KVANTNO RAČUNANJE

March 5, 2019

UNIVERZITET U TUZLI
Prirodno-matematički fakultet
Odsjek: Fizika

Dženana Buljubašić

ZAVRŠNI RAD

KVANTNO RAČUNANJE

Tuzla, mart 2019.

Mentor: Dr. sc. Hedim Osmanović, vanredni profesor
Rad sadrži: 49 stranica
Redni broj završnog rada:

for my mom and dad

Sažetak

U okviru ovog rada istražujemo granice moderne računarske tehnologije i probleme sa kojima se danas suočava. Uveli smo i objasnili osnovne koncepte i zakone kvantne mehanike na kojima se kvantni računari baziraju, uključujući vektorsku reprezentaciju kvantnog stanja u Diracovoj notaciji, kao i operacije koje se vrše nad takvim stanjima. Definisali smo u sklopu toga i vezana stanja koja su od izrazite važnosti u simulaciji i riješavanju kompleksnih problema.

Vratili smo se korak unatrag i na primjeru klasičnih logičkih kola koji podliježu osnovama Booleanske algebre, formirali reverzibilna logička kvantna kola gdje ne dolazi do gubitka informacija. U okviru poglavlja o kvantnim kolima posebnu pažnju smo posvetili Hadamard kolu i simulaciji Bellovih stanja korištenjem IBM Q editora.

Na samom kraju smo se pozabavili koracima i primjenama nekih od najznačajnijih kvantnih algoritama, uključujući Deutsch-Jozsa algoritam.

Abstract

In this paper we are exploring the limits of modern computer technology and the problems which it is facing. We have introduced and explained basic concepts and laws of quantum physics which quantum computors are based upon, including vector representation of quantum state in Dirac notation, as well as the operations that are applied to such states. In that context we defined entangled states that are highly important when simulating and solving complex problems.

We also took a step back and, using an example of classical logic gates which operate according to the laws of Boolean algebra, formed a reversible logic quantum gate where there is no loss of information. Within chapter on quantum gates, we paid special attention to Hadamard gate and Bell state simulations using IBM Q editor.

In the end, we dealt with steps and applications of some of the most useful quantum algorithms, including Deutsch-Jozsa algorithm.

Sadržaj

1 Uvod

"I don't like it, and I'm sorry I ever had anything to do with it."

Erwin Schrödinger on Quantum Mechanics

Današnji moderni računari vrše obradu podataka bazirajući se na standardnom modelu proračuna, koji datira još od Turinga[1] i von Neumanna[2]. U okviru ovog modela svaka se informacija svodi na bite, koji mogu da imaju vrijednost 0 ili 1, a nad kojima se vrše relativno jednostavne operacije primjenom logičkih kola (AND, OR, NOT, $NAND$) koja djeluju na jedan ili dva bita u datom trenutku. U svakom momentu uz ovako definisane operacije, stanje računara je u potpunosti određeno stanjem svih bita, tako da se računar sa n bita nalazi u jednom od 2^n stanja, u granicama od 00...0 do 11...1.

Snaga kvantnog računara, s druge strane, leži upravo u širem spektru mogućih stanja. Kvantni računar, također posjeduje bite, ali koji, pored vrijednosti 0 i 1, mogu poprimiti i vrijednosti koje odgovaraju njihovoj linearnoj kombinaciji, što je poznato i kao osobina *superpozicije*. Kvantni bit, jednom riječju, nazivamo *qubit*. Kvantni računar koristi osobinu superpozicije koja dozvoljava održavanje ekponencijalno mnogo logičkih stanja u istom trenutku, od $|00...0\rangle$ do $|11...1\rangle$. Najkorisnija stanja nad kojima kvantni računar operiše su *vezana stanja* - stanja koja nisu dodijeljena ni jednom analognom ili digitalnom stanju pojedinačnog qubita. Kvantni računar je nedvojbeno, upravo zbog ove osobine, brži od običnog, klasičnog računara. Za mnoge probleme, kao što je defaktorizacija velikih brojeva, kvantni računar uveliko stoji u prednosti ispred klasičnog, obzirom da takav problem riješava u periodu od jednog dana, za što bi inače bilo potrebno nekoliko miliona godina.

Pomislili bismo da je razumijevanje kvantnog računanja ili kvantne fizike zahtjevno, ali matematički gledano kvantni koncepti, ako ih možemo tako objediniti, su samo nešto

[1] Alan Turing, rođen 1912. godine (London, Engleska) se često smatra ocem modernog računarstva. Dao je doprinos konceptu algoritma i računanja na Turingovoj mašini. Za vrijeme II svjetskog rata konstruisao je mašinu uz pomoć koje su saveznici dekodirali šifrirane poruke njemačke mornarnice i zrakoplovstva.

[2] John von Neumann rođen 1903. godine (Budimpešta, Austro-Ugarska monarhija) je mađarski matematičar koji je dao veliki doprinos kvantnoj fizici, funkcionalnoj analizi, računarskoj nauci i ekonomiji. Zajedno sa J. P. Eckertom i J. Mauchlyom formulisao je *von Neumannovu arhitekturu* čiji se princip primjenjuje u skoro svim današnjim računarima.

kompleksniji od srednjoškolske algebre. Kvantna fizika, kao i Einsteinova teorija relativnosti, zahtjeva suštinsko shvatanje nečega što je kontra-intuitivno.

1. Fizički sistem koji se nalazi u jendoznačno određenom stanju se i dalje može ponašati nepredvidljivo.

2. Dva sistema koja se nalaze na međusobno velikom rastojanju, bez ikakve fizičke veze, ipak mogu biti snažno povezani.

Što se tiče same potrebe za razvojem kvantnih računara, 1965. godine Gordon Moore[3], primjetio je da se ekonomski najoptimalnija gustina tranzistora unutar integrisanih krugova udvostručuje približno svakih 18 mjeseci. Zbijanjem tranzistora bliže jedan drugom ubrzava se mehanizam izmjene podataka, odnosno, povećava se brzina kojom računar operiše. Međutim, paralelno tome, postaje teže ukloniti oslobođenu toplotu tokom jednog ireverzibilnog procesa. Moore je predvidio da će se ovaj trend minijaturizacije nastaviti, što je danas poznato kao *Mooreov zakon*. Danas, velika većina računarske industrije smatra da će Mooreov zakon ostati na snazi još dvije ili tri generacije mikroprocesora, u najboljem slučaju. Tako, u naporima da se zakon održi, pribjegava se proizvodnji višejezgrenih procesora i korištenju novih, egzotičnih, poluprovodničkih materijala. U međuvremenu, ulažu se veliki napori i velika sredstva u razvoj i komercijalizaciju kvantnih računara.

[3]Gordon Moore rođen 1929. godine (San Francisco, California, USA) je američki biznismen, inženjer i su-osnivač Intel korporacije.

2 Kvantizacija sistema

2.1 Diracova notacija

Kvantni sistemi posjeduju određene osobine koje omogućuvaju kodiranje bita kao realnih fizičkih stanja. Jedna takva osobina je *spin* elektrona, koji prilikom mjerenja može imati samo dvije vrijednosti: spin *up* ili $|\uparrow\rangle$ (spin je tokom mjerenja bio paralelan osi posmatranja) i spin *down* ili $|\downarrow\rangle$ (spin je tokom mjerenja bio antiparalelan osi posmatranja). Ovakva unutrašnja diskretnost kvantnih sistema dozvoljava da se spin elektrona uzme za prirodnu binarnu jedinicu ili bit. Međutim, bilo koji drugi kvantni sistem za kojeg je karakteristična pojava dualnih kvatnih stanja, kao što je ravan polarizacije linearno polarizovanog fotona, smjer rotacije cirkularno polarizovanog fotona, ili diskretni energetski nivoi ekscitovanog atoma, mogu također poslužiti svrsi. Uopšteno, bilo koji kvantni sistem koji se koristi za reprezentaciju bita nazivamo kvantnim bitom (*qubit*).

Ket vektorska reprezentacija qubita

U Diracovoj[1] notaciji, qubit, koji u fizičkom sistemu predstavlja vrijednost klasičnog bita 0, ima oblik $|0\rangle$, dok qubit koji odgovara vrijednosti bita 1, ima oblik $|1\rangle$. Šta svaka od ovih notacija predstavlja ovisi isključivo o sistemu unutar kojeg vršimo kodiranje.

Matematički gledano, ket vektori su vektori kolone.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Kvantni bit nije ograničen da bude ili 0 ili 1 u datom trenutku i upravo se iz tog razloga jedan qubit predstavlja vektor kolonom sa dva faktora. Mjerenjem stanja kvantnog sistema, npr. mjerenjem spina elektrona, nalazimo da je spin ili $|\uparrow\rangle$ ili $|\downarrow\rangle$, što, predstavljeno u Diracovoj notaciji, odgovara stanjima $|0\rangle$ i $|1\rangle$, respektivno. Međutim, sve dok se sistem ne posmatra, isti se nalazi u stanju superpozicije:

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \quad |a|^2 + |b|^2 = 1$$

[1] Paul Dirac rođen 1903. godine (Bristol, Engleska, UK) je britanski fizičar i dobitnik Nobelove nagrade. Formulisao je jednačinu kojom je opisao ponašanje fermiona (Diracova jednačina), što je dovelo do pretpostavke o postojanju antimaterije.

Koeficijenti a i b su kompleksne amplitude komponenti $|0\rangle$ i $|1\rangle$. Uslovom da je $|a|^2+|b|^2 = 1$ osigurava se normiranost qubita, odnosno osigurava se da očitavanjem qubita, qubit bude u stanju $|0\rangle$ sa vjerovatnoćom $|a|^2$ ili u stanju $|1\rangle$ sa vjerovatnoćom $|b|^2$.

Za svaki ket vektor postoji odgovarajući bra vektor koji nosi ekvivalentnu informaciju o kvantnom stanju od interesa.

$$|\psi\rangle = a\,|0\rangle + b\,|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

$$\langle\psi| = a^*\,\langle 0| + b^*\,\langle 1| = \begin{pmatrix} a^* & b^* \end{pmatrix}$$

Unutrašnji i vanjski proizvod bra i ket vektora daje nam uvid u sličnosti između dva kvantna stanja. Tako, za par qubita u stanjima $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$ i $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$, definišemo unutrašnji proizvod $\langle\psi|\phi\rangle$ kao:

$$\langle\psi|\phi\rangle = (\langle\psi|)\cdot(|\phi\rangle) = \begin{pmatrix} a^* & b^* \end{pmatrix}\cdot\begin{pmatrix} c \\ d \end{pmatrix} = a^*c + b^*d.$$

Unutrašnji proizvod opisuje preklapanje stanja $|\psi\rangle$ i $|\phi\rangle$ jer varira od 0, za ortogonalna stanja, do 1, za normirana.

Vanjski proizvod $|\psi\rangle\,\langle\phi|$, definišemo kao:

$$|\psi\rangle\,\langle\phi| = (|\psi\rangle)\cdot(\langle\phi|) = \begin{pmatrix} a \\ b \end{pmatrix}\cdot\begin{pmatrix} c^* & d^* \end{pmatrix} = \begin{pmatrix} ac^* & ad^* \\ bc^* & bd^* \end{pmatrix}.$$

Vanjskim proizvodom se opisuje struktura unitarnih operatora koji, kako ćemo vidjeti, odgovaraju kvatnim logičkim kolima.

2.2 Blochova sfera

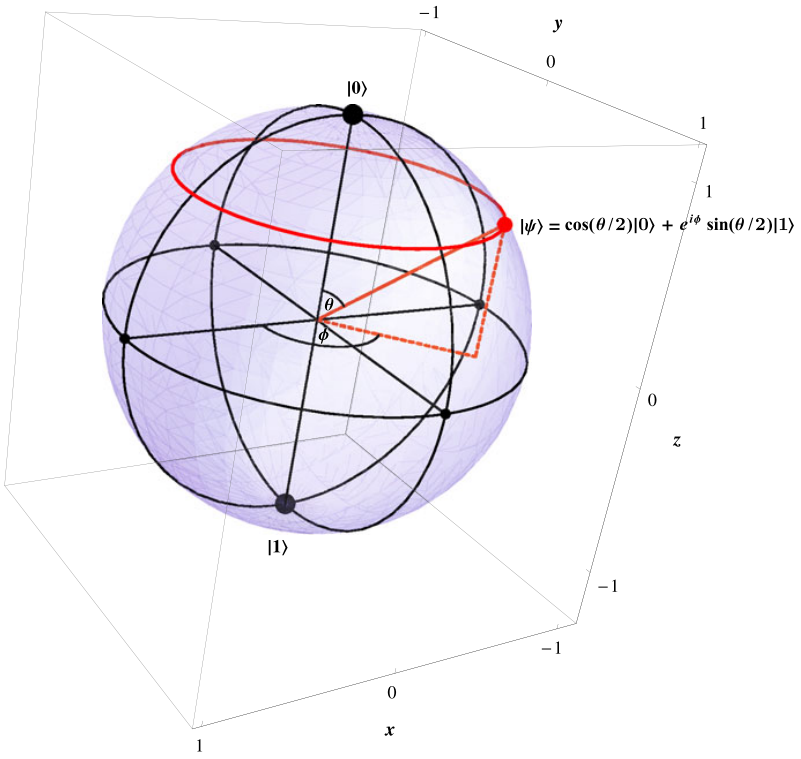
Ponašanje qubita analiziramo u kompleksnom dvodimenzionalnom vektorskom prostoru, ali koja je korelacija između takvog, dvodimenzionalnog, prostora i prostora u tri dimenzije? Kako se trodimenzionalni prostor preslikava u dvodimenzionalni prostor kompleksnih vektora?

Kvantno stanje jednog qubita možemo predstaviti jediničnim vektorom na Blochovoj sferi, koji je opisan sa dva parametra θ i ϕ.

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \qquad \begin{matrix} 0 \le \theta \le \pi \\ 0 \le \phi \le 2\pi \end{matrix}$$

Stanje qubita opisano je kao $|\psi\rangle = a\,|0\rangle + b\,|1\rangle$, gdje su a i b kompleksni brojevi, za koje vrijedi uslov normiranosti.

Dva su načina na koja predstavljamo kompleksne brojeve u dvodimenzionalnom prostoru. U kompleksnoj ravni, kompleksni broj c možemo pisati kao $c = a + ib$, ili preko polarnih koordinata definišući radijus vektor (intenzitet) kompleksnog broja c i ugao koji zaklapa za realnom osom, ugao ϕ, $c = re^{-i\phi}$.



Slika 2.2.1: Stanja računskih baza $|0\rangle$ i $|1\rangle$, i stanje qubita $|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$ u reprezentaciji Blochove sfere

Sada za stanje qubita, možemo pisati:

$$|\psi\rangle = r_0 e^{i\phi_0}\,|0\rangle + r_1 e^{i\phi_1}\,|1\rangle = e^{i\phi_0}(r_0\,|0\rangle + r_1 e^{i(\phi_1-\phi_0)}\,|1\rangle).$$

Faza $e^{i\phi_0}$ je fizički irelevantna. Mjerenjem, pomenuta faza neće uticati na konačan ishod sveukupnog stanja sistema, pa je možemo zanemariti.[2] Kako su r_0 i r_1 realni brojevi, vrijedi iz uslova normiranosti:

$$|r_0|^2 + |r_1|^2 = 1 \quad \Longrightarrow \quad \begin{aligned} r_0 &= \cos\frac{\theta}{2}, \\ r_1 &= \sin\frac{\theta}{2}, \end{aligned}$$

[2] Ovo je posljedica faznog *kick-back* efekta o kojem će biti riječi u narednim poglavljima. Više o efektu možete pogledati u dodatku B.

te dobivamo ranije definisani izraz za stanje qubita u zavisnosti od dva parametra, ugla θ i ugla ϕ.

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

Obzirom da qubit mora imati isključivo ili vrijednost $|0\rangle$, za $\theta = 0$, ili $|1\rangle$ za $\theta = 90^o$, sva kvantna stanja nalaze se na površini hemisfere, ne sfere. Ako želimo da stanja qubita odgovaraju površini cijele sfere, uvodimo novi ugao $\theta' = 2\theta$. Na ovaj način, umjesto da posmatramo qubit u dvodimenzionalnom kompleksnom vektorskom prostoru, možemo zamisliti da se nalazi na površini jedinične sfere u trodimenzionalnom prostoru. Direktna posljedica ove reprezentacije jest da su ortogonalna stanja ψ i ϕ, za koja vrijedi $\langle\psi|\phi\rangle = 0$, predstavljena kao antipodalne tačke na Blochovoj sferi, tj. u trodimenzionalnom prostoru se nalaze pod uglom od 180^o.

