Univerzitet u Sarajevu

Prirodno-Matematički Fakultet
Odsjek za Matematiku,
Teorijska Kompjuterska Nauka

Odabrana poglavlja kompjuterskih nauka
(Seminarski rad)

Uvod u Kvantno Izračunavanje

Autor:
Haris Smajlović

Mentor:
doc. dr. Elmedin
Selmanović

22. prosinca 2014.

Sažetak

Kvantno Izračunavanje(Quantum Computing) je, kao grana Prirodnog Izračunavanje(Natural Computing), jedna od najmlađih znanosti Teorijske Kompjuterske Nauke koja koristi stanje superpozicije kvantnog sistema i preplitanje(entanglement) kao gradivne elemente izračunljivosti. Zašto Kvantno Izračunavanje? Naime, već na kraju ovog rada u kome ćemo dati generalni pregled osnova Kvantnog Izračunavanja, ćemo uvidjeti velike prednosti spram klasičnog izračunavanja. Rad je struktuiran tako da uvede čitaoca u osnove ove teorije koja se u mnogome razlikuje od ostalih metoda izračunavanja. Tako ćemo najprije uvesti gradivni element informacije u Kvantom Izračunavanju(Kvantni bit), zatim ćemo se upoznati sa jednim od načina manipulacije informacije na kvantom nivou(Kvantna kola). Nakon toga prelazimo na dva primjera primjene kvantih kola pri formiranju kvantnih algoritama i na kraju ćemo navesti neke prednosti i zanimljivosti Kvantnog Izračunavanja. Čitalac će na kraju imati generalni uvid u ovu znanost i poznavati njene osnovne osobine.

1 Uvod

Kvantno Izračunavanje(u nastavku je mjestimično korišten termin QC-Quantum Computing), kao i ostale grane Prirodnog Izračunavanja, je zasnovana na nekom prirodnom fenomenu, tačnije na fenomenima Kvantne Mehanike. Naime, formiranjem Kvantne Teorije 1920-tih, tim fizičara i matematičara na čelu sa Max Planck-om, dolazi do saznanja da se Kvantni Sistemi(npr. elektron, foton, ...) mogu nalaziti u različitim fizičkim stanjima. Daljim istraživanjem se razaznaje da su ta stanja uvijek u obliku linearne kombinacije neka dva fiksirana stanja i to dva ortogonalna stanja. Kasnije se otkrivaju i neke "čudne" osobine stanja kvantnih sistema kao sto su Bell-ova stanja(EPR par) koje će poslužiti kao jedan koristan alat u QC. 1980-tih, nakon ideje korištenja kvantnih stanja kao gradivnih elemenata izračunljivosti(elemenata analognih bitu u klasičnim sistemima), se udara temelj kvantnog izračunavanja. QC doživljava svoj procvat tek početkom drugog milenija, nakon otkrića Deutch-Jozsa algoritma i Shor-ovog algoritma koji su pokazali prednosti kvantnog izračunavanja nad klasičnim modelima. Od tada se na ovoj oblasti intenzivno radi i do danas smo posvjedocili mnogim otkricima koja nas ohrabruju da sve više vjerujemo da će nas Kvantno Izračunavanje uvesti u eru brzog procesuiranja kakvo do sada nismo doživjeli.

2 Qubit

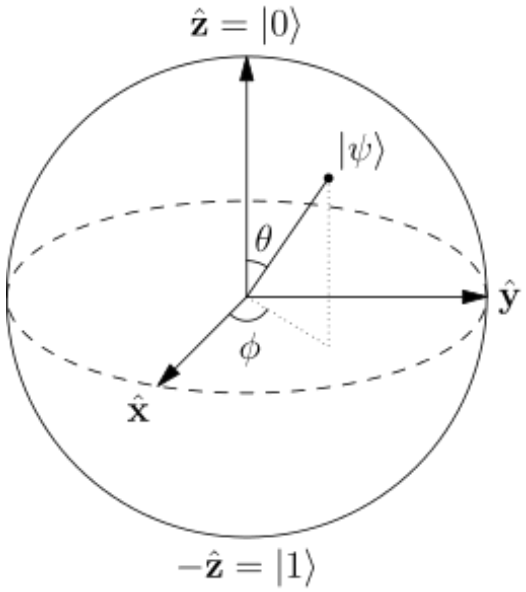
Riječ Qubit je nastala od riječi Quantum Bit i on je analogija klasičnom bitu. Qubit zapravo predstavlja jedan kvantni sistem i kao što smo već pomenuli ti sistemi se mogu nalaziti u različitim stanjima. Međutim, za razliku od klasičnog bita gdje imamo samo dva diskretna stanja 0 i 1, kvantni bit ima beskonačno mnogo mogućih stanja. Svako stanje kvantnog bita se može predstaviti kao liearna kombinacija dva ortogonalna stanja, tako da kada govorimo o stanjima Qubita-a mozemo reći da imamo stanja $|0\rangle$ i $|1\rangle$ koja su ortogonalna, a da su sva ostala stanja predstavljena kao $\alpha|0\rangle + \beta|1\rangle$ gdje $\alpha, \beta \in \mathbb{C}$. Ortogonalna stanja se još nazivaju i bazna stanja, a stanje linearne kombinacije baznih stanja se naziva još i superpozicija. (Notacija $|\psi\rangle$ se naziva Ket notacija i ona je potpuni analogon vektorskoj notaciji $\vec{\psi}$, postoji još i Bra notacija oblika $\langle\psi|$ istog značenja koja se najviše koristi u notaciji unutrašnjeg proizvoda vektora koja je oblika $\langle\psi|\phi\rangle$. Dakle primijetimo da su stanja kvantnih sistema zapravo vektori. Bra-Ket notacije se još zovu i Dirac-ove notacije)
S obzirom da su kubiti zapravo vektori to možemo uvesti i matrični zapis kubita:

$$|0\rangle \equiv \begin{bmatrix}1\\0\end{bmatrix} \quad |1\rangle \equiv \begin{bmatrix}0\\1\end{bmatrix} \quad \Rightarrow \alpha|0\rangle + \beta|1\rangle = \alpha\begin{bmatrix}1\\0\end{bmatrix} + \beta\begin{bmatrix}0\\1\end{bmatrix} = \begin{bmatrix}\alpha\\\beta\end{bmatrix}$$

Matrični zapis je vrlo koristan i uglavnom se koristi prilikom bilo kakve manipulacije sa kubitima.

