OSNOVE KVANTNEGA RAČUNALNIŠTVA, 1. DEL

MATIJA PRETNAR

Fakulteta za matematiko in fiziko
Univerza v Ljubljani

Math. Subj. Class. (2010): 68Q12, 81P68

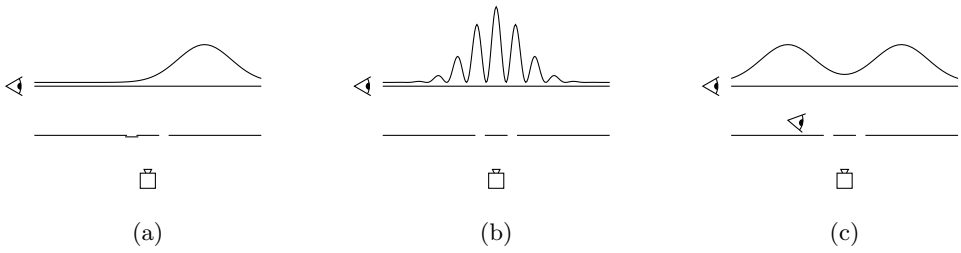
Kvantno računalništvo skuša z izkoriščanjem kvantnih pojavov, kakršni sta superpozicija in prepletenost, učinkoviteje reševati računsko zahtevne probleme. V prvem delu si ogledamo postulate kvantne mehanike ter kvantno teleportacijo.

THE BASICS OF QUANTUM COMPUTING, PART 1

Quantum computing uses quantum phenomena such as superposition and entanglement in order to efficiently solve computationally hard problems. The first part describes the quantum mechanics postulates and quantum teleportation.

Uvod

V svetu majhnih delcev ne veljajo več pravila klasične Newtonove mehanike, kot smo jih navajeni, temveč nastopijo nenavadna pravila kvantne mehanike. Po teh pravilih se delci obnašajo tako, kot bi bili na več koncih hkrati, vendar le toliko časa, dokler jim ne izmerimo položaja. Ko pa ga enkrat izmerimo, se obnašajo le v skladu z rezultatom meritve. Primer takega vedenja vidimo v poskusu z dvojno režo (slika 1), v katerem streljamo fotone proti zaslonu z dvema ozkima režama, za zaslonom pa postavimo senzor, ki meri, kam so prileteli fotoni, ki jim je uspelo priti mimo.



Slika 1. Količina fotonov, ki jo izmerimo pri poskusu z dvojno režo ob (a) eni odprti reži, (b) obeh odprtih režah in (c) obeh odprtih režah in dodatnem senzorju, ki meri, kje je potoval foton.

Če eno od rež zapremo, največ zadetkov po pričakovanjih izmerimo za drugo režo. Če odpremo obe reži, bi tako pričakovali dva vrhova, za vsako

režo po enega. V resnici pa dobimo interferenčni vzorec. Lahko bi si ga poskušali razložiti s tem, da fotoni na svoji poti motijo drug drugega, vendar dobimo tako sliko tudi, če poskrbimo, da naenkrat streljamo samo en foton. Torej obe možni poti, po katerih bi lahko potoval foton, motita druga drugo. Še več: če postavimo dodaten senzor, s katerim poskušamo ugotoviti, skozi katero režo je šel foton, interferenca izgine, za zaslonom pa izmerimo vrhova, ki smo ju pričakovali prej.

Kvantno računalništvo poskuša te neobičajne kvantne pojave izkoristiti za učinkovitejše računanje. S kvantnim računalništvom je pričel znani fizik Richard Feynman, ko je leta 1981 v svojem govoru [1] predlagal, da bi za simulacijo kvantnih sistemov uporabljali računalnike, ki sami temeljijo na kvantnih načelih. Kvantne sisteme bi sicer lahko simulirali tudi z običajnimi računalniki, a le, če bi bili ti sistemi precej majhni, saj že za sistem z nekaj sto delci potrebujemo računalnik z več pomnilnika, kot je delcev v vesolju.

