Kvantno računanje

Matija Kazalicki

1 Uvod

Krajem listopada 2019. u popularnim medijima odjeknula je vijest da je Googlovo kvantno računalo Sycamore (na hrvatskom javor) demonstriralo kvantnu premoć - za 200 sekundi je izračunalo nešto za što bi najboljem klasičnom superračunalu trebalo 10 000 godina. [1] Iako program koje 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 javno 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 Deutch, počinje se ozbiljnije proučavati. Tako je na primjer Deutch 1985. u analogiji sa 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 nije odgovoreno. 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

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

je konstruirao neke (ne baš praktične) algoritme koji sugeriraju da bi to moglo biti tako, no pravo iznenađenje se dogodilo 1994. kad 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 problemi faktorizacije prirodnih brojeva i problem diskretnog logaritma. Danas je opće prihvaćeno da se ti problemi ne mogu efikasno riješiti na klasičnom računalu, ali to nije dokazano.

No, što je to kvantno računalo?

Najkraće rečeno, kvantno računalo je kvantno mehanički sustav koji efikasno uzorkuje vjerojatnosnu distribuciju koja je opisana programom koje računalo izvodi. Slikovito, zamislimo da želimo simulirati milijun bacanja neke komplicirane igraće kocke sa 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 bacanje kocke pojavljuje) trebalo oko petabajt memorije što je jedva dostupno na najvećim svjetskim superračunalima. S druge strane, kvantno računalo, uređaj koji je baziran na čudesnim zakonima kvantne mehanike takvu kocku može simulirati sa 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 težini se temelji moderna kriptografija). Ono što je najvažnije je 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 ovih predavanja je bez ulaženja u kvantnu mehaniku izložiti matematički model kvantnog računanja (koji je opisan jezikom linearne algebre) i nakon toga opisati neke kvantne algoritme. Studenti te algoritme (za domaću zadaću) mogu implementirati na IBM-ovim kvantnim računalima koji se nalaze na oblaku (IBM Q Experience).

2 Osnovni pojmovi kvantnog računjanja

Osnovne pojmove ćemo uvesti preko analogije sa klasičnim računarstvom.

2.1 Kvantni bit

Kvantni bit ili *qubit* je osnovna jedinica informacije u kvantnom računarstvu. Za razliku od klasičnog bita koji se može nalaziti u jednom od dva stanja - 0 ili 1, stanje qubita se opisuje vektorom norme 1 u dvodimenzionalnom unitarnom vektorskom prostoru $(V/\mathbb{C}, \langle\cdot|\cdot\rangle)$ s ortonormiranom bazom čiji se elementi tradicionalno označavaju s $|0\rangle$ i $|1\rangle$. Prostor V se naziva *prostor stanja*.

Primjer. Na primjer, jedan takav *vektor stanja* je

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

Na klasičnom računalu, ako pristupamo nekom bitu, na primjer u stanju 1, pohranjenom na hard disku, uvijek ćemo očitati (izmjeriti) 1 (osim ako slučajno neka kozmička zraka nije 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 ćemo dobiti $|\Phi_0\rangle$ s vjerojatnošću $\langle\Psi|\Phi_0\rangle^2$ i $|\Phi_1\rangle$ s vjerojatnošću $\langle\Psi|\Phi_1\rangle^2$. Ako $|\Psi\rangle$ iz primjera izmjerimo u bazi $\{|0\rangle, |1\rangle\}$ (gotovo uvijek ćemo mjeriti u toj bazi tako da ako kod mjerenja ne specificiramo bazu u kojoj mjerimo na tu bazu mislimo) dobit ćemo $|0\rangle$ s vjerojatnošću $\frac{1}{2}$ te $|1\rangle$ s vjerojatnošću $\frac{1}{2}$. Primijetimo da isto vrijedi i za stanje $\left|\tilde{\Psi}\right\rangle = \frac{i}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ iako su ta dva stanja različita.

Sada je jasno zašto zahtjevamo 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.