2.1 Monokubitni sistemi

Jedan i samo jedan kvantni sistem čini monokubitni sistem. Kao što smo već rekli, kvantna stanja su zapravo vektori i to takvi da je svaki vektor jednak linearnoj kombinaciji dva fiksirana i ortogonalna vektora, tj. za vektorski prostor V kojeg čine kvantna stanja nekog kvantnog sistema vrijedi $\forall|\psi\rangle \in V \Rightarrow |\psi\rangle = \alpha|0\rangle + \beta|1\rangle|\alpha, \beta \in \mathbb{C} \wedge |0\rangle\perp|1\rangle$ i vrijedi $|\alpha|^2 + |\beta|^2 = 1$ tj. $\langle\psi^*|\psi\rangle = 1$. Ortogonalna kvantna stanja, u ovom slučaju $|0\rangle$ i $|1\rangle$, se nazivaju baznim stanjima nekog kvantnog sistema. Dalje, može se primijetiti da ovako definisani vektori(kvantna stanja) čine Hilbertov prostor nad poljem kompleksnih brojeva.
Najčešća reprezentacija monokubitnih sistema je geometrijska reprezentacija pomoću Bloch-ove sfere. Naime, ukoliko pretpostavimo da $\alpha \in \mathbb{R} \wedge \alpha \geq 0$



Slika 1: Bloch-ova sfera, $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + (\cos\phi + \imath\sin\phi)\sin\frac{\theta}{2}|1\rangle$

u $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, što možemo uraditi bez umanjenja opštosti, zatim uzevši u obzir da vrijedi $\langle\psi^*|\psi\rangle = 1$, stanje superpozicije se da zapisati u obliku $|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + \mathrm{e}^{\imath\phi}\sin\frac{\theta}{2}|1\rangle = \cos\frac{\theta}{2}|0\rangle + (\cos\phi + \imath\sin\phi)\sin\frac{\theta}{2}|1\rangle$, gdje $0 \leq \theta \leq \pi \wedge 0 \leq \phi < 2\pi$. Odatle možemo formirati sferu kvantnih stanja kao na slici 1.

2.2 Polikubitni sistemi i preplitanje

Skup od dva ili više kvantnih sistema se naziva polikubitni sistem. Stanje polikubitnog sistema sastavljenog od stanja $|\psi\rangle$ i $|\phi\rangle$ se piše kao $|\psi\rangle|\phi\rangle$ i ukoliko je $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \wedge |\phi\rangle = \gamma|0\rangle + \delta|1\rangle|\alpha, \beta, \gamma, \delta \in \mathbb{C}$ tada je $|\psi\rangle|\phi\rangle = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle = \alpha'|00\rangle + \beta'|01\rangle + \gamma'|10\rangle + \delta'|11\rangle$ gdje $\alpha', \beta', \gamma', \delta' \in \mathbb{C} \wedge |\alpha'|^2 + |\beta'|^2 + |\gamma'|^2 + |\delta'|^2 = 1$. Primijetimo da ukoliko se radi o baznim stanjima, u našem slučaju $|0\rangle$ i $|1\rangle$, tada se $|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle$ piše redom kao $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. (Analogno, ukoliko je $|\xi\rangle$ neko bazno stanje, tada se $|\xi\rangle|\xi\rangle \ldots |\xi\rangle$ piše kao $|\xi\xi \ldots \xi\rangle$)
U ovom slučaju stanja $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ postaju bazna stanja polikubitnog sistema. Analogno, za polikubitni sistem sastavljen od n stanja vrijedi $|\psi_1\rangle|\psi_2\rangle \ldots |\psi_n\rangle = \alpha'_1|000 \ldots 00\rangle + \alpha'_2|000 \ldots 01\rangle + \cdots + \alpha'_{n+1}|100 \ldots 00\rangle +$

$\cdots + \alpha'_{2^n-1}|111\ldots11\rangle$ gdje je $|\psi_i\rangle = \lambda|0\rangle + \mu|1\rangle|\lambda, \mu \in \mathbb{C}$.
Nerijetko se dešava da stanja kvantnih sistema nekog polikubitnog sistema nisu nezavisna, tj. polikubitni sistem se mora tretirati kao jedan monokubitni sistem sastavljen od više baznih stanja. U tom slučaju kazemo da je došlo do preplitanja(entanglement) kvantnih sistema(kubita). Npr. ukoliko dva kubita dovedemo u stanje preplitanja, tada će bilo kakvo djelovanje na prvi kubit uticati i na drugi kubit, čak i ako su ta dva kubita razdvojena nakon preplitanja. Ova osobina je nagnala fizičare dvadesetog stoljeća da postave hipotezu prenosa informacije brže od brzine svjetlosti. Preplitanje je jedan od fundamentalnih alata kvantnog izračunavanja.

2.3 EPR par

Najosnovnija stanja preplitanja su takozvana Bell-ova stanja. To su stanja oblika:

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

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

Ova stanja kvantnih sistema su prvi put primijećena 20tih godina prošlog stoljeća. Primijetili su ih Einstein, Podolsky i Rosen po čijim inicijalima je par kubita sa nekim od ova dva stanja nazvan EPR par. Postoji i istoimeni paradoks, EPR pradoks, koji je koristeći upravo primjer Bell-ovih stanja poljuljao Kvantnu Teoriju (Više o EPR paradoksu u podpoglavlju 5.2).