2.3 Multi-qubitni kvantni memorijski registri

Iako smo dosad razmatrali isključivo jedinične qubite, funkcionalni kvantni računar mora imati multi-qubitni kvantni memorijski registar koji se sastoji iz grupe od n qubita koji nose odgovarajuće indekse i adrese, tako da se potrebne operacije mogu primjeniti na bilo koji jedinični qubit ili par qubita. Ukoliko se dva qubita ne nalaze jedan pored drugog postoji cijela sekvenca operacija kojima se postiže njihova interakcija kao da jesu.

Kao što se jedinični qubit u bilo kojem trenutku može naći u stanju superpozicije svih mogućih vrijednosti između $|0\rangle$ i $|1\rangle$, tako se i n-qubitski memorijski registar može naći u superpoziciji svih 2^n mogućih vrijednosti, $|00...0\rangle, |00...1\rangle, ..., |11...1\rangle$.

Računske baze

Kada opisujemo stanje multi-qubitnog kvantnog memorijskog registra kao superpoziciju mogućih bit-znakovnih konfiguracija, kažemo da je stanje predstavljeno u nekoj računskoj bazi, npr. stanje 2-qubitnog memorijskog registra je opisano kao:

$$|\psi\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle.$$

Ovo implicira na činjenicu da kvantni memorijski registar može biti opisan sa svih 2^n mogućih stanja u isto vrijeme, što ovisi o njihovim amplitudama. Uopšteno:

$$|\psi\rangle = c_0|00...0\rangle + c_1|00...1\rangle + ... + c_{2^n-1}|11...1\rangle = \sum_{i=0}^{2^n-1} c_i|i\rangle,$$

gdje je $\sum_{i=0}^{2^n-1} c_i = 1$, i gdje $|i\rangle$ predstavlja računsku bazu vlastitog stanja čija vrijednost odgovara vrijednosti decimalnog broja i u binarnoj notaciji. Npr., 5-qubitna računska

baza vlastitog stanja $|6\rangle$ je $|00110\rangle$. Naime, 6 je u binarnom sistemu predstavljeno kao 110. Dvije nule sa lijeve strane dodajemo kako bismo formirali ukupno 5 bita. Veličine vektor kolona, kojima predstavljamo stanja qubita, rastu eksponencijalno sa brojem istih. Tako, 100-qubitni kvantni memorijski registar zahtjeva 2^{100} kompleksnih amplituda da bi se u potpunosti definisao, stoga je nemoguće simulirati kvantni računar na klasičnom. U multi-qubitnim kvantnim stanjima poželjno je da neke amplitude imaju vrijendost 0. Recimo da je 3-qubitno kvantno stanje:

$$|\psi\rangle = c_0\,|000\rangle + c_1\,|001\rangle + c_2\,|010\rangle + c_3\,|011\rangle + c_4\,|100\rangle + c_5\,|101\rangle + c_6\,|110\rangle + c_7\,|111\rangle$$

i da ne sadrži apsolutno nikakve doprinose vlastitih stanja za $|000\rangle$, $|011\rangle$, $|101\rangle$, $|110\rangle$ i $|111\rangle$. Tada je amplituda pripadajućih komponenti nula.

$$|\psi\rangle = a\,|001\rangle + b\,|010\rangle + c\,|100\rangle \equiv \begin{pmatrix} 0 \\ a \\ b \\ 0 \\ c \\ 0 \\ 0 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} \text{amplituda} & |000\rangle & \text{komponente} \\ \text{amplituda} & |001\rangle & \text{komponente} \\ \text{amplituda} & |010\rangle & \text{komponente} \\ \text{amplituda} & |011\rangle & \text{komponente} \\ \text{amplituda} & |100\rangle & \text{komponente} \\ \text{amplituda} & |101\rangle & \text{komponente} \\ \text{amplituda} & |110\rangle & \text{komponente} \\ \text{amplituda} & |111\rangle & \text{komponente} \end{pmatrix}$$

Tenzor multi-qubitnih stanja

Tenzorom n individualnih kvantnih stanja opisujemo relaciju između n-qubitnog memorijskog registra i individualnih qubita. Neka je $|\phi\rangle = \sum_{j=0}^{2^m-1} a_j\,|j\rangle$ m-qubitno stanje i $|\psi\rangle = \sum_{k=0}^{2^n-1} b_k\,|k\rangle$ n-qubitno stanje. Tada je stanje kvantnog memorijskog registra formirano iz vlastitih stanja $|\phi\rangle$ i $|\psi\rangle$ određeno tenzorom tih stanja.

$$|\phi\rangle \otimes |\psi\rangle = \sum_{j=0}^{2^m-1} a_j\,|j\rangle \otimes \sum_{k=0}^{2^n-1} a_k\,|k\rangle = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{2^m-1} \end{pmatrix} \otimes \begin{pmatrix} b_0 \\ b_1 \\ \vdots \\ b_{2^n-1} \end{pmatrix}$$

Za stanja $|\phi\rangle = a\,|0\rangle + b\,|1\rangle$ i $|\psi\rangle = c\,|0\rangle + d\,|1\rangle$, tenzor iznosi:

$$|\phi\rangle \otimes |\psi\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a\begin{pmatrix} c \\ d \end{pmatrix} \\ \\ b\begin{pmatrix} c \\ d \end{pmatrix} \end{pmatrix} = \begin{pmatrix} ac \\ ad \\ bc \\ bd \end{pmatrix} = ac\,|00\rangle + ad\,|01\rangle + bc\,|10\rangle + bd\,|11\rangle\,.$$

Efekti interferencije i vezana stanja

Neka su $|j\rangle$ i $|k\rangle$ dva vlastita stanja n-qubitnog memorijskog registra. Stanja su ortogonalna ($\langle k|j\rangle = 0$) i normirana ($\langle j|j\rangle = \langle k|k\rangle = 1$). Sve dok se ne posmatra, kvantni memorijski registar može da se nalazi u superpoziciji vlastitih stanja $|j\rangle$ i $|k\rangle$. Stanje superpozicije tih stanja pisano je kao $|\psi\rangle = c_j\,|j\rangle + c_k\,|k\rangle$, sa vjerovatnoćom $|c_j|^2$ da se nađe u stanju $|j\rangle$ i vjerovatnoćom $|c_k|^2 = 1 - |c_j|^2$ da se nađe u stanju $|k\rangle$. Možda izgleda da se kvantni memorijski registar ponaša u skladu sa klasičnom teorijom vjerovatnoće, ali to nije slučaj. Neka je A opservabla koja se ponaša kao n-qubitni memorijski registar i neka je vlastita vrijednost opservable za odgovarajuće stanje memorijskog registra $|\psi_a\rangle$, a, odnosno: $A\,|\psi_a\rangle = a\,|\psi_a\rangle$. Postavlja se pitanje, sa kojom vjerovatnoćom će mjerenje opservable A dati vrijednost a kada se kvantni memorijski registar nađe u stanju $|\psi\rangle = c_j\,|j\rangle + c_k\,|k\rangle$?

Po klasičnoj teoriji vjerovatnoće, vjerovatnoća dobivanja vrijednosti a kada se registar nalazi u stanju $|j\rangle$ je $P_j(a) = |\,\langle\psi_a|j\rangle\,|$. Analogno za stanje registra $|k\rangle$. Međutim, u ovom slučaju nije bitno u kojem se stanju registar nalazi, te vjerovatnoću dobivanja vrijednosti a nakon mjerenja, definišemo kao:

$$p^{kl}(a) = P_j(a)p_j + P_k(a)p_k = |c_j|^2 P_j(a) + |c_k|^2 P_k(a) = |c_j|^2 |\,\langle\psi_a|j\rangle\,|^2 + |c_k|^2 |\,\langle\psi_a|k\rangle\,|^2.$$

Ali, kako se memorijski registar ponaša u skladu sa zakonima kvantne mehanike, ne možemo zanemariti činjenicu da se registar doista nalazi u stanju superpozicije $|\psi\rangle = c_j\,|j\rangle + c_k\,|k\rangle$, pa je:

$$\begin{aligned} p^{qu}(a) &= |\,\langle\psi_a|\psi\rangle\,|^2 = |c_j\,\langle\psi_a|j\rangle + c_k\,\langle\psi_a|k\rangle\,|^2 \\ &= |c_j|^2 |\,\langle\psi_a|j\rangle\,|^2 + |c_k|^2 |\,\langle\psi_a|k\rangle\,|^2 + 2Re(c_j c_k^*\,\langle\psi_a|j\rangle\,\langle\psi_a|k\rangle^*). \end{aligned}$$

Sada se javlja i dodatni član koji doprinosi ukupnoj vjerovatnoći i koji je rezultat interferencije različitih načina na koje je moguće dobiti konačnu vrijednost a. Još jedna karakteristika po kojoj se kvantni memorijski registar razlikuje od klasičnog, je pojava *vezanih* stanja. Ova osobina kvantnih sistema je ključna za ostvarivanje eksponencijalnog ubrzanja prilikom izvođenja kvantnih algoritama. Ukoliko dva qubita dovedemo u vezano stanje, tada će svaka promjena stanja prvog qubita uticati i na drugi, bez obzira na njihovu eventualnu razdvojenost. Ova osobina je podstakla fizičare dvadesetog stoljeća da postave hipotezu o prijenosu informacije brzinom većom od brzine svjetlosti.

Einstein, Podolsky, Rosen (EPR) Paradox - EPR par

Za homogeno multi-qubitno stanje kažemo da je vezano ako i samo ako se ne može rastaviti na faktore tenzora konačnih stanja svakog individualnog qubita, tj. ako i samo ako $|\psi\rangle_{AB} \neq |\psi\rangle_A \otimes |\psi\rangle_B$ za bilo koje stanje $|\psi\rangle_A$ i $|\psi\rangle_B$.

Neka se 2-qubitni memorijski registar nalazi u stanju $\frac{1}{\sqrt{2}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B)$. Ako mjerenjem qubita A nađemo da se nalazi u stanju $|1\rangle$, tada, iako nije izvršeno nikakvo mjerenje qubita B, znamo da se i on nalazi u stanju $|1\rangle$. Mjerenje qubita A je uticalo na stanje qubita B. Zbog jednostavnosti, vezana stanja se uglavnom zapisuju u obliku (A, B). Najosnovnija stanja, tzv. *Bellova stanja*, predstavljamo kao:

$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \qquad |\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}} \qquad |\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Ovakva stanja kvantnih sistema prvi su primijetili Einstein[3], Podolsky[4] i Rosen[5]. Vezanost je temelj kvantnih algoritama. Posmatrajmo dva vezana kvantna registra, A i B, takva da registar A sadrži set indeksa od 0 do $2^n - 1$, a registar B set vrijednosti neke funkcije čije ponašanje isključivo ovisi o vrijednosti indeksa registra A. Njihovo vezano stanje opisano je kao $\sum_{i_0}^{2^n-1} = |i\rangle_A |f(i)\rangle_B$. Mjerenjem vrijednosti funckije u registru B, recimo c, možemo projektovati set indeksa u registru A koji je u saglasnosti sa mjerenom vrijednosti funkcije, te tako definišemo superpoziciju stanja oblika $\sum_{i':f(i')=c} |i'\rangle_A |c\rangle$. Ovim jednostavnim potezom dobivamo sve indekse iz registra A koji daju istu vrijednost funkcije u registru B.

Vezana stanja u različitim numeričkim bazama

Kada razmišljamo o kvantnom računanju prirodno pravimo paralelu sa binarnim sistemom ($|0_{10}\rangle = |0_2\rangle, |1_{10}\rangle = |1_2\rangle, |2_{10}\rangle = |10_2\rangle, |3_{10}\rangle = |11_2...\rangle$). Kvantno kolo, predstavljeno unitarnom matricom U, koje djeluje na n qubita, ima dimenzije $2^n \times 2^n$. Slično tome, unitarna matrica koja odgovara kvantnom kolu koje djeluje na qutrite (računska baza 3), imat će dimenzije $3^n \times 3^n$. Međutim, danas se uglavnom koristi binarna baza, primarno iz razloga što je manipulacija qubitima (2-body interaction) jednostavnija od manipulacije qutritima (3-body interaction).

[3]Albert Einstein rođen 1879. godine (Ulm, Njemačko carstvo) je najistaknutiji fizičar i začetnik novog doba u fizici. Njegovi najznačajniji doprinosi uključuju specijalnu i generalnu teoriju relativnosti, objašnjenje fotoelektričnog efekta (za što je dobio Nobelovu nagradu), ekvivalentnost energije i mase, unificirana teorija polja, EPR paradoks, Bose-Einsteinova statistika itd.

[4]Boris Y. Podolsky rođen 1896. godine (Taganrog, Rusko Carstvo) je američko-ruski fizičar koji je dao značajan doprinos razvoju kvantne mehanike, Bellove teorije i teorije kvantne informacije. O Podolskom postoje izvjesne spekulacije da je bio član zloglasnog KGB-a.

[5]Nathan Rosen rođen 1909. godine (Brooklyn, New York, USA) je američki fizičar izraelskog porijekla čiji je najznačajniji doprinos analizi strukture atoma vodika i objašenju vezanih stanja.

2.4 Razvoj kvantnog memorijskog registra: Schrödingerova jednačina

Vremenski zavisna Schrödingerova[6] jednačina ima oblik:

$$i\hbar\frac{\partial\left|\psi(t)\right\rangle}{\partial t}=\mathcal{H}\left|\psi(t)\right\rangle,$$

gdje $\left|\psi(t)\right\rangle$ opisuje trenutno stanje kvantnog memorijskog registra, a Hamiltonijan $\mathcal{H}$ je operator ukupne energije sistema i njegove vlastite vrijednosti su moguće vrijednosti mjerenja ukupne energije sistema. Hamiltonijan za određeni kvantni sistem se formira uzimajući u obzir moguće interkacije unutar sistema. Hydra kvantni procesor ima Hamiltonijan oblika:

$$\mathcal{H}=\sum_{i=1}^{N}h_iZ_i+\sum_{i<j=2}^{N}J_{ij}Z_iZ_j+\sum_{i=0}^{N}\Delta_i(t)X_i,$$

gdje su $Z_i=\sigma_z^i$ i $X_i=\sigma_x^i$ Pauli-Z i Pauli-X[7] matrice za qubit i, h_i je napon polarizacije primijenjen na qubit i, $\Delta_i(t)$ je matrica *tunelovanja* za qubit i, a J_{ij} opisuje spregnutost qubita i i j. Kako je $\mathcal{H}$ operator (opservabla) ukupne energije n-qubitnog sistema (realan broj), to znači da je $\mathcal{H}$, $2^n\times2^n$ hermitska matrica, takva da postoje vlastita stanja $\left|\psi_i\right\rangle$ i vlastite vrijednosti energije E_i, odnosno da vrijedi $\mathcal{H}\left|\psi_i\right\rangle=E_i\left|\psi_i\right\rangle$. Kako su vrijednosti E_i jedine dozvoljene vrijednosti ukupne energije sistema, to uvijek postoji određena baza za koju je $\mathcal{H}$ dijagonalna matrica, $\mathcal{H}=\sum_i E_i\left|\psi_i\right\rangle\left\langle\psi_i\right|$.

$$\mathcal{H}=\begin{pmatrix}E_0 & 0 & 0 & 0\\ 0 & E_1 & 0 & 0\\ 0 & 0 & \ddots & 0\\ 0 & 0 & 0 & E_k\end{pmatrix}\quad,\quad k=2^n-1$$

Međutim, Hamiltonijan se uglavnom definiše u odnosu na neku drugu bazu, recimo računsku bazu $(\left|00...0\right\rangle,\left|00...1\right\rangle,...,\left|11...1\right\rangle)$, tako da je nekada neophodno promijeniti bazu prilikom opisivanja stanja i operatora. Najjednostavniji slučaj je onaj koji je vremenski nezavisan. Tada riješenje Schrödingerove jednačine, ima oblik:

$$\psi(t)=\psi(0)e^{(-i\mathcal{H}t/\hbar)}.$$

Kako je $\mathcal{H}$ hermitski operator, to je matrični eksponent $exp(-i\mathcal{H}t/\hbar)$ unitaran. Unitarna matrica ima osobinu da je njena inverzna matrica jednaka kompleksno konjugovanoj $U^{-1}=U^{\dagger}$, što znači da je matrica reverzibilna. Moguće je invertovati matricu bez ikakvog gubitka informacija.

[6] Erwin Schrödinger rođen 1887. godine (Beč, Austrija) je austrijski fizičar i jedan od osnivača kvantne teorije. Schrödingerovom jednačinom opisuje se talasna funkcija sistema kao i promjena funkcije u toku vremena.