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 se opisuje 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 $V^{\otimes n}$ je unitaran vektorski prostor dimenzije 2^n s istaknutom ortonormiranom bazom $\{|00\cdots00\rangle, |00\cdots01\rangle, |00\cdots10\rangle, \ldots, |11\cdots11\rangle\}$. Kako su elementi te baze indeksirani binomnim razvojem brojeva od 0 do 2^n-1, nekada elemente te baze označavamo i ovako $\{|0\rangle, |1\rangle, \ldots, |2^n-1\rangle\}$. Također, na primjer, umjesto $|010\rangle$ možemo pisati $|0\rangle|1\rangle|0\rangle$ ili još matematički najpravilnije $|0\rangle \otimes |1\rangle \otimes |0\rangle$.

Ono što razlikuje tenzorski produkt od ostalih unitarnih vektorskih dimenzije 2^n je operacija $\otimes$ - tenzorsko množenje. Ta operacija je definirana preko bilinearnog preslikavanja $V \times V \times \cdots \times V \to V^{\otimes n}$ 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 $\{0, 1\}$.

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

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

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

Uočimo da se ne mogu svi vektori iz $V^{\otimes n}$ "faktorizirati". Stanje $\frac{1}{\sqrt{34}}(|00\rangle + 2|01\rangle + 2|10\rangle + 5|11\rangle)$ je jedan takav primjer. U tom slučaju kažemo da su qubiti koji to stanje opisuje *kvantno spregnuti* (eng. quantum entaglement). Posebno to 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 je posebno teško kvalitetno implementirati (problem je što se u interakciji s okolinom brzo "raspadaju") što 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 su Alice i Bob svaki u posjedu po jednog qubita (npr. elektrona 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 $\frac{\alpha_{10}|10\rangle+\alpha_{11}|11\rangle}{\sqrt{|\alpha_{11}|^2+|\alpha_{11}|^2}}$.

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

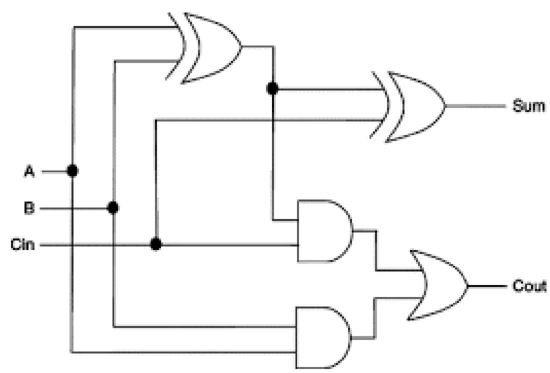
Primjer (EPR paradoks). Promotrimo takozvano Bellovo stanje

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

Možemo opet zamisliti Alice i Bob na različitim krajevima svijeta koji su u posjedu tih qubita. 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! Ovo je malo zbunjujuće, je li došlo do prijenosa informacije brzinom većom od brzine svjetlosti? Ovaj pararodoks je zbunjivao i poznate fizičare (EPR = Einstein, Podolsky i Rosen).

2.3 Kvantna vrata

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



Slika 1: Zbrajalo

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

Što su to kvantna vrata? Općenito kvantna vrata su proizvoljni unitarni operatori na prostoru stanja. Slično kao u klasičnom slučaju, istaknut ćemo mali broj kvantnih vrata pomoću kojih možemo "simulirati" proizvoljan unitaran operator.

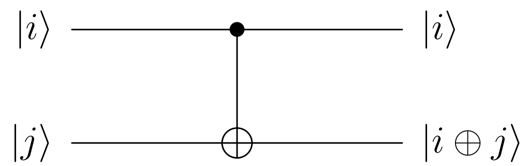
Krenimo s vratima koja djeluju na jedan qubit.

- NOT ili X vrata: $X\left|0\right\rangle = \left|1\right\rangle$, $X\left|1\right\rangle = \left|0\right\rangle$, tj. $X(\alpha\left|0\right\rangle + \beta\left|1\right\rangle) = \beta\left|1\right\rangle + \alpha\left|0\right\rangle$. Matrično $X = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.