3 Kvantna kola

Kvanta kola u QC su potpuna analogija ulaznim kolima(gate-ovima) u klasičnim modelima. Međutim, za razliku od klasičnih kola, kvanta kola mogu biti invertibilna. Dakle, ukoliko primijenimo neko kvantno kolo X na polikubitni sistem $|\psi\rangle|\phi\rangle$ i pri tome dobijemo polikubitni sistem $|\psi'\rangle|\phi'\rangle$, tada djelovanjem nekog kvantnog kola Y na rezultat, možemo dobiti početni polikubitni sistem. U ovom slučaju kazemo da je Y inverz od X,($Y = X^{-1}$). Kao i kubit, kvanto kolo se može pisati u matričnom obliku(vidjećemo u nastavku na koji način). Da bi stvar bila jos bolja, kvanto kolo zapravo mora biti invertibilno, čak šta više, može se dokazati da bilo koje kolo čija matrica A je unitarna,

Slika 2: Simbolni zapis

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

Slika 3: Matrični zapis

tj. da vrijedi $A^*A = I$, je neko kvantno kolo. Postoje simbolni i matrični zapis kvantnih kola (Slika 2 i Slika 3).

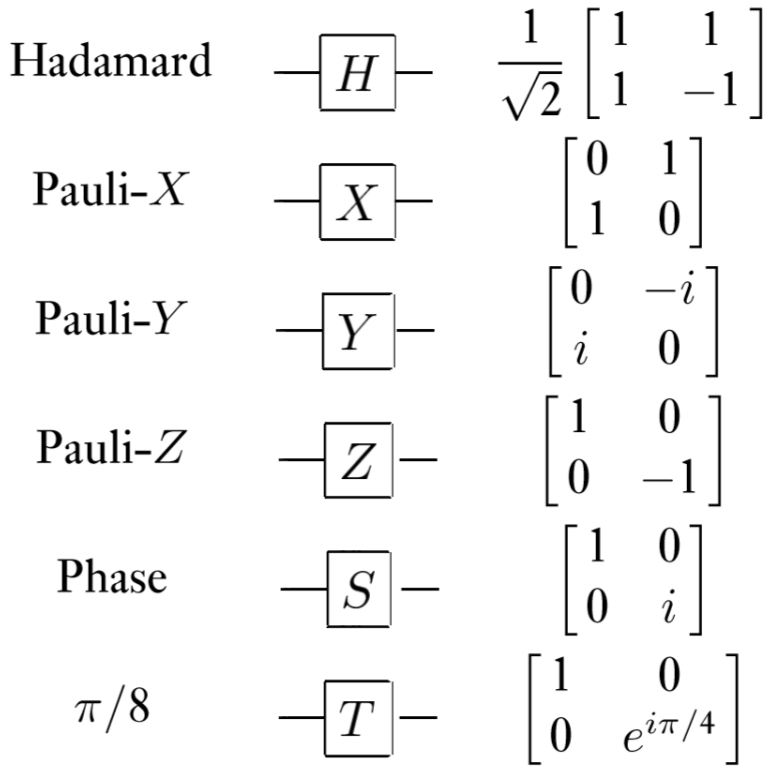
3.1 Kola monokubitnih sistema (monokubitna kola)

Kola monokubitnih sistema su kola koja djeluju na jedan i samo jedan kubit. To su sva kola čiji matrični zapis je unitarna matrica formata 2×2. Dakle za razliku od klasičnog modela gdje postoje najviše četiri moguća unarna ulazna kola, u QC ih imamo više (Sve unitarne matrice od ukupno 16 mogućih, formata 2×2). Osnovno kolo monokubitnih sistema je NOT kolo koje je analongo istoimenom kolu u klasičnim sistemima. Na ovom kolu ćemo pokazati primjer rada kvantnih kola. NOT kolo se zove još i Paulijevo X kolo (Slka 4). Ukoliko želimo da vidimo u kojem obliku će biti stanje $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ nakon djelovanja NOT kola na njega, dovoljno je da pomnožimo stanje $|\psi\rangle$ kubita sa matricom kola X tj.:

$$X|\psi\rangle = X \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} \beta \\ \alpha \end{bmatrix} = \beta|0\rangle + \alpha|1\rangle$$

Primijetimo da smo dobili upravo negaciju od $\alpha|0\rangle + \beta|1\rangle$ jer je $|0\rangle$ prešlo u $|1\rangle$, a $|1\rangle$ prešlo u $|0\rangle$. Na isti način rade i ostala kola monokubitnih sistema.

Slika 4: NOT kolo, simbolni i matrični zapis



Slika 5: Najpoznatija monokubitna kola

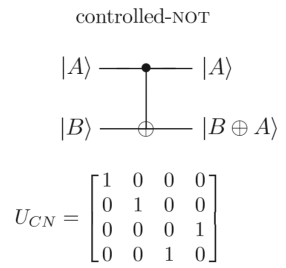
Lista najpoznatijih monokubitnih kola je data na slici 5.

3.2 Kola polikubitnih sistema (polikubitna kola)

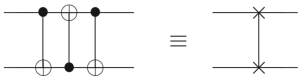
Kola polikubitnih sistema su kola koja djeluju na dva ili više kubita. Najpoznatije kolo polikubitnih sistema je takozvano CNOT(controlled-not) kolo (Slika 6). To je ujedno i univerzalno kolo QC-a, dakle kombinacijom ovih kola je moguće simulirati bilo koje drugo polikubitno kolo. Još jedno korisno polikubitno kolo je SWAP kolo koje razmjenjuje stanja kubita. SWAP kolo je sastavljeno od tri uzastopna CNOT kola (Slika 7) i lako se vrši njegova verifikacija:

$$|a,b\rangle \to |a, a\oplus b\rangle \to |a\oplus a\oplus b, a\oplus b\rangle \to |a\oplus a\oplus b, a\oplus b\oplus b\rangle = |b,a\rangle$$

Lista najpoznatijih polikubitnih kola je data na slici 8.