Kvantno računalništvo se je hitro razširilo še na druga področja, največji razmah pa je doživelo leta 1994, ko je Peter Shor predstavil učinkovit algoritem za razcep na praštevila [3]. Ta algoritem si bomo v drugem delu tudi natančneje ogledali. Ker šifriranje RSA, ki je danes eno najpogosteje uporabljanih, temelji ravno na težavnosti takega razcepa, bi s kvantnimi računalniki postalo neuporabno. No, do sedaj so zaradi tehničnih omejitev leta 2001 razcepili število 15, leta 2012 pa so uspeh ponovili še na številu 21, zato kvantni računalniki za zdaj še ne pomenijo resne grožnje. Za takrat, ko jo bodo, pa odgovore že pripravlja kvantna kriptografija.

Zakaj bi se lotili kvantnega računalništva? Če pogledamo zadnjih 70 let razvoja računalništva, vidimo, da zlata doba kvantnega računalništva šele prihaja in da bo zanimivo biti zraven. Pa tudi če zaradi nepremostljivih tehničnih omejitev ta doba nikoli ne pride, je kvantno računalništvo zanimivo že zato, ker ponuja elegantno formulacijo fizikalno sicer zapletenih kvantnih pojavov.

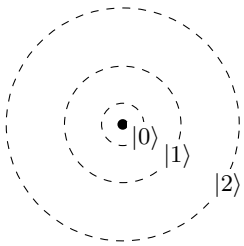
V prvem delu bomo to formulacijo predstavili ter si v njej ogledali enega bolj popularnih kvantnih pojavov: kvantno teleportacijo. V drugem delu pa se bomo osredotočili na kvantne algoritme. Vsem, ki jih kvantno računalništvo še posebej zanima, predlagam v branje [2].

Postulati kvantne mehanike

Prostor stanj kvantnega sistema

Vzemimo kvantni sistem s k ločenimi stanji, ki jih imenujemo *bazna* in jih običajno označimo z $|0\rangle, |1\rangle, \ldots, |k-1\rangle$. Poskus z dvojno režo je primer

kvantnega sistema z dvema baznima stanjema, ki ustrezata potema skozi prvo in drugo režo. Pogosto uporabljan primer kvantnega sistema je tudi vodikov atom (slika 2), v katerem je elektron bodisi v osnovnem bodisi v enem od vzbujenih stanj. Energija atoma namreč ne more biti poljubna, temveč lahko zasede le točno določene vrednosti — pravimo, da je *kvantizirana*, od koder tudi izvira ime kvantne mehanike.



Slika 2. Shema vodikovega atoma, v katerem je elektron v osnovnem stanju $|0\rangle$ ali pa v enem od vzbujenih stanj. S tem da omejimo največjo možno energijo elektrona, omejimo tudi število stanj, ki jih lahko zaseda.

Kvantna mehanika nam govori, da je sistem, ki je lahko v danih stanjih, lahko tudi v poljubni *superpoziciji* teh stanj, torej v več stanjih hkrati. Tako superpozicijo opišemo kar z linearno kombinacijo vseh stanj, v katerih se nahaja sistem.

Postulat 1 (načelo superpozicije). *Stanje kvantnega sistema opišemo z enotskim vektorjem v* prostoru stanj $\mathcal{H}$*, ki je kompleksni vektorski prostor s skalarnim produktom, v katerem bazna stanja* $|0\rangle, |1\rangle, \ldots, |k-1\rangle$ *tvorijo ortonormirano bazo.*

Skalarni produkt vektorjev $|\varphi\rangle$ in $|\psi\rangle$ v prostoru $\mathcal{H}$ pišemo kot $\langle\varphi|\psi\rangle$, od koder izhaja tudi *Diracov zapis*, v katerem vektorje pišemo kot $|\varphi\rangle$, kar beremo kot *ket* φ. Če v skalarnem produktu prvi vektor držimo pri miru, drugega pa spreminjamo, dobimo *dual* vektorja $|\varphi\rangle$. To je linearni funkcional, ki vektor $|\psi\rangle$ slika v kompleksno število $\langle\varphi|\psi\rangle$. Dual zato označimo z $\langle\varphi|$, kar beremo kot *bra* φ.

Stanje sistema z baznimi stanji $|0\rangle, |1\rangle, \ldots, |k-1\rangle$ torej opišemo z vektorjem

$$|\varphi\rangle = \sum_{j=0}^{k-1} \alpha_j |j\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle + \cdots + \alpha_{k-1}|k-1\rangle,$$

pri čemer so koeficienti α_j, ki jim pravimo *amplitude*, kompleksna števila, za katera velja $\sum_{j=0}^{k-1} |\alpha_j|^2 = 1$. Absolutne vrednosti amplitud nam povedo

delež posameznega stanja v superpoziciji, argumenti (torej kompleksni koti) amplitud, ki jih imenujemo *faze*, pa vplivajo na interferenco med stanji, na primer tisto iz poskusa z dvojno režo.