[7] Wolfgang Pauli, rođen 1900. godine (Zürich, Švicarska) je jedan od utemeljitelja kvantne teorije. Nobelovu nagradu je dobio za formiranje principa isključenja i spin teorije.

2.5 Izvođenje podataka iz kvantnih računara

Prilikom mjerenja, kvantni računar je povezan sa mjernim uređajem gdje se informacija iz kvantnog memorijskog registra privremeno skladišti kako bi se konvertovala u klasičnu informaciju koju možemo očitati. Kako je u kvantnoj mehanici operator hermitski, to su njegove vlastite vrijednosti realne. Uzastopnim mjerenjem stanja $|\psi\rangle$, dobivamo srednju vrijednost opservable $\mathcal{O}$:

$$\langle \mathcal{O} \rangle = \langle \psi | \, \mathcal{O} \, | \psi \rangle \, .$$

Sumirajmo sada glavne osobine kvantnih sistema:

1. *Rezultat mjerenja je realan broj.*

2. Na kvantnom nivou sam čin mjerenja sistema će uticati na njegovo konačno stanje. Npr., položaj elektrona možemo odrediti primjenom Comptonovog efekta. Talas koji nailazi na elektron se odbija te mijenja svoju talasnu dužinu. Što je frekvencija upadnog talasa veća to je tačnije mjerenje položaja elektrona, ali je veća i promjena impulsa elektrona usljed interakcije, što znači da preciznije mjerenje položaja rezultira većom neodređenošću implusa i obratno. *Mjerenje uzrokuje promjenu stanja sistema.*

3. Mjerenjem spina elektrona nalazimo da je on ili paralelan ili antiparalelan osi mjerenja, što su ujedno i jedine dvije dozvoljene vrijednosti. *Mjerene vrijednosti su diskretne.*

4. Ako tokom eksperimenta prvo mjerimo svojstvo opservable A, a zatim svojstvo opservable B, rezultat će se razlikovati od slučaja gdje prvo mjerimo svojstvo opservable B. *Način na koji vršimo sekvencu mjerenja utiče na konačan rezultat.*

5. Postoji određeni limit na preciznost prilikom mjerenja para opservabli.

$$\Delta \mathcal{O}_A = \mathcal{O}_A - \langle \mathcal{O}_A \rangle$$

$$\Delta \mathcal{O}_B = \mathcal{O}_B - \langle \mathcal{O}_B \rangle$$

$$\Delta \mathcal{O}_A \Delta \mathcal{O}_B \geq const.$$

   Preciznije mjerenje jedne opservable rezultirat će većom neodređenošću druge.

Za hermitske operatore također vrijedi:

1. **Kvantizirane vrijednosti**. Jedini dozvoljeni rezultati mjerenja su vlastite vrijednosti operatora $\mathcal{O}_{\mathcal{A}}$.

2. **Realne vrijednosti**. Kako je operator $\mathcal{O}_{\mathcal{A}}$ hermitski njegove vlastite vrijednosti moraju biti realne.

3. **Mjerenje mijenja stanje sistema**. Ako se sistem nalazi u stanju superpozicije prije mjerenja, tada očitavanjem vrijednosti λ_i sistem je projektovan u stanje $|\psi_i\rangle$. $|\psi_i\rangle$ je vlastito stanje operatora $\mathcal{O}_\mathcal{A}$ tako da vrijedi $\mathcal{O}_\mathcal{A}|\psi_i\rangle = \lambda_i|\psi_i\rangle$.

4. **Nekomutaciona mjerenja**. Ako nas interesuju dvije opservable A i B koje su predstavljene hermitskim matricama $\mathcal{O}_\mathcal{A}$ i $\mathcal{O}_\mathcal{B}$, tada će način na koji vršimo mjerenje bitno uticati na konačni ishod jer $\mathcal{O}_\mathcal{A} \cdot \mathcal{O}_\mathcal{B} \neq \mathcal{O}_\mathcal{B} \cdot \mathcal{O}_\mathcal{A}$. Operatori ne komutiraju.

5. **Princip neodređenosti**. Za bilo koji par opservabli $\mathcal{O}_\mathcal{A}$ i $\mathcal{O}_\mathcal{B}$ postoji minimalna neodređenost sa kojom svojstva A i B mogu biti mjerena istovremeno tako da vrijedi $\Delta\mathcal{O}_\mathcal{A}\Delta\mathcal{O}_\mathcal{B} \geq \frac{1}{4}|\langle|\mathcal{O}_\mathcal{A}, \mathcal{O}_\mathcal{B}|\rangle|$.

Mjerenja u računskim bazama

Baza n-qubitnog kvantnog memorijskog registra može biti bilo koji kompletan ortonormirani set vlastitih stanja, takav da bilo koje n-qubitno stanje može biti izraženo kao superpozicija stanja isključivo iz ovako definisanog seta. Najčešće korištena je Bellova[8] baza za vezana stanja..

Baza	Vlastita stanja
θ^o rotacija	$\|\overline{0}\rangle = \cos\theta\|0\rangle + \sin\theta\|1\rangle$ $\|\overline{1}\rangle = \cos\theta\|0\rangle - \sin\theta\|1\rangle$
Dijagonalna	$\|\nearrow\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$ $\|\swarrow\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
Kiralna	$\|\circlearrowright\rangle = \frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$ $\|\circlearrowleft\rangle = \frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$
Bellova	$\|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$ $\|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(\|01\rangle + \|10\rangle)$ $\|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$ $\|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(\|01\rangle - \|10\rangle)$

Tabela 2.1: Primjeri alternativnih baza

[8] John S. Bell je rođen 1928. godine (Belfast, Sjeverna Irska). Njegov glavni doprinos odnosi se na formulaciju tzv. Bellove teoreme, koja je od ključnog značaja u kvantnoj mehanici u okviru teorije skrivenih varijabli.

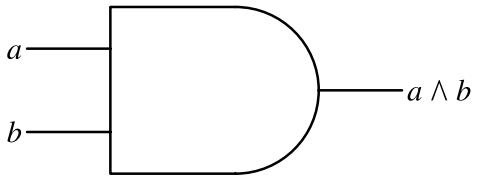
3 Kvantna kola

3.1 Booleanske funkcije i kombinatorna logika

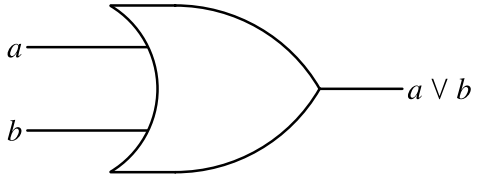
Booleova[1] algebra je oblast matematičke logike - algebarska struktura koja sadrži definisane operacije AND, OR i NOT kao i skup teorijskih operacija, unija ($A \cup B$), presjek ($A \cap B$) i komplement(A^c). Vrijednosti primarnih operacija možemo predstaviti tablicom stanja.

a	b	$a \wedge b$	$a \vee b$	$\neg a$
0	1	0	0	1
1	0	0	1	0
0	1	0	1	1
1	1	1	1	0

Tabela 3.1: Primarna kombinatorna logika



Slika 3.1.1: Simbol AND kola

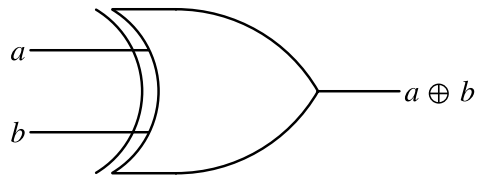


Slika 3.1.2: Simbol OR kola

Logičko kolo može se posmatrati kao fizički uređaj koji uzima jednu ili više Booleanskih vrijednosti za ulazne podatke i vraća isključivo jednu vrijednost. Logička kola su ključna komponenta modernih računara. Bilo koja operacija može biti raščlanjena na sekvencu logičkih kola koja djeluju na samo par bita u određenom trenutku. Kola AND i OR su logički ireverzibilna, što znači da nije moguće odrediti jedinstvene ulazne podatke za sve izlaze. Ako je izlazni podatak 0, ne možemo ustanoviti da li su ulazni podaci bili 00, 01

[1]George Boole, utemeljitelj Booleove algebre, je britanski matematičar i filozof rođen 1815. godine (Lincoln, Engleska).

ili 10. Analogno za OR kolo gdje za, recimo, izlazni podatak 1, ulazni podaci su mogli primiti vrijednosti 01, 10 i 11. Postoji također i varijanta OR kola, $exclusive - OR$ ili XOR u oznaci $\otimes$, koje se pokazalo jako korisnim u oblasti kvantnog računanja.

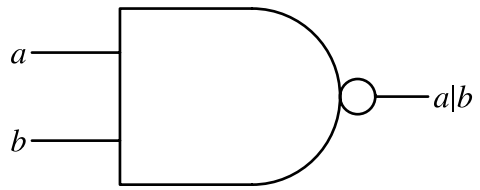


Slika 3.1.3: Simbol XOR kola

a	b	$a \otimes b$
0	0	0
0	1	1
1	0	1
1	1	0

Tabela 3.2: XOR tablica stanja

Postoji i posebna klasa logičkih kola, tzv. *univerzalna* kola. Njihova osnovna karakteristika je da je potrebno samo jedno kolo kako bi se formirao bilo kakav Booleanski izraz. U ovu grupu spadaju $NAND$ i NOR kola. Danas se industrijska konstrukcija mikroprocesora uglavnom bazira na $NAND$ univerzalnom logičkom kolu. Matematički gledano, $\neg(a \wedge b)$, ili, u notaciji $a|b$, je osnova klasičnog ireverzibilnog računanja.



Slika 3.1.4: Simbol $NAND$ kola

a	b	$a\|b$
0	0	1
0	1	1
1	0	1
1	1	0

Tabela 3.3: $NAND$ tablica stanja

Da bismo dokazali da je $NAND$ kolo doista univerzalno, dovoljno je samo uočiti da je iz $NAND$ kola moguće formirati AND i NOT kolo.

a	a	$a\|a$	$\neg a$
0	0	1	1
1	1	0	0

Tabela 3.4: NOT iz $NAND$ kola

a	b	$a\|b$	$(a\|b)\|(a\|b)$	$a \wedge b$
0	0	1	0	0
0	1	1	0	0
1	0	1	0	0
1	1	0	1	1

Tabela 3.5: AND iz $NAND$ kola

Kako se bilo koja logička operacija može razložiti na pravilnu kombinaciju $\wedge$ i $\neg$ operatora, a da se $\wedge$ i $\neg$ operatori mogu pisati u terminima $NAND$ logičkih operacija, tim smo ustanovili da se ipak, bilo koja logička operacija može predstaviti u terminima $NAND$

logičkih operacija, što je dobra vijest za industriju, jer je sada potrebno usavršiti samo način impementacije jednog kola, $NAND$ kola. Nažalost logička ireverzibilnost dolazi sa cijenom. Po zakonima fizike, kada dolazi do gubitka (brisanja) određene inormacije, dolazi i do gubitka energije u vrijednosti $kT \log 2$ po izgubljenom bitu, gdje je k Boltzmanova konstanta i iznosi $1.3805 \times 10^{-23} JK^{-1}$. Ukoliko se trend minijaturizacije računarske tehnologije nastavi, bez obzira na nove vrste materijala koje se budu razvijale shodno tome, ipak će postati jako teško ukloniti toplotu emitovanu unutar ireverzibilnih kola.

3.2 Reverzibilna kola

Jedan od načina na koji se oslobođena toplota kao nusproizvod rada ireverzibilnih kola može spriječiti je modifikacija mikroprocesora, odnosno korištenje reverzibilnih logičkih kola. U ovakvim kolima postoji jedinstvena jednosmjerna veza između ulaznih i izlaznih podataka, što znači da nema gubitka informacije. Najjednostavnije reverzibilno logičko kolo je NOT kolo, koje invertuje vrijednost bita. Tako, ukoliko nam je poznat izlazni podatak, automatski znamo i ulazni. Drugi primjer reverzibilnog kola je $SWAP$ logičko kolo, koje predstavlja sistem izmjene za dva ulazna i dva izlazna podatka, te $CNOT$ logičko kolo ($controlled - NOT$). Date su i tablice stanja ovih kola u tabelama 3.6 i 3.7.

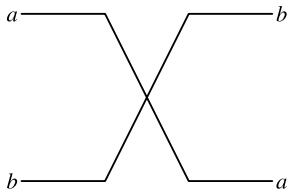
a	b	a'	b'
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

Tabela 3.6: $SWAP$ kolo

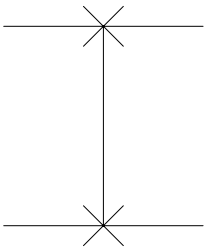
a	b	a'	b'
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

Tabela 3.7: $CNOT$ kolo

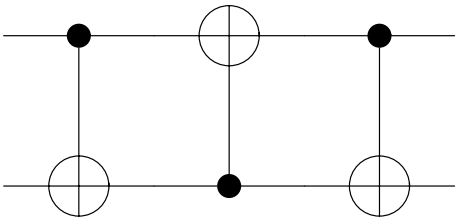
U kvantnom računanju kvantni krug ne mora nužno imati žice, niti bilo koju drugu fizičku poveznicu između kvantnih kola. Umjesto toga, krug možemo zamisliti kao sekvencu logičkih operacija koje se vrše unutar kvantnih kola, u zavisnosti od vremena; pozitivan smjer je sa lijeva na desno, odnosno smjer u kojem se sukcesivno primjenjuju kvantne operacije. Stoga se u kvantnom računanju $SWAP$ logičko kolo češće predstavlja alternativnim simbolom, na slici 3.2.2. $CNOT$ kolo mijenja vrijednost drugog bita, ako i samo ako je vrijednost prvog bita 1; odluka da se drugi bit negira ili ne negira, kontrolisana je vrijednošću prvog bita. $SWAP$ kolo je moguće realizovati sekvencom od tri $CNOT$ kola. (Slika 3.2.3).



Slika 3.2.1: Simbol $SWAP$ kola



Slika 3.2.2: Alternativni prikaz



Slika 3.2.3: Realizacija $SWAP$ kola sekvenciranjem $CNOT$ logičkih operacija

Univerzalna reverzibilna logička kola

Analogno univerzalnom ireverzibilnom računanju, također definišemo i univerzalna reverzibilna kola, $FREDKIN$[2] $(controlled - SWAP)$ i $TOFFOLI$[3] $(controlled - CNOT)$, koja zahtijevaju minimalno tri ulazna podatka.

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Tabela 3.8: $TOFFOLI$ kolo

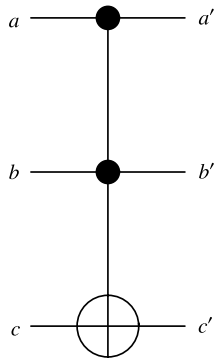
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

Tabela 3.9: $FREDKIN$ kolo

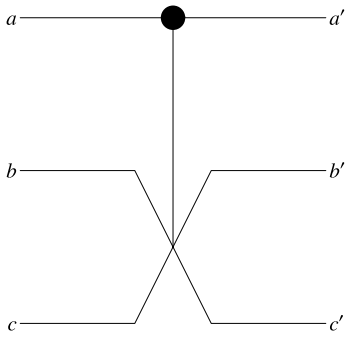
$TOFFOLI$ logičko kolo invertuje treći ulazni podatak, ako i samo ako su i prvi, i drugi ulazni podatak 1, te iste drži nepromijenjenim, dok $FREDKIN$ kolo invertuje

[2]Edward Fredkin, rođen 1934. godine (Los Angeles, California, USA) radi kao profesor na Carnegie Mellon Univerzitetu (Pennsylvania) i smatra se pionirom tzv. *digitalne fizike*.

[3]Tommaso Toffoli, rođen 1943. godine (Montereale Valcellina, Italija) je američko-italijanski profesor računarske tehnologije na Univerzitetu u Bostonu, gdje radi od 1995. Zajedno sa Fredkinom radio je na razvoju ćelijskih automata i umjetnog života.



Slika 3.2.4: $TOFFOLI$ simbol



Slika 3.2.5: $FREDKIN$ simbol

vrijednost drugog i trećeg bita, ako i samo ako je prvi bit 1, te ako su drugi i treći ulazni biti različiti, i održava njegovu vrijednost.

Reverzibilna kola kao matrice permutacije

Bilo koje n-bitno reverzibilno kolo mora imati tačno definisan način na koji se vrši mapiranje ulaznih podataka u izlazne, što znači da bilo koja dva ulazna podatka ne mogu biti mapirana u isti izlazni podatak, i obratno. Upravo nam ova osobina osigurava reverzibilnost sistema. Zamislimo reverzibilno kolo kao permutator 2^n ulaznih podataka. $SWAP$ kolo ulazne podatke 00, 01, 10 i 11, mapira, respektivno u $00 \to 00$, $01 \to 10$, $10 \to 01$ i $11 \to 11$.

