Gerlach ovim su eksperimentom pokazali da je taj magnetski moment (spin) kvantiziran – postoje samo dva smjera (kuta) otklona (klasično bi svaki kut bio moguć). Ako se atom otklonio prema gore, kažemo da atom ima spin prema gore i njegovo stanje (nakon prolaska kroz aparaturu) označavamo s $|\uparrow\rangle$. Analogno, drugo stanje označavamo s $|\downarrow\rangle$. Prostor stanja ovog sustava kompleksan je vektorski prostor $\mathcal{H}$ razapet s vektorima $\{|\uparrow\rangle, |\downarrow\rangle\}$. Na $\mathcal{H}$ definiramo skalarni produkt u odnosu na koji će vektori $|\uparrow\rangle$ i $|\downarrow\rangle$ biti međusobno okomiti i norme jedan. Prema tom modelu elektron prije ulaska u Stern-Gerlachovu aparaturu (odnosno prije mjerenja spina u smjeru z osi) nalazi se u stanju $|\Psi\rangle = a\,|\uparrow\rangle + b\,|\downarrow\rangle$, gdje su $a, b \in \mathbb{C}$ takvi da je $|a|^2 + |b|^2 = 1$. Nakon što definiramo mjerenja u Odjeljku 3.3 vidjet ćemo da je vjerojatnost da se taj elektron otkloni prema gore jednaka $|a|^2$.



Slika 7: Stern-Gerlachov eksperiment: atomi srebra putuju kroz nehomogeno magnetsko polje koje ih zakrene prema dolje ili gore ovisno o njihovom spinu; (1) izvor, (2) zraka atoma srebra, (3) nehomogeno magnetsko polje, (4) klasično predviđanje, (5) opaženi rezultat

Izvor: Tatoute, CC BY-SA 4.0, via Wikimedia Commons

Za pristupačnu "analizu" čestica spina $\frac{1}{2}$ pogledajte šesto poglavlje u Feynmanovim predavanjima [FLSL66].

3.2 Dinamika kvantnog sustava

U ovom odjeljku opisujemo kako se vektor stanja $|\Psi\rangle$ mijenja s vremenom.

Postulat 2. *Dinamika zatvorenog kvantnog sustava opisana je unitarnom transformacijom. Preciznije, stanje $|\Psi\rangle$ sustava u trenutku t_1 povezano je sa stanjem $|\Psi'\rangle$ u trenutku t_2 unitarnim operatorom U (koji ovisi samo o t_1 i t_2, a ne i o vektorima stanja) tako da vrijedi*

$$|\Psi'\rangle = U\,|\Psi\rangle\,.$$

Postoji i ekvivalentna formulacija (u kojoj pretpostavljamo da su vektori stanja funkcije) ovog postulata preko valne jednadžbe.

Postulat (2'). *Dinamika zatvorenog kvantnog sustava određena je Schrödingerovom jednadžbom*

$$i\hbar\frac{\mathrm{d}\,|\Psi\rangle}{\mathrm{d}t} = H\,|\Psi\rangle\,,$$

gdje je H hermitski operator koji zovemo Hamiltonijan sustava, a $\hbar$ je Planckova konstanta.

Nas će najviše zanimati sustavi kod kojih H ne ovisi o vremenu (jer ne želimo da se kvantna vrata mijenjaju u vremenu). Tada jednadžba ima rješenje

$$|\Psi(t)\rangle = e^{-it\frac{H}{\hbar}}\,|\Psi(0)\rangle\,,$$

gdje je $|\Psi(t)\rangle$ stanje sustava u trenutku t. Operator $e^{-it\frac{H}{\hbar}}$ igra ulogu unitarnog operatora iz Postulata 2.

Zadatak 3.1. Neka je V konačno dimenzionalan kompleksan vektorski prostor. Za linearan operator $X \in L(V)$ definiramo $e^X := I + X + \frac{X^2}{2!} + \cdots + \frac{X^n}{n!} + \ldots$. Koristeći svojstva standardne norme $||\cdot||$ (nejednakost trokuta i submultiplikativnost) na $M_n(\mathbb{C})$ dokažite da e^X konvergira.

Zadatak 3.2. Za prirodan broj n neka je dana matrica $X \in M_n(\mathbb{C})$. Definirajmo funkciju $f : \mathbb{R} \to M_n(\mathbb{C})$ formulom

$$f(t) = e^{tX}.$$

Dokažite da je $\frac{\mathrm{d}}{\mathrm{d}t} f(t) = Xe^{tX}$.

Zadatak 3.3. Dokažite da je operator $e^{-it\frac{H}{\hbar}}$ iz Postulata 2' unitaran.

U kvantnom računarstvu vrijeme je diskretizirano pa ovaj postulat koristimo za opisivanje djelovanja kvantnih vrata na qubite. Tako, na primjer, za sustav čija je dinamika opisana Hamiltonijanom H možemo reći da implementira kvantna vrata čije je djelovanje na qubit $|\Psi\rangle$ dano operatorom $e^{-it\frac{H}{\hbar}}$. Problem je onda za kvantna vrata U konstruirati kvantni sustav (s Hamiltonijanom H) koji ga implementira (tj. takav da je $U = e^{-it\frac{H}{\hbar}}$ za neki $t > 0$).

Ako se vratimo na realizaciju qubita preko elektrona iz prethodnog odjeljka, primjer unitarne transformacije tog sustava (odnosno kvantnih vrata) bila bi rotacija Stern-Gerlachove aparature oko osi kretanja elektrona za kut θ. Na primjer, ako je elektron u stanju $|\uparrow\rangle$ (tj. ako bi se sa sigurnošću otklonio prema "gore" u početnoj konfiguraciji), koja je vjerojatnost da će se otkloniti prema "gore" nakon što aparaturu rotiramo za kut θ? Kratak odgovor je da rotacija aparature djeluje na vektor stanja kao operator rotacije koji je u bazi $\{|\uparrow\rangle, |\downarrow\rangle\}$ dan matricom $\begin{pmatrix} \cos(\theta/2) & -\sin(\theta/2) \\ \sin(\theta/2) & \cos(\theta/2) \end{pmatrix}$, tako da vektor stanja $|\uparrow\rangle$ prelazi u vektor $\cos\frac{\theta}{2}|\uparrow\rangle + \sin\frac{\theta}{2}|\downarrow\rangle$, odnosno vjerojatnost otklanjanja elektrona prema "gore" jednaka je $\cos^2\frac{\theta}{2}$. Za detaljniju "analizu" pogledajte šesto poglavlje u [FLSL66].

3.3 Mjerenje sustava

Postulat 3. *Kvantno mjerenje definirano je skupom $\{M_m\}_{m\in I}$ operatora mjerenja. Ti operatori djeluju na prostor stanja sustava koji se mjeri. Skup I indeksira moguće ishode eksperimenta. Ako se sustav nalazi u*

stanju $|\Psi\rangle$ *u trenutku mjerenja, tada je vjerojatnost* $p(m)$ *ishoda* $m \in I$ *(kao rezultata mjerenja) jednaka*

$$p(m) = \left\langle \Psi \middle| M_m^\dagger M_m \middle| \Psi \right\rangle$$

i stanje sustava nakon mjerenja je

$$\frac{M_m |\Psi\rangle}{\sqrt{\left\langle \Psi \middle| M_m^\dagger M_m \middle| \Psi \right\rangle}}.$$

Operatori mjerenja zadovoljavaju takozvanu jednadžbu potpunosti

$$\sum_m M_m^\dagger M_m = I.$$

S $M_m^\dagger$ *označavamo operator adjungiran operatoru* M_m *(za definiciju i osnovna svojstva pogledajte Dodatak A).*

Napomena 3.4. Jednadžba potpunosti implicira

$$1 = \langle \Psi | \Psi \rangle = \left\langle \Psi \middle| \sum_m M_m^\dagger M_m \middle| \Psi \right\rangle = \sum_m \left\langle \Psi \middle| M_m^\dagger M_m \middle| \Psi \right\rangle = \sum_m p(m).$$

Primjer. (Mjerenje qubita u bazi $\{|0\rangle, |1\rangle\}$.) Odaberimo mjerenje $\{M_0, M_1\}$, gdje je $M_0 = |0\rangle\langle 0|$ i $M_1 = |1\rangle\langle 1|$ (u Diracovoj notaciji $|\Psi\rangle\langle\Psi|$ označava projektor na vektor $|\Psi\rangle$, pogledajte Dodatak A). Budući da za proizvoljan $|\Psi\rangle$ vrijedi $|\Psi\rangle = |0\rangle \langle 0|\Psi\rangle + |1\rangle \langle 1|\Psi\rangle$, slijedi da je $I = |0\rangle\langle 0| + |1\rangle\langle 1|$. S druge strane, za proizvoljne $|\Psi\rangle$ i $|\Psi'\rangle$ vrijedi

$$\langle M_0(|\Psi\rangle)|\Psi'\rangle = \langle 0|\Psi\rangle \langle 0|\Psi'\rangle = \langle \Psi | M_0 | \Psi' \rangle$$

pa zaključujemo da su operatori M_0 i M_1 hermitski, tj. vrijedi $M_0 = M_0^\dagger$ i $M_1 = M_1^\dagger$. Kako su M_0 i M_1 projektori (tj. $M_i^2 = M_i$), slijedi

$$I = M_0 + M_1 = M_0^2 + M_1^2 = M_0^\dagger M_0 + M_1^\dagger M_1,$$

odnosno jednadžba potpunosti je zadovoljena.

Ako je $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle$, onda je vjerojatnost mjerenja stanja $|0\rangle$ po Postulatu 3 jednaka

$$p(0) = \left\langle \Psi \middle| M_0^\dagger M_0 \middle| \Psi \right\rangle = \langle \Psi | M_0 | \Psi \rangle = \langle a\,|0\rangle + b\,|1\rangle | a\,|0\rangle \rangle = \bar{a}a = |a|^2$$

i slično $p(1) = |b|^2$.

Zadatak 3.5. Neka su $|\Psi_1\rangle$ i $|\Psi_2\rangle$ dva različita stanja jednog qubita (vektori norme jedan u $\mathbb{C}^2$) koji nisu ortogonalni (odnosno vrijedi $\langle \Psi_1 | \Psi_2 \rangle \neq 0$). Postoji li mjerenje $\{M_m\}_{m \in I}$ koje gotovo sigurno (tj. s vjerojatnošću 1) može utvrditi je li neko treće stanje $|\Psi\rangle$ – za koje unaprijed znamo da je jednako $|\Psi_1\rangle$ ili $|\Psi_2\rangle$ – jednako $|\Psi_1\rangle$?

U kvantnom računanju najčešće se upotrebljavaju projektivna mjerenja.

3.3.1 Projektivna mjerenja

Definicija 3.6. *Projektivno mjerenje definira se opservablom (eng. observable) M, hermitskim operatorom na prostoru stanja sustava koje se opaža. Opservabla ima spektralnu dekompoziciju $M = \sum mP_m$, gdje je P_m projektor na svojstveni potprostor od M sa svojstvenom vrijednošću m (znamo da se svaki hermitski operator može dijagonalizirati pa opisana spektralna dekompozicija postoji). Vjerojatnost ishoda m pri mjerenju stanja $|\Psi\rangle$ je $p(m) = \langle \Psi | P_m | \Psi \rangle$. Ako izmjerimo m, sustav prelazi u stanje $\frac{P_m|\Psi\rangle}{\sqrt{p(m)}}$.*

Napomena 3.7. Ako u Postulatu 3 za familiju $\{M_m\}$ uzmemo familiju ortogonalnih projektora, tj. ako za svaki M_m uzmemo projektor P_m (tj. $P_m^2 = P_m$) tako da vrijedi $P_m P_n = 0$ za sve $m \neq n$, onda dobijemo mjerenje ekvivalentno projektivnom mjerenju kod kojeg je opservabla M jednaka $M = \sum mP_m$.

3.3.2 Faza

Promotrimo dva vektora stanja $|\Psi\rangle$ i $e^{i\theta}|\Psi\rangle$ za neki $\theta \in \mathbb{R}$. Kažemo da su ta dva stanja jednaka do na globalni fazni faktor $e^{i\theta}$. Ono što je važno jest da ta dva stanja imaju jednake statistike mjerenja, tj. za sva mjerenja $\{M_m\}_m$ vrijedi

$$\langle \Psi | M_m^\dagger M_m | \Psi \rangle = \langle e^{i\theta}\Psi | M_m^\dagger M_m | e^{i\theta}\Psi \rangle ,$$

tako da ta dva stanja eksperimentalno ne možemo razlikovati.

S druge strane, na primjer, za stanja

$$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad \text{i} \quad \frac{|0\rangle - |1\rangle}{\sqrt{2}},$$

kažemo da se razlikuju u relativnoj fazi. Njih ne možemo razlikovati mjerenjem u bazi $\{|0\rangle, |1\rangle\}$ jer je vjerojatnost mjerenja vektora $|1\rangle$ za oba vektora stanja jednaka $\frac{1}{2}$ iako vektori imaju različite amplitude uz element baze $|1\rangle$ (to su $\frac{1}{\sqrt{2}}$ i $-\frac{1}{\sqrt{2}}$). Amplitude se razlikuju za kompleksan broj apsolutne vrijednosti 1 pa zato kažemo da se ti vektori stanja razlikuju za relativnu fazu. Za domaću zadaću nađite bazu u kojoj se ta dva stanja "razlikuju".

3.4 Složeni sustavi

U ovom odjeljku objasnit ćemo kako se stanje sustava opisuje preko stanja komponenti tog sustava. To će nam omogućiti razumijevanje sustava koji se sastoje od velikog broja qubita (tj. kvantnih računala). Za to će nam trebati pojam tenzorskog produkta (unitarnih) vektorskih prostora. Prije nego što definiramo sve potrebne pojmove, iskažimo postulat o složenim sustavima.

Postulat 4. *Prostor stanja složenog sustava jednak je tenzorskom produktu prostora stanja komponenti. Preciznije, ako se svaki od (nespregnutih) podsustava $i = 1, 2, \ldots, n$ nalazi u stanju $|\Psi_i\rangle$, onda je stanje cijelog sustava opisano vektorom*

$$|\Psi_1\rangle \otimes |\Psi_2\rangle \otimes \cdots \otimes |\Psi_n\rangle .$$

Neka su $V_1, V_2, \dots V_n$ konačno dimenzionalni (unitarni) vektorski prostori (na primjer prostori stanja nekih sustava). Tenzorski produkt $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ vektorski je prostor s definiranim multilinearnim (linearnim u svakoj varijabli) preslikavanjem

$$\tau : V_1 \times V_2 \times \cdots \times V_n \to V_1 \otimes V_2 \otimes \cdots \otimes V_n,$$

koje zadovoljava sljedeće univerzalno svojstvo: ako je $h : V_1 \times V_2 \times \cdots \times V_n \to W$ bilo koje multilinearno preslikavanje u vektorski prostor W, onda postoji jedinstveni linearni operator $\tilde{h} : V_1 \otimes V_2 \otimes \cdots \otimes V_n \to W$ takav da vrijedi $h = \tilde{h} \circ \tau$. Pišemo $\tau(v_1, v_2, \dots, v_n) = v_1 \otimes v_2 \otimes \cdots \otimes v_n$.

Ovo je poprilično apstraktna definicija, pa ju pokušajmo malo "konkretizirati". Za svaki $i = 1, 2, \dots, n$ označimo sa $(v_j^i)_j$ neku bazu vektorskog prostora V_i. Iz univerzalnoga svojstva slijedi da vektori $v_{j_1}^1 \otimes v_{j_2}^2 \otimes \cdots \otimes v_{j_n}^n$ za sve kombinacije $(j_1, j_2, \dots, j_n)$ čine bazu za $V_1 \otimes V_2 \otimes \cdots \otimes V_n$. Dakle vrijedi $\dim V_1 \otimes V_2 \otimes \cdots \otimes V_n = \dim V_1 \dim V_2 \cdots \dim V_n$.

Na primjer, ako je $V = \langle |0\rangle, |1\rangle \rangle$ prostor stanja jednog qubita, onda sustav od dva qubita opisujemo s tenzorskim produktom $V^2 = V \otimes V$ čija je baza skup $\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}$. Općenito, dimenzija sustava stanja n qubita jednaka je $\dim V^n = 2^n$. Kraće zapisujemo $v_1 v_2 \cdots v_n := v_1 \otimes v_2 \otimes \cdots \otimes v_n$ ili kod qubita na primjer $|01\rangle := |0\rangle |1\rangle = |0\rangle \otimes |1\rangle$.

Preslikavanje τ nam je važno iz više razloga. Prvo, govori nam kako pomoću stanja (izoliranih) podsustava $\{v_1, v_2, \dots, v_n\}$ konstruiramo stanje cijelog sustava – to je interpretacija vektora $v_1 \otimes v_2 \otimes \cdots \otimes v_n$, a ujedno i razlog zašto koristimo tenzorski produkt za modeliranje složenih sustava.

Također, omogućava nam da koristeći unitarnost prostora V_i definiramo na tenzorskom produktu skalarni produkt. Ako su $\langle \cdot | \cdot \rangle_i$ za $i = 1, 2, \dots, n$ skalarni produkti na $V_1, V_2, \dots, V_n$ tada na $V_1 \otimes V_2 \otimes \cdots \otimes V_n$ definiramo preslikavanje $\langle \cdot | \cdot \rangle$ formulom

$$\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n | w_1 \otimes w_2 \otimes \cdots \otimes w_n \rangle := \langle v_1 | w_1 \rangle_1 \cdot \langle v_2 | w_2 \rangle_2 \cdots \langle v_n | w_n \rangle_n$$

koje onda po linearnosti proširujemo do skalarnog produkta na cijelom

$V_1 \otimes V_2 \otimes \cdots \otimes V_n$. Primijetimo da ako je svaki v_i stanje, onda je i $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ stanje (odnosno vektor norme jedan).

Naglasimo još jednom da nije svaki vektor iz tenzorskog produkta oblika $v_1 \otimes v_2 \otimes \cdots \otimes v_n$ (odnosno iz slike preslikavanja τ). Na primjer, lako se provjeri da se stanje dva qubita $|\Psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}} \in V^2$ ne može faktorizirati, tj. ne postoje $|\Psi_1\rangle, |\Psi_2\rangle \in V$ takvi da je $|\Psi\rangle = |\Psi_1\rangle \otimes |\Psi_2\rangle$.

U tom slučaju kažemo da je sustav $V_1 \otimes V_2$ u stanju *kvantne spregnutosti* (eng. quantum entanglement).

Intuitivno, ako sustav nije u stanju kvantne spregnutosti, onda djelovanjem na sustav V_1 ne utječemo na sustav V_2.

Opišimo još kako se (unitarni) operatori proširuju s podsustava na cijeli sustav. Neka su za sve $i = 1, 2, \ldots, n$ dani linearni operatori $A_i \in L(V_i)$. Definirajmo $A_1 \otimes A_2 \otimes \cdots \otimes A_n \in L(V_1 \otimes V_2 \otimes \cdots \otimes V_n)$ formulom

$$A_1 \otimes A_2 \otimes \cdots \otimes A_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = A_1(v_1) \otimes A_2(v_2) \otimes \cdots \otimes A_n(v_n),$$

koju onda proširujemo po linearnosti. Lako se provjeri da je ovdje sve dobro definirano. Pretpostavimo sada da djelujemo na jedan qubit (u sustavu od dva qubita $V^2 = V \otimes V$) nekim unitarnim operatorom $A \in L(V)$ (na primjer, za A možemo uzeti kvantna NOT vrata $A = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$). Budući da A ne djeluje na drugi qubit, djelovanje operatora na cijeli sustav dano je operatorom $A \otimes I$. Ako se na primjer sustav nalazi u stanju $|00\rangle$, onda djelovanjem operatora A na prvi qubit sustav prelazi u stanje $A \otimes I(|00\rangle) = A(|0\rangle) \otimes |0\rangle = |10\rangle$.

3.4.1 Kroneckerov produkt matrica

Ako je $A(e) = [a_{ij}]_{i,j}$ matrični prikaz operatora $A \in L(V)$ u bazi $e = \{e_i\}_i$ i $B(f) = [b_{ij}]_{i,j}$ matrični prikaz operatora $B \in L(W)$ u bazi $f = \{f_i\}_i$, kako izgleda matrični prikaz operatora $A \otimes B$ u bazi $e \otimes f = \{e_i \otimes f_j\}_{i,j}$?

Općenito, ako je $A = [a_{ij}]$ $m \times n$ matrica i $B = [b_{ij}]$ $p \times q$ matrica,

onda je *Kroneckerov produkt* $A \otimes B$ $mp \times nq$ (blok) matrica

$$\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}.$$

Propozicija 3.8. *Matrični prikaz operatora* $A \otimes B$ *u bazi* $e \otimes f$ *jednak je Kroneckerovom produktu* $A(e) \otimes B(f)$.