- Z vrata: $Z\left|0\right\rangle = \left|0\right\rangle$, $Z\left|1\right\rangle = -\left|1\right\rangle$. Matrično $Z = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

- Hadamardova vrata H: $H\left|0\right\rangle = \frac{\left|0\right\rangle+\left|1\right\rangle}{\sqrt{2}}$, $H\left|1\right\rangle = \frac{\left|0\right\rangle-\left|1\right\rangle}{\sqrt{2}}$. Matrično $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. Uočimo da je $H^2 = Id$.

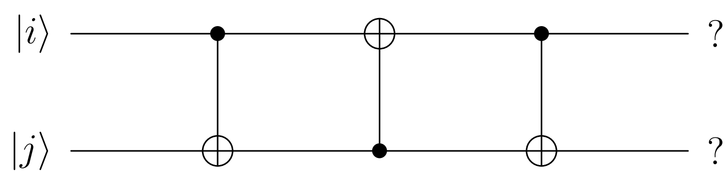
Od vrata koja djeluju na dva qubita trebat će nam kontrolirana NOT ili CNOT vrata. Ona djeluju na dva qubita, kontrolni qubit $|i\rangle$ i qubit $|j\rangle$. Kontrolni qubit se ne mijenja, dok se na drugi qubit primjenjuju NOT ili X vrata ako je kontrolni qubit jednak $|1\rangle$, inače se ništa ne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



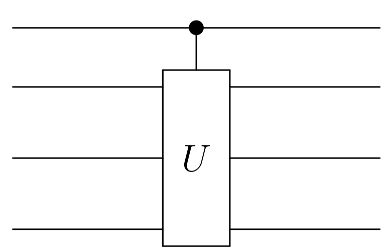
Slika 2: CNOT vrata

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

Zadatak 1. Što radi ovaj program?



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

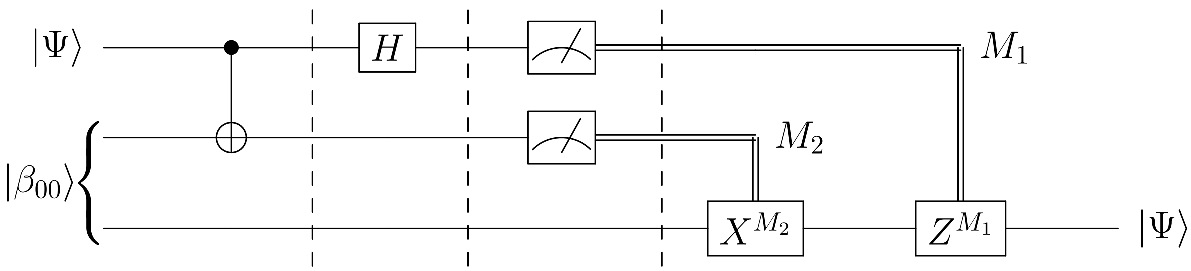


Slika 3: CU vrata

2.4 Primjer - Kvantna teleportacija

Pretpostavimo da Alice i Bob dijele Bellovo stanje $|\beta_{00}\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ - Alice je u posjedu prvog qubita, a Bob drugog. Alice želi prenijeti (teleportirati) qubit $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$ Bobu. Problem je što ni sama ne zna koeficijente α i β, 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 je u posjedu prva dva qubita, dok Bob ima pristup trećem).



Slika 4: Kvantna teleportacija

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

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

Nakon primjene CNOT vrata dobivamo stanje

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

Primjenom Hadamardovih vrata na prvi qubit dobivamo stanje

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

Primijetimo da smo u drugoj jednakosti promijenili način označavanja qubita (npr. $|0\rangle|01\rangle \mapsto |00\rangle|1\rangle$) kako bi 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 $|\Psi_B\rangle$ će biti 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 sa X vratima dobit ćemo stanje $|\Psi\rangle$. Preostali slučajevi se dokazuju na sličan način.

Nekoliko komentara za kraj. Uočimo da je Alicina kopija stanja $|\Psi\rangle$ uništena u ovom procesu. 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 većeom od brzine svjetlosti. Bez rezultata Alicinog mjerenja Bob ne zna u kojem od četiri moguća stanja se nalazi njegov qubit i zato iz njega ne može "izvući" nikakvu klasičnu informaciju. Teleportacija nije samo teorijski koncept, 2017. godine su kineski znanstvenici 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/`.