Včasih namesto Diracovega uporabljamo tudi običajni zapis, pri čemer za standardno bazo zaporedoma vzamemo bazna stanja $|0\rangle, |1\rangle, \ldots, |k-1\rangle$. Zgoraj omenjena stanja tako predstavimo z naslednjimi stolpci:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} \quad \cdots \quad |k-1\rangle = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix} \qquad |\varphi\rangle = \sum_{j=0}^{k-1} \alpha_j |j\rangle = \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{k-1} \end{bmatrix}.$$

Spomnimo se, da je za $|\psi\rangle = \sum_{j=0}^{k-1} \beta_j |j\rangle$ skalarni produkt $\langle\varphi|\psi\rangle$ enak $\sum_{j=0}^{k-1} \overline{\alpha}_j \beta_j$, zato dual $\langle\varphi|$ predstavimo z vrstico $\begin{bmatrix} \overline{\alpha}_0 & \overline{\alpha}_1 & \cdots & \overline{\alpha}_{k-1} \end{bmatrix}$.

Najbolj preprost kvantni sistem je *kubit*. To je sistem z dvema ločenima stanjema $|0\rangle$ in $|1\rangle$. Primer kubita je vodikov atom, v katerem omejimo energijo tako, da lahko elektron doseže le prvo vzbujeno stanje. Tedaj je po načelu superpozicije poljubno stanje kubita oblike $\alpha_0|0\rangle + \alpha_1|1\rangle$, kjer velja $|\alpha_0|^2 + |\alpha_1|^2 = 1$.

Stvari postanejo zares zanimive, ko si ogledamo več kubitov hkrati. Ker ima kubit bazni stanji $|0\rangle$ in $|1\rangle$, lahko v združenem sistemu dveh kubitov ločimo štiri bazna stanja, ki jih označimo z $|00\rangle$, $|01\rangle$, $|10\rangle$ in $|11\rangle$. Toda po načelu superpozicije je tak sistem lahko tudi v superpoziciji teh stanj, torej v enotskem vektorju oblike

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle.$$

Za opis take strukture je kot nalašč *tenzorski produkt*. Za prostora $\mathcal{H}$ in $\mathcal{H}'$ je namreč njun produkt $\mathcal{H} \otimes \mathcal{H}'$ vektorski prostor, sestavljen najprej iz vseh parov vektorjev $|\varphi\rangle \in \mathcal{H}$ in $|\psi\rangle \in \mathcal{H}'$, ki jih pišemo kot $|\varphi\rangle \otimes |\psi\rangle$, nato pa še iz vseh linearnih kombinacij takih parov. Pri tem je operacija $\otimes$ bilinearna, torej velja:

$$\begin{aligned} \lambda|\varphi\rangle \otimes |\psi\rangle &= |\varphi\rangle \otimes \lambda|\psi\rangle = \lambda(|\varphi\rangle \otimes |\psi\rangle) \\ (|\varphi\rangle + |\varphi'\rangle) \otimes |\psi\rangle &= |\varphi\rangle \otimes |\psi\rangle + |\varphi'\rangle \otimes |\psi\rangle \\ |\varphi\rangle \otimes (|\psi\rangle + |\psi'\rangle) &= |\varphi\rangle \otimes |\psi\rangle + |\varphi\rangle \otimes |\psi'\rangle. \end{aligned}$$

Par $|\varphi\rangle \otimes |\psi\rangle$ dostikrat napišemo tudi kot $|\varphi\rangle|\psi\rangle$ ali celo kot $|\varphi\,\psi\rangle$, kar smo storili tudi zgoraj pri baznih stanjih sistema dveh kubitov.

Preverimo lahko, da s predpisom

$$\langle \varphi_1\, \psi_1 | \varphi_2\, \psi_2 \rangle = \langle \varphi_1 | \varphi_2 \rangle \cdot \langle \psi_1 | \psi_2 \rangle$$

dobro definiramo skalarni produkt na prostoru $\mathcal{H} \otimes \mathcal{H}'$. V tem primeru tudi hitro vidimo, da pari baznih vektorjev tvorijo ortonormirano bazo tenzorskega produkta, to pa ustreza naši prejšnji opazki, da so bazna stanja združenega sistema kar vsi možni pari baznih stanj posameznih sistemov.