Dokaz. Izračunajmo prvo $(A \otimes I)(e \otimes f)$. Primijetimo da je za sve $1 \leq i \leq n = \dim V$ i $1 \leq j \leq m = \dim W$

$$(A \otimes I)(e_i \otimes f_j) = A(e_i) \otimes f_j = \sum_{k=1}^{n} a_{ki} e_k \otimes f_j,$$

pa je

$$(A \otimes I)(e \otimes f) = \begin{bmatrix} a_{11}I & a_{12}I & \cdots & a_{1n}I \\ a_{21}I & a_{22}I & \cdots & a_{2n}I \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}I & a_{n2}I & \cdots & a_{nn}I \end{bmatrix}.$$

S druge strane, $(I \otimes B)(e_i \otimes b_j) = \sum_{k=1}^{m} b_{kj} e_i \otimes f_k$, pa je

$$(I \otimes B)(e \otimes f) = \begin{bmatrix} B & 0 & \cdots & 0 \\ 0 & B & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B \end{bmatrix}.$$

Budući da je $(A \otimes B)(e \otimes f) = (A \otimes I)(e \otimes f) \cdot (I \otimes B)(e \otimes f)$ (jer je operator $A \otimes B$ jednak kompoziciji operatora $A \otimes I$ i $I \otimes B$) tvrdnja slijedi. □

Zadatak 3.9. Izračunajte tenzorski produkt matrica

a) $[1, 2, 3] \otimes [4, 5]$,

b) $\left(\begin{smallmatrix}1 & 2\\ 3 & 4\end{smallmatrix}\right) \otimes \left(\begin{smallmatrix}4 & 3\\ 2 & 1\end{smallmatrix}\right)$.

Zadatak 3.10. Može li se matrica A prikazati kao tenzorski produkt 2×2 matrica ako je

$$A = \begin{bmatrix} 1 & 2 & 2 & 4 \\ 0 & 1 & 0 & 2 \\ 3 & 6 & 4 & 8 \\ 0 & 3 & 0 & 4 \end{bmatrix}, \text{odnosno ako je } A = \begin{bmatrix} 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \\ 1 & 2 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}?$$

3.4.2 Mjerenje podsustava – primjer kvantne teleportacije

Prisjetimo se protokola kvantne teleportacije. Prije nego što Alice izmjeri svoja dva qubita (u standardnoj bazi), sustav se nalazi u stanju

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

To njeno mjerenje možemo definirati kao projektivno mjerenje opisano opservablom

$$M = P_{00} + P_{01} + P_{10} + P_{11},$$

gdje su P_{ij} projektori na potprostore razapete s $\{|ij\rangle|0\rangle, |ij\rangle|1\rangle\}$, tj.

$$P_{ij} = |ij0\rangle\langle ij0| + |ij1\rangle\langle ij1|.$$

Prisjetimo se, vjerojatnost ishoda ij jednaka je $p(ij) = \langle\Psi_2|P_{ij}|\Psi_2\rangle$, pa je na primjer $p(00) = \left\langle \Psi_2 \middle| \frac{1}{2}(\alpha|000\rangle + \beta|001\rangle) \right\rangle = \frac{1}{4}(|\alpha|^2 + |\beta|^2) = \frac{1}{4}$. Stanje sustava nakon što Alice izmjeri 00 je

$$\frac{P_{00}|\Psi_2\rangle}{\sqrt{p(00)}} = \frac{\frac{1}{2}(\alpha|000\rangle + \beta|001\rangle)}{\frac{1}{2}} = \alpha|000\rangle + \beta|001\rangle.$$

Ovaj primjer možemo iskoristiti za ilustraciju razlike između faktoriziranog stanja i kvantne spregnutosti. Prije nego što je Alice izmjerila svoja dva qubita, vjerojatnost da Bob izmjeri svoj qubit u stanju $|0\rangle$(ili $|1\rangle$) bila je jednaka $\frac{1}{2}$. Mjerenjem svoja dva qubita, na primjer s ishodom 00, Alice je "promijenila" tu vjerojatnost (slično kao i kod EPR paradoksa), ona sada iznosi $|\alpha|^2$. Taj fenomen ne bi bio moguć da stanje $|\Psi_2\rangle$ nije bilo spregnuto.

3.5 Heisenbergova relacija neodređenosti

Lako je izračunati prosjek (očekivanje) projektivnog mjerenja

$$\langle M\rangle := \sum_m mp(m) = \sum_m m\,\langle\Psi|P_m|\Psi\rangle = \left\langle \Psi \middle| \sum_m mP_m \middle| \Psi \right\rangle = \langle\Psi|M|\Psi\rangle\,,$$

kao i standardnu devijaciju

$$[\Delta(M)]^2 = \left\langle (M - \langle M\rangle)^2 \right\rangle = \left\langle M^2 - 2\,\langle M\rangle\, M + \langle M\rangle^2 \right\rangle = \left\langle M^2\right\rangle - \langle M\rangle^2\,.$$

Ova definicija ima smisla jer je M^2 opservabla kao i M.

Za operatore C i D uvedimo oznake $[C, D] = CD - DC$ i $\{C, D\} = CD + DC$. Poznata Heisenbergova relacija neodređenosti može se ovako precizno matematički formulirati.

Teorem 3.11 (Heisenbergova relacija neodređenosti)**.** *Neka su C i D dvije opservable i $|\Psi\rangle$ proizvoljno stanje. Tada vrijedi*

$$\Delta(C)\Delta(D) \geq \frac{|\,\langle\Psi|[C, D]|\Psi\rangle\,|}{2}.$$

Intuitivno, ako pripremimo velik broj identičnih stanja $|\Psi\rangle$ i neka od njih mjerimo s C, a neka s D, tada će standardne devijacije tih mjerenja $\Delta(C)$ i $\Delta(D)$ zadovoljavati nejednakost iz teorema.

Dokaz teorema. Označimo sa $A := C - \langle C\rangle\, I$ i $B := D - \langle D\rangle\, I$ (pa je $\langle A\rangle = \langle B\rangle = 0$). Pretpostavimo da je $\langle\Psi|AB|\Psi\rangle = x + iy$, gdje su

$x, y \in \mathbb{R}$. Kako je $AB = \frac{1}{2}\left([A,B] + \{A,B\}\right)$, imamo

$$\langle\Psi|AB|\Psi\rangle = \frac{1}{2}\langle\Psi|[A,B]|\Psi\rangle + \frac{1}{2}\langle\Psi|\{A,B\}|\Psi\rangle = x + iy.$$

Budući da su operatori $\{A,B\}$ i $[A,B]$ redom hermitski i antihermitski (dokažite), vrijedi da je $\langle\Psi|[A,B]|\Psi\rangle = 2iy$ i $\langle\Psi|\{A,B\}|\Psi\rangle = 2x$. Naime, za hermitski operator H općenito vrijedi

$$\overline{\langle H\Psi|\Psi\rangle} = \langle\Psi|H|\Psi\rangle = \left\langle H^\dagger\Psi\middle|\Psi\right\rangle = \langle H\Psi|\Psi\rangle\,,$$

iz čega slijedi da je $\langle H\Psi|\Psi\rangle \in \mathbb{R}$. Slično, za antihermitski G vrijedi da je $\langle\Psi|G\Psi\rangle \in i\mathbb{R}$, pa tvrdnja slijedi. Sada iz $4y^2 + 4x^2 = 4(x^2+y^2)$ slijedi

$$|\langle\Psi|[A,B]|\Psi\rangle|^2 + |\langle\Psi|\{A,B\}|\Psi\rangle|^2 = 4|\langle\Psi|AB|\Psi\rangle|^2. \tag{3.1}$$

Iz Cauchy-Schwarzove nejednakosti (i činjenice da su A i B hermitski operatori) slijedi

$$|\langle\Psi|AB|\Psi\rangle|^2 = |\langle A\Psi|B\Psi\rangle|^2 \leq \langle A\Psi|A\Psi\rangle\langle B\Psi|B\Psi\rangle = \left\langle\Psi\middle|A^2\middle|\Psi\right\rangle\left\langle\Psi\middle|B^2\middle|\Psi\right\rangle.$$

Uvrštavanjem u (3.1) dobivamo

$$\frac{1}{4}\left(|\langle\Psi|[A,B]|\Psi\rangle|^2 + |\langle\Psi|\{A,B\}|\Psi\rangle|^2\right) \leq \left\langle\Psi\middle|A^2\middle|\Psi\right\rangle\left\langle\Psi\middle|B^2\middle|\Psi\right\rangle.$$

Kako je $\langle A\rangle = \langle B\rangle = 0$, pa onda i $\Delta(A) = \left\langle A^2\right\rangle$ odnosno $\Delta(B) = \left\langle B^2\right\rangle$, slijedi

$$\Delta(A)\Delta(B) \geq \frac{1}{2}|\langle\Psi|[A,B]|\Psi\rangle|.$$

Iz konstrukcije operatora A i B slijedi da je $\Delta(A) = \Delta(C)$, $\Delta(B) = \Delta(D)$ i $[A,B] = [C,D]$ (provjerite), pa tvrdnja teorema slijedi. □

O Heisenbergovoj relaciji neodređenosti puno se filozofira u popularnoznanstvenoj literaturi – često pogrešno i neprecizno. Tako, na primjer, na Wikipediji piše:

> Prema Heisenbergovim relacijama neodređenosti, nemoguće je oboje, položaj i količinu gibanja (na primjer elektrona), odrediti apsolutno točno, čak ni idealnim hipotetičkim pokusom, jer se postupkom mjerenja položaja nužno remeti količina gibanja, i obratno.

Spomenimo još primjer kvantnog sustava koji opisuje gibanje elektrona po pravcu (njegov položaj i količinu gibanja). Primijetimo da je prostor stanja tog sustava beskonačno dimenzionalan (jer je npr. skup položaja na kojima se elektron može nalaziti beskonačan), pa se onda očekivanje opservabli definira preko integrala. Bez ulaženja u detalje, opservable A i B koje redom odgovaraju projektivnim mjerenjima položaja i količine gibanja elektrona ne komutiraju, preciznije vrijedi $[A, B] = i\hbar I$ pa je desna strana relacije neodređenosti za svaki vektor stanja $|\Psi\rangle$ jednaka $\hbar/2$, odnosno, slijedi da je $\Delta(A)\Delta(B) \geq \frac{\hbar}{2}$.

Pretpostavimo da elektronu poznajemo proizvoljno točno položaj i količinu gibanja (npr. to smo zaključili iz rezultata nekog mjerenja) – znamo da su ϵ-blizu x_0 i p_0 za neki mali ϵ. Što to znači? Ako sa $|\Psi\rangle$ označimo vektor stanja tog elektrona, onda ćemo mjerenjem položaja stanja $|\Psi\rangle$ preko opservable A dobiti vrijednost koja je ϵ-blizu x_0 (slično i za B, vrijednost mjerenja bit će ϵ-blizu p_0). Posebno to znači da će standardne devijacije $\Delta(A)$ i $\Delta(B)$ (istovremeno) biti manje od ϵ, što je u kontradikciji s relacijom neodređenosti za $\epsilon < \sqrt{\frac{\hbar}{2}}$.

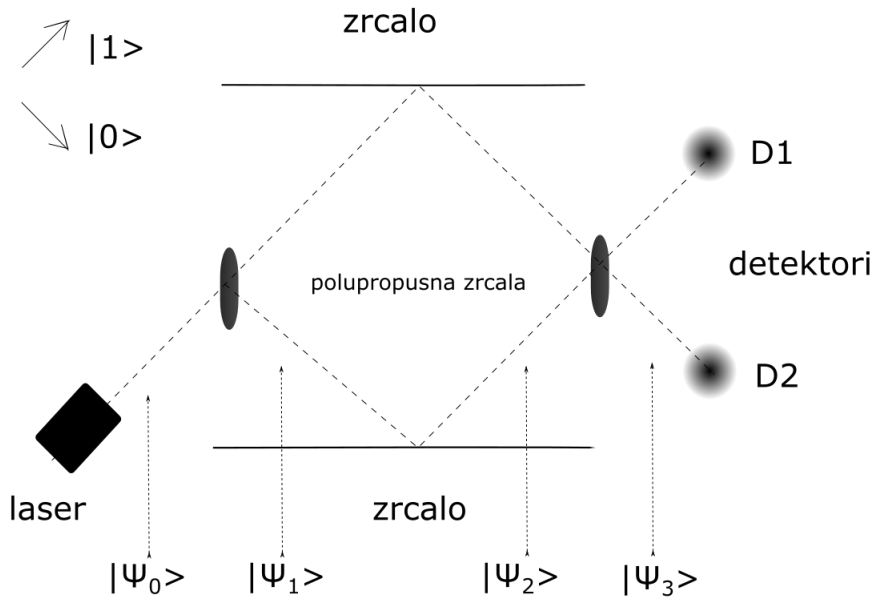
Uočimo da je pogrešno (ili barem nepotrebno) govoriti da ne možemo istovremeno znati položaj i količinu gibanja elektrona zbog toga što postupak mjerenja položaja remeti količinu gibanja (odnosno brzinu) jer su neodređenosti u mjerenju položaja i brzine ($\Delta(A)$ i $\Delta(B)$ redom) fundamentalna svojstva kvantnog sustava neovisna od toga kako točno mjerimo te opservable.

4 Primjeri kvantnih sustava

4.1 Elitzur-Vaidmanovo testiranje bombi

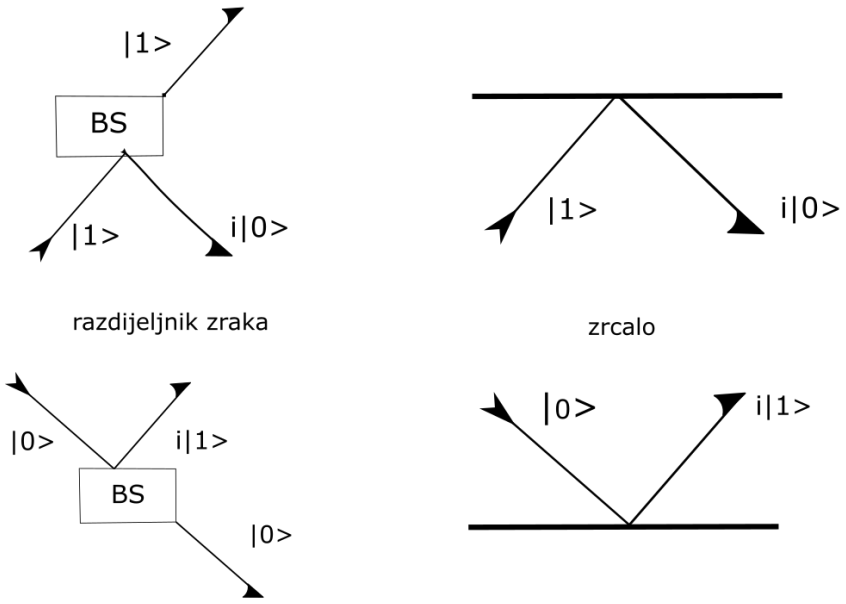
Vlasnik ste tvornice koja proizvodi bombe. Bomba ima fotodetektor koji ju aktivira, osim ako je neispravna, u tom slučaju foton samo prođe kroz bombu kao da je nema. Možete li ispitati ispravnost bombe bez da ju aktivirate? Čini se nemoguće, ali je odgovor potvrdan.

Promotrimo sljedeći sklop.



Slika 8: Mach-Zehnderov interferometar

Osim lasera koji emitira pojedinačne fotone i dva detektora D_1 i D_2, sklop se još sastoji od polupropusnog zrcala BS koje ima funkciju razdjelnika zraka (foton ima vjerojatnost 50% za prolazak, a 50% za refleksiju) i običnog zrcala. Ako se foton giba prema gore, reći ćemo da se nalazi u stanju $|1\rangle$, a ako se giba prema dolje, onda je u stanju $|0\rangle$. Početno stanje je $|\Psi_0\rangle = |1\rangle$. Zrcala djeluju kao kvantna vrata kao što je opisano na Slici 9. Polupropusno zrcalo u standardnoj bazi opisujemo matricom $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$, a obično zrcalo matricom $\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Izračunajmo stanje



Slika 9: Razdjelnik i zrcalo kao kvantna vrata

sustava prije mjerenja (detektori D_0 i D_1 realiziraju mjerenje qubita u standardnoj bazi)

$$
\begin{aligned}
|\Psi_0\rangle &= |1\rangle\,, \\
|\Psi_1\rangle &= \frac{1}{\sqrt{2}}(i\,|0\rangle + |1\rangle), \\
|\Psi_2\rangle &= \frac{1}{\sqrt{2}}(-\,|1\rangle + i\,|0\rangle), \\
|\Psi_3\rangle &= \frac{1}{\sqrt{2}}\left[i\frac{1}{\sqrt{2}}(|0\rangle + i\,|1\rangle) - \frac{1}{\sqrt{2}}(i\,|0\rangle + |1\rangle)\right] = \frac{1}{2}(-2\,|1\rangle) = -\,|1\rangle\,.
\end{aligned}
$$

Dakle, detektor D_1 aktivirat će se prolaskom fotona kroz sklop.

Postavimo sada bombu u Mach-Zehnderov interferometar dolje između prvog polupropusnog zrcala i običnog zrcala. Dvije su mogućnosti:

- Ako je bomba neispravna, onda kao da je nema, aktivirat će se detektor D_1.

- Ako je bomba ispravna, u 50% slučajeva bomba će eksplodirati, a u 25% slučajeva aktivirat će se detektor D_0 (kao i detektor D_1). Kad se to dogodi, sa sigurnošću možemo reći da je bomba prava.

Ako je bomba ispravna i ako nije eksplodirala (to će se dogoditi u 50% slučajeva), onda je foton na polupropusnom zrcalu "produžio" ravno, tj. $|\Psi_1\rangle = |1\rangle$. Zrcalo mijenja stanje u $|\Psi_2\rangle = i\,|0\rangle$, dok je završno stanje jednako $|\Psi_3\rangle = \frac{1}{\sqrt{2}}\,(i\,|0\rangle + |1\rangle)$. Stoga, mjerenjem tog stanja vidimo da je vjerojatnost detekcije fotona detektorom D_0 jednaka $\frac{1}{2}$.

Zadatak 4.1. Možete li osmisliti uspješniji algoritam od ovog?

Napomena 4.2. Zainteresirani čitatelj može u knjizi [Ana18] pronaći još nekoliko sličnih eksperimenata koji pokazuju svu čudnovatost naše kvantne stvarnosti.

4.2 Bellov teorem

Jedno od najzanimljivijh "filozofskih" pitanja povezanih s kvantnom mehanikom jest ono o prirodi vjerojatnosti koje se javljaju kod mjerenja. Jesu li te vjerojatnosti (odnosno nedostatak determinizma) odraz našeg neznanja (kao što je to na primjer slučaj kod bacanja novčića – to što mi ne možemo predvidjeti hoće li pasti pismo ili glava ne znači da netko drugi s više informacija o eksperimentu to ne bi mogao učiniti) ili fundamentalno svojstvo svemira u kojem živimo? Već smo spomenuli da su Einstein, Podolsky i Rosen još 1935. zbog paradoksalnih svojstava kvantne spregnutosti tvrdili da je problem u našem neznanju, odnosno da je kvantna mehanika nepotpuna teorija (najviše zbog toga "jezivog" djelovanja na daljinu). Na prvu nije baš jasno kako bi se uopće znanstveno pristupilo tom pitanju i zaista za prvi značajan pomak prema rješenju trebalo je pričekati skoro trideset godina. Fizičar J. S. Bell je 1964. u članku "On the Einstein Podolsky Rosen Paradox" pokazao da Einstein nije bio u pravu. Njegov teorem H. Stapp označio je kao najdublje otkriće u znanosti, dok su J. Clauser i A. Aspect 2022. g. podijelili Nobelovu nagradu za fiziku (zajedno s A. Zeilingerom koji je bio

nagrađen za rad na kvantnoj teleportaciji) za eksperimentalnu potvrdu Bellovih nejednakosti. Eksperiment je vrlo jednostavno opisati.

Pretpostavimo da Alice i Bob (prostorno jako udaljeni) dijele dva qubita u stanju $|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$. Alice na svom qubitu može mjeriti opservable $Q := Z_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$ i $R = X_1 = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, dok Bob na svom mjeri opservable $S = \frac{-Z_2 - X_2}{\sqrt{2}} = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} -1 & -1 \\ -1 & 1 \end{smallmatrix}\right)$ i $T = \frac{Z_2 - X_2}{\sqrt{2}} = \frac{1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & -1 \\ -1 & -1 \end{smallmatrix}\right)$. Svojstvene vrijednosti operatora Q, R, S i T su ± 1, pa su i mogući ishodi svih mjerenja, označit ćemo ih također s Q, R, S i T, jednaki ± 1 (prisjetimo se, kod projektivnih mjerenja ishodi mjerenja svojstveni su vektori, odnosno, svojstvene vrijednosti opservable). U jednom koraku eksperimenta Alice od dva mjerenja slučajno odabere jedno koje će izvršiti, isto tako i Bob. Nakon mjerenja zapišu rezultat i ponavljaju cijeli postupak, ovaj put na novom paru qubita koji se također nalaze u stanju $|\Psi\rangle$. Na osnovu dobivenih podataka, kad se ponovno sretnu, mogu procijeniti očekivanja slučajnih varijabli $\langle Q \cdot S \rangle$, $\langle Q \cdot T \rangle$, $\langle R \cdot S \rangle$ i $\langle R \cdot T \rangle$ (na primjer, za procjenu očekivanja $\langle QS \rangle$ Alice i Bob pogledaju rezultate mjerenja onih koraka u kojima je Alice odabrala Q, a Bob S i izračunaju prosjek produkta ishoda). Velik broj provedenih eksperimenata u zadnjih tridesetak godina pokazao je da se rezultati podudaraju s predviđanjima kvantne mehanike. Vrijedi da je $\langle Q \cdot S \rangle = \langle R \cdot S \rangle = \langle R \cdot T \rangle = \frac{1}{\sqrt{2}}$ dok je $\langle Q \cdot T \rangle = -\frac{1}{\sqrt{2}}$.