3 Kvantni algoritmi

3.1 Deutsch-Jozsa algoritam

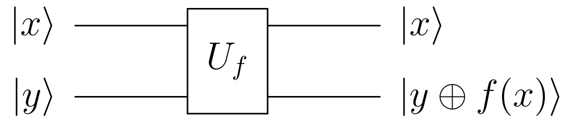
Pretpostavimo da nam je dana funkcija $f : \{0,1\} \to \{0,1\}$ za koju se zna da je ili konstanta ili balansirana (tj. $\# f^{-1}(\{0\}) = \# f^{-1}(\{1\}) = 2^{n-1}$). Problem je koristeći što manje poziva funkcije f odrediti je li funkcija konstantna ili balansirana. Klasično, u najgorem slučaju nam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

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

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

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

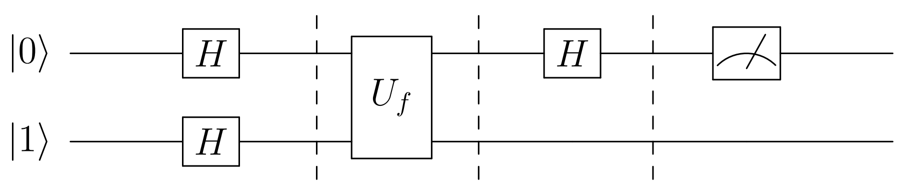
Primijetimo da je U_f uistinu unitaran operator pa predstavlja neka kvantna vrata. Inače, nismo mogli definirati funkciju na samo jednom



Slika 5: Kvantna proročica

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 program.



Slika 6: Deutschov algoritam

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

Lema 3.1. *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

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

što je trebalo i dokazati. $\square$

Računamo međustanja nakon svake barijere.

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

Za domaću zadaću poopćite ovaj algoritam tako da radi za proizvoljan n.

3.2 Groverov algoritam pretraživanja

3.2.1 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 ćemo identificirati sa elementima kanonske baze prostora stanja n qubita $V^{\otimes n}$, tako 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 Detschovog algoritma, funkcija $f(x)$ je implementirana pomoću kvantnih vrata U_f koja su na bazi prostora $V^{\otimes n} \otimes V$ definirana formulom

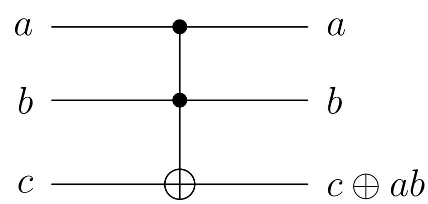
$$|x\rangle\, |q\rangle \mapsto |x\rangle\, |q \oplus f(x)\rangle\,.$$

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 bi osigurali invertibilnost operatora U_f. Taj operator se tradicionalno naziva kvantna proročica jer u opisu algoritma pretraživanja nećemo ulaziti u detalje njene implementacije nego ćemo slijepo vjerovati onome što kaže. Ilustrirajmo na primjeru faktorizacije da ove postavke imaju smisla.

Neka je zadan velik prirodan broj n (recimo od 200 znamenaka) koji je produkt dva prosta broja. Naš zadatak je pronaći te proste brojeve (odnosno razbiti RSA kriptosustav). Prva što nam padne na pamet je da za svaki broj od 2 do $\sqrt{m}$ provjerimo dijeli li m - to je problem pretraživanja. Modeliramo ga pomoću funkcije $f : \{2, 3, \ldots, \lfloor\sqrt{2}\rfloor\} \to \{0, 1\}$, 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).