Postulat 2 (združitev kvantnih sistemov). *Prostor stanj sistema, ki ga dobimo z združitvijo sistemov s prostoroma stanj $\mathcal{H}$ in $\mathcal{H}'$, je enak tenzorskemu produktu $\mathcal{H} \otimes \mathcal{H}'$. Če je prvi sistem v stanju $|\varphi\rangle$ in drugi sistem v stanju $|\psi\rangle$, je združeni sistem v stanju $|\varphi\rangle \otimes |\psi\rangle$.*

Če imamo dva kubita, od katerih je prvi v stanju $|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, drugi pa v stanju $|\psi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$, lahko nanju gledamo kot na en sam kvantni sistem, ki je v stanju

$$\begin{aligned} |\varphi\rangle \otimes |\psi\rangle &= (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle) \\ &= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle. \end{aligned} \tag{1}$$

Stanjem, ki se dajo zapisati kot $|\varphi\rangle \otimes |\psi\rangle$, pravimo *produktna*.

Z ustreznimi spremembami lahko sistem spravimo v stanje, ki ni produktno. Takim stanjem pravimo *prepletena*. Posebno znan primer prepletenega stanja je *Bellovo stanje* $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Iz primerjave amplitud s splošnim produktnim stanjem (1) vidimo, da Bellovo stanje ne more biti produktno, saj bi sicer veljalo $0 = (\alpha_0\beta_1)(\alpha_1\beta_0) = (\alpha_0\beta_0)(\alpha_1\beta_1) = \frac{1}{2}$.

Razvoj kvantnega sistema

Kvantni sistem smo tako v celoti opisali, zdaj pa se lahko posvetimo njegovemu obnašanju. Z večino delujočih kvantnih računalnikov upravljamo prek zunanjih vplivov, na primer z vklopom magnetnega polja ali z obsevanjem s fotoni. S tem spremenimo interakcije v sistemu, s čimer dosežemo, da se sistem začne razvijati proti želenemu stanju. Natančneje obnašanje sistema opišemo s Schrödingerjevo enačbo, s katero pa se tokrat ne bomo ukvarjali, saj bo za naše potrebe dovolj že njena posledica, ki jo bomo privzeli za postulat.

Postulat 3 (unitarnost razvoja). *Za vsak razvoj izoliranega kvantnega sistema obstaja unitarna preslikava U, ki začetno stanje $|\varphi_0\rangle$ slika v stanje po spremembi $U|\varphi_0\rangle$.*

Spomnimo se, da je unitarna preslikava U linearna preslikava z inverzom U^{-1}, enakim adjungirani preslikavi U^*, torej velja $U^*U = UU^* = I$. Če preslikavo U predstavimo z matriko, je adjungirana preslikava U^* enaka

$$\begin{bmatrix} \alpha_{00} & \alpha_{01} & \cdots & \alpha_{0,k-1} \\ \alpha_{10} & \alpha_{11} & \cdots & \alpha_{1,k-1} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k-1,0} & \alpha_{k-1,1} & \cdots & \alpha_{k-1,k-1} \end{bmatrix}^* = \begin{bmatrix} \overline{\alpha}_{00} & \overline{\alpha}_{10} & \cdots & \overline{\alpha}_{k-1,0} \\ \overline{\alpha}_{01} & \overline{\alpha}_{11} & \cdots & \overline{\alpha}_{k-1,1} \\ \vdots & \vdots & \ddots & \vdots \\ \overline{\alpha}_{0,k-1} & \overline{\alpha}_{1,k-1} & \cdots & \overline{\alpha}_{k-1,k-1} \end{bmatrix}.$$

Matriko torej transponiramo, vse njene elemente pa konjugiramo.

Iskane unitarne preslikave po navadi predstavimo s *kvantnim vezjem*, ki je sestavljeno iz enostavnejših unitarnih preslikav. Tem pravimo tudi *kvantna vrata*, saj imajo podobno vlogo kot logična vrata (in, ali, negacija, ...) v klasičnem računalništvu.