Primjer. Pokažimo da je $\langle QS \rangle = \frac{1}{\sqrt{2}}$. Vrijedi da je $\langle QS \rangle = \langle \Psi | Q \otimes S | \Psi \rangle$ (zašto?), gdje je $Q \otimes S = \frac{-1}{\sqrt{2}} \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \otimes \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. Računamo

$$\begin{aligned} (Q \otimes S) |\Psi\rangle &= \frac{-1}{2} \left(|0\rangle \left(|0\rangle - |1\rangle \right) + |1\rangle \left(|0\rangle + |1\rangle \right) \right) \\ &= \frac{1}{2} \left(- |00\rangle + |01\rangle - |10\rangle - |11\rangle \right). \end{aligned}$$

Slijedi da je

$$\langle QS \rangle = \left\langle \Psi \middle| \frac{1}{2} \left(- |00\rangle + |01\rangle - |10\rangle - |11\rangle \right) \right\rangle = \frac{1}{\sqrt{2}} \cdot \frac{1}{2} + \frac{1}{\sqrt{2}} \cdot \frac{1}{2} = \frac{1}{\sqrt{2}}.$$

Sada dolazimo do glavnog dijela. Pretpostavimo da postoji netko, recimo Eve, tko zna rezultate svih mjerenja još prije nego što ih Alice

i Bob odaberu i provedu. Dakle, Eve za svaki eksperiment na listiću ima upisana četiri broja, npr. $(Q, R, S, T) = (1, -1, -1, 1)$ tako da ako npr. Alice u tom koraku odabere Q, a Bob T, Eve zna da će oni redom izmjeriti 1 i 1. Nije bitno kako Eve to zna, ako hoćete možete zamisliti da Eve ima pristup nekoj boljoj teoriji od kvantne mehanike koja joj omogućava da rezultate svih eksperimenata sa sigurnošću predvidi. Ovdje zamišljamo da su Alice i Bob dovoljno udaljeni jedno od drugog tako da ishod jednog mjerenja ne utječe na ishod drugog (u tom slučaju kažemo da teorija ima svojstvo lokalnosti, primjer takve teorije je teorija relativnosti). U svakom slučaju, budući da Eve ima pristup ishodima svih eksperimenata, ona može u svakom koraku izračunati broj

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T.$$

Budući da očekivanja slučajnih varijabli QS, RS, RT i QT (eksperimentalno) postoje i podudaraju se s predviđanjima kvantne mehanike, slijedi i da slučajna varijabla $QS + RS + RT - QT$ ima očekivanje i da je ono jednako

$$\langle QS + RS + RT - QT \rangle = \langle QS \rangle - \langle QT \rangle + \langle RS \rangle + \langle RT \rangle = 2\sqrt{2} > 2.$$

Međutim, upravo smo dobili kontradikciju jer se lako provjeri (na primjer uvrštavanjem) da je

$$QS + RS + RT - QT = (Q + R)S + (R - Q)T = \pm 2,$$

pa očekivanje ne može biti veće od 2.

Kako je ovo moguće? Koja je od naših pretpostavki pogrešna?

Napomena 4.3. Filozofsku raspravu o posljedicama Bellovog teorema zainteresiran čitatelj može potražiti u [GNTZ11]. O neočekivanoj vezi između Bellove nejednakosti i ne-lokalnih igara kao i o generiranju slučajnih brojeva pomoću ideja kvantne mehanike može se pročitati u popularno pisanim člancima [Aarb, Aara]. Spomenimo još i Kochen-Speckerov teorem [KS75], koji (komplementarno Bellovom teoremu) pokazuje da je kontekstualnost nužno svojstvo svih teorija skrivenih varijabli.

5 Univerzalnost kvantnih vrata

Iz klasičnog računarstva poznato nam je da se svaka logička funkcija $f : \{0,1\}^n \to \{0,1\}$ može implementirati koristeći samo AND, OR i NOT vrata. Za skup vrata s tim svojstvom kažemo da je univerzalan za klasično računanje.

Zadatak 5.1. Pokažite da su vrata NAND univerzalna za klasično računanje.

U ovom odjeljku govorit ćemo o univerzalnosti kvantnih vrata. Budući da unitarnih operatora na prostorima stanja ima neprebrojivo mnogo, ne možemo, kao u klasičnom računarstvu, konačnim skupom vrata opisati sva kvantna vrata, ali ih možemo proizvoljno dobro aproksimirati. Skupove s tim svojstvom zvat ćemo *univerzalnima* za kvantno računanje.

Pretpostavimo da je U unitaran operator koji želimo aproksimirati operatorom V (na primjer, V je operator sklopa koji smo konstruirali pomoću vrata iz fiksnog (konačnog) skupa vrata), definirajmo grešku

$$E(U,V) = \max_{|\Psi\rangle} \|(U-V)\,|\psi\rangle\|,$$

gdje gledamo maksimum po svim normaliziranim vektorima $|\psi\rangle$ iz prostora stanja.

Intuitivno, operatori za koje je greška $E(U,V)$ mala imat će slične statistike mjerenja. Preciznije, fiksirajmo jedno projektivno mjerenje opisano opservablom $M = \sum mP_m$ zajedno s jednim ishodom mjerenja m (odnosno, svojstvenu vrijednost hermitskog operatora M) i jedan vektor stanja $|\psi\rangle$. Označimo s P_U i P_V vjerojatnosti ishoda m pri mjerenju stanja $U\,|\psi\rangle$ i $V\,|\psi\rangle$ redom, tj. $P_U = \langle U\psi|P_m|U\psi\rangle = \langle\psi|U^\dagger P_m U|\psi\rangle$ i analogno za P_V. S malo algebre i jednostavnom primjenom Cauchy-Schwarzove nejednakosti dobivamo

$$|P_U - P_V| \leq 2E(U,V),$$

pa vidimo da greška $E(U,V)$ uistinu kontrolira vjerojatnosti ishoda mjerenja.

Zadatak 5.2. Dokažite prethodnu nejednakost.

Zadatak 5.3. Dokažite da je

$$E(U_m U_{m-1} \dots U_1, V_m V_{m-1} \dots V_1) \leq \sum_{i=1}^{n} E(U_i, V_i).$$

Prethodni zadatak možemo ovako interpretirati. Ako svaki od m "potprograma" U_i ϵ-dobro aproksimiramo sklopom V_i (tj. $E(U_i, V_i) \leq \epsilon$) koji je, na primjer, konstruiran iz fiksnog konačnog skupa vrata, onda cijeli program možemo $m\epsilon$-dobro aproksimirati s kompozicijom svih sklopova – greška se povećava najviše linearno s brojem sklopova.

Osim ranije definiranih Hadamardovih H, $CNOT$ i $S = \left(\begin{smallmatrix} 1 & 0 \\ 0 & i \end{smallmatrix}\right)$ vrata, za konstrukciju univerzalnog skupa trebat će nam i $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & e^{2\pi i/8} \end{smallmatrix}\right)$ vrata (koja još zovemo "$\pi/8$" vrata). U ovom odjeljku dokazat ćemo sljedeći teorem.

Teorem 5.4. *Hadamardova H, $CNOT$, S i "$\pi/8$" vrata čine univerzalni skup vrata za kvantno računanje. Preciznije, za svaki unitaran operator U i svaki $\epsilon > 0$ postoji kvantni sklop V koji se sastoji samo od prije spomenutih vrata takav da je $E(U, V) \leq \epsilon$.*

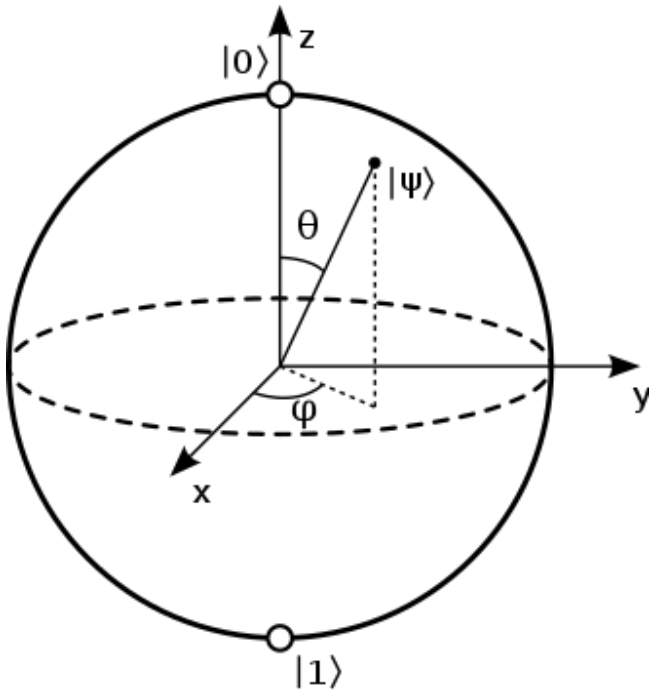
Prvo ćemo istražiti univerzalnost operatora koji djeluju samo na jedan qubit.

5.1 Blochova sfera i kvantna vrata koja djeluju na jedan qubit

Kvantna vrata koja djeluju na jedan qubit (odnosno unitarni operatori na dvodimenzionalnom kompleksnom prostoru) mogu se elegantno opisati preko rotacija sfere – ta se geometrijska reprezentacija prema fizičaru Felixu Blochu naziva Blochova sfera.

Proizvoljno stanje $|\Psi\rangle = e^{i\psi}(a\,|0\rangle + b\,|1\rangle)$, gdje smo realnu fazu ψ odabrali tako da je a realan broj, reprezentiramo na jediničnoj sferi u $\mathbb{R}^3$ točkom sa sfernim koordinatama (θ, ϕ)

$$(\cos\phi \sin\theta, \sin\phi \sin\theta, \cos\theta) \in \mathbb{R}^3,$$



Slika 10: Blochova sfera

Izvor: Smite-Meister, CC BY-SA 3.0, via Wikimedia Commons

gdje je $a = \cos\frac{\theta}{2}$ i $b = e^{i\phi}\sin\frac{\theta}{2}$.

Prisjetimo se matrica (koje još zovemo Paulijevim matricama)

$$X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right), Y = \left(\begin{smallmatrix} 0 & -i \\ i & 0 \end{smallmatrix}\right) \quad \text{i} \quad Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right),$$

pomoću kojih definiramo unitarne operatore

$$R_x(\theta) = e^{-i\theta X/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}X = \begin{pmatrix} \cos\theta/2 & -i\sin\theta/2 \\ -i\sin\theta/2 & \cos\theta/2 \end{pmatrix},$$
$$R_y(\theta) = e^{-i\theta Y/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Y = \begin{pmatrix} \cos\theta/2 & -\sin\theta/2 \\ \sin\theta/2 & \cos\theta/2 \end{pmatrix},$$
$$R_z(\theta) = e^{-i\theta Z/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}Z = \begin{pmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{pmatrix}.$$

Općenitije, za proizvoljan jedinični vektor $\hat{n} = (n_x, n_y, n_z) \in \mathbb{R}^3$ i vektor $\vec{\sigma} = (X, Y, Z)$ Paulijevih matrica definiramo

$$R_{\hat{n}}(\theta) = e^{-i\theta\hat{n}\cdot\vec{\sigma}/2} = \cos\frac{\theta}{2}I - i\sin\frac{\theta}{2}(n_xX + n_yY + n_zZ).$$

Razlog zašto uvodimo sve ove pojmove je sljedeći teorem.

Teorem 5.5. *Neka je $|\psi\rangle$ vektor stanja i $\vec{\psi}$ njemu odgovarajući vektor na Blochovoj sferi. Tada stanju $R_{\hat{n}}(\theta)|\psi\rangle$ odgovara vektor na Blochovoj sferi koji se dobije rotacijom vektora $\vec{\psi}$ za kut θ oko osi određene vektorom $\hat{n}$. Drugim riječima, unitarni operator $R_{\hat{n}}(\theta)$ odgovara operatoru rotacije (za kut θ oko osi $\hat{n}$) na Blochovoj sferi.*

Ovaj teorem daje nam potpuno razumijevanje unitarnih operatora koji djeluju na jedan qubit preko operatora rotacija u $\mathbb{R}^3$ jer vrijedi sljedeća propozicija.

Propozicija 5.6. *Svaki unitaran operator U na $\mathbb{C}^2$ može se zapisati u obliku*

$$U = e^{i\alpha}R_{\hat{n}}(\theta),$$

za neke $\alpha, \theta \in \mathbb{R}$ i jedinični vektor $\hat{n} \in \mathbb{R}^3$.

Sada sva pitanja o unitarnim operatorima na $\mathbb{C}^2$ (koja nas zanimaju u kvantnom računarstvu) možemo svesti na operatore rotacija u $\mathbb{R}^3$ (globalnu fazu $e^{i\alpha}$ možemo zanemariti jer nije fizikalno mjerljiva), što je velika prednost zbog geometrijske intuicije koju imamo o trodimenzionalnom prostoru.

Zadatak 5.7. Dokažite Teorem 5.5 i Propoziciju 5.6.

Zadatak 5.8. Odredite α, θ i $\hat{n}$ iz Propozicije 5.6 za

a) Hadamardova vrata H i

b) fazna vrata S.

Dokazat ćemo sljedeći teorem.

Teorem 5.9. *Hadamardova H i "$\pi/8$" vrata čine univerzalan skup vrata za unitarne operatore koji djeluju na jednom qubitu.*

Dokaz. Promotrimo kako operatori T i HTH djeluju na Blochovu sferu. Kako je $T = e^{\pi i/8}\begin{pmatrix} e^{-\pi i/8} & 0 \\ 0 & e^{\pi i/8} \end{pmatrix} = e^{\pi i/8} R_z(\pi/4)$, vidimo da "$\pi/8$" vrata odgovaraju rotaciji na Blochovoj sferi za kut $\pi/4$ oko z osi. Slično, vrata HTH odgovaraju rotaciji za kut $\pi/4$ oko x osi (provjerite!). Komponirajući ova dva operatora dobivamo operator $THTH$ koji je do na globalnu fazu jednak

$$\begin{aligned} e^{-i\frac{\pi}{8}Z} e^{-i\frac{\pi}{8}X} &= \left[\cos\frac{\pi}{8} I - i \sin\frac{\pi}{8} X\right]\left[\cos\frac{\pi}{8} I - i\sin\frac{\pi}{8} Z\right] \\ &= \cos^2\frac{\pi}{8} I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8} Y\right]\sin\frac{\pi}{8} \\ &= \cos^2\frac{\pi}{8} I - i\sin\frac{\pi}{8}\sqrt{1+\cos^2\frac{\pi}{8}} \cdot \frac{\cos\frac{\pi}{8}X + \sin\frac{\pi}{8}Y + \cos\frac{\pi}{8}Z}{\sqrt{1+\cos^2\frac{\pi}{8}}} \\ &= \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2} \cdot \frac{\cos\frac{\pi}{8}X + \sin\frac{\pi}{8}Y + \cos\frac{\pi}{8}Z}{\sqrt{1+\cos^2\frac{\pi}{8}}} \\ &= R_{\hat{n}}(\theta), \end{aligned}$$

gdje je $\theta \in \mathbb{R}$ takav da je $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$ (tada je $\sin\frac{\theta}{2} = \sin\frac{\pi}{8}\sqrt{1+\cos^2\frac{\pi}{8}}$) i $\hat{n} = \frac{(\cos\frac{\pi}{8},\sin\frac{\pi}{8},\cos\frac{\pi}{8})}{\sqrt{1+\cos^2\frac{\pi}{8}}}$. Ključna činjenica (iz teorije brojeva, nećemo ju dokazati) jest da je broj $\frac{\theta}{\pi}$ iracionalan. Tada, po Dirichletovom principu, svaki kut $\alpha \in [0, 2\pi\rangle$ možemo proizvoljno dobro aproksimirati (modulo 2π) višekratnicima od θ oblika $k \cdot \theta$ za $k \in \mathbb{Z}$, što implicira da svaku rotaciju $R_{\hat{n}}(\alpha)$ možemo proizvoljno dobro aproksimirati s $R_{\hat{n}}(\theta)^k$. Lako se izračuna da za svaki $\beta \in \mathbb{R}$ vrijedi $HR_{\hat{n}}(\beta)H = R_{\hat{m}}(\beta)$, gdje je $\hat{m} = \frac{(\cos\frac{\pi}{8},-\sin\frac{\pi}{8},\cos\frac{\pi}{8})}{\sqrt{1+\cos^2\frac{\pi}{8}}}$ (izračunajte to), pa onda s potencijama od $R_{\hat{m}}(\theta)$ možemo proizvoljno dobro aproksimirati svaku rotaciju $R_{\hat{m}}(\alpha)$.

Tvrdnja slijedi iz sljedećeg zadatka. □

Zadatak 5.10. Neka su $\hat{n}$ i $\hat{m}$ linearno nezavisni jedinični vektori iz $\mathbb{R}^3$. Dokažite da se proizvoljan unitarni operator U (na $\mathbb{C}^2$) može zapisati

$$U = e^{i\alpha}R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta),$$

za neke realne brojeve α, β, γ i δ.

Kasnije kod dokaza univerzalnosti trebat će nam i ova tvrdnja.

Zadatak 5.11. Neka je U proizvoljan unitarni operator na $\mathbb{C}^2$. Dokažite da tada postoje operatori A, B i C na istom prostoru i $\alpha \in \mathbb{R}$ takvi da je $ABC = I$ i $U = e^{i\alpha}AXBXC$.

5.2 Redukcija na unitarne operatore nivoa dva i univerzalnost

Za unitaran operator U koji djeluje na d-dimenzionalnom kompleksnom unitarnom prostoru V s **fiksnom** bazom $\{v_1, \ldots, v_d\}$ kažemo da je nivoa dva ako postoje vektori $\{v_i, v_j\}$, $i \neq j$ takvi da je restrikcija od U na ortogonalni komplement 2-dimenzionalnog potprostora $\langle v_i, v_j\rangle := \mathbb{C}v_i \oplus \mathbb{C}v_j$ identiteta (budući da je baza od V fiksna, zapravo smo definirali pojam matrice nivoa dva). Pokazat ćemo da se proizvoljan unitaran operator U može prikazati kao kompozicija unitarnih operatora nivoa

dva pa ćemo time dokaz Teorema 5.4 svesti na slučaj kad je U unitaran operator nivoa dva.

Cilj nam je pronaći unitarne operatore $U_1, U_2, \cdots U_m$ nivoa dva takve da je $U_m U_{m-1} \cdots U_1 U = I$ jer je tada $U = U_1^\dagger \cdots U_m^\dagger$ traženog oblika. Dokaz provodimo induktivno. Za $v = v_1 \in V$ pokazat ćemo da postoje $U_1, U_2, \cdots U_m$ nivoa dva takvi da je $U_m U_{m-1} \cdots U_1 U v = v$. Ako sa V' označimo ortogonalni komplement od v u V, tada cijeli postupak ponavljamo za $V = V'$, $U = (U_m U_{m-1} \cdots U_1 U)|_{V'}$ i $v = v_2$ sve dok ne dobijemo da je kompozicija identiteta na cijelom prostoru.

Dakle, neka je dan $v = v_1 \in V$. Neka je U_1 unitaran operator na $\langle u_1, u_2 \rangle$ (koji je na ortogonalnom komplementu tog potprostora identiteta) takav da je $U_1 U v = \lambda v_1$ za neki $\lambda \in \mathbb{C}$. Operator U_1 možemo odabrati tako da odgovara rotaciji Blochove sfere potprostora $\langle v_1, v_2 \rangle$ koja projekciju vektora Uv na $\langle v_1, v_2 \rangle$ "zarotira" na vektor v_1 (za os rotacije možemo odabrati simetralu kuta koji koordinatna os v_1 zatvara s projekcijom vektora Uv na $\langle v_1, v_2 \rangle$, dok je kut rotacije jednak π). Radi jednostavnosti pisanja kad kažemo kut između dva vektora iz $\langle v_1, v_2 \rangle$, mislimo na kut između odgovarajućih vektora na Blochovoj sferi. Induktivno, odaberemo unitarni operator U_2 na $\langle v_1, v_3 \rangle$ koji projekciju vektora $U_1 U v$ na $\langle v_1, v_3 \rangle$ "zarotira" u v_1 i tako sve do unitarnog operatora U_{d-1} koji projekciju vektora $U_{d-2} U_{d-3} \ldots U_1 U v$ na $\langle v_1, v_d \rangle$ "zarotira" u v_1. Slijedi da je $U_{d-1} U_{d-2} \ldots U_1 U v = \lambda v$ za neki $\lambda \in \mathbb{C}$, odnosno dokazali smo sljedeći teorem.