Slika 6: Simbolni i matrični zapis CNOT kola



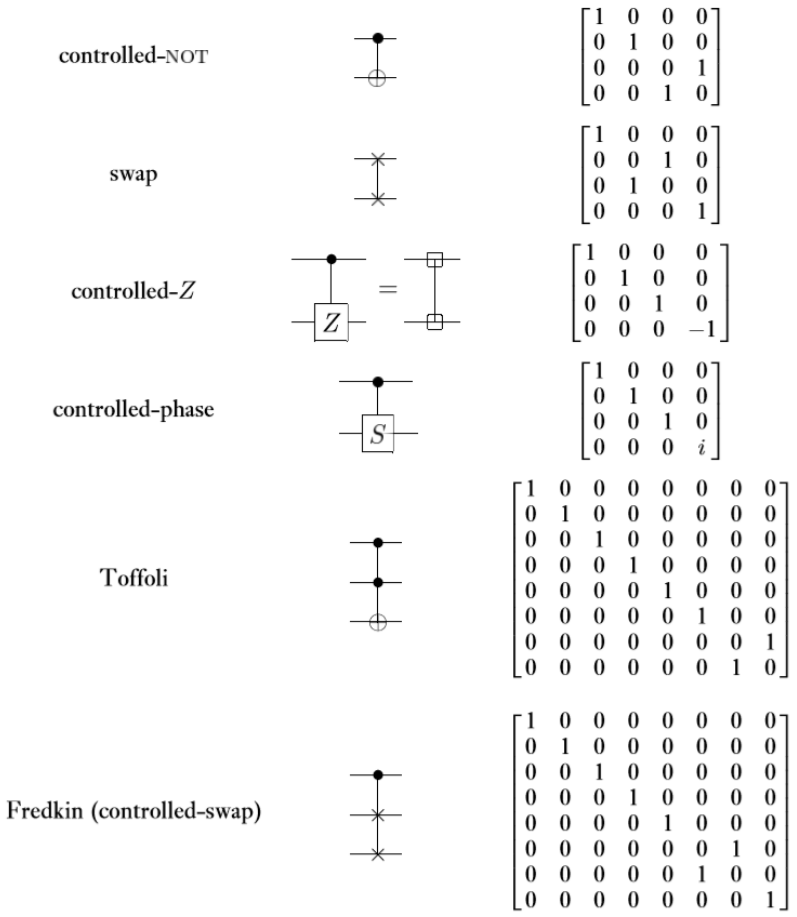
Slika 7: SWAP kolo i njegov simbolni zapis

4 Kvantni algoritmi

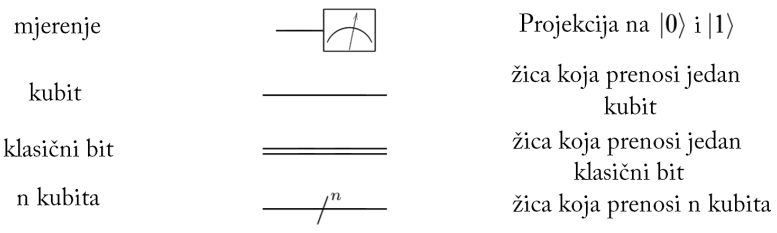
Kvantni algoritmi se uveliko razlikuju od klasičnih algoritama. Na prvom mjestu, ne mogu se interpretirati kao klasični algoritmi. Njihova interpretacija se vrsi koristeći kvantna kola ili kvantnu Turingovu mašinu. Zatim, njihova verifikacija može biti komplikovana, što ćemo vidjeti na sljedećim primjerima. No najprije da navedemo osobine QC-a neophodne za razumijevanje kvantnih algoritama, to su mjerenje i u ovom slučaju, kvantni paralelizam.

4.1 Mjerenje

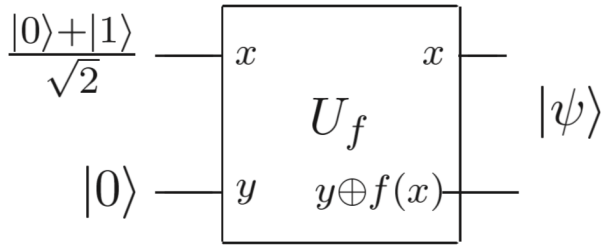
Mjerenje stanja kvantnog sistema je malo razočaravajuce. Naime, stanje kvantnog sistema je nemoguće izmjeriti, tj. nemoguće je saznati parametre α i β u stanju $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Međutim, pokušaj mjerenja kubita dovodi do sljedeće pojave, kubit prelazi u jedno od baznih stanja i u njemu ostaje do kraja života. Npr. ukoliko pokušamo izmjeriti stanje $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, kubit će preći ili u stanje $|0\rangle$ ili u stanje $|1\rangle$ i to vjerovatnoća da pređe u stanje $|0\rangle$ je $|\alpha|^2$, dok je vjerovatnoća da pređe u $|1\rangle$ jednaka $|\beta|^2$. Ovo naizgled djeluje kao jedna obeshrabrujuća činjenica, ali čak i sa ovim defektom, QC je vrlo pogodan za izračunavanje. Na slici 9 su date notacije koje se koriste prilikom mjerenja i prenosa informacije.