Najpogosteje uporabljana enokubitna kvantna vrata so *Paulijeva vrata* X, Y in Z ter *Hadamardova vrata* H. Ker se vrata na splošni superpoziciji obnašajo linearno, je dovolj, da podamo njihovo vedenje na baznih stanjih:

$$\begin{aligned} X|0\rangle &= |1\rangle \quad & Y|0\rangle &= i|1\rangle \quad & Z|0\rangle &= |0\rangle \quad & H|0\rangle &= \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle \\ X|1\rangle &= |0\rangle \quad & Y|1\rangle &= -i|0\rangle \quad & Z|1\rangle &= -|1\rangle \quad & H|1\rangle &= \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle. \end{aligned}$$

Paulijevim vratom X pravimo tudi negacija, saj obrnejo bazni stanji. Stanji $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ in $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$, ki sta rezultat uporabe Hadamardovih vrat H, pa označimo s $|+\rangle$ in z $|-\rangle$.

Z matrikami bi zgornja vrata lahko zapisali kot:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad H = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix}.$$

Za vajo lahko preverimo, da so vse naštete preslikave ne le unitarne, temveč tudi same sebi inverz.

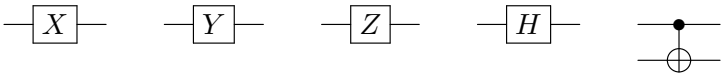
Na dveh kubitih so najpomembnejša vrata *kontrolirane negacije* CNOT, ki negirajo *ciljni* kubit, kadar je stanje *kontrolnega* kubita enako $|1\rangle$. Običajno je prvi kubit kontrolni, drugi pa ciljni. Velja torej

$$\text{CNOT}|00\rangle = |00\rangle \quad \text{CNOT}|01\rangle = |01\rangle \quad \text{CNOT}|10\rangle = |11\rangle \quad \text{CNOT}|11\rangle = |10\rangle$$

oziroma

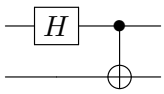
$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Zgornja kvantna vrata v vezjih predstavimo z naslednjimi simboli:



Pri vratih CNOT nam • označuje kontrolni, $\oplus$ pa ciljni kubit.

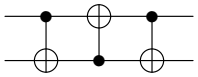
Primer kvantnega vezja je vezje



(2)

s katerim iz začetnega stanja $|00\rangle$ najprej s Hadamardovimi vrati naredimo stanje $(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle)|0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$, s kontrolirano negacijo pa še $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$, kar je ravno Bellovo stanje.

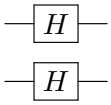
Drug enostaven in uporaben primer je vezje



(3)

s katerim zamenjamo stanji prvega in drugega kubita. Na primer stanje $|10\rangle$ s prvimi vrati spremenimo v $|11\rangle$, z drugimi, ki so ravno tako kontrolirana negacija, le z zamenjanima kontrolnim in ciljnim kubitom, pa v $|01\rangle$. Tretja vrata stanje ohranijo na $|01\rangle$, saj je stanje kontrolnega kubita enako $|0\rangle$. Podobno velja za vsa bazna stanja in po linearnosti posledično za vsako superpozicijo. V posebnem primeru vezje stanje $|\varphi\rangle|\psi\rangle$ spremeni v $|\psi\rangle|\varphi\rangle$.

Tretje vezje, v katerem kubita sploh ne vplivata drug na drugega, pa je *Walsh-Hadamardovo vezje*



(4)

ki ga označimo tudi s $H \otimes H$, saj velja $(H \otimes H)(\varphi \otimes \psi) = H\varphi \otimes H\psi$. Če $H \otimes H$ uporabimo na baznem stanju $|00\rangle$, dobimo

$$\begin{aligned}(H \otimes H)|00\rangle &= H|0\rangle \otimes H|0\rangle \\ &= (\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle) \otimes (\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle) \\ &= \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)\end{aligned}$$

oziroma superpozicijo vseh baznih stanj. Podobno lahko sestavimo tudi vezje $H^{\otimes n}$, ki je namesto iz dveh sestavljeno iz n vzporednih Hadamardovih vrat. To vezje bazno stanje $|00\cdots0\rangle = |0^n\rangle$ slika v superpozicijo

$$\frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle,$$

kjer $\sum_{x\in\{0,1\}^n}$ oziroma dostikrat tudi kar $\sum_x$ označuje vsoto po vseh 2^n kombinacijah n bitov, torej po vseh baznih stanjih.