Teorem 5.12. *Svaki unitaran operator na d-dimenzionalnom kompleksnom unitarnom prostoru s fiksnom bazom $\{v_1, v_2, \ldots, v_d\}$ može se prikazati kao kompozicija*

$$U = U_1 U_2 \ldots U_m,$$

gdje su U_i unitarni operatori nivoa dva (u odnosu na fiksnu bazu).

5.3 Univerzalnost skupa vrata $\{CNOT, H, T\}$

Pretpostavimo da je U unitarni operator nivoa dva na prostoru stanja n qubita s fiksnom standardnom bazom koja se sastoji od vektora

$|s\rangle = |s_1 s_2 \dots s_n\rangle$ za $s \in \{0, 1, \dots, 2^n - 1\}$. Nadalje, pretpostavimo da U djeluje netrivijalno na potprostor razapet vektorima $|s\rangle$ i $|t\rangle$ gdje su $s = s_1 s_2 \dots s_n$ i $t = t_1 t_2 \dots t_n$ binarni zapisi brojeva $s, t \in \{0, 1, \dots 2^n - 1\}$. U ovom odjeljku cilj nam je pokazati da se U može implementirati koristeći samo $CNOT$ vrata i vrata koja djeluju na jedan qubit. Tada će iz prethodna dva odjeljka slijediti univerzalnost skupa vrata $\{CNOT, H, T\}$.

Za konstrukciju ćemo koristiti Grayov kod.

Definicija 5.13. *Za dana dva različita binarna broja s n znamenaka s i t, Grayov kod niz je binarnih brojeva koji počinje s s, a završava s t takav da se svaka dva uzastopna člana niza razlikuju u točno jednom bitu.*

Primjer. Ako je $s = 000$ i $t = 111$, tada je jedan Grayov kod jednak nizu

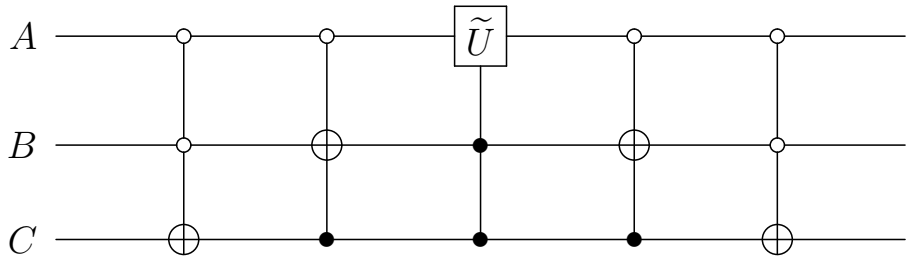
$$\begin{aligned} & ABC \\ g_1 =& 0\,0\,0 (= s) \\ g_2 =& 0\,0\,1 \\ g_3 =& 0\,1\,1 \\ g_4 =& 1\,1\,1 (= t). \end{aligned}$$

Ideju konstrukcije najlakše je objasniti na primjeru. Neka je $n = 3$ i neka je U u standardnoj bazi dan matricom

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix},$$

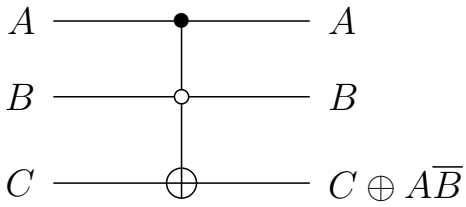
gdje su $a, b, c, d \in \mathbb{C}$ takvi da je matrica $\widetilde{U} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ unitarna.

Primijetimo da U netrivijalno djeluje samo na potprostor razapet vektorima $|000\rangle$ i $|111\rangle$. Restrikcija od U na taj potprostor je $\widetilde{U}$. Promotrimo sklop na Slici 11 i uvjerimo se da implementira operator U.



Slika 11: Implementacija operatora U. Bijela (odnosno crna) točkica u kontroliranim vratima označava da će se vrata "izvršiti" ako je odgovarajući qubit u stanju $|0\rangle$ (odnosno $|1\rangle$).

U konstrukciji smo koristili generalizirana $CNOT$ vrata (Slika 12) kao i dvostruko kontrolirana $\tilde{U}$ vrata (vrata $\tilde{U}$ djelovat će na treći qubit ako i samo ako su prva dva u stanju $|1\rangle$, vidi Sliku 13).



Slika 12: Generalizirana CNOT vrata

Ključno je primijetiti da će se vrata $\widetilde{U}$ izvršiti jedino ako na njih kao input dođu vektori $|011\rangle$ ili $|111\rangle$. Budući da su vrata koja se nalaze prije $\widetilde{U}$ vrata sama sebi inverz, lako se vidi (i to je ono za što nam je trebao Grayov kod) da će se to dogoditi upravo onda kad je input programa jednak $|000\rangle$ i $|111\rangle$ redom. Nakon izvršavanja kontroliranih $\widetilde{U}$ vrata ponavljamo operatore koji su im prethodili da bismo "vratili" vektore $|011\rangle$ i $|111\rangle$ natrag u vektore $|000\rangle$ i $|111\rangle$.

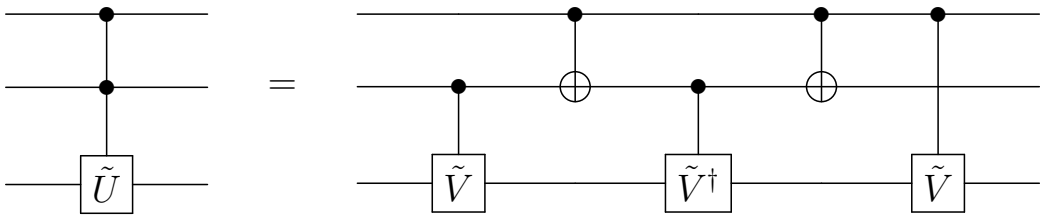
Analogno se implementira proizvoljan unitaran operator stupnja dva.

Zadatak 5.14. Konstruirajte kvantni krug koji implementira operator

$$U = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{bmatrix},$$

gdje su $a, b, c, d \in \mathbb{C}$ takvi da je matrica $\widetilde{U} = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ unitarna.

Preostaje još pokazati da se svaka dvostruko kontrolirana $\tilde{U}$ vrata mogu implementirati pomoću $CNOT$ vrata i vrata koja djeluju na jedan qubit. Iz Propozicije 5.6 slijedi da postoji $\tilde{V}$ takav da je $\tilde{U} = \tilde{V}^2$ (ako je $\tilde{U} = e^{i\alpha} R_{\hat{n}}(\theta)$, onda je $\tilde{V} = e^{i\alpha/2} R_{\hat{n}}(\theta/2)$). Na Slici 13 objašnjeno je kako se dvostruko kontrolirana vrata mogu prikazati pomoću $CNOT$ i kontroliranih vrata (provjerite tu jednakost).

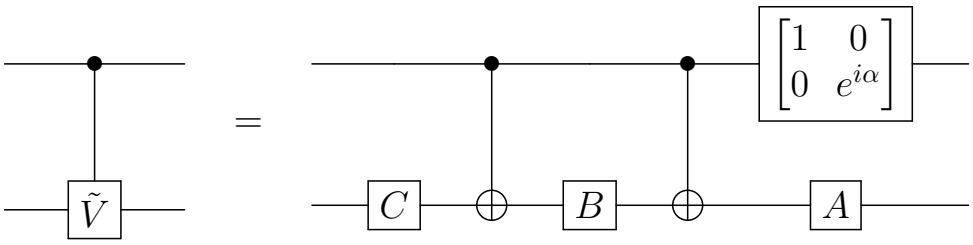


Slika 13: Dvostruko kontrolirana U vrata

S druge strane, iz Zadatka 5.11 slijedi da postoje unitarni operatori A, B i C na $\mathbb{C}^2$ i $\alpha \in \mathbb{R}$ takvi da je $ABC = I$ i $\tilde{V} = e^{i\alpha} AXBXC$. Tada kontrolirana $\tilde{V}$ vrata možemo implementirati sklopom koji je opisan na Slici 14 (provjerite to).

Time smo dokazali Teorem 5.4.

Za više informacija o teorijskom aspektu kvantnog računanja pogledajte knjigu [Aar13].



Slika 14: Kontrolirana $\tilde{V}$ vrata

6 Kvantni algoritmi

U ovom poglavlju opisat ćemo najvažnije kvantne algoritme – Groverov [Gro96] i Shorov [Sho97] algoritam. Glavna su referenca peto i šesto poglavlje u [NC09].

6.1 Groverov algoritam pretraživanja

6.1.1 Opis problema

Neka skup koji pretražujemo ima $N = 2^n$ elemenata $\{0, 1, 2, \ldots, N-1\}$ tako da svaki element možemo opisati s n bitova koji predstavljaju njegov binarni zapis. Elemente koje pretražujemo identificirat ćemo s elementima kanonske baze prostora stanja n qubita $V^{\otimes n}$; na primjer, za $n = 7$ element 19 identificiramo s vektorom $|19\rangle = |0010011\rangle$. Pretragu opisujemo funkcijom $f : \{0, 1, \ldots, N-1\} \to \{0, 1\}$ za koju vrijedi da je $f(x) = 1$ ako i samo ako je x jedno od M rješenja pretrage.

Slično kao i kod Deutschovog algoritma, funkcija $f(x)$ implementirana je pomoću kvantnih vrata U_f koja su na bazi prostora $V^{\otimes n} \otimes V$ definirana formulom

$$|x\rangle |q\rangle \mapsto |x\rangle |q \oplus f(x)\rangle .$$

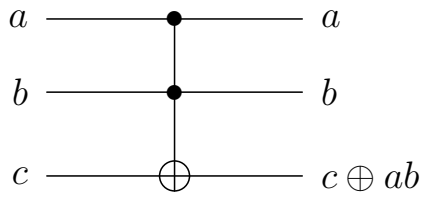
Ovdje je $|x\rangle \in V^{\otimes n}$ element baze vektora stanja koji odgovara elementu $x \in \{0, 1, \ldots, N-1\}$, dok je $|q\rangle \in \{|0\rangle, |1\rangle\}$ vektor stanja pomoćnog qubita koji smo dodali da bismo osigurali invertibilnost operatora U_f. Taj operator tradicionalno se naziva kvantna proročica jer u opisu algoritma

pretraživanja nećemo ulaziti u detalje njezine implementacije, nego ćemo slijepo vjerovati onome što kaže. Ilustrirajmo na primjeru faktorizacije da ove postavke imaju smisla.

Neka je zadan velik prirodni broj n (recimo od 200 znamenaka) koji je produkt dva prosta broja. Naš je zadatak pronaći te proste brojeve (odnosno razbiti RSA kriptosustav). Prvo što nam pada napamet jest da za svaki broj od 2 do $\sqrt{m}$ provjerimo dijeli li m – to je problem pretraživanja. Modeliramo ga pomoću funkcije $f : \{2, 3, \ldots, \lfloor\sqrt{m}\rfloor\} \to \{0, 1\}$, za koju je $f(k) = 1$ ako i samo ako k dijeli m. Ovdje je važno naglasiti da klasično funkciju $f(x)$ možemo efikasno implementirati (npr. koristeći samo vrata AND, OR i NOT) iako unaprijed ne znamo proste faktore od m (kao što ne znamo ni efikasan algoritam za faktorizaciju brojeva).

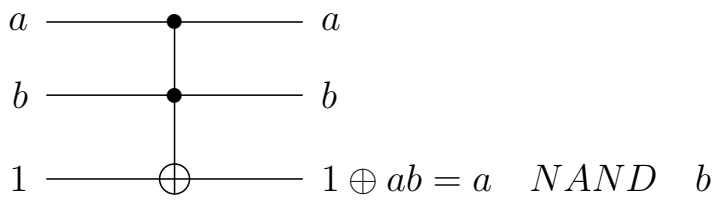
Drugo važno pitanje koje nismo do sada spomenuli u ovim predavanjima pitanje je "prevođenja" klasičnih programa u kvantne programe. Konkretno, ako imamo efikasnu implementaciju funkcije $f(x)$ pomoću logičkog kruga koji se sastoji od vrata AND, OR i XOR, možemo li zamjenom klasičnih vrata njihovim kvantnim verzijama dobiti jednako efikasnu kvantnu implementaciju operatora U_f?

Odgovor je da uz malo pažnje možemo. Očiti je problem to što vrata AND, OR i XOR nisu invertibilna pa nemaju svoje kvantne verzije, no to nije važno jer je ionako odabir tih vrata proizvoljan – iz klasičnog računarstva poznato je da postoje invertibilna (reverzibilna) vrata koja mogu simulirati sva ostala vrata. Primjer takvih vrata su Toffolijeva vrata.



Slika 15: Toffolijeva vrata

Na primjer, ona mogu jednostavno simulirati NAND (= NOT AND) vrata.



Nije se teško uvjeriti da u logičkom krugu koji implementira funkciju $f(x)$ možemo svaki AND, OR i XOR zamijeniti odgovarajućim Toffolijevim vratima (uz dodavanje novih bitova) i tako dobiti reverzibilan krug koji računa $f(x)$. Budući da su Toffolijeva vrata ujedno i kvantna vrata (provjerite unitarnost), možemo tako konstruirati (do na neke tehničke detalje vezanu uz nepoželjnu spregnutost qubitova o kojima nećemo sada govoriti) efikasan kvantni krug koji računa U_f.

U implementaciji algoritma, radi jednostavnosti, pomoćni qubit q na koji primjenjujemo operator U_f postavit ćemo na $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Tada za svaki x iz skupa koji pretražujemo vrijedi

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

tj. pomoćni qubit q uvijek ostaje isti. Radi jednostavnosti nećemo ga ni pisati pa da bismo to naglasili, umjesto U_f koristit ćemo proročicu $\mathcal{O}$ koju na elementu (ortonormirane) baze $|x\rangle$ definiramo formulom $\mathcal{O}\,|x\rangle = (-1)^{f(x)}\,|x\rangle$.

6.1.2 Osnovna ideja

Pomalo iznenađujuće, osnovna je ideja Groverovog algoritma geometrijska.

Neka je $|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$ početno stanje (kasnije ćemo vidjeti kako ga možemo konstruirati). Definirajmo dva normalizirana vektora $|\alpha\rangle = \frac{1}{\sqrt{N-M}} \sum_x^{'} |x\rangle$ i $|\beta\rangle = \frac{1}{\sqrt{M}} \sum_x^{''} |x\rangle$ gdje $\sum^{'}$ (odnosno $\sum^{''}$)) označava sumaciju preko indeksa koji nisu rješenja (odnosno jesu rješenja) pro-

blema traženja. Tada se početno stanje $|\Psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle$ nalazi u potprostoru razapetom s $|\alpha\rangle$ i $|\beta\rangle$.

Kako $\mathcal{O}$ djeluje na $|\alpha\rangle$ i $|\beta\rangle$? Jasno, $\mathcal{O}\,|\alpha\rangle = |\alpha\rangle$, odnosno $\mathcal{O}\,|\beta\rangle = -\,|\beta\rangle$. Geometrijski, $\mathcal{O}$ je refleksija u odnosu na vektor $|\alpha\rangle$ u dvodimenzionalnom potprostoru razapetom s $|\alpha\rangle$ i $|\beta\rangle$. Naš je cilj nekako se dočepati vektora $|\beta\rangle$ jer ako izmjerimo vektor $|\beta\rangle$ u standardnoj bazi kao rezultat mjerenja dobit ćemo neko rješenje problema pretraživanja.

Uvedimo još jednu oznaku, za proizvoljan vektor $|\Phi\rangle$ sa $|\Phi\rangle\langle\Phi|$ označit ćemo operator projekcije na vektor $|\Phi\rangle$, tj. $|\Phi\rangle\langle\Phi|\,(|\gamma\rangle) = |\Phi\rangle \cdot \langle\Phi|\gamma\rangle$, za proizvoljan vektor $|\gamma\rangle$.

Po definiciji, operator $2\,|\Psi\rangle\langle\Psi| - I$ refleksija je u odnosu na $|\Psi\rangle$ (u potprostoru razapetom s $|\alpha\rangle$ i $|\beta\rangle$) (dokažite to!). Tada je operator $G = (2\,|\Psi\rangle\langle\Psi| - I)\,\mathcal{O}$ kao kompozicija dviju refleksija rotacija u tom istom potprostoru za kut θ, gdje je $\cos\frac{\theta}{2} = \sqrt{\frac{N-M}{N}}$ (dokažite i to). Uočimo da je onda $|\Psi\rangle = \cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|\beta\rangle$. Specijalno, za prirodni broj k imamo

$$G^k\,|\Psi\rangle = \cos\left(\frac{2k+1}{2}\theta\right)|\alpha\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle\,.$$

Cilj nam je odabrati k takav da $G^k\,|\Psi\rangle$ bude blizu vektora $|\beta\rangle$, odnosno (prema prethodnoj formuli) takav da je $\sin\left(\frac{2k+1}{2}\theta\right) \approx 1$. U tom slučaju, mjerenjem stanja $G^k\,|\Psi\rangle$ s velikom ćemo vjerojatnošću izmjeriti vektor koji će biti rješenje problema traženja (što je $G^k\,|\Psi\rangle$ bliže stanju $|\beta\rangle$, to će ta vjerojatnost biti veća).

6.1.3 Implementacija i analiza algoritma

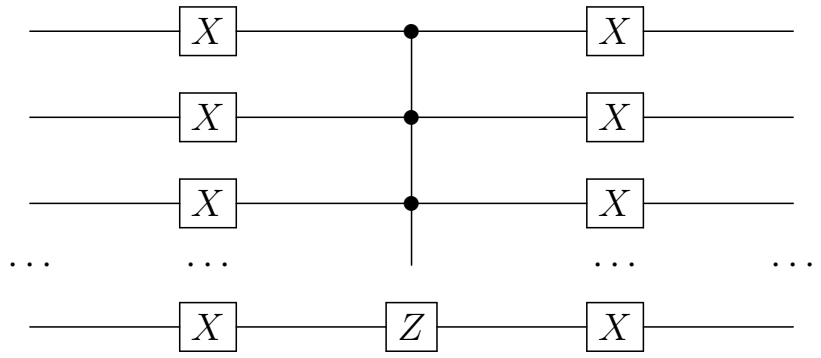
Kako bismo konstruirali stanje $|\Psi\rangle = \frac{1}{\sqrt{N}}\sum_{x=0}^{N-1}|x\rangle$, možemo na svaki qubit početnog stanja $|00\cdots0\rangle = |0\rangle^{\otimes n}$ primijeniti operator H. Lako se vidi da je vektor $H^{\otimes n}\,|0\rangle^{\otimes n} = (\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle))^{\otimes n}$, nakon što sve izmnožimo, jednak $|\Psi\rangle$.

Kako implementirati operator refleksije $(2\,|\Psi\rangle\langle\Psi| - I)$?
Ključno je primijetiti da je

$$H^{\otimes n}\,(2\,|00\cdots0\rangle\langle00\cdots0| - I)\,H^{\otimes n} = (2\,|\Psi\rangle\langle\Psi| - I)\,.$$

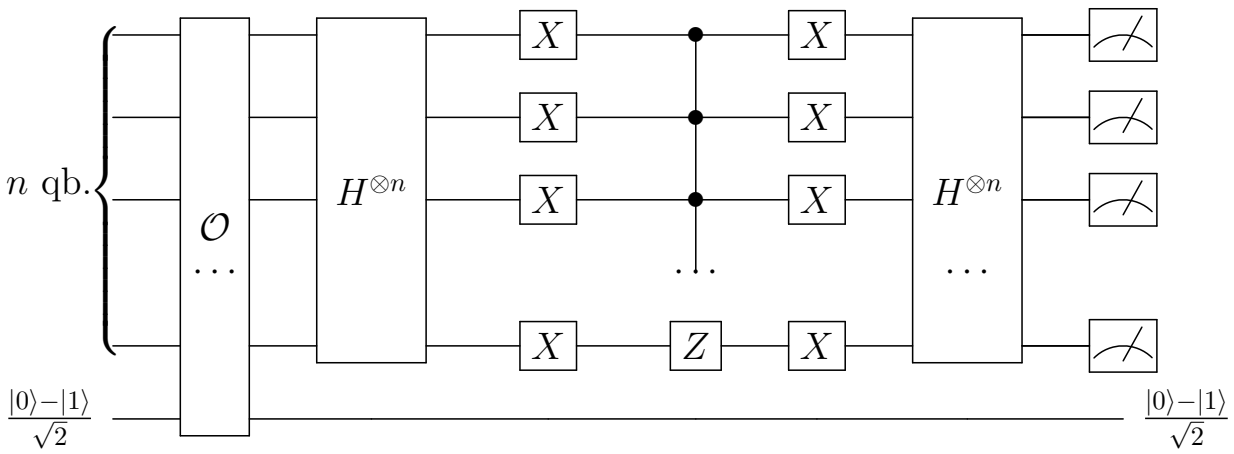
(Općenito, ako je W refleksija u odnosu na vektor w i U neki unitarni operator (čuva skalarni produkt), onda je $U^{-1}WU$ refleksija u odnosu na vektor $U^{-1}w$ – dokažite to. U našem je slučaju $(H^{\otimes n})^{-1} = H^{\otimes n}$.) Refleksiju oko vektora $|00\cdots0\rangle$ (komponiranu s centralnom simetrijom) možemo implementirati (Slika 16) pomoću vrata X i kontroliranih Z vrata (prvih $N-1$ qubita kontrolira primjenu vrata Z na preostali qubit).