Slika 8: Najpoznatija polikubitna kola



Slika 9: Mjerenje i prenos informacije



Slika 10: Kvantno kolo U_f koje za stanje $|x\rangle|y\rangle$ na ulazu vraća $|x\rangle|y \oplus f(x)\rangle$ na izlazu

4.2 Kvantni paralelizam

Neka je data funkcija $f : \{0,1\} \to \{0,1\}$. Sposobnost simultane evaluacije funkcije $f(x)$ za dva različita parametra se naziva kvantni paralelizam. Ovu sposobnost posjeduje QC i ona radi na sljedeći način. Najprije formiramo kvanto kolo U_f koje primijenjeno na stanje $|x\rangle|y\rangle$ daje stanje $|x\rangle|y \oplus f(x)\rangle$. Ovakvom kvantnom kolu dovedemo na ulaz stanje $(\frac{|0\rangle+|1\rangle}{\sqrt{2}})|0\rangle$, kao na slici 10. Tada ćemo na izlazu kvantnog kola U_f dobiti stanje

$$(\frac{|0\rangle + |1\rangle}{\sqrt{2}})(|0 \oplus f(\frac{|0\rangle + |1\rangle}{\sqrt{2}})\rangle) = \frac{|0\rangle|f(\frac{|0\rangle+|1\rangle}{\sqrt{2}})\rangle + |1\rangle|f(\frac{|0\rangle+|1\rangle}{\sqrt{2}})\rangle}{\sqrt{2}} =$$

$$= \frac{|0\rangle|f(0)\rangle + |1\rangle|f(1)\rangle}{\sqrt{2}}$$

Dakle u stanju na izlazu je smještena vrijednost $f(0)$ kao i $f(1)$, time je simultano evaluirana funkcija f za oba parametra.

4.3 Deutsch-Jozsa algoritam

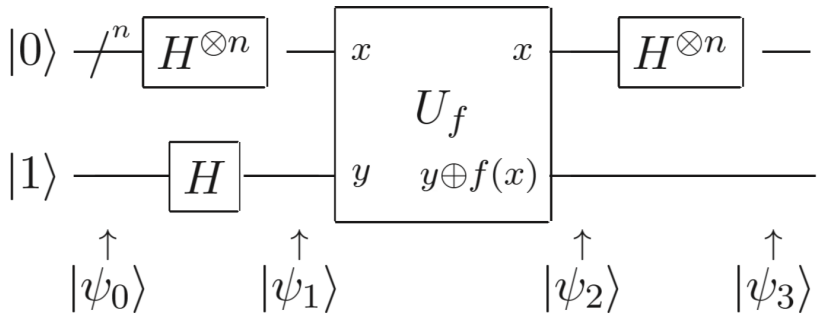
Deutsch-Jozsa algoritam je algoritamsko rješenje Deutsch-ovog problema. Iako nema nikakvu primjenu u praksi, dobar je primjer prednosti QC-a spram klasičnog izračunavnja. Deutsch-ov problem se sastoji u sljedećem:
Neka su Amela i Ulfrik prijatelji i Amela je u Sarajevu a Ulfrik u Windhelmu (Udaljenost Sarajevo-Windhelm je tu radi povećanja kompleksnosti problema). Amela šalje Ulfriku po jedan broj između 0 i $2^n - 1$. Ulfrik posjeduje jednu funkciju f koja prima jedan cjelobrojni parametar i koja je ili

balansirana ili konstantna (balansirana je ukoliko za 2^n različitih parametara vraća tačno 2^{n-1} nula i 2^{n-1} jedinica, a konstanta ukoliko vraca nulu ili jedinicu za svaki parametar). Nakon što primi broj od Amele, Ulfrik proslijedi taj broj kao parametar svojoj funkciji f i rezultat šalje nazad Ameli. Postavlja se pitanje, koliko najmanje brojeva mora Amela poslati Ulfriku da bi saznala sa sigurnošću kakvog je oblika funkcija f (balansirana ili konstantna). Klasični deterministički algoritam za rješavanje ovog problema bi bio kompleksnosti $O(2^n)$. Zaista, da bi Amela bila potpuno sigurna o kojoj funkciji se radi, mora poslati tačno $2^{n-1}+1$ brojeva Ulfriku.
Kvantni algoritam za ovaj problem je puno brži. Kompleksnost Deutsch-Jozsa kvantnog algoritma za Deutsch-ov problem je $O(1)$, čak šta više potrebne su samo dvije iteracije, tj. dva slanja (jedno slanje od Amele ka Ulfriku i drugo od Ulfrika ka Ameli) za rješenje ovog problema na kvantnom nivou. Deutsch-Jozsa algoritam okvirno radi na sljedeći način:
Pretpostavimo da će Ulfrik pristati da koristiti U_f kolo za evaluaciju svoje funkcije f. Neka Amela ima registar od n kubita za smještanje jednog od brojeva $0-2^n-1$ u binarnom obliku i jedan jednokubitni registar koji će slati Ulfriku da smjesti rezultat svoje funkcije u njega. Amela najprije pripremi sve svoje kubite prebacujući ih u stanje superpozicije Hadamord-ovim kolom (vidjeti sliku 5 za Hadamard-ovo kolo). Ovakve kubite Amela šalje Ulfriku i on koristeći U_f kolo smješta rezultat u jednokubitni registar koji šalje nazad Ameli. Sada sve što treba Amela da uradi jeste da ponovo primijeni Hadamardovo kolo na svoj n-kubitni registar i koristeći prikladno mjerenje jednokubitnog registra može zaključiti o kojoj funkciji f se radi. U nastavku vršimo detaljnu verifikaciju Deutsch-Jozsa algoritma:
Algoritam koji smo prethodno opisali je dat na slici 11. Notacija $H^{\otimes n}$ je drugačiji zapis za n uzastopnih Hadamardovih kola. Algoritam ćemo analizirati analizirajući redom stanja $|\psi_i\rangle \,|\, i = \overline{0\ldots3}$ na slici. Dakle, Amela posjeduje n-kubitni registar popunjen kubitima baznih stanja $|0\rangle$ i jedan jednokubitni registar sa kubitom stanja $|1\rangle$. Za stanje $|\psi_0\rangle$ primijetimo da je

$$|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$$

Nakon djelovanja Hadamardovih kola imamo stanje

$$|\psi_1\rangle = \frac{(|0\rangle+|1\rangle)^n}{2^{\frac{n}{2}}}\frac{|0\rangle-|1\rangle}{\sqrt{2}} = \sum_{x\in\{0,1\}^n}\frac{|x\rangle}{\sqrt{2^n}}\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)$$