Na teh treh primerih lahko opazimo pomembno lastnost vseh kvantnih vezij. Ker vsa vezja predstavljajo unitarne preslikave, se število kubitov v kvantnem vezju ohranja. V tem se kvantna vezja razlikujejo od klasičnih, pri katerih se število vhodov in izhodov lahko razlikuje: logična vrata AND recimo iz dveh vhodnih bitov izračunajo en izhodni bit.

Zapletenejšim vezjem se bomo še posvetili, a že zdaj vidimo, kje se skriva osnovna ideja kvantnega računalništva. Klasični računalnik dobi neki vhod in iz njega izračuna želeni rezultat. Če želimo izračunati rezultat še za kak drug vhod, moramo postopek ponoviti. Pri kvantnemu računalniku bi z vezjem (4) najprej ustvarili superpozicijo vseh možnih vhodov, nato pa bi iz njih s primernim kvantnim vezjem hkrati izračunali superpozicijo vseh možnih rezultatov.

Meritve kvantnih stanj

Žal je ta ideja preveč optimistična, saj moramo, če želimo prebrati rezultate, stanje pomeriti. Težava z meritvami kvantnih sistemov pa je v tem, da rezultati niso natančno določeni, poleg tega pa z meritvijo sistem *kolabira* v izmerjeno stanje, s čimer celotno superpozicijo izgubimo.

Postulat 4 (načelo meritve). *Če merimo sistem v stanju* $\sum_{j=0}^{k-1}\alpha_j|j\rangle$, *z verjetnostjo* $|\alpha_j|^2$ *izmerimo stanje* $|j\rangle$, *po meritvi pa je stanje sistema enako* $|j\rangle$.

Na primer, če merimo sistem v stanju $\frac{\sqrt{3}}{2}|0\rangle-\frac{i}{2}|1\rangle$, bomo v treh četrtinah primerov izmerili stanje $|0\rangle$, v preostali četrtini pa bomo izmerili stanje $|1\rangle$. V obeh primerih pa bo stanje kolabiralo v izmerjeno stanje, zato bomo ob vseh nadaljnjih meritvah dobili enak odgovor.

Kaj pa, če bi pred meritvijo superpozicijo prenesli na neki drug kubit in si s tem naredili varnostno kopijo? Potrebovali bi torej vezje U, ki bi sprejelo kubit v stanju $|\varphi\rangle$ ter „prazen“ kubit v stanju $|0\rangle$, vrnilo pa bi dva kubita, vsakega v stanju $|\varphi\rangle$. To žal ne gre.

Izrek 1 (izrek o nepodvajanju). *Ne obstaja unitarna preslikava* U, *za katero za vsako stanje enega kubita* $|\varphi\rangle$ *velja* $U(|\varphi\rangle\otimes|0\rangle)=|\varphi\rangle\otimes|\varphi\rangle$.

Dokaz. Ker bi preslikava U podvajala vsa stanja, bi morala podvojiti tudi stanji $|0\rangle$ in $|1\rangle$. Torej bi veljalo

$$U|00\rangle=|00\rangle \quad \text{in} \quad U|10\rangle=|11\rangle.$$

Tedaj pa bi za splošno stanje $|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ zaradi linearnosti U veljalo

$$U(|\varphi\rangle \otimes |0\rangle) = U(\alpha_0|00\rangle + \alpha_1|10\rangle) = \alpha_0|00\rangle + \alpha_1|11\rangle,$$

kar pa ni isto kot stanje $|\varphi\rangle \otimes |\varphi\rangle$, ki smo ga želeli. ∎

Ta rezultat je izjemno pomemben v kvantni kriptografiji, ker izloči kakršnokoli prisluškovanje. Če bi prisluškovalec namreč želel, da sogovornika ne bi opazila njegovih dejanj, bi moral njuno sporočilo podvojiti, preden bi ga izmeril.

V združenem sistemu meritev poteka podobno. Torej, če je sistem dveh kubitov v stanju $\frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$, bomo v četrtini primerov izmerili stanje $|00\rangle$, v četrtini stanje $|10\rangle$, v polovici pa stanje $|11\rangle$.