Zašto nam je minus refleksija (odnosno refleksija komponirana s centralnom simetrijom) jednako dobra kao i refleksija? Zato što nam je na kraju, u trenutku mjerenja, svejedno mjerimo li stanje $|\psi\rangle$ ili $-|\psi\rangle$ – vjerojatnosti različitih ishoda mjerenja ne mijenjaju se ako vektor stanja pomnožimo kompleksnim brojem norme 1 tako da fizikalno ne razlikujemo ta dva stanja.



Slika 16: Refleksija komponirana s centralnom simetrijom

Operator G onda izgleda ovako.



Slika 17: Operator G

Koliko puta trebamo primijeniti G da bismo zarotirali $|\Psi\rangle$ tako da bude blizu $|\beta\rangle$, odnosno koja je složenost Groverovog algoritma?

Prisjetimo se,

$$|\Psi\rangle = \sqrt{\frac{N-M}{N}}\,|\alpha\rangle + \sqrt{\frac{M}{N}}\,|\beta\rangle = \cos\frac{\theta}{2}\,|\alpha\rangle + \sin\frac{\theta}{2}\,|\beta\rangle\,.$$

Radi jednostavnosti analize pretpostavimo da je $M = 1$, a N velik. Tada je kut θ mali, pa je $\theta \approx \sin\theta = 2\sin\frac{\theta}{2}\cos\frac{\theta}{2} = \frac{2\sqrt{M(N-M)}}{N} \approx \frac{2}{\sqrt{N}}$. Odaberimo minimalan $k \in \mathbb{N}$ takav da je

$$\left|\frac{\pi}{2} - k\cdot\theta\right| < \frac{\theta}{2}.$$

To možemo postići već u prvom "prolasku" pokraj vektora $|\beta\rangle$

$$k \approx \left|\frac{\frac{\pi}{2}-\frac{\theta}{2}}{\theta}\right| = \left|\frac{\pi}{2\theta} - \frac{1}{2}\right| \approx \frac{\pi}{4/\sqrt{N}} = \sqrt{N}\cdot\frac{\pi}{4}.$$

Ugrubo, nakon $O(\sqrt{N})$ koraka (odnosno primjena vrata G) dobit ćemo stanje $a\,|\alpha\rangle + b\,|\beta\rangle$ gdje je $a = \cos(\frac{\theta}{2} \pm \delta)$ za $0 \le \delta \le \frac{\theta}{2}$. Tada je $|a| = |\sin\delta| \le |\sin\frac{\theta}{2}|$, pa je $|a|^2 \le \sin^2\frac{\theta}{2} = \frac{M}{N} = \frac{1}{N}$.

Ako sad izvršimo mjerenje tog stanja (prvih n qubita) u standardnoj bazi vjerojatnost je manja od $\frac{1}{N}$ da nećemo izmjeriti rješenje potrage (zašto?).

Možemo zaključiti da Groverov algoritam pretraživanja u odnosu na klasični algoritam nudi ubrzanje s $O(N)$ na $O(\sqrt{N})$.

6.2 Simonov problem

Dana je funkcija $f : \{0,1\}^n \to \{0,1\}^n$ implementirana proročicom B_f gdje je

$$B_f \left|x\right\rangle \left|y\right\rangle = \left|x\right\rangle \left|y \oplus f(x)\right\rangle ,$$

za sve $\left|x\right\rangle , \left|y\right\rangle \in V^{\otimes n}$, gdje je $V = \langle \left|0\right\rangle , \left|1\right\rangle \rangle$ i $\oplus$ je zbrajanje modulo 2 po komponentama.

Poznato je da postoji $s \in \{0,1\}^n$, različit od nul-niza, takav da za sve različite $x, y \in \{0,1\}^n$ vrijedi $f(x) = f(y)$ ako i samo ako $y = x \oplus s$. Posebno, funkcija f je $2:1$ – u svaki element slike f preslika dva elementa domene. Problem je pronaći s.

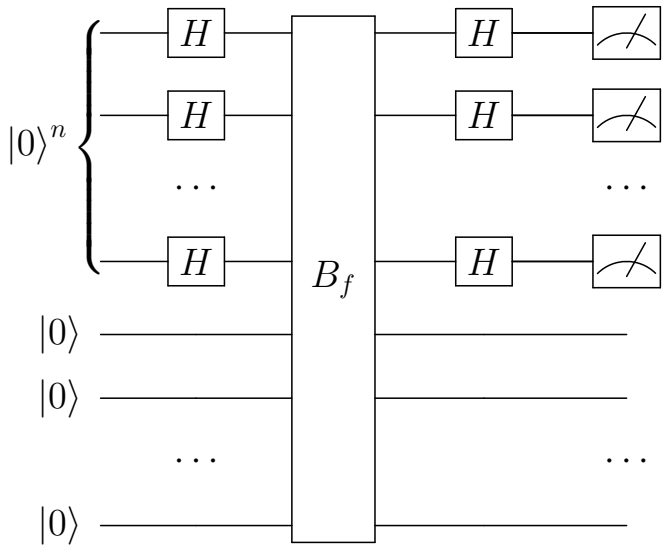
Primjer. Neka je za $n = 3$ funkcija $f(x)$ zadana sljedećom tablicom.

x	f(x)
000	101
001	010
010	000
011	110
100	000
101	110
110	101
111	010

Tada je rješenje problema $s = 110$.

Klasično, najbolje što možemo učiniti jest evaluirati funkciju sve dok ne dobijemo dvije iste vrijednosti. U najgorem slučaju za to će nam trebati $2^{n-1} + 1$ koraka (jer slika funkcije ima 2^{n-1} elemenata) dok je očekivani broj koraka jednak $\Omega(\sqrt{2^n})$ (dokažite to, taj rezultat zove se paradoks rođendana).

Promotrimo sljedeći sklop.



Slika 18: Simonov algoritam

Početno stanje je $|\Psi_0\rangle = |0\rangle^{\otimes n} \otimes |0\rangle^{\otimes n}$. Nakon primjene Hadamardovih operatora dobivamo stanje $|\Psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\, |0\rangle^{\otimes n}$. Primjenom proročice B_f dobivamo $|\Psi_2\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle\, |f(x)\rangle$. Budući da je $H^{\otimes n}\, |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x\cdot y}\, |y\rangle$ (dokažite to!, ovdje je $x\cdot y = \sum_i x_i y_i$ skalarni produkt modulo 2) dobivamo

$$|\Psi_3\rangle = \frac{1}{2^n} \sum_x \sum_y (-1)^{x\cdot y}\, |y\rangle\, |f(x)\rangle\,.$$

Vjerojatnost da ćemo mjerenjem prvog registra izmjeriti string y jednaka je

$$\left\| \frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{x\cdot y}\, |f(x)\rangle \right\|^2 .$$

Neka je $z \in R(f)$ element iz slike od $f(x)$. Tada postoje $x_z, x'_z \in$

$\{0,1\}^n$ takvi da je $f(x_z) = f(x'_z) = z$ te vrijedi $x_z = x'_z \oplus s$. Računamo

$$\begin{aligned}
\| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{x \cdot y} |f(x)\rangle \|^2 &= \| \frac{1}{2^n} \sum_{z \in R(f)} \left((-1)^{x_z \cdot y} + (-1)^{x'_z \cdot y} \right) |z\rangle \|^2 \\
&= \| \frac{1}{2^n} \sum_{z} \left((-1)^{x_z \cdot y} + (-1)^{(x_z \oplus s) y} \right) |z\rangle \|^2 \\
&= \| \frac{1}{2^n} \sum_{z} (-1)^{x_z \cdot y} \left(1 + (-1)^{s \cdot y} \right) |z\rangle \|^2 \\
&= \begin{cases} 2^{-(n-1)} & \text{ako je } s \cdot y = 0 \\ 0 & \text{ako je } s \cdot y = 1. \end{cases}
\end{aligned}$$

Dakle, uvijek ćemo izmjeriti string y za koji je $y \cdot s = 0$.
Ponavljanjem algoritma $n-1$ puta dobivamo sustav

$$\begin{aligned}
y_1 \cdot s &= 0 \\
y_2 \cdot s &= 0 \\
&\vdots \\
y_{n-1} \cdot s &= 0.
\end{aligned}$$

Ako skup $\{0,1\}^n$ identificiramo s vektorskim prostorom $\mathbb{F}_2^n$, onda stringove y_i možemo interpretirati kao vektore koji su okomiti na vektor s. Ako su izmjereni vektori y_i linearno nezavisni, onda s možemo izračunati rješavanjem sustava – u tom je slučaju rješenje sustava jedinstveno jer je ortogonalni komplement $n-1$ dimenzionalnog vektorskog prostora u n-dimenzionalnom vektorskom prostoru dimenzije jedan.

Kolika je vjerojatnost da su vektori $y_1, y_2, \ldots, y_{n-1} \in \mathbb{F}_2^n$ linearno nezavisni? Vjerojatnost da su y_1 i y_2 nezavisni je $(1 - \frac{1}{2^{n-1}})$ – to je vjerojatnost da smo odabrali dva različita vektora u skupu od 2^{n-1} vektora. Slično y_1, y_2 i y_3 linearno su nezavisni ako su y_1 i y_2 linearno nezavisni i ako se y_3 ne nalazi u dvodimenzionalnom vektorskom prostoru razapetom s vektorima y_1 i y_2 (koji ima 2^2 elemenata), tj. vjerojatnost je

jednaka $(1-\frac{1}{2^{n-1}})(1-\frac{1}{2^{n-2}})$. Induktivno zaključujemo da je vjerojatnost P da su $y_1, y_2, \ldots, y_{n-1}$ linearno nezavisni jednaka

$$P = \prod_{k=1}^{n-1}\left(1-\frac{1}{2^k}\right) > \prod_{k=1}^{\infty}\left(1-\frac{1}{2^k}\right) = 0.288788\ldots > \frac{1}{4}.$$

Vidimo da je vjerojatnost veća od $\frac{1}{4}$ (za svaki n) pa zaključujemo da smo opisali vjerojatnosni algoritam koji rješava Simonov problem u $O(n)$ kvantnih koraka. Koja je klasična složenost rješavanja sustava?

6.3 Kvantna Fourierova transformacija i primjene

6.3.1 Kvantna Fourierova transformacija

Definicija 6.1. *Diskretna Fourierova transformacija (DFT) linearno je preslikavanje $\mathbb{C}^N \to \mathbb{C}^N$ koje vektor $(x_0, x_1, \ldots, x_{N-1})$ preslikava u vektor $(y_0, \ldots, y_{N-1})$ tako da je za sve k*

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i j k/N}.$$

Napomena 6.2. Ovakva (kvantna) definicija nije uobičajena. Najčešće se suma normalizira s $\frac{1}{N}$ dok je predznak u argumentu eksponencijalne funkcije negativan.

DFT je neizostavan alat u analizi digitalnog signala. Tako, na primjer, ako je y_t jednak intenzitetu zvuka u trenutku t (u danom signalu), onda je x_k amplituda frekvencije k u tom signalu.

Inverz od DFT dan je formulom

$$x_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} y_j e^{-2\pi i j k/N}.$$

Kvantna Fourierova transformacija (QFT) ista je transformacija, pri

čemu jedino koristimo drukčije oznake

$$|j\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{2\pi i jk/N} |k\rangle ,$$

odnosno, uz oznake iz Definicije 6.1,

$$\sum_{j=0}^{N-1} x_j |j\rangle \mapsto \sum_{k=0}^{N-1} y_k |k\rangle .$$

U standardnoj bazi QFT ima matrični prikaz jednak (uz $\omega = e^{2\pi i \frac{1}{N}}$)

$$QFT = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ \dots & \dots & \dots & \ddots & \dots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)^2} \end{bmatrix} .$$

Uočimo da je matrica simetrična (ali ne i hermitska) te da je operator unitaran ($QFT \cdot QFT^\dagger = QFT^\dagger \cdot QFT = I$).

Odaberimo $N = 2^n$ i neka je $\{|0\rangle, |1\rangle, \dots |2^n - 1\rangle\}$ baza za prostor stanja sustava od n qubita. Proizvoljan j možemo zapisati u binarnoj bazi $j = \overline{j_1 j_2 \dots j_n} = j_1 \cdot 2^{n-1} + j_2 \cdot 2^{n-2} + \dots + j_n \cdot 2^0$, odnosno, $0.j_1 j_2 \dots j_n = \frac{j_1}{2} + \frac{j_2}{4} + \dots \frac{j_n}{2^n}$. Pišemo još $|j\rangle = |j_1 j_2 \dots j_n\rangle$.

Lema 6.3. *QFT ima sljedeću produktnu reprezentaciju*

$$|j\rangle = |j_1 j_2 \dots j_n\rangle \mapsto \frac{1}{2^{n/2}} \left(|0\rangle + e^{2\pi i 0.j_n} |1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_{n-1} j_n} |1\rangle\right) \\ \dots \left(|0\rangle + e^{2\pi i 0.j_2 j_3 \dots j_n} |1\rangle\right) \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n} |1\rangle\right)$$

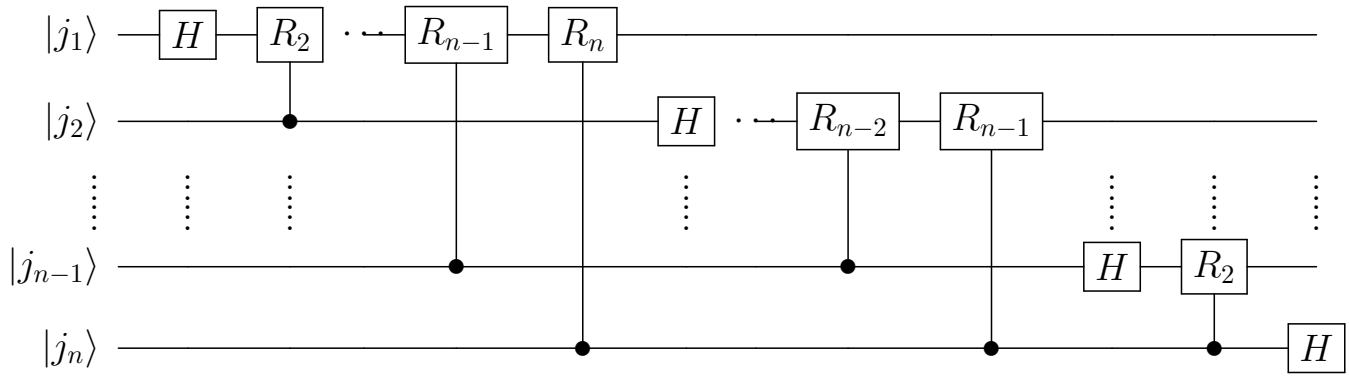
Dokaz. Uočimo da je $e^{2\pi i 0.j_1 j_2 \dots j_n} = e^{2\pi i \frac{\overline{j_1 j_2 \dots j_n}}{2^n}} = e^{2\pi i \frac{j}{N}}$, odnosno, $e^{2\pi i 0.j_l j_{l+1} \dots j_n} =$

$e^{2\pi i 2^{l-1}\frac{j}{N}}$ pa je produkt iz iskaza leme jednak

$$\begin{aligned}
&\frac{1}{2^{n/2}} \otimes_{l=1}^{n} \left[|0\rangle + e^{2\pi i \frac{j}{N} 2^{l-1}} |1\rangle \right] \\
&= \frac{1}{2^{n/2}} \sum_{k=0}^{N-1} |k\rangle \, e^{2\pi i \frac{j}{N} \sum_{k_l=1} 2^{l-1}} (\text{gdje je } k = \overline{k_1 k_2 \dots k_n}) \\
&= \frac{1}{n/2} \sum_{k=0}^{N-1} e^{2\pi i j k/N} |k\rangle \, .
\end{aligned}$$

□

Označimo sa $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{2\pi i/2^k} \end{bmatrix}$. Tada QFT možemo implementirati sljedećim sklopom.



Slika 19: QFT

Uočimo da djelovanje Hadamardovog operatora na qubit u stanju $|j_1\rangle$ (gdje je $j_1 \in \{0, 1\}$) možemo zapisati kao $\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.j_1} |1\rangle \right)$. Ako na to stanje primijenimo kontrolirana (s j_2) R_2 vrata dobivamo $\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.j_1 j_2} |1\rangle \right)$, odnosno nakon djelovanja svih kontroliranih R_k vrata stanje prvog qubita je $\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.j_1 j_2 \dots j_n} |1\rangle \right)$. Analogno, završno stanje k-tog qubita je $\frac{1}{\sqrt{2}} \left(|0\rangle + e^{2\pi i 0.j_k j_{k+1} \dots j_n} |1\rangle \right)$, pa je završno stanje sustava jednako pro-

duktu

$$\frac{1}{\sqrt{2^n}} \prod_{k=1}^{n} \left(|0\rangle + e^{2\pi i 0.j_k j_{k+1} \ldots j_n} |1\rangle \right),$$

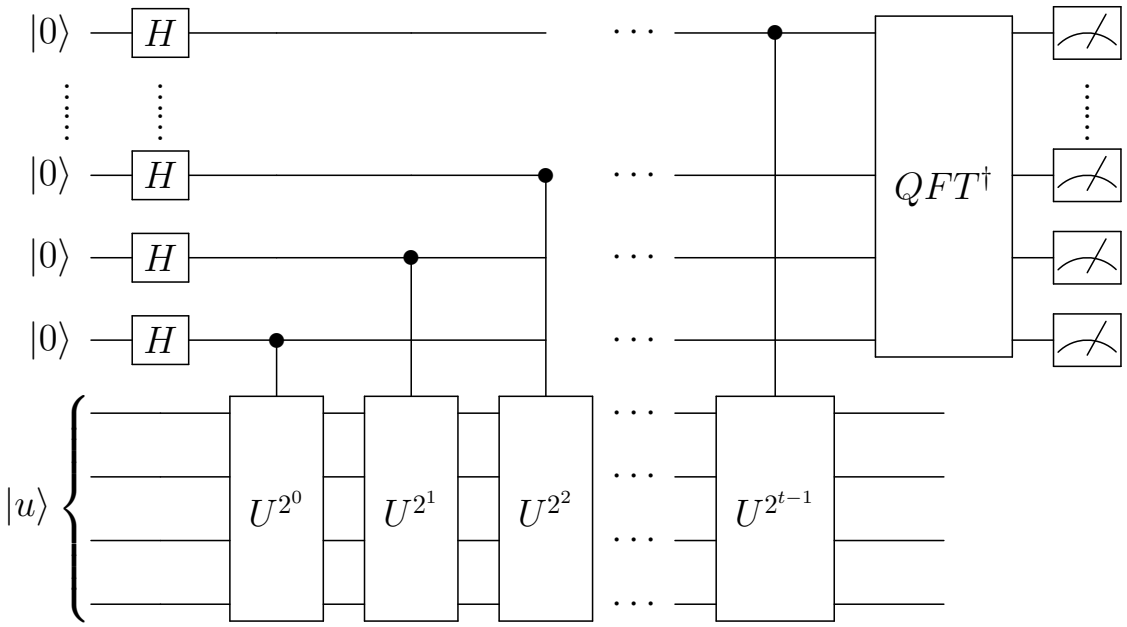
koji je prema Lemi 6.3 jednak $QFT\,|j_1 j_2 \ldots j_n\rangle$.

6.3.2 Problem određivanja faze svojstvenog vektora

Pretpostavimo da nam je dan unitaran operator U (odnosno kvantna vrata koja ga implementiraju) i njegov svojstveni vektor $|u\rangle$ (kao stanje registra qubita). Budući da je U unitaran, znamo da je svojstvena vrijednost vektora $|u\rangle$ kompleksan broj norme 1 pa ga možemo zapisati u obliku $e^{2\pi i\phi}$ za neki $\phi \in [0, 1\rangle$ koji zovemo faza. Kako odrediti fazu ϕ?

Ovo naoko "tehničko" pitanje ključan je dio Shorovog algoritma (odnosno, algoritma za određivanje reda elementa modulo N koji ćemo raditi u idućem odjeljku).

Pretpostavimo da je $\phi = 0.\phi_1\phi_2 \ldots \phi_t$ binarni zapis od ϕ. Radi jednostavnosti pretpostavljamo da je zapis konačan. Promotrimo sljedeći sklop.



Slika 20: Algoritam za određivanje faze

Prvi registar sastoji se od t qubita od kojih će svaki na kraju sadržavati informaciju o jednoj znamenci faze ϕ. Možemo pretpostaviti da je stanje drugog registra u svakom trenutku jednako početnom stanju $|u\rangle$ (budući da je $|u\rangle$ svojstveni vektor za sve operatore koji djeluju na njega pa ćemo razliku u fazi "prenijeti" u prvi registar), pa ga prilikom računa nećemo ni pisati.