Slično tome, $CNOT$ mapira ulazne podatke u $00 \to 00$, $01 \to 01$, $10 \to 11$ i $11 \to 10$. Stoga je prirodan način predstavljanja n-bitnog reverzibilnog kola kao matrice sa odgovarajućim indeksima redova i kolona. Element (i, j) matrice je 1, ako i samo ako je ulazni podatak u i-tom redu mapiran u izlazni podatak j kolone. $SWAP$ i $CNOT$ kola stoga možemo predstaviti u matričnom obliku.

$$SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Da bismo vidjeli kako reverzibilno logičko kolo, recimo $TOFFOLI$, djeluje na ulazni podatak, prvi bit predstavimo kao vektor kolonu koja odgovara njegovoj vrijednosti, te potom vršimo uobičajenu operaciju vektorskog množenja ovih matrica.

Kako $TOFFOLI$ operiše sa tri bita, možemo zamisliti vektor kolonu kojom opisujemo ulazni podatak da se sastoji iz $2^3 = 8$ članova, od kojih jedan ima vrijednost 1, dok su

svi ostali 0.

$$|000\rangle = \begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix} \qquad |001\rangle = \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix} \qquad |010\rangle = \begin{pmatrix}0\\0\\1\\0\\0\\0\\0\\0\end{pmatrix} \qquad \cdots \qquad |111\rangle = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix}$$

$$TOFFOLI\,|110\rangle = \begin{pmatrix}1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&1\\0&0&0&0&0&0&1&0\end{pmatrix} \cdot \begin{pmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix} = |111\rangle$$

Simulacije ireverzibilnih operacija

Danas se većina mikroprocesora zasniva na kolima koja su logički ireverzibilna. Logička ireverzibilnost znači da određeni izlazni podatak odgovara većem broju ulaznih podataka. Npr., AND logičko kolo mapira dva bita a i b u jedan bit c. Izlazni podatak $c = 0$ odgovara kombinaciji ulaznih bitova $a = 0 \wedge b = 0$, $a = 0 \wedge b = 1$ i $a = 1 \wedge b = 0$. Ulazni podatak je višeznačan, te je stoga operacija logički ireverzibilna. Logička ireverzibilnost ima određene termodinamičke posljedice. Prvenstveno dolazi do gubitka energija od $kT \log 2$ po izgubljenom (obrisanom) bitu. Na sobnoj temperaturi, $T = 300K$, energija koja se oslobodi u vidu toplote iznosi $3 \cdot 10^{-24}J$.

Međutim, ukoliko bismo za vršenje logičkih operacija koristili isključivo reverzibilna logička kola, ne bi dolazilo do disipacije energije. Da bi operacija bila logički reverzibilna, svaki korak te operacije mora biti logički reverzibilan, ali kada je upitanju reverzibilno računanje, prirodno se nameću dva pitanja. Prvo, kako formirati optimalni reverzibilni krug za implementaciju potrebne Booleanske funkcije? I drugo, sa kojom efikasnošću takav, reverzibilni, računar, može simulirati ireverzibilne operacije? Toffoli je pokazao da je reverzibilna baza, sastavljena iz NOT, $CNOT$ i $TOFFOLI$ kola, univerzalna za reverzibilne operacije. Tačnije, pokazao je da se svaka permutacija iz skupa podataka $\{0,1\}^n$ može realizovati unutar reverzibilnog NOT, $CNOT$, $TOFFOLI$ kruga, korištenjem *ancilla* (pomoćnog, skladišnog) bita. Ancillae su ključni elementi u klasičnom

reverzibilnom računanju. Npr., svaki krug sa više od tri ulazna podatka koji se obrađuju unutar $NOT - CNOT - TOFFOLI$ kombinacije, ostvaruju paran broj permutacija. Tako, za realizaciju neparnog broja permutacija na $\{0,1\}^n$, potreban je barem jedan dodatni bit (ancilla bit) sa fiksnom konstantnom vrijednošću. Toffoli je pokazao da je za ove potrebe, dovoljan samo jedan ancilla bit. Posmatrajmo Booleansku funkciju za koju vrijedi $f = \{0,1\}^n \to \{0,1\}$. Svaki reverzibilni krug sa m ulaznih podataka, izvršavanjem operacije nad funkcijom f, generiše tačno m izlaznih podataka, od kojih jedan nosi vrijednost funkcije f. Za $m = n$, ancilla bit ne postoji, što znači da je funkcija po čijim pravilima se vrši mapiranje, izbalansirana. [4] Izbalansirana funkcija, dakle, vraća vrijednost 1 za jednu polovinu 2^{n-1} ulaznih podataka i vrijednost 0 za drugu polovinu. Stoga, ako funkcija koju želimo simulirati nije izbalansirana, potrebno je da vrijedi $m > n$, što znači da mora postojati barem jedan ancilla bit.

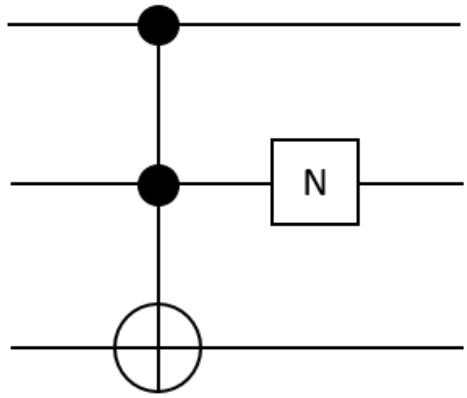
3.3 Reverzibilna logika uz minimalno korištenje ancilla bita

Vidjeli smo da u konstrukciji reverzibilnih kola iz ireverzibilnih, ancilla biti se koriste kako bi se uklonila ograničenja koja ireverzibilni sklopovi nameću. Sa neograničenim ancilla bitima, kola kao što su $TOFFOLI$ i $FREDKIN$, postaju univerzalna reverzibilna kola. Međutim, implementacija ancilla bita nije ekonomski najpovoljnija, pa se javlja potreba za pronalaskom optimalnog sistema sa minimalnim brojem ancilla bita. U logičkom sklopu, reverzibilno kolo se definiše kao kolo u kojem ne dolazi do gubitka informacije u toku vršenja ma kakvog proračuna. Strogo govoreći, n-bitno reverzibilno kolo, za n ulaznih podataka, generiše n izlaznih podataka, i za date izlazne podatke možemo jednoznačno rekonstruisati ulazne. Npr., NOT kolo, koje implementira logičku negaciju je reverzibilno jer se ulazni podatak može rekonstruisati invertovanjem izlazne informacije. AND kolo, koje implementira logičku konjunkciju, nije reverzibilno, jer četiri ulazna podatka generišu dva izlazna.

TOFFOLI kolo i univerzalnost

Konstruišimo varijaciju $TOFFOLI$ kola serijskim vezivanjem sa NOT kolom, čime se osigurava njegova reverzibilnost. Vidimo da usljed ovakve modifikacije svakom izlaznom podatku odgovara jedna i samo jedna kombijacija ulaznih podataka, te je rekonstrukcija moguća.

[4] Funkcija $f(x)$ je *konstantna* ako vraća istu vrijednost za bilo koju kombinaciju ulaznih podataka, za funkciju $f(x)$ kažemo da je *izbalansirana* ako za jednu polovinu ulaznih podataka vraća jednu vrijednost, npr. 0, a za drugu polovinu 1.(detaljnije u poglavlju *Kvantni algoritmi*)



Slika 3.3.1: Modifikacija kola

ulazni podaci	izlazni podaci
000	010
001	011
010	000
011	001
100	110
101	111
110	101
111	100

Tabela 3.10: Tablica stanja

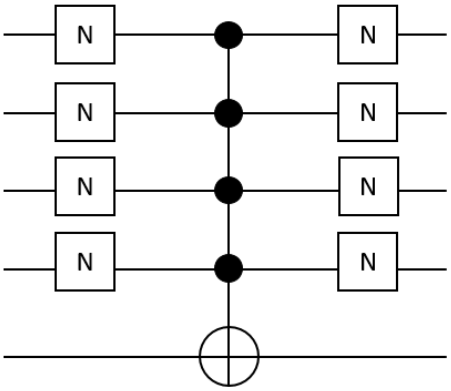
Reverzibilna kola iz C^{i}NOT

Započinjemo konstrukcijom bilo kojeg reverzibilnog kola koristeći tzv. *multikontrolna* $TOFFOLI$ kola. Označimo sa T_n set kola NOT, $CNOT$, $CCNOT$,..., C^nNOT. Neka se n-bitna kola t_1 i t_2 mogu konstruisati serijskim vezivanjem kola iz seta T_n, za koje vrijedi:

1. t_1 vrši izmjenu 0 i 1,

2. t_2 premješta k u $(k+1)$ mod.

Kolo t_1 izmijenjuje elemente 0 i 1, što je u binarnom okruženju ekvivalentno mapiranju ulaznih podataka $(0,0,...,0)$ u $(0,0,...,1)$, odnosno, mapiranju $(0,0,...,1)$ u $(0,0,...,0)$.



Slika 3.3.2: Reprezentacija t_1 kola

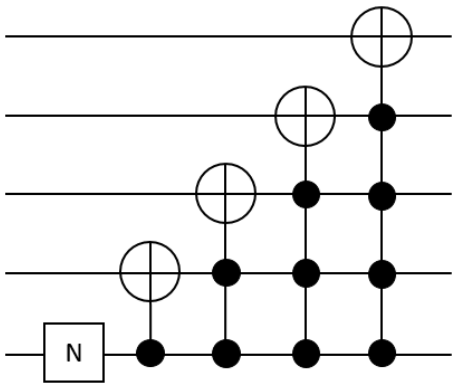
Ovo je ekvivalentno invertovanju posljednjeg bita ako i samo ako je prethodnih $n-1$ bita 0, što je opet u potpunosti suprotno od multikontrolnog $TOFFOLI$ kola. Tako se,

t_1 može konstruisati primjenom NOT kola na svaki od $n-1$ bita, praćeno $C^{n-1}NOT$ kolom gdje je posljedni bit ustvari ciljna tačka. I konačno, NOT kolo, ponovno na svaki od $n-1$ bita, u cilju vraćanja njihove početne vrijednosti.

Kolo t_2 dodaje 1 na svaki element. U standardnom binarnom okruženju, posljednji bit je uvijek invertovan. Posljednji bit je invertovan ako i samo ako postoji *prenešeni* bit koji je rezultat zbrajanja nad posljednim bitom. Uopšteno, i bit je invertovan ako i samo ako je bit prenešen sa $(i+1)$ bita, ili, kažemo da je i bit invertovan ako i samo ako su svi niži bitovi 1, dok je $i = 1, 2, ..., n-1$. Stoga se t_2 može implementirati kao serija sljedećih kola:

1. NOT kolo na zadnjem bitu
2. $CNOT$ kolo na zadnja dva bita sa $(n-1)$ bitom kao ciljanom tačkom
3. C^2NOT kolo na zadnja tri bita sa $(n-2)$ bitom kao ciljanom tačkom
   ...
4. $C^{n-1}NOT$ kolo na svih n bita, sa najvišim bitom kao ciljanom tačkom

Kombiniranjem ova dva primjera, možemo zaključiti da bilo koje n-bitno reverzibilno kolo može biti konstruisano serijskom vezom multikontrolnih $TOFFOLI$ kola sa do $n-1$ kontrolnih linija.



Slika 3.3.3: Reprezentacija t_2 kola

3.4 Kvantna logička kola

Kao što se bilo koji klasični proračun može razložiti na sekvencu klasičnih logičkih kola koja djeluju na određeni broj bita u datom trenutku, tako se i bilo koji kvantno-mehanički proračun može predstaviti serijom kvantnih logičkih kola koja operišu nad setom qubita. Osnovna razlika je u tome što klasična kola manipuliraju klasičnim bitima,

koji imaju vrijednost ili 0, ili 1, dok kvantna logička kola djeluju nad proizvoljnim multilateralnim kvantnim stanjima, uključujući i stanja superpozicije računskih baza, koja su uglavnom vezana.

Kvantna black-box funkcija i implementacija

Bilo koji kvantno-mehanički razvoj opisan je unitarnim, a samim tim i logički reverzibilnim operacijama. Da bi operacija bila logički reverzibilna, određeni ulazni podatak se mora jasno mapirati u samo jedan, tačno definisan, izlazni podatak, i obratno.

Međutim, mapiranje oblika $|x\rangle \rightarrow |f(x)\rangle$ unutar black-boxa nije nužno logički reverzibilno. Ako je funkcija $|f(x)\rangle$ konstanta, tada se dvije moguće vrijednosti $|x\rangle$ mapiraju u istu vrijednost za $f(x)$. To znači da, ako je operacija koja se vrši unutar black-boxa kvantno-mehaničke prirode, specifikacija $|x\rangle \rightarrow |f(x)\rangle$ neće imati baš nekog značaja.[5] Ali uvedimo sada dodatni registar koji će nam služiti za održavanje jedne te iste vrijednosti prilikom mjerenja.

Neka je početna konfiguracija registara $|x\rangle |0\rangle$ i neka je stanje drugog registra postavljeno na $|0\rangle$. U ovom slučaju, black-box vrši operaciju mapiranja kao $|x\rangle |0\rangle \rightarrow |x\rangle |f(x)\rangle$. Vidimo da nam je drugi registar samo mjesto gdje ćemo izvršiti očitavanje vrijednosti za $f(x)$. Ulazni podatak $|x\rangle$ je sada zabilježen na izlazu, čime nam je omogućeno invertovanje procesa mapiranja, jednoznačno, bez obzira na vrijednost $f(x)$.

Međutim, kvantna mehanika nalaže da sam proces mapiranja mora biti unitaran,pa je potrebno izvršiti kompletno mapiranje, odnosno, specifizirati način na koji se svaki zasebni ulazni podatak, mapira u izlaznu informaciju. Mapiranje oblika $|x\rangle |0\rangle \rightarrow |x\rangle |f(x)\rangle$ unutar black-boxa odnosi se na samo jednu polovinu mogućih ulaza; onu koja završava sa $|0\rangle$, čime problem određivanja funkcije $f(x)$ opet nije riješen.

x	$f(x)$	$y \otimes f(x)$
0	0	0
0	1	1
1	0	1
1	1	0

Tabela 3.11: XOR tablica stanja

Da bismo osigurali da je priroda procesa unutar black-boxa unitarna, moramo jasno definisati način na koji se ulazni podaci koji završavanju i na $|0\rangle$ i na $|1\rangle$ mapiraju u izlazne. Iz tog razloga, operaciju unutar black-boxa definišemo kao:

$$|x\rangle |y\rangle \rightarrow |x\rangle |y \otimes f(x)\rangle .$$

[5] Više o black-box funkciji u dodatku A.

Operacija $y \otimes f(x)$ je ekskluzivna OR operacija (XOR). Za slučaj kada je $y = 0$, $y \otimes f(x) = f(x)$, definicija $|x\rangle |y\rangle \to |x\rangle |y \otimes f(x)\rangle$ uključuje slučaj $|x\rangle |0\rangle \to |x\rangle |f(x)\rangle$.

Ali, definisanjem operacije sa drugim qubitom koji može primiti vrijednost ili $|0\rangle$ ili $|1\rangle$, osiguravamo da radnja unutar black-boxa bude unitarne prirode, odnosno, reverzibilna, čime je određeno kompletno mapiranje svih mogućih 2-qubitnih ulaznih podataka i svih mogućih 2-qubitnih izlaznih podataka. Operacija $|x\rangle |y\rangle \xrightarrow{\text{f-c-N}} |x\rangle |y \otimes f(x)\rangle$ je poznata i kao *f-controlled-NOT* operacija ($f-c-N$), obzirom da vrijednost funkcije $f(x)$ određuje da li će vrijednost y biti negirana ili ne.