Kaj pa, če pomerimo le en kubit? V tem primeru stanje preostalih kubitov ni natanko določeno, mora pa biti skladno z meritvijo. To najenostavneje vidimo, če združeno stanje zapišemo v obliki, v kateri vsakemu stanju prvega kubita pridružimo superpozicijo vseh skladnih stanj drugega kubita:

$$\tfrac{1}{2}|00\rangle + \tfrac{1}{2}|10\rangle - \tfrac{1}{\sqrt{2}}|11\rangle = \tfrac{1}{2}|0\rangle \otimes |0\rangle + \tfrac{\sqrt{3}}{2}|1\rangle \otimes \left(\sqrt{\tfrac{1}{3}}|0\rangle - \sqrt{\tfrac{2}{3}}|1\rangle\right).$$

Če pomerimo stanje prvega kubita, bomo v četrtini primerov tako izmerili stanje $|0\rangle$, po meritvi pa bo stanje enako $|00\rangle$, saj stanji $|10\rangle$ in $|11\rangle$ nista skladni z meritvijo. V treh četrtinah primerov pa izmerimo stanje $|1\rangle$, po meritvi pa je stanje združenega sistema enako $\sqrt{\frac{1}{3}}|10\rangle - \sqrt{\frac{2}{3}}|11\rangle$.

Postulat 5 (meritev v združenem sistemu). *Če je združen sistem v stanju* $\sum_{j=0}^{k-1} \alpha_j|j\rangle \otimes |\psi_j\rangle$*, kjer so vsi vektorji* $|\psi_j\rangle$ *enotski, potem pri meritvi prvega sistema z verjetnostjo* $|\alpha_j|^2$ *izmerimo stanje* $|j\rangle$*, po meritvi pa je stanje združenega sistema enako* $|j\rangle \otimes |\psi_j\rangle$*.*

Sistem v produktnem stanju $|\varphi\rangle \otimes |\psi\rangle$, kjer je $|\varphi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$, lahko zapišemo kot

$$(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |\psi\rangle = \alpha_0|0\rangle|\psi\rangle + \alpha_1|1\rangle|\psi\rangle,$$

zato posamezne meritve prvega sistema dobimo z enako verjetnostjo, kot bi jih v ločenem sistemu, v obeh primerih pa drugi sistem ostane v stanju $|\psi\rangle$. V stanjih, ki niso produktna, tako kot v prejšnjem primeru, pa lahko z

meritvijo enega kubita določimo tudi stanje drugega. Prav zato taka stanja imenujemo prepletena.

Recimo, da meritev izvedemo na Bellovem stanju $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Vidimo, da je po kakršnikoli meritvi enega od kubitov tudi drugi kubit v enakem stanju kot prvi. Če pazimo, da ni zunanjih vplivov, se prepletenost ohrani tudi takrat, ko kubita fizično ločimo in odnesemo daleč narazen. In tudi sedaj bo v trenutku, ko pomerimo prvi kubit, drugi v natanko istem stanju. Videti je, da smo s tem kršili načela teorije relativnosti, saj informacija ne more potovati hitreje od svetlobe. To imenujemo tudi Einstein-Podolski-Rosenov oziroma EPR paradoks. Poenostavljeno ga lahko razrešimo, če vidimo, da nimamo vpliva na rezultat meritve prvega kubita, zato same prepletenosti v resnici ne moremo uporabiti za prenos informacije.

Kvantna teleportacija

A vseeno si s prepletenostjo lahko pomagamo pri prenosu stanja prek velikih razdalj, kjer nam vezje (3) ne koristi. Ena možnost je, da kubit v želenem stanju fizično odnesemo na cilj, vendar lahko stanje zaradi motenj med prenosom izgubimo. Drugo možnost ponuja *kvantna teleportacija*.

Stanja kubita, ki ga označimo z A, bomo prenesli s pomočjo vnaprej pripravljenega prepletenega para kubitov v Bellovem stanju $\frac{1}{\sqrt{2}}|00\rangle+\frac{1}{\sqrt{2}}|11\rangle$. Ta dva kubita, ki ju označimo z B in C, ločimo in odnesemo na konca, med katerima želimo prenesti stanje. V tem primeru nas motnje med prenosom ne skrbijo, saj lahko z vezjem (2) enostavno ustvarimo cel kup prepletenih parov. Začnemo torej v stanju

$$(\alpha_0|0\rangle+\alpha_1|1\rangle)\otimes(\tfrac{1}{\sqrt{2}}|00\rangle+\tfrac{1}{\sqrt{2}}|11\rangle) = \tfrac{\alpha_0}{\sqrt{2}}|000\rangle+\tfrac{\alpha_0}{\sqrt{2}}|011\rangle+\tfrac{\alpha_1}{\sqrt{2}}|100\rangle+\tfrac{\alpha_1}{\sqrt{2}}|111\rangle,$$

končati pa želimo tako, da bo kubit C v stanju $\alpha_0|0\rangle + \alpha_1|1\rangle$.