Označimo sa $|\psi\rangle$ stanje prvog registra prije $QFT^\dagger$ vrata. Uočimo da qubiti prvog registra međusobno ne "komuniciraju" pa nije teško vidjeti da se $|\psi\rangle$ ovako faktorizira

$$|\psi\rangle = \frac{1}{2^{t/2}} \left(|0\rangle + e^{2\pi i \cdot 2^{t-1}\phi} |1\rangle\right) \left(|0\rangle + e^{2\pi i \cdot 2^{t-2}\phi} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i \cdot 2^{0}\phi} |1\rangle\right),$$

odnosno

$$|\psi\rangle = \frac{1}{2^{t/2}} \left(|0\rangle + e^{2\pi i \cdot 0.\phi_t} |1\rangle\right) \left(|0\rangle + e^{2\pi i \cdot 0.\phi_{t-1}\phi_t} |1\rangle\right) \cdots \left(|0\rangle + e^{2\pi i 0.\phi_1 \ldots \phi_t} |1\rangle\right).$$

Sada iz Leme 6.3 slijedi da je $QFT^\dagger(|\psi\rangle) = |\phi_1 \ldots \phi_t\rangle = |\phi\rangle$.

Općenito, bez ulaženja u detaljnu analizu, ako želimo s vjerojatnosti $\geq 1-\epsilon$ izračunati n-bitnu aproksimaciju faze ϕ, onda će nam za to prvi registar trebati biti veličine od $t = n + \lceil \ln(2 + \frac{1}{2\epsilon}) \rceil$ qubita. Pritom je složenost algoritma $O(t^2)$ kvantnih operacija.

Primijetimo da nas ništa ne sprječava da na ulaz u drugi registar umjesto svojstvenog vektora $|u\rangle$ postavimo, ako nam je poznata, linearnu kombinaciju $\frac{1}{\sqrt{k}} \sum_{i=1}^{k} |u_i\rangle$ svojstvenih vektora $|u_i\rangle$ sa svojstvenim vrijednostima $e^{2\pi i \varphi_i}$ (jer je naš program linearan operator). Tada ćemo na izlazu dobiti vektor

$$\frac{1}{\sqrt{k}} \sum_{i=1}^{k} |\tilde{\varphi}_i\rangle \, |u_i\rangle$$

gdje je $\tilde{\varphi}_i$ t-bitna aproksimacija faze φ_i (sada navodimo i stanje drugog registra). Mjerenjem prvog registra dobivamo aproksimaciju faze nekog svojstvenog vektora $|u_i\rangle$. Ovo će nam biti važno u idućem odjeljku.

6.3.3 Određivanje reda elementa u $(\mathbb{Z}/N\mathbb{Z})^\times$

Pomalo iznenađujuće, ali Shorov algoritam za faktorizaciju bazira se na efikasnom algoritmu za određivanje reda elementa u $(\mathbb{Z}/N\mathbb{Z})^\times$ koji ćemo sada objasniti. Za $x, y \in \mathbb{N}$ s $NZM(x, y)$ označavamo njihovu najveću zajedničku mjeru.

Za $x, N \in \mathbb{N}$ takve da je $x < N$ i $NZM(x, N) = 1$, red od x modulo N najmanji je prirodni broj r takav da je $x^r \equiv 1 \pmod{N}$ (tj. to je red od $x \in (\mathbb{Z}/N\mathbb{Z})^\times$). Problem je za dane x i N odrediti r.

Klasično je to težak problem, nije poznat polinomijalan algoritam u broju bitova $L = \lceil \log_2 N \rceil$.

Primjer. Lako se provjeri da je red od 5 modulo 21 jednak 6 jer je $5^6 \equiv 1 \pmod{21}$, a $5^k \not\equiv 1 \pmod{21}$ za prirodne brojeve $k < 6$.

Za cijeli broj $0 \leq y < 2^L$ definiramo operator (na prostoru stanja $\langle |0\rangle, |1\rangle \rangle^{\otimes L}$ – uobičajeno identificiramo y s njegovim prikazom u bazi 2)

$$U\,|y\rangle = \begin{cases} |xy \pmod{N}\rangle & \text{ako je } y < N, \\ |y\rangle & \text{inače.} \end{cases}$$

Zadatak 6.4. Dokažite da je U unitaran operator.

Svojstveni vektori (odnosno pripadne svojstvene vrijednosti) operatora U sadrže informaciju o redu r.

Za sve $0 \leq s \leq r-1$ neka je

$$|u_s\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi isk}{r}\right) \left|x^k \bmod N\right\rangle .$$

Kako je

$$\begin{aligned} U\,|u_s\rangle &= \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \exp\left(\frac{-2\pi isk}{r}\right) \left|x^{k+1} \bmod N\right\rangle \\ &= \exp\left(\frac{2\pi is}{r}\right) |u_s\rangle , \end{aligned}$$

zaključujemo da su vektori $|u_s\rangle$ svojstveni vektori za U sa svojstvenim vrijednostima $\exp\left(\frac{2\pi is}{r}\right)$.

Pretpostavimo na trenutak da nam je dan vektor $|u_s\rangle$ za neki (ali nama nepoznati) $s \in \{0, 1, \ldots, r-1\}$. Primjenom algoritma za određivanje faze (iz prethodnog odjeljka) možemo efikasno izračunati aproksimaciju ϕ nepoznatog razlomka $\frac{s}{r}$. Možemo li iz ϕ izračunati r? Uz malo sreće možemo.

Vrijedi sljedeći teorem iz teorije diofantskih aproksimacija.

Teorem 6.5. *Neka je $\phi \in \mathbb{R}$. Pretpostavimo da je $\frac{s}{r}$ racionalan broj takav da je*

$$\left|\frac{s}{r} - \phi\right| \leq \frac{1}{2r^2}.$$

Tada je $\frac{s}{r}$ konvergenta verižnog razlomka od ϕ.

Više o verižnim razlomcima i ovom teoremu možete pročitati u Dodatku B. Sada ćemo samo naglasiti da postoji efikasan klasični algoritam za računanje konvergenti (racionalan broj ima konačno mnogo konvergenti) koji možemo primijeniti na aproksimaciju ϕ razlomka $\frac{s}{r}$ (točnije, u

svjetlu Teorema 6.5 na razlomak $\frac{s}{r}$ gledamo kao na aproksimaciju broja ϕ). Svaka konvergenta koju tako izračunamo daje nam jednog kandidata za r. Budući da je jednostavno provjeriti je li dani broj period broja x modulo N, ako smo imali sreće s aproksimacijom ϕ (tj. ako je $\left|\frac{s}{r} - \phi\right| \leq \frac{1}{2r^2}$), ovim postupkom pronaći ćemo period r.

Dakle, kad bismo mogli generirati vektore $|u_s\rangle$, efikasno bismo riješili problem određivanje perioda. Taj ćemo problem riješiti zaobilaznim putem. Ključno je primijetiti (raspišite!) da je

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} |u_s\rangle = |1\rangle \,.$$

Ako u algoritmu za određivanje faze iz prethodnog odjeljka u drugi registar umjesto jednog svojstvenog vektora kao ulaz postavimo njihovu linearnu kombinaciju vektor $|1\rangle$, onda ćemo na izlazu dobiti vektor

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} \left|\tilde{\psi}_s\right\rangle |u_s\rangle \,,$$

gdje je $\tilde{\psi}_s$ aproksimacija broja $\frac{s}{r}$ – faze vektora $|u_s\rangle$. Mjerenjem prvog registra dobivamo $\tilde{\psi}_s$ za neki (nama nepoznati) s. Kao i ranije, primjenom Teorema 6.5 možemo (uz malo sreće) odrediti period r.

6.3.4 Shorov algoritam faktorizacije

Opišimo sada kako se efikasan kvantni algoritam za određivanje reda elementa iz prethodnog odjeljka može iskoristiti za faktorizaciju.

Neka je dan prirodni broj $N = pq$ koji je jednak produktu dva prosta broja (koji su u kriptografskoj praksi veličine od stotinjak znamenaka). Problem je odrediti brojeve p i q.

Opišimo (klasični) algoritam koji koristi kvantnu proceduru za određivanje reda elementa.

1. Slučajno odaberimo prirodni broj x, $1 \leq x \leq N$. Ako je $NZM(x, N) > 1$, onda je $NZM(x, N)$ jednak p ili q pa smo gotovi. (Prisjetimo

se da za računanje najveće zajedničke mjere koristimo Euklidov algoritam tako da je složenost ovog koraka $O(\ln N)$.)

2. Izvršimo kvantnu proceduru koja vraća red r od x modulo N (tj. najmanji r takav da je $x^r \equiv 1 \pmod{N}$.

3. Ako je r paran i $x^{\frac{r}{2}} \not\equiv -1 \pmod{N}$, onda je $NZM(x^{\frac{r}{2}} - 1, N)$ jedan od faktora ($NZM(x^{\frac{r}{2}} + 1, N)$ je drugi), inače se vraćamo natrag na prvi korak.

Objašnjenje trećeg koraka je sljedeće. Ako je r paran i ako je $x^{\frac{r}{2}} \not\equiv 1 \pmod{N}$, onda N dijeli $x^r - 1 = (x^{\frac{r}{2}} - 1)(x^{\frac{r}{2}} + 1)$, ali ne dijeli ni jedan od faktora (jer kad bi N dijelio $x^{\frac{r}{2}} - 1$, to bi značilo da je red od x modulo N manji od r). Zaključujemo da zato p dijeli jedan faktor, a q drugi; stoga računajući najveću zajedničku mjeru svakog od faktora i broja N dolazimo do brojeva p i q.

Primjer. Za ilustraciju, faktorizirajmo ovim algoritmom broj 15.

1. Pretpostavimo da smo slučajno odabrali broj $x = 7$.

2. Računamo red od 7 modulo 15. Krenimo s početnim stanjem $|0\rangle^{\otimes t} |1\rangle^{\otimes L}$, gdje prvi registar ima $t = 11$ qubitova, a drugi L qubitova, gdje je $L = 4$ broj bitova potrebnih za zapisivanje broja 15. Primjenom Hadamardovih vrata na prvi registar dobivamo stanje $\frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle |1\rangle$. Sljedeće, primjenom operatora $|z\rangle |y\rangle \mapsto |z\rangle |x^z y \bmod N\rangle$ (vidi prethodni odjeljak) dobivamo stanje

$$\begin{aligned} |\psi\rangle &= \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} |k\rangle \left|x^k \bmod N\right\rangle \\ &= \frac{1}{\sqrt{2^{11}}} \left(|0\rangle |1\rangle + |1\rangle |7\rangle + |2\rangle |4\rangle + |3\rangle |13\rangle + |4\rangle |1\rangle + |5\rangle |7\rangle + \cdots\right). \end{aligned}$$

Sada primjenjujemo $QFT^\dagger$ na prvi registar koji onda mjerimo. Primijetimo (zbog lakšeg razumijevanja) da se ništa neće promijeniti sa statistikom mjerenja ako prvo izmjerimo drugi registar, a tek

onda na prvi primijenimo $QFT^\dagger$ te ga onda izmjerimo. Zašto? To je opći princip. Kad bi statistika mjerenja ovisila o tome jesmo li mjerili drugi registar ili ne, to bi onda značilo da bi mjerenjem prvog registra mogli utvrditi je li netko mjerio drugi registar – odnosno tada bi dva registra mogla komunicirati brže od brzine svjetlosti (sjetite se Alice i Boba kod teleportacije).

Pretpostavimo da smo mjereći drugi registar dobili 4 (mogući ishodi mjerenja su $1, 4, 7$ i 13). Tada $QFT^\dagger$ primjenjujemo na stanje

$$\sqrt{\frac{4}{2^{11}}}\left(|2\rangle + |6\rangle + |10\rangle + |14\rangle + \cdots\right).$$

Može li kvantna Fourierova transformacija "vidjeti" razliku ovog aritmetičkog niza (jer je ona jednaka redu elementa x)? Dobivamo stanje $\alpha_1|0\rangle + \alpha_2|512\rangle + \alpha_3|1024\rangle + \alpha_4|1536\rangle$, gdje su sve vjerojatnosti $|\alpha_i|^2$ jednake $\frac{1}{4}$. Pretpostavimo da smo izmjerili $l = 1536$. Preostaje nam još izračunati konvergente verižnog razlomka od

$$\frac{1536}{2048} = \cfrac{1}{1 + \cfrac{1}{3}}.$$

Broj $\frac{3}{4}$ je jedna konvergenta pa provjerom otkrivamo da je $r = 4$ red od $x = 7$.

3. Budući da je r paran računamo $NZM(x^{r/2} - 1, 15)$ i dobivamo netrivijalan faktor 3. Dakle $15 = 3 \cdot 5$.

Motivirani gornjim primjerom, promotrimo malo detaljnije kako $QFT^\dagger$ djeluje na "aritmetičke nizove".

Neka je $|\Psi\rangle = \frac{1}{\sqrt{n+1}}\left(|i_0\rangle + |i_0 + r\rangle + |i_0 + 2r\rangle + \cdots + |i_0 + n \cdot r\rangle\right)$ stanje prostora s bazom $\{|0\rangle, |1\rangle, \ldots |N-1\rangle\}$, gdje su i_0, r, n i N nenegativni cijeli brojevi takvi da je $i_0 + n \cdot r < N$. Može li $QFT^\dagger$ vidjeti razliku r (jedino nam je N poznat)?

Prema definiciji inverzne kvantne Fourierove transformacije računamo

$$\begin{aligned} QFT^\dagger |\Psi\rangle &= \frac{1}{\sqrt{n}} \sum_{k=0}^{n} \sum_{s=0}^{N-1} e^{-2\pi i s \frac{i_0 + k\cdot r}{N}} |s\rangle \\ &= \frac{1}{\sqrt{n}} \sum_{s=0}^{N-1} e^{-2\pi i s \frac{i_0}{N}} |s\rangle \sum_{k=0}^{n} e^{-2\pi i s \frac{k\cdot r}{N}}. \end{aligned}$$

Budući da je $|e^{-2\pi i s \frac{i_0}{N}}| = 1$, vjerojatnost mjerenja stanja $|s\rangle$ jednaka je

$$\frac{1}{n} \left| \sum_{k=0}^{n} \left(e^{-2\pi i s \frac{r}{N}} \right)^k \right|^2.$$

Označimo s $\omega = e^{-2\pi i s \frac{r}{N}}$. Kako je gornja vjerojatnost najveća ako je $\omega = 1$, ako mjerenjem stanja $QFT^\dagger |\Psi\rangle$ izmjerimo $|s\rangle$, intuitivno možemo očekivati da će ω približno biti jednak 1, odnosno da će vrijediti $s \cdot \frac{r}{N} \approx m$ ili ekvivalentno $\frac{s}{N} \approx \frac{m}{r}$, za neki cijeli broj m. Tada će, uz malo sreće, razlomak $\frac{m}{r}$ biti konvergenta nama poznatog (jer smo s izmjerili) racionalnog broja $\frac{s}{N}$ pa tada r možemo detektirati računajući konvergente po Lemi B.1.

Zadatak 6.6. Neka je p (velik) prost broj. Pretpostavimo da nam je dano stanje

$$|\Psi\rangle = \frac{1}{\sqrt{p-1}} \sum_{x=1}^{p-1} |x\rangle \, |ax + b \bmod p\rangle \,,$$

gdje su $a, b < p$ nepoznati prirodni brojevi. Odredite brojeve a i b.

Rješenje. Prvo ćemo odrediti a. Primjenom QFT na oba registra dobivamo

$$\begin{aligned} &\frac{1}{\sqrt{p-1}} \sum_{x=1}^{p-1} \left(\frac{1}{\sqrt{p}} \sum_{s=0}^{p-1} e^{2\pi i s x/p} |s\rangle \right) \otimes \left(\frac{1}{\sqrt{p}} \sum_{t=0}^{p-1} e^{2\pi i t(ax+b)/p} |t\rangle \right) \\ &= \frac{1}{p\sqrt{p-1}} \sum_{s=0}^{p-1} \sum_{t=0}^{p-1} \sum_{x=1}^{p-1} |s\rangle \, |t\rangle \, e^{2\pi i (xs + (ax+b)t)/p}. \end{aligned}$$

Kako je vjerojatnost mjerenja stanja $|s\rangle\,|t\rangle$ jednaka

$$\left|\frac{1}{p\sqrt{p-1}}\sum_{x=1}^{p-1}e^{2\pi ix(s+at)/p}\right|^2=\begin{cases}\left(\frac{\sqrt{p-1}}{p}\right)^2=\frac{p-1}{p^2} & \text{ako je } s+at\equiv 0 \pmod p\\ \frac{1}{p^2(p-1)} & \text{ako je } s+at\not\equiv 0 \pmod p,\end{cases}$$

očekuje se da ćemo izmjeriti par (s,t) za koji je $s+at\equiv 0 \pmod p$. Ako je pritom $(s,t)\neq(0,0)$, onda a možemo izračunati prema formuli $a\equiv -st^{-1} \pmod p$.

Problem računanja broja b svest ćemo na prvi dio zadatka. Invertiranjem modulo p prvog registra (provjerite da je to unitarna transformacija) dobivamo stanje

$$\frac{1}{\sqrt{p-1}}\sum_{x=1}^{p-1}\left|x^{-1}\right\rangle|ax+b \bmod p\rangle\,,$$

a množenjem drugog registra s prvim (provjerite da je i to unitarna operacija) dobivamo stanje

$$\frac{1}{\sqrt{p-1}}\sum_{x=1}^{p-1}\left|x^{-1}\right\rangle\left|a+bx^{-1} \bmod p\right\rangle=\frac{1}{\sqrt{p-1}}\sum_{y=1}^{p-1}|y\rangle\,|by+a \bmod p\rangle\,.$$

Primjenom algoritma iz prvog dijela zadatka nalazimo b.

7 Kvantno ispravljanje grešaka

Problem je svih tehnologija koje se danas istražuju i koriste za fizičku realizaciju kvantnih računala taj da nije moguće izolirati qubite (kako god oni bili realizirani) od okoline pa se zbog toga prilikom računanja nužno javljaju greške. U ovom poglavlju objasnit ćemo kako se neke od tih grešaka mogu ispraviti. Počet ćemo s klasičnom teorijom ispravljanja grešaka. U izlaganju pratimo deseto poglavlje iz knjige [NC09].

7.1 Klasični kodovi za ispravljanje grešaka

Krenimo s definicijama.

Definicija 7.1. *Neka je dan skup A. Kod nad A dužine n podskup je $\mathcal{C}$ skupa A^n nizova duljine n koji sadrži barem dva elementa. Elementi od $\mathcal{C}$ zovu se kodne riječi. Veličina od $\mathcal{C}$, u oznaci $|\mathcal{C}|$, broj je elemenata u $\mathcal{C}$. Binarni kod je kod nad $A = \{0, 1\}$.*

Ilustrirajmo osnovnu ideju detektiranja i ispravljanja grešaka na primjeru.

Primjer. Neka je $\mathcal{C} = \{00000, 11111\}$ binarni kod dužine pet s dvije kodne riječi (veličine dva). Pretpostavimo da Alice šalje Bobu poruku koja se sastoji od jednog bita informacije (0 ili 1) "bučnim" komunikacijskim kanalom. Alice tu poruku može kodirati kodnim riječima iz koda $\mathcal{C}$ tako da Bobu umjesto bita 0 pošalje pet bitova 00000 te umjesto bita 1 kodnu riječ 11111. Bob primljenu riječ $a_1a_2a_3a_4a_5$ (koja zbog grešaka u komunikaciji ne mora biti jednaka poslanoj riječi) dekodira u bit 0 ili 1 ovisno o tome ima li u primljenoj riječi više nula ili jedinica.

Uočimo da ovaj kod može detektirati četiri greške, a ispraviti dvije greške.

Ovu ideju možemo elegantno opisati i generalizirati pomoću pojma Hammingove metrike.

Definicija 7.2. *Neka su $u, v \in A^n$ riječi duljine n. Hammingova udaljenost riječi u i v, u oznaci $d(u, v)$, definira se kao broj pozicija na kojima se u i v razlikuju. Hammingova kugla radijusa t oko $u \in A^n$ je skup $B_t(u) = \{v \in A^n : d(u, v) \leq t\}$.*

Napomena 7.3. Vrijedi nejednakost trokuta, za sve riječi u, v i w

$$d(u, w) \leq d(u, v) + d(v, w)$$

pa budući da su ostali aksiomi metrike trivijalno zadovoljeni, vidimo da funkcija d definira metriku na skupu A^n.

Primjer. Neka je $A = \{0, 1\}$. Hammingova kugla radijusa 1 u A^4 sa središtem u 0101 je jednaka

$$B_1(0101) = \{0101, 1101, 0001, 0100, 0111\}.$$

Alice poruku koju želi poslati kodira koristeći riječi iz koda $\mathcal{C}$ koje zatim šalje Bobu kroz bučan komunikacijski kanal. Bob riječ u koju primi dekodira kao riječ iz koda $\mathcal{C}$ koja je najbliža riječi u (u Hammingovoj metrici).