Slika 11: Deutsch-Jozsa algoritam

Stanje $|\psi_1\rangle$ Amela šalje Ulfriku i on primjenivši U_f kolo na njega dobija stanje

$$|\psi_2\rangle = \frac{(|0\rangle + |1\rangle)^n}{2^{\frac{n}{2}}} \left(\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right) \oplus f \left(\frac{(|0\rangle + |1\rangle)^n}{2^{\frac{n}{2}}} \right) \right) =$$

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

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

Posljednja jednakost vrijedi jer funkcija f vraća vrijednosti ili 0 ili 1, pa je desna zagrada jednaka ili $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ ili $\frac{-|0\rangle + |1\rangle}{\sqrt{2}}$ u zavisnosti od funkcije f.
Prije nego što pređemo na stanje $|\psi_3\rangle$, tj. nakon što Amela primijeni Hadamardova kola na n-kubitni registar, posmatrajmo pojednostavljen slučaj. Posmatrajmo slučaj kada primjenjujemo Hadamardovo kolo na neko bazno stanje $|\xi\rangle$, dakle $\xi = 0 \vee \xi = 1$. Imamo

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

Ovo drugačije možemo zapisati kao

$$H|\xi\rangle = \sum_{z=0}^{1} \frac{(-1)^{\xi z}|z\rangle}{\sqrt{2}}$$

Analogno za n baznih stanja ξ_i imamo

$$\left(H^{\otimes n}\right)|\xi_1\rangle|\xi_2\rangle\cdots|\xi_n\rangle = \prod_{i=1}^{n} H|\xi_i\rangle = \prod_{i=1}^{n}\sum_{z_i=0}^{1}\frac{(-1)^{\xi_i z_i}|z_i\rangle}{\sqrt{2}} =$$

$$= \prod_{i=1}^{n}\frac{|0\rangle + (-1)^{\xi_i}|1\rangle}{\sqrt{2}} = \frac{|0\rangle|0\rangle\cdots|0\rangle + (-1)^{\xi_n})|0\rangle|0\rangle\cdots|1\rangle + \cdots + (-1)^{\sum_{k=1}^{n}\xi_k}|1\rangle|1\rangle\cdots|1\rangle}{\sqrt{2^n}} =$$

$$= \sum_{(z_1,z_2,\ldots,z_n)\in\{0,1\}^n}\frac{(-1)^{\sum_{i=1}^{n} z_i\xi_i}|z_1\rangle|z_2\rangle\cdots|z_n\rangle}{\sqrt{2^n}}$$

Dobijeni rezultat možemo kraće napisati kao

$$H^{\otimes n}|\xi\rangle = \sum_{z}\frac{(-1)^{\langle z|\xi\rangle}|z\rangle}{\sqrt{2^n}} \qquad (*)$$

gdje je $|\xi\rangle = |\xi_1,\xi_2,\ldots,\xi_n\rangle = |\xi_1\rangle|\xi_2\rangle\cdots|\xi_n\rangle \wedge |z\rangle = |z_1,z_2,\ldots,z_n\rangle = |z_1\rangle|z_2\rangle\cdots|z_n\rangle$, a $\langle z|\xi\rangle$ kanonski unutrašnji proizvod vektora $|z\rangle$ i $|\xi\rangle$.
Upravo formula $(*)$ je ta koja nam treba da bismo izračunali stanje $|\psi_3\rangle$, jer Amela treba da primijeni n Hadamardovih kola $(H^{\otimes n})$ na stanje $\sum_{x\in\{0,1\}^n}\frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}}$ u $|\psi_2\rangle$. Tj. treba da izračuna $H^{\otimes n}|x\rangle$. Koristivši formulu $(*)$ imamo da je

$$H^{\otimes n}|x\rangle = \sum_{z}\frac{(-1)^{\langle z|x\rangle}|z\rangle}{\sqrt{2^n}}$$

i odatle je

$$|\psi_3\rangle = \sum_{z}\sum_{x}\frac{(-1)^{\langle x|z\rangle+f(x)}|z\rangle}{2^n}\frac{|0\rangle-|1\rangle}{\sqrt{2}} \quad x,z\in\{0,1\}^n$$

Primijetimo sada da je koeficijent uz stanje $|z\rangle = |0,0,\ldots,0\rangle$ jednak $\sum_x\frac{(-1)^{f(x)}}{2^n}(\star)$. Ukoliko je f konstantna tada je $(\star)$ jednak ili $\sum_x\frac{-1}{2^n}$ ili $\sum_x\frac{1}{2^n}$, tj.

$$(\star) = \begin{cases} -1 & f(x) = 1\,\forall x\in\{0,1\}^n \\ 1 & f(x) = 0\,\forall x\in\{0,1\}^n \end{cases}$$

S obzirom da zbir kvadrata svih keoficijenata nekog kvantnog stanja mora biti jednak 1, znači da koeficijenti uz sve $|z\rangle \mid z\in\{0,1\}^n\backslash(0,0,\ldots,0)$ moraju

biti jednaki 0. Što znači da ukoliko se radi o konstantnoj funkciji, Amelin n-kubitni registar će na kraju sadržavati vrijednost $(0, 0, \ldots, 0)$.
S druge strane, ukoliko se radi o balansiranoj funkciji f, tada je $(\star) = 0$ (ima tačno $\frac{2^n}{2}$ članova $\frac{-1}{2^n}$ i tačno $\frac{2^n}{2}$ članova $\frac{1}{2^n}$ pa se oni pokrate).Što znači da, ukoliko je f balansirana, Amela nikada neće moći izmjeriti stanje $0^{\otimes n} = |0, 0, \ldots, 0\rangle$ na kraju, tj. na barem jednom mjestu se mora pojaviti jedinica. Na osnovu ovih razmatranja zaključujemo da ukoliko na kraju u Amelinom n-kubitnom registru budu sve nule, radi se o kontantnoj funkciji f, dok se u suprotnom radi o balansiranoj funkciji f.