Vrijednost funkcije i interferencija

Odgovor na pitanje da li je funkcija $f(x)$ konstantna ili izbalansirana tražimo pomoću black-boxa koji nosi implicitno informaciju o toj funkciji. Ako se ograničimo na unos onih kvantnih stanja koja odgovaraju klasičnim binarnim ulaznim podacima $|0\rangle |0\rangle$, $|0\rangle |1\rangle$, $|1\rangle |0\rangle$ i $|1\rangle |1\rangle$, u black-box, tada naša kvantno-mehanička metoda ne bi imala nikakvu prednost u odnosu na dosadašnje klasične metode. Potrebno je, naime, da kvantna stanja koja unosimo u black-box, budu apsolutno neklasična, odnosno, da nemaju nikakvu sličnost sa standardnim, klasičnim, ireverzibilnim, binarnim podacima. Pogledajmo šta se dešava sa ulazom $|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ kada na njega djelujemo $f - c - N$ operacijom:

$$|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \xrightarrow{\text{f-c-N}} |x\rangle \frac{1}{\sqrt{2}}(|0 \otimes f(x)\rangle - |1 \otimes f(x)\rangle \,.$$

Kako razmatramo samo najjednostavniji slučaj ($n = 1$), x može primiti vrijednosti 0 ili 1, kao i vrijednost samo funkcije $f(x)$.

x	$f(x)$	$\|x\rangle \frac{1}{\sqrt{2}}(\|0 \otimes f(x)\rangle - \|1 \otimes f(x)\rangle$	$(-1)^{f(x)} \|x\rangle \frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$
0	0	$\|0\rangle (\|0\rangle - \|1\rangle)$	$\|0\rangle (\|0\rangle - \|1\rangle) = \|0\rangle (\|0\rangle - \|1\rangle)$
0	1	$\|0\rangle (\|1\rangle - \|0\rangle)$	$-\|0\rangle (\|0\rangle - \|1\rangle) = \|0\rangle (\|1\rangle - \|0\rangle)$
1	0	$\|1\rangle (\|0\rangle - \|1\rangle)$	$\|1\rangle (\|0\rangle - \|1\rangle) = \|1\rangle (\|0\rangle - \|1\rangle)$
1	1	$\|1\rangle (\|1\rangle - \|0\rangle)$	$-\|1\rangle (\|0\rangle - \|1\rangle) = \|1\rangle (\|1\rangle - \|0\rangle)$

Tabela 3.12: Veza između vrijednosti x i $f(x)$, i desne strane tabele

Uočavamo da su konačni izrazi u trećoj i četvrtoj koloni, za istu kombinacija x i $f(x)$, identični! Oba izraza predstavljaju dobar matematički opis izlaznih kvantnih stanja na koja je prethodno primijenjena $f-c-N$ operacija. Stoga transformaciju koju $f-c-N$ vrši nad kvantnim stanjima, možemo opisati i kao:

$$|x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle \xrightarrow{\text{f-c-N}} (-1)^{f(x)} |x\rangle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

Ova reinterpretacija konačnog stanja nam dozvoljava da funkciju $f(x)$ posmatramo kao da je iz ket stanja prenijeta u fazni faktor $(-1)^{f(x)}$. Efekti kvantno-mehaničke interferencije utiču na vjerovatnoću mogućih ishoda.

3.5 Jednoqubitna kola

Pauli spin matrice

Jedna od osnovnih osobina čestica u kvantnoj mehanici je spin, ili kako se još definiše, vlastiti (intrisični) angularni (ugaoni) moment. Na početku smo vidjeli da se operator spina, kao i operator energije, predstavlja u matričnom obliku, i za kojeg važe ista komutaciona pravila. Operator spina reprezentiran je Pauli spin matricama.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Operator vlastitog angularnog momenta je važan za opisivanje kretanja čestice u centralno-simetričnim potencijalima, te se primjenjuje uglavnom u okviru sfernog koordinatnog sistema, što je praktično kada qubite posmatramo u okviru Blochove sfere. Za jedan qubit, Pauli matrica oblika (I, X, Y, Z) je unitarna i hermitska.

Pauli X matrica se još jednostavnije označava kao X kolo obzirom da vrši rotaciju stanja za π radijana duž x-ose. Ako se, dakle, u početnom trenutku nalazimo u stanju $|0\rangle$ na samom vrhu blochove sfere, X kolo nas rotacijom dovodi u stanje $|1\rangle$ na dnu iste.

NOT kolo

U klasičnoj teoriji NOT kolo u matričnoj reprezentaciji:

$$NOT = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

ima isti oblik kao i Pauli X matrica, što znači da bi Pauli X matrica imala u okviru kvantnog računanja istu ulogu - ulogu negiranja stanja qubita.

$$X|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$$

$$X|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$$

Karakteristično je da rotacija sistema u okviru kojeg opisujemo stanja qubita, tj. rotacija Blochove sfere, nije simetrična za period 2π, već za period 4π. Pa, da li doista Pauli X matrica ima istu ulogu za proizvoljne qubite, kao što ima NOT kolo za klasične bite? Odgovor je ne, što vrlo jednostavno možemo i dokazati. Stanje qubita na Blochovoj sferi opisano je, kako smo vidjeli, izrazom:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \qquad \begin{matrix} 0 \leq \theta \leq \pi \\ 0 \leq \phi \leq 2\pi \end{matrix}$$

Da bismo pronašli antipodalnu tačku ovako definisanog stanja, prosto se pomjeramo na suprotnu hemisferu mijenjanjem ugla θ za π radijana ili za 180^o. Stoga, antipodalno stanje $\bar{\psi}$ ili možda simboličnije, $\psi^{\perp}$, je:

$$\begin{aligned} \left|\psi^{\perp}\right\rangle &= \cos\left(\frac{\pi-\theta}{2}\right)|0\rangle + e^{i(\phi+\pi)}\sin\left(\frac{\pi-\theta}{2}\right)|1\rangle \\ &= \cos\left(\frac{\pi-\theta}{2}\right)|0\rangle - e^{i\phi}\sin\left(\frac{\pi-\theta}{2}\right)|1\rangle \\ &= \sin\left(\frac{\theta}{2}\right)|0\rangle - e^{i\phi}\cos\left(\frac{\theta}{2}\right)|1\rangle. \end{aligned}$$

S druge strane, djelujmo Pauli X matricom na stanje $|\psi\rangle$:

$$\begin{aligned} X|\psi\rangle &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \cos\left(\frac{\theta}{2}\right) \\ e^{i\phi}\sin\left(\frac{\theta}{2}\right) \end{pmatrix} = \begin{pmatrix} e^{i\phi}\sin\left(\frac{\theta}{2}\right) \\ \cos\left(\frac{\theta}{2}\right) \end{pmatrix} \\ &= e^{i\phi}\sin\left(\frac{\theta}{2}\right)|0\rangle + \cos\left(\frac{\theta}{2}\right)|1\rangle. \end{aligned}$$

Pauli X matrica samo negira stanje računske baze (uz stanje $|0\rangle$ sada stoji sinusni član sa faznim faktorom $e^{i\phi}$, dok uz stanje $|1\rangle$ stoji kosinusni član), ali stanje superpozicije ostaje nepromijenjeno.

$$a|0\rangle + b|1\rangle \rightarrow b|0\rangle + a|1\rangle$$

Ovo možemo dalje pojednostaviti, množeći izraz faznim faktorom, obzirom da su stanja svakako, za globalni fazni fakor, identična.

$$X|\psi\rangle = \sin\left(\frac{\theta}{2}\right)|0\rangle + e^{-i\phi}\cos\left(\frac{\theta}{2}\right)|1\rangle \neq \left|\psi^{\perp}\right\rangle$$

Ovi izrazi se očito razlikuju, te zaključujemo da se Pauli X matrica ipak ne ponaša kao klasično NOT kolo. Pauli X matrica ne negira stanje qubita u standardnom smislu jer dobiveni rezultat nije $\left|\psi^{\perp}\right\rangle$.

SQR-NOT kolo

$SQR - NOT$ kolo ili $\sqrt{NOT}$ kolo ima oblik:

$$\sqrt{NOT} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{\frac{1}{2}} = \begin{pmatrix} \frac{1}{2} + \frac{i}{2} & \frac{1}{2} - \frac{i}{2} \\ \frac{1}{2} - \frac{i}{2} & \frac{1}{2} + \frac{i}{2} \end{pmatrix}.$$

Zanimljiva osobina $\sqrt{NOT}$ kola je da uzastopnom primjenom daje iste rezultate kao i NOT kolo, dok jednokratnom primjenom qubit dovodi u takvo stanje koje u klasičnom smislu ne odgovara ni bitu 0, ni bitu 1.

3.6 Hadamard kolo

Hadamardov proizvod matrica

Hadamardov[6] proizvod ili, kako se još naziva Schurov proizvod, je binarna operacija koja uzima dvije matrice istih dimenzija i generiše treću, gdje je svaki i, j element proizvod elemenata i, j originalnih matrica. Hadamardov proizvod nosi osobine asocijativnosti i distributivnosti, a za razliku od standardnih matričnih proizvoda, i osobinu komutativnosti. Za dvije matrice A i B, istih dimenzija, Hadamardov proizvod, $A \otimes B$, je matrica istih dimenzija kao i faktori matrice, čiji se elementi definišu kao:

$$(A \otimes B)_{i,j} = (A)_{i,j}(B)_{i,j}.$$

Npr., Hadamardov proizvod matrica A i B, dimenzija 2×2 je:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \otimes \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{12}b12 \\ a_{21}b_{21} & a_{22}b_{22} \end{pmatrix}.$$

Hadamard matrica je kvadratna matrica dimenzija $n \times n$ čiji elementi imaju vrijednosti 1 ili -1, i čiji su redovi međusobno ortogonalni, što znači da dva reda Hadamard matrice predstavljaju dva međusobno okomita vektora. Ista osobina vrijedi i za kolone matrice. Neka je H Hadamard matrica reda n. Za takvu matricu vrijedi:

$$HH^T = nI_n,$$

gdje je I_n $n \times n$ unitarna matrica, a H^T transponova H matrica.

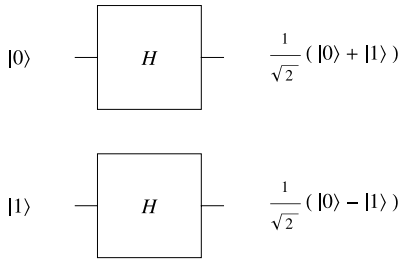
[6] Jacques Hadamard rođen 1865. godine (Versailles, Francuska) je francuski matematičar koji je dao veliki doprinos teoriji brojeva, teoriji kompleksnih funkcija, diferencijalnoj geometriji i parcijalnim diferencijalnim jednačinama.

Hadamard kolo

Hadamard kvantno kolo, koje definišemo kao:

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

To je najkorisnije kolo s kojim se susrećemo u okviru kvantnog računanja, koje stanja računaskih baza, prevodi u stanje superpozicije i obratno.



Slika 3.6.1: Simbol Hadamard kvantnog kola i operacije transformacije

Kada na stanje baze $|x\rangle$ djelujemo Hadamard operatorom, ulazni podatak se transformira u skladu sa:

$$H|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^x |1\rangle),$$

ili u opštem slučaju:

$$a|0\rangle + b|1\rangle \to a\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right) + b\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = \frac{a+b}{\sqrt{2}}|0\rangle + \frac{a-b}{\sqrt{2}}|1\rangle.$$

Predstavimo Hadamard kolo u matričnom obliku i djelujmo na stanja $|0\rangle$ i $|1\rangle$.

$$H|0\rangle = H\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\cdot\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

$$H|1\rangle = H\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix}\cdot\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Uzimajući sve navedene osobine Hadamard kola, možemo barem pretpostaviti što će se desiti sa, recimo, stanjem $|0\rangle$ kada na njega uzastopno djeluju dva Hadamard operatora, dva Hadamard kola. Naime, prvo kolo, kako smo vidjeli, stanje qubita prebacuje u stanje superpozicije $|0\rangle \to \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, dok drugo kolo sada djeluje na oba stanja $|0\rangle$ i $|1\rangle$:

$$|0\rangle \to \frac{|0\rangle + |1\rangle}{\sqrt{2}} \to \frac{1}{\sqrt{2}}\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} + \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) = |0\rangle.$$

Analogno za stanje $|1\rangle$ dobivamo:

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

Ovaj dio kvantnog kruga, HH kolo, je ekvivalentan kvantnoj konturi. Ali posmatrajmo sada prozvoljni ulazni podatak $|\psi\rangle$, gdje se stanje preko prvog kola provodi u $H|\psi\rangle$, a nakon drugog u $HH|\psi\rangle$. Za Hadamard matricu vrijedi $HH = I$, gdje je I jedinična matrica, i upravo zbog toga kažemo da je dio kvantnog kruga sa HH kolom, ustvari, kvantna kontura.[7] Hadamard kolo predstavlja rotaciju oko ose $x + z$ za π radijana na Blochovoj sferi. Usljed ovakve rotacije, tačke sa x-ose se premještaju na z-osu i obratno, a vrijednost tačke na y-osi sada ima negativnu vrijednost.

Na oficijalnoj stranici IBM-a, možemo, nakon jednostavne registracije, pristupiti kvantnom računaru u njihovom sjedištu i vršiti simulacije od interesa. Kada na stanje $|0\rangle$ djelujemo Hadamard kolom, dobivamo:

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

Slika 3.6.2: Primjena Hadamard kola u IBM Q editoru

Simulacijom predstavljenje strukture sa samo jednim Hadamard kolom primjenjenim na jedan qubit, dobivamo histogram za 100 izvedenih operacija pod istim uslovima. Iako očekujemo iste vrijednosti pojavljivanja za $|0\rangle$ i $|1\rangle$, malo je vjerovatno da će nam bilo koji set konačnog broja mjerenja, bez obzira koja cifra je u pitanju, dati takav rezultat.

Slika 3.6.3: Hadamard kolo - histogram

[7] Kvantna kontura je električki provodljiva kontura u kojoj kvantni efekti utiču na same osobine prijenosa neke informacije

Slika 3.6.4: Primjena X i Hadamard kola u IBM Q editoru

Zajedno sa stanjem $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ što je u suštini vektor u negativnom smjeru x-ose, možemo definisati novu bazu mjerenja - bazu superpozicije. Stanje $|-\rangle$ formiramo korištenjem kvantnog kruga na slici iznad. X kolo invertuje $|0\rangle$ u $|1\rangle$, a zatim Hadamard kolo rotira qubit oko ose $x + z$ da bi se formiralo $|-\rangle$ stanje.

Rezultat je isti kao i u prvom slučaju gdje smo izvršili simulaciju samo Hadamard kola. Zaključujemo da različita stanja daju iste rezultate.

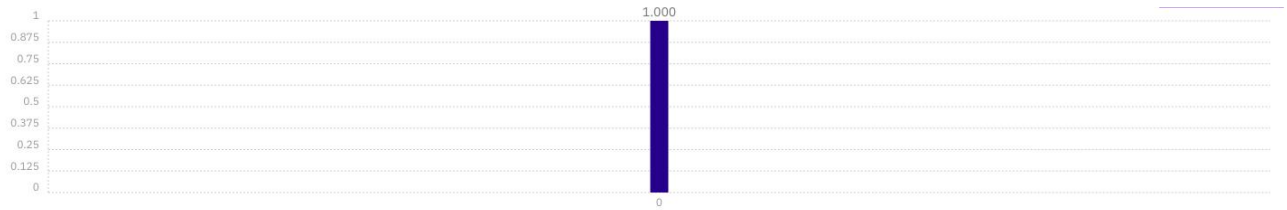
Slika 3.6.5: X i Hadamard kolo - histogram

Da bismo vidjeli koja je razlika između stanja $|+\rangle$ i $|-\rangle$, mjerenje moramo izvršiti u bazi superpozicije. Eksperimentalno, mjerenje ne možemo vršiti u različitim, proizvoljnim, pravcima Blochove sfere, ali možemo napraviti da izgleda kao da rotacijom qubita primjenom kvantnih kola, mijenjamo stanje kompletnog sistema, prije nego što doista izvršimo stanardno mjerenje duž z-ose. Da bismo izvršili mjerenje u bazi X, rotiramo stanje qubita tako da njegova x komponenta bude u smjeru z-ose, što ostvarujemo primjenom Hadamard kola prije konačnog mjerenja.