Definicija 7.4. *Kažemo da kod $\mathcal{C}$ duljine n ispravlja t grešaka ako su za sve različite $u, u' \in \mathcal{C}$ lopte $B_t(u)$ i $B_t(u')$ disjunktne. Kažemo da $\mathcal{C}$ detektira t grešaka ako je za sve različite $u, u' \in \mathcal{C}$ udaljenost $d(u, u') > t$.*

Primjer. Neka je $\mathcal{C} = \{00000, 11100, 00111, 11011\}$. Pretpostavimo da je Bob primio riječ $v = 11111$. Kako je $d(v, 11011) = 1$ i $d(v, u) > 1$ za sve $u \in \mathcal{C} \setminus \{11011\}$, Bob riječ v dekodira kao 11011.

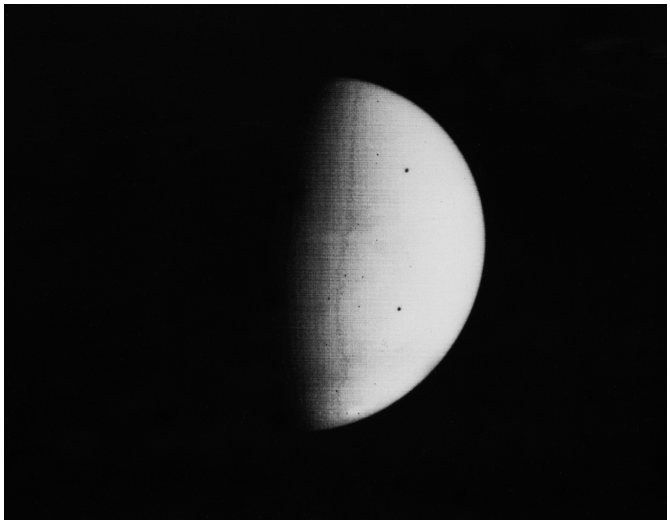
Pretpostavimo da je Bob primio riječ $v = 01010$. Kako je $d(v, 00000) = d(v, 11011) = 2$ (a za ostale elemente koda udaljenost je i veća), Bob ne može dekodirati v (no zna da su se prilikom prijenosa dogodile barem dvije greške). Lako se provjeri da ovaj kod ispravlja jednu, a detektira dvije greške.

Ako je $\mathcal{C}$ kod duljine n, veličine M i minimalne udaljenosti $d = d(\mathcal{C}) := \min\{d(u, v) : u, v \in \mathcal{C}, u \neq v\}$, onda kažemo da je $\mathcal{C}$ (n, M, d)-kod.

Zadatak 7.5. Dokažite da kod minimalne duljine d ispravlja $\lfloor \frac{d-1}{2} \rfloor$ grešaka.

7.2 Linearni kod

Letjelica Mariner 9 ušla je 1971. godine u orbitu Marsa (bila je to prva letjelica koja je ušla u orbitu nekog drugog planeta). Poslala je na zemlju 7329 crno-bijelih fotografija (vidi Sliku 21). Jedan piksel slike bio je kodiran sa šest bitova. Vjerojatnost greške prilikom slanja jednog bita bila je 5%, tako da bi bez kodiranja 26% piksela slike bilo pogrešno. Zbog brzine prijenosa podataka (brzina slanja bila je 8 bitova u sekundi



Slika 21: Mars fotografiran s Marinera 9

Izvor: NASA/JPL

– za jednu fotografiju trebalo je oko osam sati) kodna poruka nije mogla biti više od pet puta dulja od samih podataka. Jednostavan kod, u kojem bi se svaki bit ponovio pet puta, može ispraviti dvije greške, što bi rezultiralo fotografijama s 1% krivih piksela.

Odlučeno je da će se koristiti Reed-Mülerov kod koji ispravlja 7 grešaka, što je reduciralo vjerojatnost greške jednog piksela na 0.014%.

Definicija 7.6. *Neka je $\mathcal{C}$ binarni kod duljine n. Kažemo da je $\mathcal{C}$ linearan ako za sve $u, w \in \mathcal{C}$ vrijedi da je $u + w \in \mathcal{C}$ (riječi zbrajamo modulo 2, $u + v := u \oplus v$), odnosno, ako je $\mathcal{C}$ potprostor vektorskog prostora $\mathbb{F}_2^n$ (ovdje polje $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ identificiramo sa skupom $\{0, 1\}$).*

Definicija 7.7. *Reed-Mülerov kod $\mathcal{R}(1, m)$ je binarni kod definiran (rekurzivno) za sve $m \in \mathbb{N}$ formulama*

i) $\mathcal{R}(1, 1) = \{00, 01, 10, 11\} = \mathbb{F}_2^2$,

ii) za $m > 1$

$$\mathcal{R}(1, m) = \{(u, u), (u, u + \underline{1}) : u \in \mathcal{R}(1, m - 1)\},$$

gdje je $\underline{1} = (1, 1, \ldots, 1)$ *vektor u* $\mathbb{F}_2^m$.

Primjer. $\mathcal{R}(1,2) = \{0000, 0011, 0101, 0110, 1010, 1001, 1111, 1100\}$.

Sljedeću propoziciju možete lako dokazati za vježbu.

Propozicija 7.8. *Za $m \in \mathbb{N}$, Reed-Mülerov kod $\mathcal{R}(1,m)$ je linearan kod dužine 2^m u kojem svaki vektor (osim vektora $\underline{0}$ i $\underline{1}$) ima pola znamenaka 0, a pola 1 (kažemo još da ima Hammingovu težinu, tj. Hammingovu udaljenost od vektora $\underline{0}$, jednaku 2^{m-1}).*

Za Reed-Mülerov kod $\mathcal{R}(1,m)$ kažemo da je $[a,b,c] = [2^m, m+1, 2^{m-1}]$ kod jer su kodne riječi duljine $a = 2^m$, ima ih ukupno $2^b = 2^{m+1}$ (odnosno $\mathcal{C}$ je potprostor dimenzije $b = m+1$) pa svaku riječ možemo iskoristiti za kodiranje jedne riječi od $(m+1)$-og bita i minimalna duljina koda je $c = 2^{m-1}$ pa kod ispravlja $2^{m-2} - 1$ grešaka.

Mariner 9 je koristio $[32, 6, 16]$ kod $\mathcal{R}(1,5)$ čija svaka riječ (duljine 32) kodira 6 bitova (odnosno jedan piksel) dok kod ispravlja 7 grešaka.

Kako jednostavno zakodirati 6 bitova (jedan piksel) $(m_1, m_2, \ldots, m_6) \in \mathbb{F}_2^6$ u $\mathcal{R}(1,5)$ kod? Treba nam bijekcija $\Xi : \mathbb{F}_2^6 \to \mathcal{R}(1,5) \subset \mathbb{F}_2^{32}$. Neka je $\{\omega_1, \omega_2, \ldots, \omega_6\}$ jedna baza 6-dimenzionalnog vektorskog prostora $\mathcal{R}(1,5)$. Tada je po definiciji baze ovo tražena bijekcija

$$\Xi(m_1, m_2, \ldots, m_6) = m_1 \cdot \omega_1 + \cdots + m_6 \cdot \omega_6.$$

Zadatak 7.9. Dokažite da je Reed-Mülerov kod linearan.

Linearan kod najčešće opisujemo pomoću matrice generatora, odnosno, pomoću parity check matrice. Matrica generatora G je matrica čiji stupci čine bazu za $\mathcal{C}$. Na primjer, za $\mathcal{R}(1,2)$

$$G = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}.$$

Kodiranje je u ovom opisu posebno jednostavno, dano je funkcijom

$$x \mapsto Gx.$$

Ako je G $n \times k$ matrica, onda kažemo da je $\mathcal{C}$ $[n, k]$-linearan kod.

Parity check matrica H nekog $[n, k]$-linearnog koda $\mathcal{C}$ je $(n-k) \times n$ matrica čiji su svi elementi 0 ili 1 sa svojstvom da je $Hx = 0$ za svaki $x \in \mathcal{C}$. Drugim riječima, stupci od $\mathcal{C}$ daju bazu za jezgru matrice H. Vrijedi $HG = 0$.

Kasnije će nam biti važan pojam dualnog koda.

Definicija 7.10 (Dualan kod)**.** *Neka je $\mathcal{C}$ $[n, k]$-linearan kod s matricom generatora G i parity check matricom H. Tada možemo definirati dualan kod kodu $\mathcal{C}$, $\mathcal{C}^\perp$, kao kod pridružen matrici generatora H^T (odnosno parity check matrici G^T). Kažemo da je kod $\mathcal{C}$ slabo samo-dualan ako $\mathcal{C} \subset \mathcal{C}^T$, a striktno samo-dualan ako je $\mathcal{C} = \mathcal{C}^T$.*

Zadatak 7.11. Pokažite da je kod s matricom generatora G samo-dualan ako i samo ako je $G^T G = 0$.

Zadatak 7.12. Neka je $\mathcal{C}$ linearan kod. Pokažite da vrijedi ($x \cdot y$ označava skalarni produkt vektora $x, y \in \mathbb{F}_2^n$, gdje je n dužina koda $\mathcal{C}$)

$$\sum_{y \in \mathcal{C}} (-1)^{x \cdot y} = \begin{cases} |C| & \text{ako je } x \in \mathcal{C}^\perp \\ 0 & \text{inače.} \end{cases}$$

Za više informacija o linearnim kodovima pogledajte treće poglavlje u knjizi [RL09].

7.3 Kvantno ispravljanje grešaka

U odnosu na klasično ispravljanje grešaka u kvantnom svijetu imamo sljedeće poteškoće:

- Nije moguće kopirati (klonirati) kvantna stanja pa se, na primjer, jednostavan kod $|\psi\rangle \mapsto |\psi\rangle\,|\psi\rangle\,|\psi\rangle$ ne može (naivno) implementirati.

- Greške nisu diskretne (kod klasičnih kodova jedini tip greške je bit flip), već se stanje jednog qubita (prisjetite se Blochove sfere) može poremetiti na neprebrojivo mnogo načina.

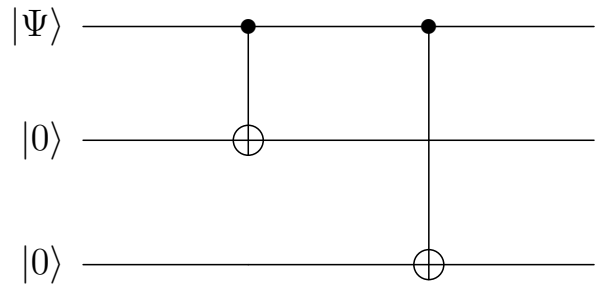
- Mjerenje uništava informacije. U klasičnom ispravljanju grešaka, mi tek nakon što "promotrimo" primljenu informaciju odlučujemo kojom ćemo ju procedurom dekodirati. U kvantnom svijetu "promatranje" uništava stanje koje mjerimo.

Mi ćemo se fokusirati na kodove koji ispravljaju dva tipa grešaka, bit flip i flip u fazi.

7.3.1 Bit flip kod za tri qubita

Pretpostavimo da šaljemo qubitove kroz komunikacijski kanal koji neke od njih "obrne" (eng. bit flip), to jest na neke od njih primijeni operator X.

Stanje $|\Psi\rangle = a\,|0\rangle + b\,|1\rangle$ ćemo kodirati s tri qubita kao $a\,|000\rangle + b\,|111\rangle$ (uočimo da ovo nije kopiranje) koristeći sklop sa Slike 22.



Slika 22: Konstrukcija stanja $a\,|000\rangle + b\,|111\rangle$

Pretpostavimo da je prolaskom kodirane poruke (tri qubita) kroz komunikacijski kanal došlo do greške (bit flip) na najviše jednom qubitu. Na primjer, $|000\rangle \mapsto |001\rangle$. Tu grešku možemo detektirati i ispraviti ovim postupkom.

(1) detekcija

Izvršit ćemo mjerenje definirano s četiri projektora (rezultat ovog

mjerenja zovemo sindromom greške, eng. error syndrome)

$$\begin{aligned}
P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| && \text{nema greške}\\
P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| && \text{bit flip na prvom qubitu}\\
P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| && \text{bit flip na drugom qubitu}\\
P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110| && \text{bit flip na trećem qubitu.}
\end{aligned}$$

Zašto? Pretpostavimo da je došlo do greške na prvom qubitu, to jest, da je primljeno stanje $\left|\tilde{\Psi}\right\rangle = a\,|100\rangle + b\,|011\rangle$. Budući da je $P_1\left|\tilde{\Psi}\right\rangle = \left|\tilde{\Psi}\right\rangle$, prema aksiomima mjerenja vidimo da ćemo P_1 izmjeriti sa sigurnošću što nam daje informaciju da je došlo do greške na prvom qubitu. Također, mjerenje ne mijenja stanje $\left|\tilde{\Psi}\right\rangle$.

(2) ispravljanje greške

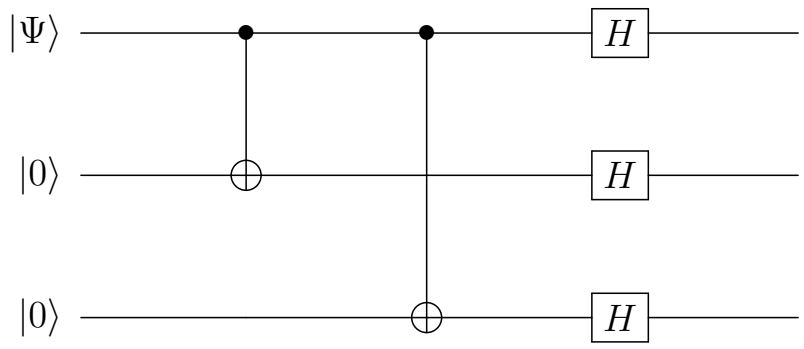
Prema izmjerenom sindromu greške određujemo koji ćemo operator primijeniti na $\left|\tilde{\Psi}\right\rangle$ kako bismo ga ispravili. Na primjer, ako smo u prvom koraku izmjerili P_1, onda ćemo na $\left|\tilde{\Psi}\right\rangle$ primijeniti operator $X \otimes I \otimes I$.

7.3.2 Flip u fazi za tri qubita

Pretpostavimo da šaljemo qubitove kroz komunikacijski kanal koji, ovaj put, neke od njih pomakne u fazi (eng. phase flip), to jest na neke od njih primijeni operator Z. Problem detektiranja i ispravljanja ovakvih grešaka svest ćemo na prethodni problem bit flipa.

Uočimo da je $Z\,|+\rangle = |-\rangle$ i $Z\,|-\rangle = |+\rangle$ gdje su $|+\rangle = H\,|0\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}$ i $|-\rangle = H\,|1\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Koristeći sklop

dobivamo stanje $a\,|+++\rangle + b\,|---\rangle$. Jasno je da smo sada problem sveli na prethodni. Detekcija greške se provodi kao i ranije, jedino sada operatore konjugiramo s H, tj. umjesto P_i koristimo $H^{\otimes 3} P_i H^{\otimes 3}$ (jer je $H^{-1} = H$). Također, grešku ispravljamo primjenom odgovarajućeg operatora (konjugiranog s H).



Kažemo da su bit flip i phase flip kanali unitarno ekvivalentni jer postoji unitarni operator U (u ovom slučaju $U = H$), takav da vrijedi

$$\text{prvi kanal} = U^\dagger \text{ drugi kanal } U.$$

7.3.3 Shorov kod

Shorov kod ispravlja greške u komunikacijskom kanalu koji generira i flip u fazi i bit flip greške prilikom prijenosa qubita.

Prvo ćemo zakodirati qubit koristeći kod

$$|0\rangle \to |+++\rangle\,, \qquad |1\rangle \to |---\rangle\,.$$

Nadalje, svaki od ova tri qubita ćemo zakodirati

$$|+\rangle \to \frac{1}{\sqrt{2}}\left(|000\rangle + |111\rangle\right), \qquad |-\rangle \to \frac{1}{\sqrt{2}}\left(|000\rangle - |111\rangle\right),$$

tako da je konačan rezultat kod

$$|0\rangle \mapsto |0_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)$$
$$|1\rangle \mapsto |1_L\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle)^{\otimes 3}.$$

Zadatak 7.13. Konstruirajte kvantni krug koji implementira taj kod.

Označimo sa $X_i = I \otimes I \otimes \cdots \otimes X \otimes I \otimes \cdots \otimes I$ i $Z_i = I \otimes I \otimes \cdots \otimes Z \otimes I \otimes \cdots \otimes I$ operatore na $V^{\otimes 9}$ kod kojih se operatori X i Z nalaze na i-toj poziciji.

Neka je $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ qubit kodiran vektorom $|\psi_L\rangle$ koji prolaskom kroz komunikacijski kanal postaje vektor $|\tilde{\psi}\rangle$. Opisat ćemo postupak koji ispravlja jednu bit flip ili flip u fazi grešku pa pretpostavljamo da se $|\tilde{\psi}\rangle$ razlikuje od $|\psi_L\rangle$ u najviše jednom bit flipu ili flipu u fazi. Za analizu sindroma (odnosno otkrivanje tipa greške) potrebne su nam opservable čiji je $|\tilde{\psi}\rangle$ svojstveni vektor (kako mjerenjem ne bismo utjecali na sustav koji mjerimo). Prisjetimo se, rezultat mjerenja opservable (hermitskog operatora) je neka njena svojstvena vrijednost dok je stanje sustava nakon mjerenja jednako projekciji stanja koje mjerimo na odgovarajući svojstven potprostor.

Pretpostavimo prvo da je došlo do bit flipa na prvom qubitu stanja. Tu grešku možemo dijagnosticirati mjerenjem dviju opservabli Z_1Z_2 i Z_2Z_3. Uočimo da su svojstveni vektori od Z_1Z_2 (pišemo svojstvenu vrijednost i samo prva tri qubita, ostali nisu važni)

$$\begin{array}{ll} +1 & |000\rangle\,, |001\rangle\,, |110\rangle\,, |111\rangle \\ -1 & |010\rangle\,, |011\rangle\,, |100\rangle\,, |101\rangle \end{array}$$

pa ako, na primjer, slanjem qubita $|0_L\rangle$ dobijemo $|\tilde{\psi}\rangle = \frac{1}{2\sqrt{2}}(|100\rangle + |011\rangle) \otimes (|000\rangle + |111\rangle)^{\otimes 2}$ mjerenjem opservable Z_1Z_2 izmjerit ćemo svojstvenu vrijednost -1 što nam daje informaciju da je došlo do bit flipa na jednom od prva dva qubita. Mjerenjem opservable Z_2Z_3 dobivamo 1 pa zaključujemo da je došlo do bit flipa na prvom qubitu. Naravno, a priori ne znamo koju kombinaciju mjerenja trebamo izvršiti, ali to nije problem jer možemo mjeriti sve kombinacije Z_iZ_j. Bitno je to da mjerenje ne mijenja stanje koje mjerimo (uvjerite se u to!). Jednom kad smo detektirali bit flip na prvom qubitu primjenom operatora X_1 na $|\tilde{\psi}\rangle$ dobivamo $|\psi_L\rangle = |0_L\rangle$.

U slučaju da je došlo do greške na fazi na prvom qubitu, $|\tilde{\psi}\rangle = Z_1\,|\psi_L\rangle$, možemo mjeriti opservable $X_1X_2\cdots X_6$ i $X_4X_5\cdots X_9$. Svojstveni vektori od $X_1X_2X_3$ su (pišemo svojstvenu vrijednosti i samo prva

tri qubita)

$$\begin{array}{ll} +1 & |000\rangle + |111\rangle\,, |011\rangle + |100\rangle\,, |010\rangle + |101\rangle\,, |001\rangle + |110\rangle \\ -1 & |000\rangle - |111\rangle\,, |011\rangle - |100\rangle\,, |010\rangle - |101\rangle\,, |001\rangle - |110\rangle\,. \end{array}$$

Na primjer, ako je $|\psi_L\rangle = |0_L\rangle$ i $|\tilde{\psi}\rangle = \frac{1}{2\sqrt{2}}(|000\rangle - |111\rangle) \otimes (|000\rangle + |111\rangle^{\otimes 2}$, mjerenjem opservable $X_1X_2X_3 \cdot X_4X_5X_6$ dobit ćemo rezultat -1 što nam kaže da je došlo do promjene u fazi između prva tri ili druga tri qubita. Mjerenjem $X_4X_5X_6 \cdot X_7X_8X_9$ dobivamo 1 pa znamo da nije bilo promjene u fazi između druga tri i treća tri qubita. Dakle, flip u fazi pojavio se na jednom od prva tri qubita – nije bitno na kojem jer je učinak na dano stanje isti. Grešku ispravljamo djelovanjem operatora Z_1 (ili Z_2 ili Z_3) na $|\tilde{\psi}\rangle$.

7.3.4 Calderbank-Shor-Steanov kod

Pretpostavimo da su $\mathcal{C}_1$ i $\mathcal{C}_2$ klasični redom $[n, k_1]$ i $[n, k_2]$-linearni kodovi takvi da je $\mathcal{C}_2 \subset \mathcal{C}_1$ i takvi da $\mathcal{C}_1$ i $\mathcal{C}_2^{\perp}$ ispravljaju t grešaka. Konstruirat ćemo (kvantni) $[n, k_1 - k_2]$-linearan kod $CSS(\mathcal{C}_1, \mathcal{C}_2)$ koji ispravlja t bit flip ili flip u fazi grešaka.