4.4 Shor-ov algoritam

Shor-ov algoritam nalazi proste faktore nekog broja u polinomialnom vremenu. Nećemo vršiti detaljnu interpretaciju ovog algoritma iz razloga što je prekomplikovana. Ono sto možemo reći jeste da je njegova kompleksnost jednaka $O((log(n))^3)$, gdje je n cijeli broj čiji se prosti faktori traže, kao i da broj kvantnih kola potrebnih za izvršavanje algoritma raste povećavanjem broja n brzinom $(log(n))^3$. Ovaj algoritam predstavlja ozbiljan problem za RSA kriptosistem koji je uveliko zastupljen u svijetu, iz tog razloga su se počeli razvijati kriptosistemi sigurni i na kvantnom nivou.

5 Zanimljivosti i prednosti QC-a

5.1 No-Cloning teorem

Za razliku od klasičnog bita, kubit je nemoguće kopirati. Ova tvrdnja se naziva No-cloning theorem i dokazuje se na sljedeći način.
Pretpostavimo želimo da kopiramo stanje $|\phi\rangle$ i da postoji određena transformacija(kvantno kolo) U koje izvršava kopiranje. Neka U ima dva ulaza na koja ćemo dovesti redom kubite stanja $|\phi\rangle$ i $|s\rangle$ (može biti i samo jedan ulaz stanja $|phi\rangle$) i dva izlaza koja na kraju trebaju da daju redom stanja $|\phi\rangle$ i $|\phi\rangle$. Tj. imamo

$$U\left(|\phi\rangle|s\rangle\right) = |\phi\rangle|\phi\rangle$$

Analogno za stanje $|\psi\rangle$ vrijedi

$$U\left(|\psi\rangle|s\rangle\right) = |\psi\rangle|\psi\rangle$$

Uzimajući unutrašnji proizvod posljednje dvije jednakosti dobijamo

$$\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^2$$

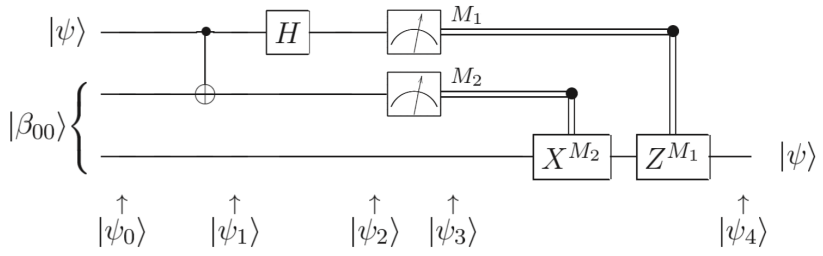
odakle slijedi da je $\langle\phi|\psi\rangle = 0 \vee \langle\phi|\psi\rangle = 1$ tj. vektori $|\phi\rangle$ i $|\psi\rangle$ su ili jednaki ili ortogonalni. Dakle ovakva transformacija U može klonirati samo ortogonalna stanja, dok je generalno kloniranje nemoguće.

5.2 EPR paradoks

U podpoglavljima 2.2 i 2.3 smo se upoznali sa preplitanjem i Bell-ovim stanjima. Kao što smo već rekli, mjerenje jednog od kubita u Bell-ovom stanju direktno utiče na stanje drugog kubita, pa čak i ako je udaljenost između ta dva kubita velika. Postavlja se pitanje, kako drugi kubit zna da je došlo do mjerenja prvog kubita. Ovo pitanje je, ugrubo, EPR paradoks. Jedno od objašnjenja je to da ova dva kubita komuniciraju ma gdje se nalazili, međutim ovo objašnjenje se kosi sa specijalnom teorijom relativiteta koja tvrdi da ne postoji brzina veća od brzine svjetlosti. Drugo objašnjenje koristi činjenicu da se ni jedan kvantni sistem ne može nalaziti u identičnom kvantnom stanju, te da svaki kvantni sistem posjeduje informaciju o svim ostalim kvantnim stanjima u univerzumu, što bi značilo da svaki elektron čuva ogromnu količinu informacije. Treće objašnjenje tvrdi da je Kvantna Mehanika čudna i da stvari treba prihvatiti onakve kakve jesu bez pokušaja razumijevanja istih klasičnim alatima logike.

5.3 Kvantna teleportacija

Kvantna teleportacija je problem razmjene stanja kubita, tačnije, problem slanja stanja kubita sa jednog mjesta na drugo. Zašto se onda ne zove kvantni prenos? Zato što se ne radi o klasičnom prenosu kubita, nego kubit nestaje na jednom mjestu, a rekonstruiše se na drugom (detaljnije u nastavku). Posmatrajmo sljedeći problem, Amela i Ulfrik su nekada generisali EPR par i razišli se tako da je svako uzeo po jedan kubit iz EPR para, sada Amela želi da pošalje neko drugo stanje $|\psi\rangle$ Ulfriku. Algoritam slanja se sastoji u sljedećem, Amela najprije vrši interakciju (vidjećemo kakvu) kubita stanja $|\psi\rangle$ sa kubitom iz EPR para, zatim mjeri ova dva kubita te rezultate šalje Ulfriku. Zanimljivo je to da Ulfrik na osnovu ovih rezultata i svog kubita iz EPR para može rekonstruisati stanje $|\psi\rangle$. Algoritam koji izvršava navedeno



Slika 12: Kvantna teleportacija

je dat na slici 12 i kao i kod Deutch-Jozsa algoritma, ovaj algoritam ćemo analizirati analizirajući redom stanja $|\psi_i\rangle$ sa slike. Dakle, $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ je stanje koje želimo teleportirati, a $|\beta_{00}\rangle$ je stanje EPR para kojeg su generisali Amela i Ulfrik. Primijetimo odmah da je

$$|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = \frac{\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|00\rangle + |11\rangle\right)}{\sqrt{2}}$$