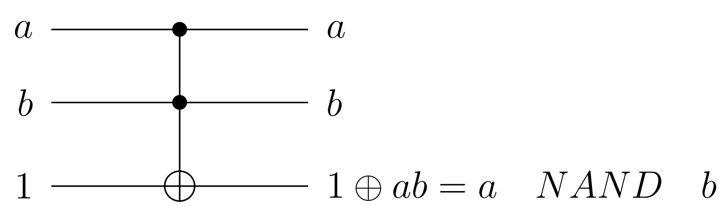
Druga važno pitanje koje nismo do sada spomenuli u ovim predavanjima je pitanje "prevođenja" klasičnih programa u kvantne programe. Konkretno, ako imate efikasnu implementaciju funkcije $f(x)$ pomoću logičkog kruga koji se sastoji od vrata AND, OR i XOR, možete li zamjenom klasičnih vrata s njihovim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

Odgovor je da uz malo pažnje možete. Očiti problem je 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 je poznato da postoje invertibilna (reverzibilna) vrata koja mogu simulirati sva ostala vrata. Primjer takvih vrata su Toffolijeva vrata.



Slika 7: Toffolijeva vrata

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



Nije se teško uvjeriti da u logickom krugu koji implementira funkciju $f(x)$ možemo svaki AND, OR i XOR zamijeniti s 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 primijenjujemo operator U_f ćemo postaviti 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 ga nećemo ni pisati pa da bi to naglasili umjesto U_f koristit ćemo proročicu $\mathcal{O}$ koju na elementu (ortonormirane) baze $|x\rangle$ definiramo formulom $\mathcal{O}|x\rangle = (-1)^{f(x)}|x\rangle$.

3.2.2 Osnovna ideja

Pomalo iznenađujuće, osnovna ideja Groverovog algoritma je 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) problema 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 cilj je 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 $|\Phi\rangle\langle\Phi|$ ćemo označiti 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 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 prirodan 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 $G^k \left|\Psi\right\rangle$ s velikom vjerojatnošću ćemo izmjeriti vektor koji će biti rješenje problema traženja (što je $G^k \left|\Psi\right\rangle$ bliže stanju $\left|\beta\right\rangle$ to će ta vjerojatnost biti veća).

3.2.3 Implementacija i analiza algoritma

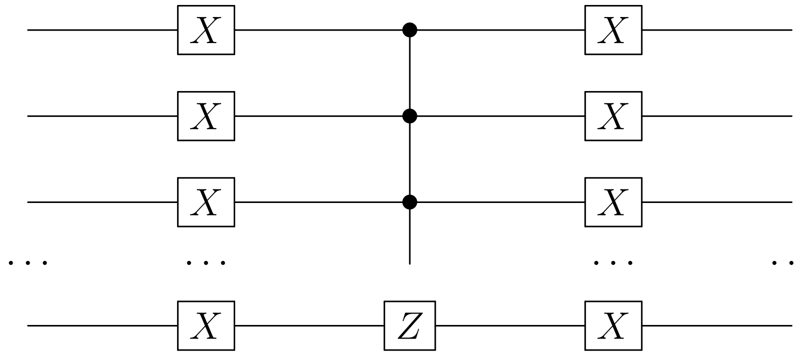
Kako bi konstruirali stanje $\left|\Psi\right\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} \left|x\right\rangle$ možemo na svaki qubit početnog stanja $\left|00\cdots 0\right\rangle = \left|0\right\rangle^{\otimes n}$ primijeniti operator H. Lako se vidi da je vektor $H^{\otimes n} \left|0\right\rangle^{\otimes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

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

$$H^{\otimes n} \left(2 \left|00\cdots 0\right\rangle\left\langle 00\cdots 0\right| - I\right) H^{\otimes n} = \left(2 \left|\Psi\right\rangle\left\langle\Psi\right| - I\right).$$