Pretpostavimo da je $x \in \mathcal{C}_1$ kodna riječ. Definiramo kvantno stanje

$$|x + \mathcal{C}_2\rangle := \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y \in \mathcal{C}_2} |x + y\rangle$$

u prostoru stanja $\{0,1\}^{\otimes n}$. Uočimo da je $|x + \mathcal{C}_2\rangle = |x' + \mathcal{C}_2\rangle$ ako je $x - x' \in \mathcal{C}_2$ tako da stanje $|x + \mathcal{C}_2\rangle$ ovisi samo o kosetu $x \in \mathcal{C}_1/\mathcal{C}_2$ u kvocijentom vektorskom prostoru $\mathcal{C}_2/\mathcal{C}_1$ (što onda i opravdava oznaku $|x + \mathcal{C}_2\rangle$). Uz to, ako x i x' pripadaju različitim kosetima od $\mathcal{C}_2$, onda ne postoje $y, y' \in \mathcal{C}_2$ takvi da je $x + y = x' + y'$ pa su stanja $|x + \mathcal{C}_2\rangle$ i $|x' + \mathcal{C}_2\rangle$ ortogonalna. Kvantni kod $CSS(\mathcal{C}_1, \mathcal{C}_2)$ se definira kao vektorski prostor razapet stanjima $|x + \mathcal{C}_2\rangle$ za sve $x \in \mathcal{C}_1$. Broj koseta od $\mathcal{C}_2$ u $\mathcal{C}_1$ je $\frac{|\mathcal{C}_1|}{|\mathcal{C}_2|}$ pa je dimenzija od $CSS(\mathcal{C}_1, \mathcal{C}_2)$ jednaka $k_1 - k_2$ – kažemo da je $CSS(\mathcal{C}_1, \mathcal{C}_2)$ kvantni $[n, k_1 - k_2]$-linearan kod.

Pokazat ćemo da možemo ispraviti t bit flip ili flip u fazi grešaka koristeći svojstva klasičnih kodova $\mathcal{C}_1$ i $\mathcal{C}_2^\perp$.

Označimo sa e_B i e_F vektore u $\mathbb{F}_2^n$ koji opisuju bit flip i flip u fazi greške koje je pretrpjela kodna riječ $x+\mathcal{C}_2$ prolaskom kroz komunikacijski kanal – vektor e_B (odnosno e_F) na i-toj poziciji ima jedinicu ako i samo ako je nastala bit flip (odnosno flip u fazi) greška na i-tom qubitu. Dakle, primljeno stanje možemo ovako zapisati (razmislite zašto)

$$|\tilde{\psi}\rangle = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)\cdot e_F} |x+y+e_B\rangle , \tag{7.1}$$

gdje je $(x+y)\cdot e_F$ standardni skalarni produkt na $\mathbb{F}_2^n$.

Primljenom stanju $|\tilde{\psi}\rangle$ dodajemo kvantni registar s $n-k_1$ qubita u početnom stanju $|0\rangle$. Tada primjenom operatora

$$|z\rangle\,|w\rangle \mapsto |z\rangle\,|H_1(z)+w\rangle ,$$

gdje je H_1 parity check matrica koda $\mathcal{C}_1$, dobivamo stanje

$$\frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)\cdot e_F} |x+y+e_B\rangle\,|H_1(e_B)\rangle ,$$

jer je $H_1(x+y)=0$ zbog $x+y\in\mathcal{C}_1$ (po definiciji je $\mathcal{C}_1=\ker H_1$).

Mjerenjem dodatnog registra, bez mijenjanja primljenog stanja $|\tilde{\psi}\rangle$, saznajemo sindrom greške $H_1(e_B)$, odnosno e_B do na jezgru $\mathcal{C}_1$. Izračunajmo bilo koji w takav da je $H_1(w)=H_1(e_B)$. Tada je $w=e_B+c_1$ za neki $c_1\in\mathcal{C}_1$. Primjenom koda za ispravljanje grešaka $\mathcal{C}_1$ na w, u slučaju kad je broj bit flip grešaka (odnosno broj jedinica u e_B) manji ili jednak t, možemo izračunati c_1 (jer $\mathcal{C}_1$ ispravlja t grešaka), a onda i $e_B=w-c_1$. Greške možemo ispraviti tako da primjenjujemo operator X na qubitove opisane s e_B i tako dobijemo stanje

$$|\tilde{\psi'}\rangle = \frac{1}{\sqrt{|\mathcal{C}_2|}} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)\cdot e_F} |x+y\rangle , \tag{7.2}$$

Da bismo detektirali flip u fazi (odnosno vektor e_F iz (7.2)) primijenit ćemo Hadamardov operator na svaki qubit stanja $|\tilde{\psi}'\rangle$. (Prisjetimo se da vrijedi formula $H|w\rangle = \frac{1}{\sqrt{2^n}} \sum_{z=0}^{2^n-1} (-1)^{w\cdot z} |z\rangle$.) Dobivamo

$$\frac{1}{\sqrt{|\mathcal{C}_2|2^n}} \sum_{z=0}^{2^n-1} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)\cdot(e_F+z)} |z\rangle ,$$

odnosno uz supstituciju $z' = z + e_F$

$$\frac{1}{\sqrt{|\mathcal{C}_2|2^n}} \sum_{z'=0}^{2^n-1} \sum_{y\in\mathcal{C}_2} (-1)^{(x+y)\cdot z'} |z' + e_F\rangle .$$

Budući da je (vidi Zadatak 7.12)

$$\sum_{y\in\mathcal{C}_2} (-1)^{y\cdot z'} = \begin{cases} |\mathcal{C}_2| & \text{ako je } z' \in \mathcal{C}_2^\perp \\ 0 & \text{inače} \end{cases}$$

dobivamo

$$\sqrt{\frac{|\mathcal{C}_2|}{2^n}} \sum_{z'\in\mathcal{C}_2^\perp} (-1)^{x\cdot z'} |z' + e_F\rangle .$$

No ovo je bit flip problem za $\mathcal{C}_2^\perp$ i vektor e_F! Kao i ranije, uvođenjem novog registra i korištenjem parity check matrice H_2 koda $\mathcal{C}_2^\perp$, mjerimo $H_2(e_2)$ i ispravljanjem grešaka dobivamo stanje

$$\frac{1}{\sqrt{2^n/|\mathcal{C}_2|}} \sum_{z'\in\mathcal{C}_2^\perp} (-1)^{x\cdot z'} |z'\rangle .$$

Konačno, primjenom Hadamardovih vrata na sve qubite dobivamo polaznu kodnu riječ

$$\frac{1}{\sqrt{\mathcal{C}_2}} \sum_{y\in\mathcal{C}_2} |x + y\rangle .$$

Primjer (Steaneov kod). Označimo sa $\mathcal{C}$ Hammingov $[7,4,3]$-linearan kod određen parity check matricom

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

i matricom generatora

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}.$$

Definirajmo $\mathcal{C}_1 = \mathcal{C}$ i $\mathcal{C}_2 = \mathcal{C}^\perp$. Kako je $\mathcal{C}_2^\perp = (\mathcal{C}^\perp)^\perp = \mathcal{C}$, kodovi $\mathcal{C}_1$ i $\mathcal{C}_2^\perp$ ispravljaju $\frac{3-1}{2} = 1$ grešku. Kako je $\mathcal{C}_2 \subset \mathcal{C}_1$(jer su stupci matrice generatora H^T koda $\mathcal{C}_2$ sadržani u potprostoru generiranom sa stupcima matrice generatora G koda $\mathcal{C}_1$, provjerite to), slijedi da je $CSS(\mathcal{C}_1, \mathcal{C}_2)$ kvantni $[7,1]$ kod.

7.4 Kvantna kriptografija

U ovom odjeljku ćemo opisati protokol kvantne kriptografije za razmjenu ključeva BB84 (Bennett, Brassard 1984). Za razliku od shema za razmjenu ključeva klasične kriptografije, ovaj protokol je dokazivo siguran.

Alice i Bob komuniciraju javnim klasičnim i kvantnim kanalima dok ih Eve (povremeno) prisluškuje.

1. Alice za početak slučajno generira dva stringa nula i jedinica duljine n, $x = x_1 \dots x_n$ i $y = y_1 \dots y_n$. Pomoću njih ona konstruira (faktorizirano) stanje sustava od n qubita

$$|\psi\rangle = \otimes_{i=1}^n |\psi_{x_i y_i}\rangle ,$$

gdje je

$$|\psi_{00}\rangle = |0\rangle\,, \quad |\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),$$
$$|\psi_{10}\rangle = |1\rangle\,, \quad |\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

2. Alice pošalje tih n qubita Bobu.

3. Bob generira slučajan string $y' \in \{0,1\}^n$ i svaki primljeni qubit mjeri po sljedećem pravilu:

   a) ako je $y'_i = 0$, onda mjeri qubit u standardnoj bazi $\{|0\rangle\,, |1\rangle\}$,

   b) ako je $y'_i = 1$, onda mjeri qubit u bazi $\{|+\rangle\,, |-\rangle\}$.

   Neka je $x' \in \{0,1\}^n$ string rezultata Bobovih mjerenja (ishode mjerenja $|0\rangle$ i $|+\rangle$ bilježi sa 0 dok ishode $|1\rangle$ i $|-\rangle$ označava sa 1).

4. Alice i Bob javno objave stringove y i y' te iz stringova x i x' izbace sve one bitove x_i i x'_i za koje je $y_i \neq y'_i$. Ono što preostane od stringova x i x' je njihov "poluprivatni" ključ. U idealnom slučaju, ako nije došlo do greške u komunikaciji (posebno, ako Eve nije utjecala na poslane qubite), zbog konstrukcije stanje $|\psi\rangle$ vidimo da $y_i = y'_i$ implicira $x_i = x'_i$ (zašto?) pa su Alice i Bob uspješno razmijenili privatni ključ.

   Što ako je došlo do greške u komunikaciji, odnosno što ako ih je Eve prisluškivala?

Objasnimo na primjeru jednu vrstu "napada" kojim Eve može doći do informacije o (poluprivatnom) ključu. Pretpostavimo da Eve presretne qubit i (za koji se kasnije ispostavi da je $y_i = y'_i$) i izmjeri ga u bazi $\{|\phi_0\rangle\,, |\phi_1\rangle\}$ gdje je

$$|\phi_0\rangle = \cos\frac{\pi}{8}\,|0\rangle + \sin\frac{\pi}{8}\,|1\rangle \quad \text{i} \quad |\phi_1\rangle = -\sin\frac{\pi}{8}\,|0\rangle + \cos\frac{\pi}{8}\,|1\rangle\,.$$

Eve zatim izmjereno stanje, $|\phi_0\rangle$ ili $|\phi_1\rangle$, pošalje Bobu (tako da on i dalje misli da je Alice pošiljatelj). Što Eve može saznati o x i x'? Pretpostavimo da je $y_i = y_i' = 0$ (drugi se slučaj slično analizira). Tada je $|\psi_{x_i y_i}\rangle$ jednak $|0\rangle$ ili $|1\rangle$. Ako Eve izmjeri $|\phi_0\rangle$, koja je vjerojatnost $P(|0\rangle \,\big|\, |\phi_0\rangle)$ da je $|\psi_{x_i y_i}\rangle = |0\rangle$, odnosno, da je $x_i = 0$? Vrijedi da je

$$|0\rangle = \cos\frac{\pi}{8}\,|\phi_0\rangle - \sin\frac{\pi}{8}\,|\phi_1\rangle \quad \text{i} \quad |1\rangle = \sin\frac{\pi}{8}\,|\phi_0\rangle + \cos\frac{\pi}{8}\,|\phi_1\rangle\,,$$

pa je prema Bayesovom teoremu (uobičajeno $P(A\big|B)$ označava uvjetnu vjerojatnost za A uz uvjet da se dogodio B)

$$P(|0\rangle \,\big|\, |\phi_0\rangle) = \frac{P(|\phi_0\rangle \,\big|\, |0\rangle)P(|0\rangle)}{P(|\phi_0\rangle)} = \cos^2\frac{\pi}{8} \approx 0.85,$$

jer je

$$\begin{aligned} P(|\phi_0\rangle) &= P(|\phi_0\rangle \,\big|\, |0\rangle) \cdot P(|0\rangle) + P(|\phi_0\rangle \,\big|\, |1\rangle) \cdot P(|1\rangle) \\ &= \frac{1}{2}(\cos^2\frac{\pi}{8} + \sin^2\frac{\pi}{8}) = \frac{1}{2}. \end{aligned}$$

Ovdje pretpostavljamo da Eve nema nikakvu dodatnu informaciju o x_i pa je a priorna vjerojatnost $P(|0\rangle) = P(|1\rangle) = \frac{1}{2}$ jer je string x slučajno odabran.

Dakle, Eve će u 85% slučajeva saznati x_i, ali nakon toga qubit će se nalaziti u stanju $|\phi_0\rangle$ pa kad ga Bob bude mjerio (u bazi $\{|0\rangle\,, |1\rangle\}$ jer je $y_i' = 0$) s vjerojatnosti od $\sin^2\frac{\pi}{8} \approx 0.15$ dobit će $x_i' \neq x_i$ – odnosno njezino uplitanje u tom će slučaju biti vidljivo u poluprivatnom ključu (x, x').

5. U ovoj fazi protokola Alice i Bob moraju procijeniti koliko Eve zna o x i x'. Za to će "žrtvovati", recimo, pola slučajno odabranih bitova stringova x i x' (iz kojih su prethodno izbacili bitove za koje je $y_i \neq y_i'$) koje će javno objaviti i usporediti. Ako je nepodudarnost (tj. broj bitova za koje je $x_i \neq x_i'$) prihvatljiva (recimo, manja od 10%) onda nastavljaju s korištenjem druge polovice ključa, inače cijeli postupak (od prvog koraka) ponove.

6. U ovom trenutku Alice i Bob imaju stringove x i x' za koje procjenjuju da se podudaraju u 90% bitova. U posljednjem koraku protokola, koristeći dvije metode klasične kriptografije (eng. information reconciliation, privacy amplification), oni transformiraju stringove x i x' tako da

   a) se transformirani x i x' podudaraju na skoro svim mjestima s velikom vjerojatnošću

   b) Eve nema skoro nikakvu informaciju o stringovima.

   Dobivene stringove Alice i Bob tada mogu sigurno koristiti kao zajednički privatni ključ.

Opišimo ukratko završnu proceduru. Alice i Bob prvo trebaju otkriti na kojim bitovima se stringovi x i x' razlikuju (ali tako da objave što manje informacija o x i x' jer, sjetimo se, njihova komunikacija je javna). Postupak (information reconciliation) je sljedeći.

i) Alice i Bob prvo primijene (svatko svoju) slučajnu permutaciju na stringove x i x' kako bi greške ravnomjerno preraspodijelili.

ii) Zatim podijele stringove u blokove od po b bitova, gdje je b odabran tako da je malo vjerojatno da blok ima više od jedne greške.

iii) Nakon toga javno usporede parnosti (sume bitova) blokova. Ako se parnosti ne podudaraju, onda binarnim pretraživanjem nastavljaju uspoređivati podblokove tog bloka sve dok ne pronađu grešku. Bit u kojem se nalazi greška izbace. Prilikom ovog postupka svima su otkrili informaciju o parnosti blokova (i podblokova) koje su obrađivali pa da bi tu informaciju "pobrisali" iz svakog takvog bloka izbacuju zadnji bit.

iv) Moguće je da ovim postupkom nisu otkrivene sve greške zbog toga što su se na početku u nekom bloku moglo nalaziti više grešaka. Zato ovaj cijeli postupak ponavljaju nekoliko puta.

U ovom trenutku, stringovi x i x' se gotovo sigurno podudaraju u svim bitovima. Problem je što Eve možda zna vrijednosti nekih bitova. U posljednjem koraku (privacy amplification) ovog protokola Alice i Bob primijene neku hash funkciju na x i x' koja ih komprimira na neku manju duljinu te tako "uništi" svaku informaciju koju je Eve imala o njima.

8 Zadaci

8.1 Zadaci

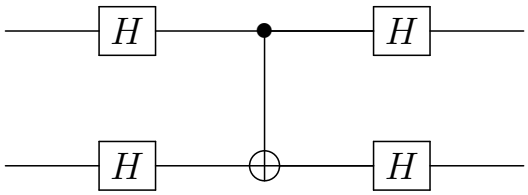
Na internetu je slobodno dostupan velik broj skripti sa zadacima iz kolegija vezanih uz kvantno računanje [Aar17, Pre13, Vaz04]. Ovdje navodimo neke zadatke koji mogu poslužiti studentima za vježbu.

1. Jesu li dva qubita opisana stanjem

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

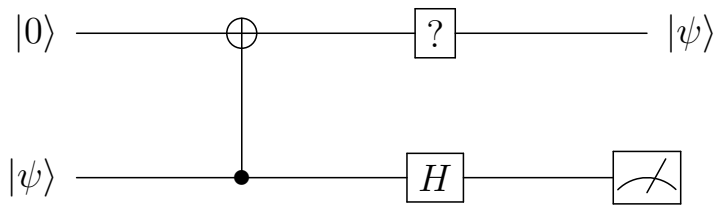
   kvantno spregnuta?

2. Što radi ovaj program?



3. Promotrite sljedeći kvantni krug. Ovisno o rezultatu mjerenja drugog 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

$$|\Psi_1\rangle = \frac{1}{\sqrt{10}} \left(3\,|0\rangle + |1\rangle\right) \text{ i } |\Psi_2\rangle = \frac{1}{\sqrt{10}} \left(3\,|0\rangle - |1\rangle\right).$$

    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.)

8.2 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.

9 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).*

B Diofantske aproksimacije i verižni razlomci

Za detaljan prikaz osnovnih rezultata iz teorije diofantskih aproksimacija čitatelja upućujemo na osmo poglavlje u knjizi [Duj20]. Ovdje ćemo obraditi samo one rezultate koji su nam važni za razumijevanje Shorovog algoritma.

Neka je α realan broj. Definirajmo $a_0 = \lfloor \alpha \rfloor$. Ako je $\alpha \neq a_0$, onda postoji realan broj $\alpha_1 > 1$ takav da je $\alpha = a_0 + \dfrac{1}{\alpha_1}$. Definirajmo $a_1 = \lfloor \alpha_1 \rfloor$. Ako je $\alpha_1 \neq a_1$, onda kao i ranije postoji $\alpha_2 > 1$ takav da je $\alpha_1 = a_1 + \dfrac{1}{\alpha_2}$, odnosno $\alpha = \alpha = a_0 + \dfrac{1}{a_1 + \dfrac{1}{\alpha_2}}$. Ponavljanjem ovog postupka dobivamo *verižni razlomak* broja α

$$[a_0, a_1, a_2, \ldots, a_n, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n + \cfrac{1}{\ddots}}}}}.$$

Verižni razlomak je konačan ako i samo ako je α racionalan broj. Racionalni brojevi $\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n]$ se nazivaju *konvergente* verižnog razlomka. Zadovoljavaju jednostavnu rekurzivnu relaciju pomoću koje ih možemo efikasno računati.

Lema B.1. *Uz početne uvjete* $p_0 = a_0$, $p_1 = a_0a_1 + 1$, $q_0 = 1$ *i* $q_1 = a_1$ *brojevi* p_n *i* q_n *zadovoljavaju rekurzivne relacije*

$$p_n = a_n p_{n-1} + p_{n-2}, \qquad q_n = a_n q_{n-1} + q_{n-2}.$$

Konvergente su važne jer su dobre racionalne aproksimacije broja α u sljedećem smislu.

U teoriji diofantskih aproksimacija "kvaliteta" racionalne aproksimacije $\frac{p}{q}$ (p i q su relativno prosti) broja α se mjeri time koliko je $\frac{p}{q}$ blizu broju α u odnosu na veličinu nazivnika. Za početak, ako fiksiramo $q \in \mathbb{N}$, jasno je da uvijek možemo naći p takav da je $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q}$ pa nam aproksimacije koje zadovoljavaju tu nejednakost nisu zanimljive. Također, ako je α iracionalan broj, nije teško pokazati koristeći Dirichletov princip da postoji beskonačno mnogo parova (p, q) za koje je $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ (Dirichletov teorem). Takvih aproksimacija i dalje ima previše da bi ih mogli klasificirati. No ako zahtjev na aproksimaciju samo malo pojačamo dobivamo vrlo zanimljiv rezultat.

Teorem B.2 (Legendre, 1798.)**.** *Neke je* $\alpha \in \mathbb{R}$. *Pretpostavimo da je* $\frac{p}{q}$ *racionalan broj takav da je*

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{2q^2}.$$

Tada je $\frac{p}{q}$ *konvergenta verižnog razlomka broja* α.

Ako je α racionalan broj, onda njegovih konvergenti ima konačno mnogo i koristeći Lemu B.1 sve ih možemo efikasno izračunati.