Groba ideja je, da kubit B dodatno prepletemo s kubitom A, nato pa z meritvami prvo prepletenost porušimo in ob tem stanje prenesemo na kubit C. To storimo tako, da uporabimo vrata CNOT na kubitih A in B, s čimer sistem spravimo v stanje

$$\tfrac{\alpha_0}{\sqrt{2}}|000\rangle + \tfrac{\alpha_0}{\sqrt{2}}|011\rangle + \tfrac{\alpha_1}{\sqrt{2}}|110\rangle + \tfrac{\alpha_1}{\sqrt{2}}|101\rangle,$$

nato pa kubit B pomerimo:

1. Če izmerimo, da je B v stanju $|0\rangle$, stanje kolabira v $\alpha_0|000\rangle + \alpha_1|101\rangle$. Tako nam je uspelo med kubitoma A in C ustvariti ustrezno prepletenost, ki se je znebimo tako, da kubit A "razpršimo" s Hadamardovimi

vrati H in s tem sistem spravimo v stanje

$$\tfrac{\alpha_0}{\sqrt{2}}|000\rangle + \tfrac{\alpha_0}{\sqrt{2}}|100\rangle + \tfrac{\alpha_1}{\sqrt{2}}|001\rangle - \tfrac{\alpha_1}{\sqrt{2}}|101\rangle.$$

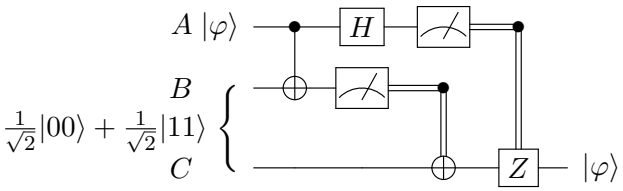
Na koncu pomerimo še A. Če izmerimo $|0\rangle$, sistem kolabira v stanje

$$\alpha_0|000\rangle + \alpha_1|001\rangle = |00\rangle \otimes (\alpha_0|0\rangle + \alpha_1|1\rangle),$$

kar je točno to, kar smo želeli. Če pa izmerimo $|1\rangle$, sistem podobno kolabira v stanje $|10\rangle \otimes (\alpha_0|0\rangle - \alpha_1|1\rangle)$, kar lahko z uporabo vrat Z na kubitu C spet spravimo v iskano stanje.

2. Če pa izmerimo, da je B v stanju $|1\rangle$, ravnamo podobno, le da kubit C poprej še negiramo.

Celotno teleportacijo lahko predstavimo s shemo:



V tej shemi simbola merilnika označujeta meritvi kubitov A in B. Odvisno od rezultata teh meritev na kubitu C po potrebi uporabimo še negacijo in fazna vrata Z. To pogojno uporabo označimo tako, kot jo pri vratih CNOT, le da za kontrolo namesto kvantnega uporabimo klasični bit, kar poudarimo z dvojno žico.

Za kvantno teleportacijo moramo torej med obema koncema prenesti še informacijo o meritvi kubitov A in B. Ker je ta informacija klasična, jo prenesemo brez večjih težav, na primer po elektronski pošti. Zaradi tega klasičnega prenosa smo prav tako omejeni s hitrostjo svetlobe, zato do EPR paradoksa v tem primeru ne pride. Tudi izreka o nepodvajanju nismo kršili, saj smo med prenosom z meritvami uničili stanje kubita A.

LITERATURA

[1] R. P. Feynman, *Simulating Physics with Computers*, Int. J. Theor. Phys. **21** (1982), 467–488.

[2] P. Kaye, R. Laflamme in M. Mosca, *An Introduction to Quantum Computing*, Oxford University Press, Inc., New York, 2007.

[3] P. W. Shor, *Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM J. Sci. Statist. Comput. **26** (1997), 1484–1509.