Slika 3.6.6: $|+\rangle$ stanje mjereno u X bazi

Slika 3.6.7: $|-\rangle$ stanje mjereno u x bazi

Vidimo da su nam rezultati mjerenja u x bazi apsolutno određeni (deterministički), dok smo mjerenjem u z bazi, nasumično dobivali vrijednosti između 0 i 1. Kao rezultat, u oba slučaja, dobivamo:

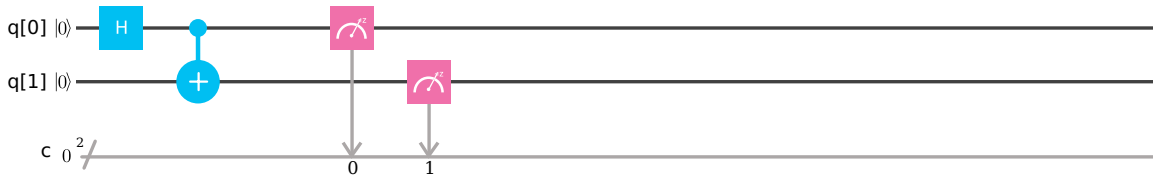


Slika 3.6.8: $|+\rangle$ i $|-\rangle$ stanje mjereno u X bazi

3.7 Vezana stanja

Jedan od koncepta kvantne mehanike, kako smo naveli na samom početku, a koji su kontra-intuitivni, jeste da kvantni sistemi koji se nalaze na jako velikim udaljenostima, mogu biti, bez ikakve fizičke spone, jako povezani. Za takva kvantna stanja kažemo da su vezana. Također, vidjeli smo da se multiqubitno vezano stanje ne može, prosto rečeno, izraziti preko pojedinačnih qubita tog stanja.

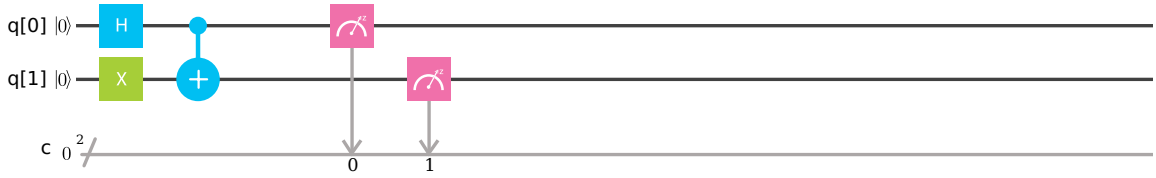
Npr., stanja $|00\rangle$, $|01\rangle$, $|10\rangle$ i $|11\rangle$, nisu vezana obzirom da svakom pojedinačnom qubitu možemo dodijeliti definisano stanje. Stanje, $\frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ također nije vezano jer prvi qubit može bit izražen kao $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, dok bi u tom slučaju drugi imao vrijednost $|0\rangle$. Međutim, stanje $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ je vezano jer ne postoji apsolutno nikakav način kojim se može izraziti preko kombinacije stanja od samo jednog qubita. Mjerenjem qubita u ovakvom, vezanom stanju, duž bilo koje ose posmatranja, nalazimo da je njegovo ponašanje potpuno neuređeno, ali čak nam i neuređeno ponašanje qubita, omogućava da sa sigurnošću predvidimo stanje drugog, ako bismo izvršili mjerenje duž iste ose. Za Bellova stanja dobivamo:



Slika 3.7.1: Prvo Bellovo stanje β_{00}

Hadamard kolo konvertuje stanje prvog para qubita $|00\rangle$ u stanje superpozicije $H|00\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$. Ovako definisano stanje sada služi kao kontrolni ulazni podatak za

CNOT kolo, koje, kako smo rekli, invertuje drugi qubit, ako i samo ako je kontrolni qubit (prvi qubit) $|1\rangle$. Tako, stanje kvantnog sistema nakon prolaska kroz *CNOT* kolo ima oblik $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ i vezano je.



Slika 3.7.2: Drugo Bellovo stanje β_{01}

Za drugo Bellovo stanje β_{01}, smo drugi qubit prethodno podvrgnuli X transformaciji iz $|0\rangle$ u $|1\rangle$.

Slika 3.7.3: Prvo Bellovo stanje β_{00} - histogram

Slika 3.7.4: Drugo Bellovo stanje β_{01} - histogram

U opštem slučaju za Bellova stanja vrijedi:

$$|\beta(x,y)\rangle = \left(\frac{|0,y\rangle + (-1)^x\,|1,Y\rangle}{\sqrt{2}}\right),$$

gdje je Y negacija od y.

4 Kvantni algoritmi

Analogno algoritmu klasičnog računarstva, kvantni algoritam se definiše kao konačan broj koraka za izračunavanje nekog problema na kvantnom računaru, primjenom zakona kvantne mehanike. Kvantni algoritmi su podijeljeni u tri grupe. Prvi su algoritmi zasnovani na kvantnoj verziji Fourierove transformacije. Shorov[1] algoritam za defaktorizaciju brojeva je jedan od algoritama iz te grupe. Drugu grupu čine kvantni algoritmi za pretragu, kao što je Groverov[2] algoritam, dok u treću grupu spadaju algoritmi koje se koriste za kvantne simulacije.

Kvantna Fourierova transformacija

Kvantna Fourierova transformacija (QFT) je slična uobičajenoj diskretnoj Fourierovoj transformaciji (DFT), osim što je proračun na kvantnog algoritma eksponencijalno brži. Prisjetimo se prvo klasične Fourierove transformacije kojom se vrši preslikavanje složenih vektora:

$$x = (x_0, ..., x_{n-1}) \to y = (y_0, ..., y_{n-1}) \in \mathbb{C}^n, \quad y_k = \frac{1}{\sqrt{n}} \sum_{j=0}^{n-1} x_j e^{\frac{2\pi i j k}{n}}, \quad k = 0, ..., n-1.$$

Izraz možemo proširiti kako bismo dobili kvantnu verziju ove transformacije. Definišimo linearnu transformaciju U na n qubita koji opisuju osnovno stanje $|j\rangle$, gdje je $0 \leq \ j \leq 2^n - 1$. Za linearnu transformiraciju vrijedi:

$$|j\rangle \to \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{\frac{2\pi i j k}{n}} |k\rangle .$$

Ova transformacija je unitarna. Na klasičnom računaru za izvršavanje Fourierove transformacije potrebno je $N \log N = n\, 2^n$ koraka da bi se faktorisalo $N = 2^n$ brojeva. Kvantni računar istu transformaciju izvrši u $\log^2 N = n^2$ koraka, što je eksponencijalna ušteda. Pokazalo se da se ova transformacija može koristiti za efikasnu transformaciju vektora stanja razloženog na 2^n kompleksnih brojeva. Najvažnija primjena ove transformacije je u eksponencijalnom ubrzavanju defaktorizacije velikih prirodnih brojeva.

[1] Peter Shor, rođen 1959. godine (New York City, New York, USA) je američki profesor primijenjene matematike na MTI Univerzitetu. Poznat je zbog svog doprinosa kvantnom računanju i razvoja algoritma za defaktorizaciju brojeva.

[2] Lov Grover je rođen 1961. godine (Delhi, India). Njegovi najznačajni doprinosi vezani su za oblast kvantnog računanja i razvoj algoritma za pretraživanje baze podataka.

NP problemi

U teoriji kompleksnosti, NP (nedeterminističko polinomijalno vrijeme) je skup problema odlučivanja riješivih u polinomijalnom vremenu na nedeterminističkoj Turingovoj mašini. Ekvivalentno, to je skup problema čija rješenja mogu da se provjere na determinističkoj Turingovoj mašini, u polinomijalnom vremenu. U teoriji kompleksnosti, polinomijalno vrijeme se odnosi na vrijeme izračunavanja problema, gdje vrijeme, $m(n)$, nije veće od polinomijalne funkcije veličine problema, n. Matematički zapisano u notaciji O, ovo znači $m(n) = O(n^k)$, gdje je k neka konstanta koja može zavisiti od problema.

4.1 Shorov algoritam

Svaki veći cijeli broj posjeduje jedinstvenu kompoziciju prostih cijelih brojeva, ali je određivanje ovih faktora problematično. Naime, sigurnost naših podataka koje svakodnevno koristimo prilikom transakcije se oslanja na činjenicu da je defaktorizacija velikih brojeva (sa preko hiljadu članova), skoro pa nemoguća. Osnova moderne kriptografije je upravo metoda defaktorizacije. Danas se za defaktorizaciju brojeva sa više od 100 članova, koristi NFS algoritam (Number Field Sieve), čije je vrijeme izvršanja problema:

$$\mathcal{O}(e^{(c+o(1))(\log n)^{1/3}(\log\log n)^{2/3}})$$

super-polinomijalno, pa defaktorizacija i dalje ostaje težak problem s kojim se suočava moderna kriptografija.

1995. Peter Shor je predložio vremenski polinomijalni kvantni algoritam za riješavanje problema defaktorizacije. Pretpostavimo da je naš zadatak odrediti proste faktore broja N sa d znakova. Standardni algoritam obično prolazi kroz sve proste brojeve p sve do vrijednosti $\sqrt{N}$, i provjerava da li je p djeljivo sa N. Shorov algoritam, s druge strane, za defaktorizaciju broja N, provjeru vrši u polinomijalnom vremenu. Nekom kvantnom kolu, je stoga za defaktorizaciju, potrebno vrijeme reda:

$$\mathcal{O}\big((\log N)^2(\log\log N)(\log\log\log N)\big),$$

što pokazuje da se ovaj problem može efikasno riješiti korištenjem kvantnih računara.

Efikasnost Shorovog algoritma posljedica je efikasnosti Fourierove transformacije i uzastopnog kvadriranja. Ako bi kvantni računar sa dovoljnim brojem kvantnih bita mogao da radi bez uticaja šumova i ostalih kvantnih smetnji, Shorov algoritam bi se mogao koristiti za razbijanja shema kriptografije javnog ključa, kao što su veoma poznate RSA sheme.

Postupak

Postavlja se sljedeći problem: za dat neparan složen broj N, naći neparan, cijeli broj d, strogo između 1 i N, koji dijeli N. Štaviše, da bi algoritam funkcionisao, potrebno je da N ne bude stepen faktora. Ovo se može testirati nalaženjem kvadratnog, kubnog.. k-tog korijena od N, za $k \leq \log_2 N$, i provjeravanjem da ni jedna od ovih vrijednosti nije cijeli broj. Ovo zapravo isključuje mogućnost da je $N = M^k$ za neke cijele brojeve M, $k > 1$. Pošto N nije stepen faktora, on je proizvod dva uzajamno prosta broja veća od 1. Kao posljedica kineske teoreme ostatka, broj 1 ima bar četiri različita korijena modula N, od kojih su dva sigurno 1 i -1. Cilj algoritma je da nađe korijen b od 1, osim 1 i -1. Takav broj b će dovesti do defaktorizacije broja N. Pronalaženje takvog broja b je svedeno na pronalaženje broja a parnog redosljeda sa određenom dodatnom osobinom. Upravo se kvantni algoritam koristi za nalaženje redosljeda nasumično odabranog elementa a, jer je nalaženje pravog redosljeda težak posao, barem na klasičnom računaru. Shorov algoritam se sastoji iz dva dijela:

1. Smanjenje problema defaktorizacije na problem nalaženja pravog redosljeda, što može da se izvrši primjenom klasičnih metoda.

2. Korištenje kvantnog algoritma za riješavanje problema redosljeda

Klasični dio

1. Odabrati nasumičan broj $a < N$.

2. Naći $NZD(a, N)$ koristeći Euklidov algoritam.

3. Ako je $NZD(a, N) \neq 1$, onda postoji netrivijalni faktor od N, tako da smo završili.

4. U suprotnom, iskoristiti podrutinu za nalaženje redosljeda da bi se našlo r:

   a) $f(x) = a^x mod(N)$

   b) $f(x + r) = f(x)$ ili $f(x + r) = a^{x+r} mod(N) = a^c mod(N)$

5. Ako je r neparno, ide se nazad na korak 1.

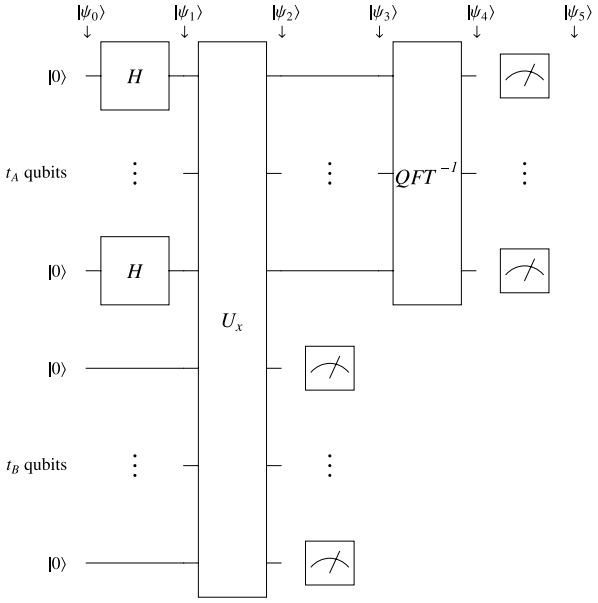
6. Ako je $a^{\frac{r}{2}} = -mod(N)$ ide se nazad na korak 1.

7. $NZD(a^{\frac{r}{2}} \pm 1, N)$ je netrivijalan faktor od N.

Npr., za $N = 15$, $a = 7$, $r = 4$, $NDZ(7^2 \pm 1, 15) = NZD(49 \pm 1, 15)$, gdje je $NZD(48, 15) = 3$ i $NZD(50, 15) = 5$. Za broj N koji je proizvod dva prosta broja p i q, vrijednost iznosi $\phi(N) = N - p - q + 1$, a koja je u ovom slučaju, za $N = 15$, 8. Primjetite da je 8 djeljivo sa r.

Kvantni dio: podrutina za nalaženje redosljeda Kvantna kola korištena za ovaj algoritam su posebno napravljena za svaki izbor N i nasumično korišteno a u $f(x) = a^x mod(N)$. Za dato N, naći $Q = 2^q$ tako da vrijedi $N^2 \leq Q \leq 2N^2$, iz čega slijedi da je $\frac{Q}{r} > N$. Ulazni i izlazni kvantni memorijski registri moraju da zadrže vrijednost superpozicije od 0 do $Q-1$, što znači da operišemo sa q kvantnih bita pojedinačno. Korištenjem duplo više qubita nego što se čini potrebnim, osiguravamo da postoji barem N različithih vrijednost x koji daju istu vrijednost funkcije $f(x)$, iako se redosljed r približava $\frac{N}{2}$. Postupamo na sljedeći način:

1. Postaviti registre na:
$$Q^{-\frac{1}{2}} \sum_{x=0}^{Q-1} |x\rangle |0\rangle .$$
Ovo početno stanje predstavlja superpoziciju Q stanja.



Slika 4.1.1: Kvantna kontura za Shorov algoritam

2. Formulisati funkciju $f(x)$ kao kvantnu funkciju i primjeniti je na gornje stanje da bi se dobilo:
$$Q^{-\frac{1}{2}} \sum_{x} |f(x)\rangle .$$
Ovo je i dalje superpozicija Q stanja.

3. Primjeniti kvantnu Fourierovu transformaciju na ulazni registar. Ova transformacija koristi, kako smo vidjeli, Q-ti jedinični korijen kao što je $\omega = e^{\frac{2\pi i}{Q}}$ da rasporedi amplitudu bilo kojeg datog $|x\rangle$ stanja jednako među svim Q $|y\rangle$ stanjima, i da uradi to na drugačiji način za svako različito $|x\rangle$ stanje:
$$U_{QFT} |x\rangle = Q^{-\frac{1}{2}} \sum_{y} \omega^{xy} |y\rangle .$$

Konačno stanje opisano je kao:

$$Q^{-1} \sum_x \sum_y \omega^{xy} |y\rangle |f(x)\rangle .$$

Izraz se nalazi u superpoziciji od mnogo više Q stanja, ali ipak mnogo manje od Q^2 stanja. Iako postoje Q^2 članovi u sumi, stanje $|y\rangle |f(x_0)\rangle$ se može zanemariti kad god x i x_0 daju istu vrijendost. Neka vrijedi:

- $\omega = e^{\frac{2\pi i}{Q}}$ Q-ti je jedinični korijen
- r je redosljed funkcije f
- x_0 je najmanji član od skupa x koji daju isto riješenje zadate funkcije $f(x)$
- $x_0 + rb < Q$

Onda je ω^{xy} jedinični vektor u kompleksnoj ravni (ω je jedninični vektor, a r i y su cijeli brojevi), a koeficijent $Q^{-1} |y\rangle |f(x_0)\rangle$ u krajnjem stanju je:

$$\sum_{x:f(x)=f(x_0)} \omega^{xy} = \sum_b \omega^{x_0+rb} = \omega^{x_0 y} \sum_b \omega^{rby}.$$

Svaki izraz u ovoj sumi predstavlja različit put do istog rezultata, pa dolazi do kvantne smetnje - kada jedinični vektori ω^{ryb} pokazuju u skoro istim smjerovima u kompleksnoj ravni, to zahtjeva da ω^{ry} pokazuje rezultat u pravcu pozitivne realne pozitivne ose.