Nakon primjene CNOT kola na stanje $|\psi\rangle$ i Amelin kubit iz EPR para stanja $|\psi_0\rangle$ dobijamo stanje

$$|\psi_1\rangle = \frac{\alpha|0\rangle\left(|00\rangle + |11\rangle\right) + \beta|1\rangle\left(|10\rangle + |01\rangle\right)}{\sqrt{2}}$$

Amela zatim šalje stanje $|\psi\rangle$ kroz Hadamardovo kolo i dobijamo stanje

$$|\psi_2\rangle = \frac{\alpha\left(|0\rangle + |1\rangle\right)\left(|00\rangle + |11\rangle\right) + \beta\left(|0\rangle - |1\rangle\right)\left(|10\rangle + |01\rangle\right)}{2} =$$

$$= \frac{\alpha\left(|000\rangle + |011\rangle + |100\rangle + |111\rangle\right) + \beta\left(|010\rangle + |001\rangle - |110\rangle - |101\rangle\right)}{2} =$$

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

Iz posljednjeg stanja zaključujemo da od mjerenja Amelinih kubita zavisi stanje Ulfrikovog kubita. Pa tako imamo

$$|\psi_3\rangle = \begin{cases} \alpha|0\rangle + \beta|1\rangle & M_1 = 0 \ \wedge \ M_2 = 0 \\ \alpha|1\rangle + \beta|0\rangle & M_1 = 0 \ \wedge \ M_2 = 1 \\ \alpha|0\rangle - \beta|1\rangle & M_1 = 1 \ \wedge \ M_2 = 0 \\ \alpha|1\rangle - \beta|0\rangle & M_1 = 1 \ \wedge \ M_2 = 1 \end{cases}$$

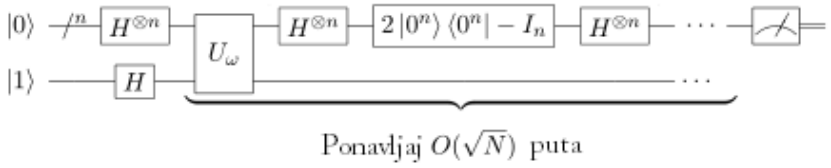
Dalje, Ulfriku su potrebni rezultati Amelinog mjerenja da bi rekonstruisao stanje $|\psi\rangle$. (Upravo ovaj razlog, tj. potreba da se prenesu dva klasična bita klasičnim prenosom, spriječava prenos informacije brže od brzine svjetlosti.) Primijetimo dalje da ukoliko Amela izmjeri stanja kao $M_1 = 0 \wedge M_2 = 0$ tada Ulfrik ne mora ništa da radi, jer već ima stanje $|\psi\rangle$, zatim, ako je $M_1 = 0 \wedge M_2 = 1$, tada ulfrik treba negirati svoje stanje da bi dobio stanje $|psi\rangle$, tj. primijeniti X kolo na svoje stanje, dalje, ako je $M_1 = 1 \wedge M_2 = 0$, tada Ulfrik treba promijeniti predznak koeficijenta β, tj. primijeniti kolo Z na njega (forma X i Z kola data na slici 5) i na kraju ukoliko je $M_1 = 1 \wedge M_2 = 1$, Ulfrik treba primijeniti i X i Z kolo na svoje stanje i rekontruisati će stanje $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. Upravo ovo je i urađeno na slici 12, kola X i Z imaju redom kontrolne bite M_1 i M_2, dakle kolo će biti pušteno u rad ako i samo ako je njegov kontrolni bit jednak 1. Dakle na kraju Ulfrik posjeduje stanje $|\psi\rangle$.
Međutim, postavlja se pitanje, zar mi upravo nismo klonirali stanje $|\psi\rangle$ i time narušili No-Cloning teorem? Nismo. Nakon što Amela izmjeri svoje kubite, ona zauvijek gubi stanje $|\psi\rangle$, tako da nikada nemamo situaciju da u nekom trenutku imamo dva identična stanja $|\psi\rangle$.

5.4 Kvantna Turingova Mašina

Kvantna Turingova Mašina, analogno klasičnoj Turingovoj Mašini,se koristi za ispitivanje moći izračunljivosti kvantnih računara, jer svaki izračunljivi kvantni algoritam je izračunljiv i na kvantnoj Turingovoj mašini. Treba pomenuti još i to da se radi i na implementaciji kvantnih algoritama u klasične modele izračunljivosti, ali još uvijek nije oborena Church-Turingova teza.

5.5 Kvantni algoritam pretraživanja

Kvantni algoritam pretraživanja ili Groover-ov algoritam je kvantni algoritam koji pretražuje nesortirani niz i njegova komleksnost je $O(\sqrt{n})$, za razliku od klasičnog cija je kompleksnost $O(n)$. Groover-ov algoritam ćemo samo navesti (Slika 13) i nećemo analizirati. Njegovu analizu ostavljamo čitaocu za korisnu vježbu.



Slika 13: Groover-ov algoritam

6 Zaključak

Vidjeli smo da je, iako još u razvoju, kvantno izračunavanje veoma moćno. Možemo zaključiti da smo dobili jednu veoma zanimljivu i sočnu oblast za istraživanje. Nažalost, kao i sve druge nauke, razvoj QC-a ne ide brzo i to najviše zbog otežane manipulacije kvantnim sistema. Vrlo je teško održati dugo na životu neki izolovani kvantni sistem kojim manipulišemo. Iz ovog razloga brzina razvoja QC-a je nepredvidljiva. Tako da možemo očekivati prvi kvantni računar nakon nekoliko godina, desetljeća ili čak stoljeća. U svakom slučaju, pred fizičarima, matematičarima i inžinjerima stoji jedna lijepa i veoma interesantna nauka koja ima veliki kapacitet da bude jedna od onih nauka koje mijenjaju svijet.

7 Literatura

-Quantum Computation and Quantum Information - Michael A. Nielsen, Isaac L. Chuang

-Wikipedia