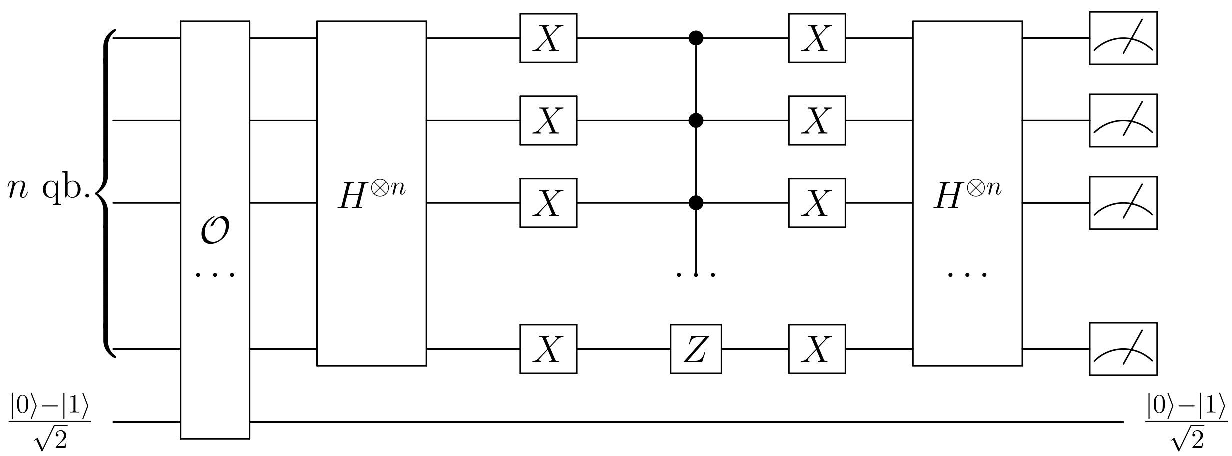
(Općenito, ako je W refleksija u odnosu na vektor w i U neki unitarni operator (čuva skalarni produkt), onda je $U^{-1}WU$ refleksija u odnosu na vektor $U^{-1}w$ - dokažite to. U našem slučaju je $(H^{\otimes n})^{-1} = H^{\otimes n}$.) Refleksiju oko vektora $\left|00\cdots 0\right\rangle$ (komponiranu s centralnom simetrijom) možemo implementirati pomoću vrata X i kontroliranih Z vrata (prvih $N-1$ qubita kontrolira primjenu vrata Z na preostali qubit).

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



Slika 8: Refleksija komponirana s centralnom simetrijom

Operator G onda ovako izgleda.



Slika 9: Operator G

Koliko puta trebamo primijeniti G da bi zarotirali $|\Psi\rangle$ 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 krugu rotiranja

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

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 $0 \leq \delta \leq \frac{\theta}{2}$. Tada je $|a| = |\sin \delta| \leq |\sin \frac{\theta}{2}|$, pa je $|a|^2 \leq \sin^2 \frac{\theta}{2} = \frac{M}{N} = \frac{1}{N}$.

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 $O(\sqrt{N})$.

4 Zadaci

Iz ovog gradiva bit će vam zadane dvije domaće zadaće. Rok za predaju je mjesec dana.

4.1 Domaća zadaća - zadaci

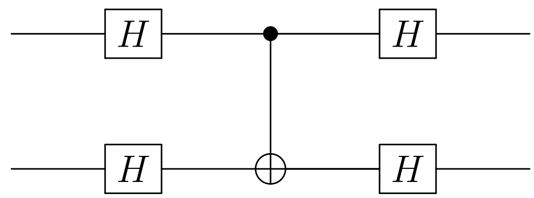
Riješite točno barem pet od sedam ponuđenih zadataka.

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 ovaj program radi?



3. 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.

4. 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 $|11\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

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

6. 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).

7. 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 vjerojatnosti koja je veća od 75%.

4.2 Qiskit projekt

Qiskit je open source okruženje (bazirano na Pythonu) za rad s IBM Q Experience kvantnim računalima. Za ovu domaću zadaću trebate ovladati s Qiskit-om te implementirati (i izvršiti) jedan od kvantnih algoritama po vlastitom izboru.
Osnovna literatura je Qiskit textbook

`https://qiskit.org/textbook/preface.html`.

Također postoje i razni tutoriali

`https://nbviewer.jupyter.org/github/Qiskit/qiskit-tutorials/blob/master/qiskit/1_start_here.ipynb`

Kao i ovaj user guide

`https://quantum-computing.ibm.com/support/guides/user-guide?section=5dcb2b45330e880045abccb0`

Literatura

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*, Cambridge University Press, Cambridge, 2010, http://doi.org/10.1017/CBO9780511976667