4. Izvršiti mjerenje. Dolazimo do nekog ishoda y na ulaznom registru i z na izlaznom. Pošto je f periodična funkcija, vjerovatnoća mjerenja takvog stanja $|y, z\rangle$ data je kao:

$$\left| Q^{-1} \sum_{x \in \{0,\ldots,Q-1\}; f(x)=z} \omega^{xy} \right|^2 = Q^{-2} \left| \sum_b \omega^{(x_0+rb)y} \right|^2 = Q^{-2} \left| \sum_b \omega^{bry} \right|^2 .$$

Analize pokazuju da je ova vjerovatnoća veća, što je vektor ω^{ry} bliže pozitivnoj realnoj osi, ili što je $\frac{yr}{Q}$ bliže cijelom broju. Ako r nije rezultat potencije na drugu, neće biti faktor od Q.

5. Kako je $\frac{yr}{Q}$ bliže nekom cijelom broju c, vrijednost $\frac{y}{Q}$ je stoga bliža nepoznatoj vrijednosti $\frac{c}{r}$. Koristeći tzv. razvoj *verižnog* razlomka nad $\frac{y}{Q}$, približno određujemo $\frac{d}{s}$, za što vrijedi:

   a) $s < N$

   b) $\left| \frac{y}{Q} - \frac{d}{s} \right| < \frac{1}{2Q}$ Uz ovako definisane uslove i pretpostavku da je sam izraz $\frac{d}{s}$ ireducibilan, s je najvjerovatnije period od r, ali čak i ako nije, onda je barem faktor perioda.

6. Provjeriti da li vrijedi $f(x) = f(x+s) \Leftrightarrow a^s = 1 mod(N)$. Ako je uslov ispunjen, problem je riješen.

7. U suprotnom, uzeti još kandidata za r koristeći vrijednosti bliže y. Ako je uslov ispunjen, problem je riješen.

8. U suprotnom, vratiti se na prvi korak.

4.2 Groverov algoritam

Groverov algoritam je kvantni algoritam za pretraživanje nesortirane baze podataka sa N unosa u $\mathcal{O}(N^{\frac{1}{2}})$ vremenu koristeći $\mathcal{O}(\log N)$ memorijskog prostora, formulisan 1996. godine. U modelima klasičnog izračunavanja, pretraživanje i sortiranje nesortirane baze podataka ne može biti ostvareno za manje od linearnog vremena, tako da je pretraživanje elementa član po član, optimalno. Groverov algoritam ilustruje da u kvantnom modelu pretraga može biti izvršena znatno brže - njegova vremenska složenost $\mathcal{O}(N^{\frac{1}{2}})$ je asimptotski najbrža moguća za pretraživanje nesortirane baze podataka u kvantnom modelu. Pruža kvadratno poboljšanje, za razliku od drugih kvantnih algoritama, koji pružaju eksponencijalno, u odnosu na njihove klasične alternative. Kao i mnogi drugi algoritmi i Groverov algoritam je probabilistički u smislu da daje tačan rezultat sa visokim procentom vjerovatnoće. Vjerovatnoća javljanja greške može bti smanjena ponavljanjem algoritma. Deutsch-Jozsa algoritam je recimo deterministički i uvijek daje tačan odgovor.

Postavka i koraci algoritma

Uzmimo nesortiranu bazu podataka sa N unosa. Algoritmu je potreban N-dimenzionalni prostor H, koji može biti obezbjeđen sa $n = \log_2 N$ qubita. Neka je f funkcija koja označava unose baze sa 0 ili 1, gdje je $f(\omega) = 1$ ako i samo ako ω zadovoljava traženi uslov. Preko black-boxa osigurava nam se pristup ka podproblemu u obliku linearnog operatora U_ω, koje se ponaša kao:

$$U_\omega |\omega\rangle = -|\omega\rangle, \quad U_\omega |x\rangle = |x\rangle, \quad x \neq \omega.$$

Naš cilj je odrediti indeks za $|\omega\rangle$. Neka je $|s\rangle$ uniformna superpozicija svih stanja:

$$|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle.$$

Tada je operator, poznat kao i Groverov difuzni operator, definisan kao:

$$U_s = 2|s\rangle\langle s| - I.$$

Koraci Groverovog algoritma su sljedeći:

1. Inicijalizirati sistem u stanje $|s\rangle = \frac{1}{\sqrt{N}} \sum_{x=1}^{N} |x\rangle$.
2. Primijeniti sljedeće Groverove iteracije:
   a) Primjena operatora U_ω.
   b) Primjena operatora U_s.
3. Primijeniti rezultate mjerenja Ω. Rezultat mjerenja će biti λ_ω sa vjerovatnoćom koja se približava jedinici za $N \gg 1$. Iz λ_ω određuje se ω.

Prva iteracija Paralelno definiciji: $U_s = 2|s\rangle\langle s| - I$, zaključujemo da U_ω može biti izraženo i na drugačiji način:

$$U_\omega = I - 2|\omega\rangle\langle\omega|.$$

Da bismo ovo dokazali dovoljno je provjeriti kako se U_ω ponaša u baznim stanjima:

$$\big(I - 2|\omega\rangle\langle\omega|\big)|\omega\rangle = |\omega\rangle - 2|\omega\rangle\langle\omega|\omega\rangle = -|\omega\rangle = U_\omega|\omega\rangle;$$

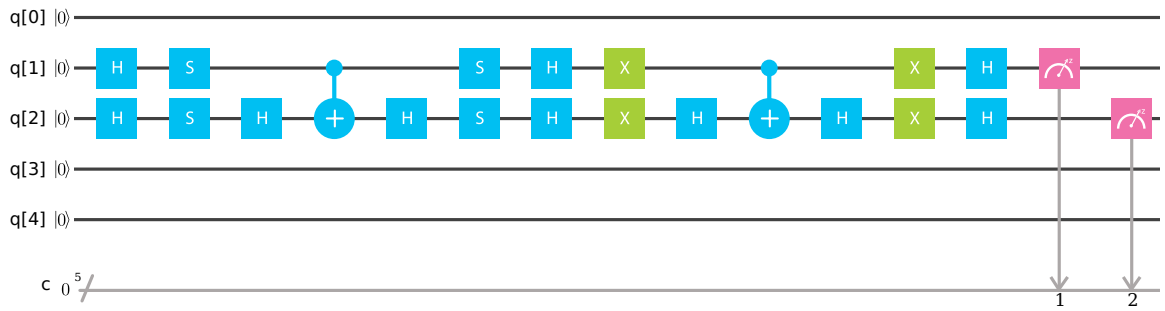
$$\big(I - 2|\omega\rangle\langle\omega|\big)|x\rangle = |x\rangle - 2|\omega\rangle\langle\omega|x\rangle = |x\rangle = U_\omega|x\rangle,$$

za svako $x \neq \omega$. Sljedeća izračunavanja pokazuju šta se dešava tokom prve iteracije:

$$\langle\omega|s\rangle = \langle s|\omega\rangle = \frac{1}{\sqrt{N}}$$

$$\langle s|s\rangle = N\frac{1}{\sqrt{N}} \cdot \frac{1}{\sqrt{N}} = 1$$

$$U_\omega|s\rangle = \big(I - 2|\omega\rangle\langle\omega|\big)|s\rangle = |s\rangle - 2|\omega\rangle\langle\omega|s\rangle = |s\rangle - \frac{2}{\sqrt{N}}|\omega\rangle$$



Slika 4.2.1: Prvi korak Groverovog algoritma predstavljen u IBM Q editoru

Groverov algoritam je optimalan. To znači, da bilo koji algoritam koji pristupa bazi podataka korištenjem isključivo operatora U_ω, mora primijeniti operator najmanje onoliko puta koliko i Groverov algoritam. Ovaj rezultat je bitan za razumijevanje ograničenja kvantnog računanja.

4.3 Deutsch-Jozsa algoritam

Pretpostavimo da nam je zadata Booleanska funkcija oblika $f : \{0,1\}^2 \to \{0,1\}$ i da znamo da je sigurno ili konstantna ili izbalansirana. Naš zadatak je odrediti koji slučaj je u pitanju.

unos	ispis
00	1
01	0
10	0
11	0

Tabela 4.1: f_{00}

unos	ispis
00	0
01	1
10	0
11	0

Tabela 4.2: f_{01}

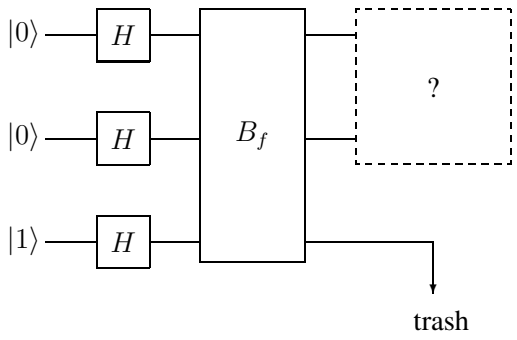
unos	ispis
00	0
01	0
10	1
11	0

Tabela 4.3: f_{10}

unos	ispis
00	0
01	0
10	0
11	1

Tabela 4.4: f_{11}

Kao i dosad, pretpostavit ćemo da je naš pristup problemu ograničen isključivo na evaluaciju transformacije B_f koja se dešava u black-boxu. U nastavku ćemo evaluaciju B_f označavati kao upit. U klasičnim sistemima, dovoljna bi bila samo tri upita da riješimo ovaj problem. Posmatrajmo dijagram:



Slika 4.3.1: Klasično riješenje problema

Stanje qubita nakon prolaska kroz Hadamardovo kolo bi bilo:

$$\left(\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right).$$

Nakon transformacije B_f, tvrimo da je stanje:

$$\left(\frac{1}{2}(-1)^{f(00)}|00\rangle + \frac{1}{2}(-1)^{f(01)}|01\rangle + \frac{1}{2}(-1)^{f(10)}|10\rangle + \frac{1}{2}(-1)^{f(11)}|11\rangle\right)\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right).$$

Posljednji qubit, kao stanje superpozicije (koje nam neće dati nikakav odgovor), ne ovisi o prethodnim stanjima, te se stoga tretira kao nepotreban (zanimaju nas samo vezana stanja), pa nam ostaje:

$$f = f_{00} \Rightarrow |\phi_{00}\rangle = -\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\,;$$

$$f = f_{01} \Rightarrow |\phi_{01}\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\,;$$

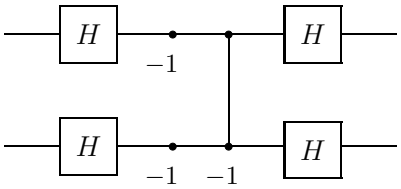
$$f = f_{10} \Rightarrow |\phi_{10}\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\,;$$

$$f = f_{11} \Rightarrow |\phi_{1}\rangle = -\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle\,.$$

Ova stanja su sva iz ortonormiranog seta. To znači da su ujedno i jedinični vektori i da su kao takvi međusobno ortogonalni. Kad god imamo ovakav ortonormiran set, uvijek je moguće izgraditi takvu kvantnu konturu koja jasno razlikuje međusobno ortogonalna stanja. U suštini, vrlo je jednostavno konstruisati odgovarajuću unitarnu matricu transformacije: vektori nam formiraju kolone matrice i kao takvu je konjugiramo. Naša matrica bi u tom slučaju imala oblik:

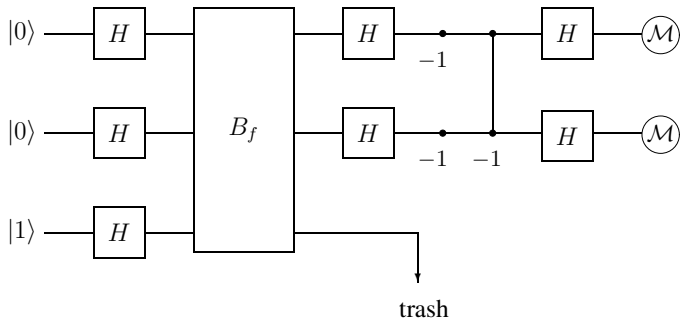
$$U = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & \frac{1}{2} & -\frac{1}{2} \end{pmatrix}$$

Konstruišimo sada i kvantnu konturu koja bi vršila operaciju unitarne matrice transformacije U.



Slika 4.3.2: Dio kvantne konture

Kvantno kolo koje je na slici predstavljeno tačkom (-1), odgovara Pauli Z operatoru, Z matrici, koja se još naziva i *fazna izmjena*. Konačna kontura ima oblik:



Slika 4.3.3: Kontura s primijenjenim kvantnim strukturama

Uopšteni Deutsch-Jozsa algoritam

Sljedeći algoritam predstavlja uopštenu verziju Deutschovog algoritma, tzv. *Deutsch*[3]-*Jozsa*[4] algoritam. Pretpostavimo da nam je data funkcija $f(x) : \{0,1\}^n \to \{0,1\}$, gdje je n neki proizvoljni cijeli, pozitivni broj, i neka su mogući sljedeći slučajevi:

1. Funkcija f je **konstantna**. Drugim riječima, ili je $f(x) = 0$ za svako $x \in \{0,1\}^n$ ili je $f(x) = 1$ za svako $x \in \{0,1\}^n$.

2. Funkcija f je **izbalansirana**. Broj unosa $x \in \{0,1\}^n$ za koje funkcija uzima vrijednosti 0 i 1 je isti:

$$\left|\{x \in \{0,1\}^n : f(x) = 0\}\right| = \left|\{x \in \{0,1\}^n : f(x) = 1\right| = 2^{n-1}.$$

Kao i za prethodna dva algoritma, pristup funkciji f je ograničen na upit uređaju koji odgovara transformaciji B_f definisanoj kao:

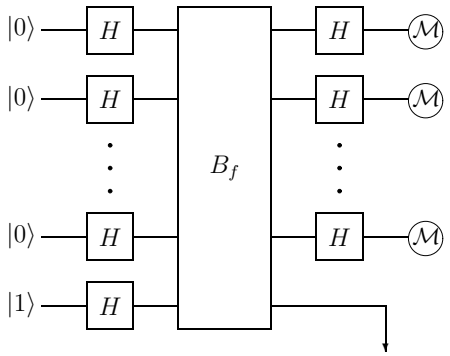
$$B_f \left|x\right\rangle \left|b\right\rangle = \left|x\right\rangle \left|b \otimes f(x)\right\rangle,$$

za svako $x \in \{0,1\}^n$ i $b \in \{0,1\}$. Klasično, ovaj problem je jako jednostavno riješiti s relativno malim brojem upita ako bismo sistemu dozvoliti nasumičnost i prihvatili da može doći do greške u rezultatu, iako sa zanemarivom vjerovatnoćom. Naime, možemo nasumično izabrati k unosa $x_1, ..., x_k \in \{0,1\}^n$, odrediti $f(x_i)$ za $i = 1, ..., k$ i zaključiti da je funkcija konstantna ako je $f(x_1) = ... = f(x_k)$ ili izbalansirana u suprotnom. Ako

[3]David Deutsch rođen 1953. godine (Haifa, Izrael) je britanski fizičar, izraelskog porijekla. Trenutno radi kao predavač na Oxfordu. Smatra se pionirom oblasti kvantnog računanja. Formulisao je opis kvantne Turingove mašine, a također je dizajnirao i algoritam koji se može izvršiti na kvantnom računaru.

[4]Richard Jozsa, rođen 1953. godine (Melbourne, Australija) trenutno radi kao profesor na Cambridge Univerzitetu. Zajedno sa Deutschom, smatra se pionirom kvantnog računanja. Njegov današnji rad se, pored razvoja kvantnih algoritama, odnosi i na razvoj ideje o kvantnoj teleportaciji. 2004. godine Udruženje matematičara iz Londona mu uručuje Naylor nagradu za doprinose na području kvantne informatike.

je funkcija doista konstantna, ova metoda će biti ispravna prilikom svakog mjerenja, ali ako je funkcija izbalansirana, algoritam će izbacivati grešku (kao rezultat će zaključivati da je funkcija kontantna) sa vjerovatnoćom $2^{-(k-1)}$. Uzmimo da je $k = 11$ i recimo, neka je vjerovatnoća greške manja od 1/1000. Međutim, ako želimo da algoritam uvijek daje tačna riješenja, tada je, u najgorem slučaju, potrebno $2^{n-1} + 1$ upita.



Slika 4.3.4: Uopšteni Deutsch-Jozsa algoritam (struktura)

Međutim u, nazovimo ga, kvantnom slučaju, samo jedan upit će biti dovoljan da sa sigurnošću utvrdimo da li je funkcija konstantna ili izbalansirana. Ako je za svih n mjerenja rezultat bio 0, zaključujemo da je funkcija konstantna, a ako je barem jedan rezultat bio 1, funkcija je izbalansirana. Ali prije nego što analiziramo sam algoritam, vratimo se na Hadamardovu transformaciju, za koju vrijedi:

$$H\left|a\right\rangle = \frac{1}{\sqrt{2}}\left|0\right\rangle + \frac{1}{\sqrt{2}}(-1)^{a}\left|1\right\rangle;$$

$$H\left|a\right\rangle = \frac{1}{\sqrt{2}}\sum_{b\in\{0,1\}}(-1)^{ab}\left|b\right\rangle.$$

Ako imamo dva qubita, inicijalno u stanju $x = x_1x_2 \in \{0,1\}^2$, i ako na njih primjenimo Hadamardovu transformaciju, dobit ćemo:

$$\begin{aligned}(H\otimes H)\left|0\right\rangle &= \left(\frac{1}{\sqrt{2}}\sum_{y_1\in\{0,1\}}(-1)^{x_1y_1}\left|y_1\right\rangle\right)\left(\frac{1}{\sqrt{2}}\sum_{y_2\in\{0,1\}}(-1)^{x_2y_2}\left|y_2\right\rangle\right)\\ &= \frac{1}{2}\sum_{y\in\{0,1\}^2}(-1)^{x_1y_1+x_2y_2}\left|y\right\rangle.\end{aligned}$$

Analogno pravilo primjenjujemo na bilo koji broj qubita. Notacijom $H^{\otimes n} = H\otimes\ldots\otimes H$, možemo pisati:

$$H^{\otimes n}\left|x\right\rangle = \frac{1}{\sqrt{2^n}}\sum_{y\in\{0,1\}^n}(-1)^{x_1y_1+\ldots+x_ny_n}\left|y\right\rangle,$$

$$H^{\otimes n} |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{xy} |y\rangle .$$

Sada je Deutsch-Jozsa algoritam jednostavniji za analizu. Stanje nakon prve Hadamardove stransformacije je:

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

Zatim, primjenom B_f transformacije, stanje ima oblik:

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

Usljed faznog kick-back efekta, posljedi qubit se odbacuje te se primjenjuje n Hadamardovih transformacija. Konačno stanje je:

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

odnosno:

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

Ono što nas zanima je vjerovatnoća da će svako mjerenje kao rezultat dati 0. Amplituda stanja $|0^n\rangle$ je:

$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)},$$

te je stoga vjerovatnoća definisana kao:

$$\left| \frac{1}{2^n} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \right|^2 = \begin{cases} 1 & \text{ako je funkcija } f \text{ konstantna,} \\ 0 & \text{ako je funkcija } f \text{ izbalansirana.} \end{cases}$$

5 Zaključak

U uvodnom dijelu rada postavili smo pitanje održivosti Mooreovog zakona, iako mu pretpostavke većine naučnika ne idu u prilog. Naime, od kraja šezdesetih godina do danas, tehnologija proizvodnje poluprovodničkih komponenti, a samim tim i računara, suštinski se nije mijenjala. Posljednji Intelov skok u proizvodnji mikroprocesora se smatra možda jednim od posljednjih udvostručavanja računarske moći. Teoretski, zakoni kvantne mehanike i kvantni efekti ne dopuštaju procesorske tehnologije manje od $10nm$. Riješenje ovog problema je naravno napuštanje klasičnih poluprovodničkih tehnologija i istraživanje novih računarskih metoda, odnosno, kvantnih računara. U praksi, kvantni računari bi koristili kvantne efekte, koji za klasične računare predstavljaju smetnje, za brže i efikasnije riješavanje problema.

5.1 Prednosti kvantnih računara

Vidjeli smo da nam kvantni algoritmi omogućavaju eksponencijalno ubrzavanje riješavanja određenih računarskih problema. Upravo se zbog toga ulažu velike svote novca u razvoj kvantnih računara. Uz njihovu pomoć, sadašnji klasični kriptografski kodovi bi se sa lakoćom mogli dešifrovati. Također, znatno ubrzanje bi dobili i algoritmi za pretraživanje baza podataka čime bi se ubrzao proces identifikacije.

Sa druge strane, komercijalni korisnici sa implementacijom kvantnog računara dobili bi veoma visok stepen privatnosti podataka. Za razliku od klasične kriptografije, kvantna kriptografija daje metode za enkripciju podataka koje su skoro nemoguće za dešifrovanje od strane neovlaštenog lica.

Drugi značajni aspekt kvantnog računarstva su kvantne mreže. Kvantna mreža je spoj dva ili više računara koji razmijenjuju resurse za riješavanje nekog problema. Implementacija kvantnih mreža na globalnom nivou omogućila bi bržu, efikasniju i sigurniju komunikaciju.

5.2 Nedostaci kvantnih računara

Kvantno računarstvo i kvantna informatika su relativno mlade naučne discipline, koje se intenzivno proučavaju tek tridesetak godina. Upravo zbog toga, javljaju se problemi

koji još uvijek nisu riješeni.

Prvi problem koji se javlja vezan je kvantne algoritme. Naime, sredinom devedesetih godina prošlog vijeka došlo je do ogromnog skoka u kvantnoj informatici pronalaskom Shorovog algoritma za defaktorizaciju brojeva. Kao što je već bilo riječi, Shorov algoritam eksponencijalno ubrzava proces defaktorizacije u odnosu na klasični računar. Smatralo se da će se ubrzo nakon ovog pronalaska, pronaći i druge klase kvantnih algoritama koji potvrđuju snagu kvantnih računara. Ako pogledamo na period od pronalaska Shorovog algoritma do danas, možemo vidjeti da nije došlo do značajnijeg teorijskog napretka na polju kvantne informatike.

Drugi veliki problem jesu fizička ostvarenja kvantnih računara. Praktično, dva osnovna problema koja se javljaju su izolovanje sistema od spoljašnje sredine i pristup tako izolovanom sistemu. Sa današnjim tehnološkim mogućnostima ova dva problema se ne mogu istovremeno riješiti. Tehnologija izolovanja sistema još uvijek nije dovoljno napredovala da može da izoluje kvantni sistem od dekoherencije na više od par sekundi, što kvantne računare u današnjoj fazi razvoja čini nepraktičnim. Današnji kvantni računari su ostvarivi samo u laboratorijskim uslovima i više su dokaz koncepta nego praktičnog, komercijalnog uređaja.

5.3 Budućnost kvantnih računara

Iako postoje mnogi dokazi da su kvantni računari realno ostvarivi, niko ne može da garantuje njihovu masovnu upotrebu u daljoj budućnosti. Veliki preokret uslovljen je pronalaskom materijala i tehnologije koji mogu izolovati kvantne sisteme u praktično neograničenim vremenskim periodima.

S druge strane, kvantni računari nisu jedini u trci za održavanje Mooreovog zakona. Pokazano je da se DNK računari, molekularni računari i drugi *bio* računari, također mogu koristiti za efikasniju i bržu obradu podataka.

Prije nego što ostvarimo masovnu proizvodnju kvantnih računara potrebno je razviti dublje teorijsko razumijevanje kvantne mehanike. U skorijoj budućnosti potrebno je također razviti tehnologiju izrade posebnih materijala koji bi kvantne sisteme efikasno zaštitili od dekoherencije.

Kvantni računari su svakako budućnost. Da li će se kao takvi komercijalizovati u narednih 5 ili 50 godina, ovisi isključivo o našem stepenu edukacije o ovom fenomenu.

Dodatak A

A.1 Black-box funkcija

Funkcija $f(x)$ je ili konstanta (vraća istu vrijednost za sve ulazne binarne podatke) ili izbalansirana (vraća jednu vrijednost za polovinu svih ulaznih podataka i drugu vrijednost za drugu polovinu). Ali nije nam dat apsolutno nikakav uvid u matematičku formulaciju funkcije $f(x)$, ali zamislimo da nam je funckija data kao *black-box* funkcija koja se ponaša tako da, za dati ulazni podatak x, vraća tačnu vrijednost za $f(x)$. Zadatak je odrediti, što se manje pozivajući na black-box, da li je funkcija konstanta ili izbalansirana.

Vodeći se klasičnim primjerom, kako je x bilo koji n-bitni binarni broj, od kojeg je moguće konstruisati ukupno 2^n znakova (ulaznih podataka), to je potrebno izvršiti provjeru na minimalno $\frac{1}{2}2^n + 1 = 2^{n-1} + 1$ podataka, kako bismo sa sigurnošću odredili tip funkcije.

Vidimo da nije potrebno provjeravati svih 2^n ulaznih bit znakovnih podataka, jer je funkcija $f(x)$ sigurno ili konstantna, ili izbalansirana, tako, ako utvrdimo da funkcija nije konstantna, onda sa sigurnošću možemo zaključiti da je izbalansirana, jer su to jedina dva moguća slučaja. Iako možemo izbjeći provjeravanje svakog ulaznog podatka pojedinačno, povećanje ulaznih znakovnih bita n rezultirat će ekponencijalnim rastom broja poziva na black-box kako bismo odredili tip funkcije od interesa. Međutim, uz korištenje kvantnih računara, da li je funkcija $f(x)$ konstantna ili izbalansirana, možemo odrediti samo jednim pozivom na black-box. Neka nam je ulazni podatak samo jedan bit ($n = 1$). Tada za funkciju $f(x)$ kažemo da je konstantna ako i samo ako vrijedi $f(0) = f(1)$, a da je izbalansirana u slučaju da je $f(0) \neq f(1)$.

Korištenjem klasičnog računara problem možemo riješiti određivanjem vrijednosti za $f(0)$, a zatim za $f(1)$, i upoređivanjem rezultata provjeriti da li je ispunjen slučaj $f(0) = f(1)$, odnosno da li je funkcija konstantna ili je izbalansirana za $f(0) \neq f(1)$. Ovom metodom je potrebno se dva puta pozvati na black-box u cilju utvrđivanja tipa funkcije. No, kvantni računar ovaj problem može riješiti metodom tzv. *kvantnog paralelizma.*

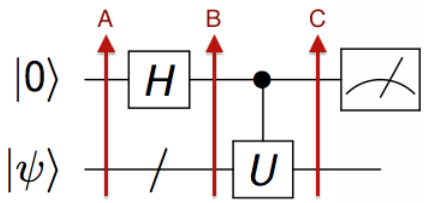
Dodatak B

B.1 Fazni kick-back efekat

Ključna stvar prilikom razumijevanja faznog *kick-back* efekta jeste da je $|\psi\rangle$ vlastiti vektor operatora U sa vlastitom vrijednošću $e^{2\pi i\phi}$. Drugim riječima:

$$U|\psi\rangle = e^{2ii\phi}|\psi\rangle,$$

gdje je ϕ faza koju želimo odbaciti. Da bismo objasniti kako kick-back mehanizam funkcioniše, započnimo sa primjerom:



Slika 5.3.1: Primjer prostog kvantnog kola

U tački A, stanje sistema je $|0\rangle|\psi\rangle$. Primjenom Hadamardove transformacije (operatora), tj. prolaskom stanja kroz Hadamard kolo, u tački B stanje $|0\rangle$ je konvertovano u $H|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, odnosno, ukupno stanje je sada:

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

Između tačaka B i C, nalazi se kontrolni operator U. Kontrolno kolo (kontrolni operator) se primjenjuje samo na gornji qubit kada je gornji qubit $|1\rangle$. Tako, u tački C, konačno stanje sistema je:

$$\frac{|0\rangle|\psi\rangle + |1\rangle U|\psi\rangle}{\sqrt{2}} = \frac{|0\rangle|\psi\rangle + |1\rangle e^{2\pi i\phi}|\psi\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2\pi i\phi}|1\rangle}{\sqrt{2}}|\psi\rangle.$$

Kako $|\psi\rangle$ ostaje nepromijenjeno? Iz prethodne analize vidimo da je to moguće iz prostog razloga što primjenom U operatora na $|\psi\rangle$, faktor $e^{2\pi i\phi}$ izlazi ispred kao vlastita

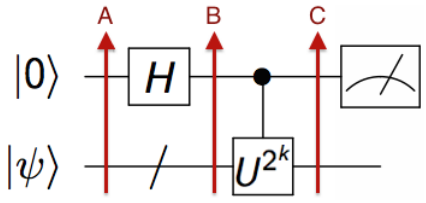
vrijednost vektora $|\psi\rangle$, te stanje (vektor) ostaje nepromijenjeno. Posmatrajmo sada više redove operatora U. Kao i prethodnom slučaju, $|\psi\rangle$ je i dalje vlastiti vektor operatora, recimo, U^2:

$$U^2 |\psi\rangle = U(U |\psi\rangle) = e^{2\pi i\phi} U(|\psi\rangle) = e^{2*2\pi i\phi} |\psi\rangle ,$$

ili općenito:

$$U^x |\psi\rangle = e^{2*x\pi i\phi} |\psi\rangle .$$

U skoro svim primjenama faznog kick-back efekta, riječ je o određenim potencijama operatora U, oblika U^{2^k}.

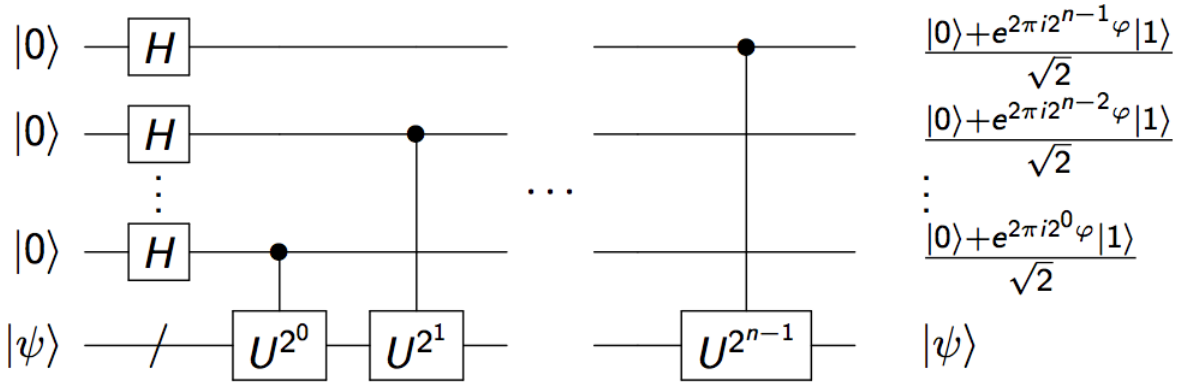


Slika 5.3.2: Primjena operatora U^{2^k}

Konture su iste. U tački B stanje sistema ima oblik $\frac{1}{\sqrt{2}}(|0\rangle |\psi\rangle + |1\rangle U |\psi\rangle)$. Primjenom kontrolnog kola, konačno stanje sistema u tački C je:

$$\frac{|0\rangle |\psi\rangle + |1\rangle U^{2^k} |\psi\rangle}{\sqrt{2}} = \frac{|0\rangle |\psi\rangle + |1\rangle e^{2*2^k\pi i\phi} |\psi\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{2*2^k\pi i\phi} |1\rangle}{\sqrt{2}} |\psi\rangle .$$

Vidimo da se i u ovom slučaju faza ϕ prebacuje (odbacuje) da gornji qubit, dok donji ostaje nepromijenjen.



Slika 5.3.3: Kontura sa n operatora

Donji qubit ostaje $|\psi\rangle$, dok je informacija o fazi sadržana u stanjima gornjih qubita.

Literatura

[1] Colin P. Williams. *Explorations in Quantum Computing*. Springer, 2011.

[2] Phillip Kaye. *An Introduction to Quantum Qomputing*. Oxford, 2016.

[3] Isaac Chuang and Michael Nielsen. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[4] Hedim Osmanović i Jugoslav Stahov. *Kvantna Mehanika u Primjerima*. Blicdruk, Sarajevo, 2013.

[5] David J. Griffiths. *Introduction to Quantum Mechanics*. Pearson Education, 2016.

[6] Elisa Bäumer, Jan-Grimo Sobez, Stefan Tessarini. *Shor's Algorithm*. ETH Zürich, 2014.

[7] Peter Shor. *Polynomial-time algorithms for prime factorization and discrete logarithms on quantum computer*. SIAM journal on computing, 1997.

[8] John Wright. *Lecture 4: Grover's Algorithm*. Carnegie Mellon University, 2015.

[9] John Watrous. *Lecture 5: A simple searching algorithm; the Deutsch-Joza algorithm*. University of Calgary, 2006.

[10] Niklas Johansson, Jan-Ake Larsson. *Efficient Classical Simulation of the Deutsch-Jozsa and Simon's Algorithms*. SpringerLink, 2018.