Kvantalgoritmid

Helger Lipmaa

Küberneetika AS; http://www.cyber.ee

helger@cyber.ee; http://home.cyber.ee/helger

8. november 1998. a.

Esmalt ette kantud 1998. a. Noorte Füüsikute Sügiskoolis.

Klassikalised arvutusmudelid

Church-Turingi printsiip: kõik, mis on arvutatav, on arvutatav kasutades klassikalist Turingi masinat.

Täiendus: Klassikalised arvutusmudelid (Turingi masin, λ-arvutus, Posti masin ...) on võimelised teineteist emuleerima polünomiaalses ajas: mis on efektiivne arvelaual, on efektiivne Cray'l.

Seega saab *ülesandeid* keerukusklassidesse jagada vastavalt sellele, kui efektiivsed algoritmid nende ülesannete jaoks on *põhimõtteliselt* võimalikud (näiteks) Turingi masinatel.

Keerukusklassi **P** (determineeritud polünomiaalses ajas lahenduvad ülesanded) kuuluvaid ülesandeid samastatakse tavaliselt "lihtsate" ehk "efektiivselt lahenduvate" ülesannetega.

Näiteid

1. Kahe arvu korrutamine on lihtne (keerukusklassist **P**).

2. Algarvutest on lihtne ülesanne, kui kasutada randomiseeritud Turingi masinat (keerukusklassist **BPP**).

3. Arvu faktoriseerimine on (arvatavasti) raske. Parim teadaolev faktoriseerimisalgoritm (arvkorpuste sõel) töötab ajas $\exp(c\sqrt{(\log n)^{1/3}(\log\log n)^{2/3}})$. Ülesannete 1, 2 ja 3 suhtelisel keerukusel põhineb RSA krüptosüsteem.

4. Tõestatavalt salajase ühisteadmuse tekkimine kahe osapoole vahele ilma eelnevat ühist salajast informatsiooni omamata on *põhimõtteliselt* võimatu klassikalistes arvutusmudelites.

Kvantarvutid. Motivatsioon.

Feynman, 1982: teatud kvantsüsteeme ei ole põhimõtteliselt võimalik simuleerida klassikaliste arvutusmudelite abil ilma tööaja eksponentsiaalse kasvuta.

Moore'i seadus, kiirus: 2020. aastaks kulub ühe biti salvestamiseks üks aatom. Sellisel miniatuursuse astmel on *vaja* arvesse võtta kvanteffekte.

Seega, kvantmehaanika efektide arvestamine ei pruugi olla mitte ainult kasulik, vaid muutuda ka paratamatuks.

Motivatsioon II: energia

Moore'i seadus, energiakulu: 2020. aastaks kahaneb loogikaoperatsioonile (ntks ühe biti kustutamisele) kuluv energiavajadus suuruseni $1\ kT$, kus k on Boltzmanni konstant ning T on temperatuur.

Landaueri printsiip: informatsiooni kustutamisega kaasneb energiakulu. Informatsiooni kustutavad ka kõik mittepööratavad arvutused (näiteks loogiline AND kahe biti vahel)

Lahendus: pööratav arvutusmudel, kus kõik arvutustehted on pööratavad ning kus ei kulu tänu sellele arvutamisele energiat.

"Kvantarvutid on pööratavad arvutid".

Olekuruum I

Kvantsüsteemi olekuruum on kirjeldatav lainefunktsioonide Hilberti ruumina. Kvantarvutuste jaoks on vaja vaid *lõplikumõõtmelisi* vektorruume üle korpuse $\mathbb{C}$. Sellistel olekuruumidel leiduvad ortonormeeritud baasid, mida tähistatakse Dirac'i bra/ket notatsiooni kasutades järgmiselt:

- $|x\rangle$ (*ket*) on veeruvektor; suuruste $|x\rangle$ abil kirjeldatakse tavaliselt kvantolekuid.

- $\langle x|$ (*bra*) on vektori $|x\rangle$ transponeeritud kaasvektor.

Kahemõõtmelise $\mathbb{C}$ vektorruumi ortonormeeritud baasi $\left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$ võib tähistada kui $\{|0\rangle, |1\rangle\}$.

Olekuruum II

Vektorruumi suvaline element $|x\rangle$ avaldub baasivektorite $|0\rangle$ ja $|1\rangle$ lineaarse kombinatsioonina $a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$, kus $a, b \in \mathbb{C}$ ning $a^2 + b^2 = 1$. Selles tähistuses on $\langle x|y\rangle$ võrdne vektorite $\langle x|$ ning $|y\rangle$ skalaar- ehk *sisekorrutisega*, $|x\rangle\langle y|$ on aga nende vektorite *väliskorrutis*: 2×2 unitaarmaatriks, mida võib standardsel viisil vaadelda lineaarkujutusena.

Näiteks

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

on unitaarmaatriks, mis teisendab baasvektori $|0\rangle$ vektoriks $|1\rangle$ ning vektori $|1\rangle$ vektoriks $|0\rangle$.

Kvantbitt

Kvantbitt (*qubit*) on normeeritud vektor kahemõõtmelises vektorruumis üle korpuse $\mathbb{C}$, mille jaoks on fikseeritud konkreetne baas $\{|0\rangle, |1\rangle\}$. Baasolekud $|0\rangle$ ja $|1\rangle$ vastavad klassikalistele bitiväärtustele 0 ja 1.

Näide: Kvantbitid $|0\rangle$ ning $|1\rangle$ võivad vastata footoni horisontaalsele ning vertikaalsele polarisatsioonile ($|\rightarrow\rangle$, $|\uparrow\rangle$), kuid ka nende kahe polarisatsiooni suvalistele ortonormeeritud lineaarkombinatsioonidele, näiteks vektoritele

$$|\nearrow\rangle := \frac{1}{\sqrt{2}}(|\rightarrow\rangle + |\uparrow\rangle)$$

ning

$$|\nwarrow\rangle := \frac{1}{\sqrt{2}}(|\rightarrow\rangle - |\uparrow\rangle) \ .$$

NB! Baas peab olema fikseeritud enne arvutuste algust.

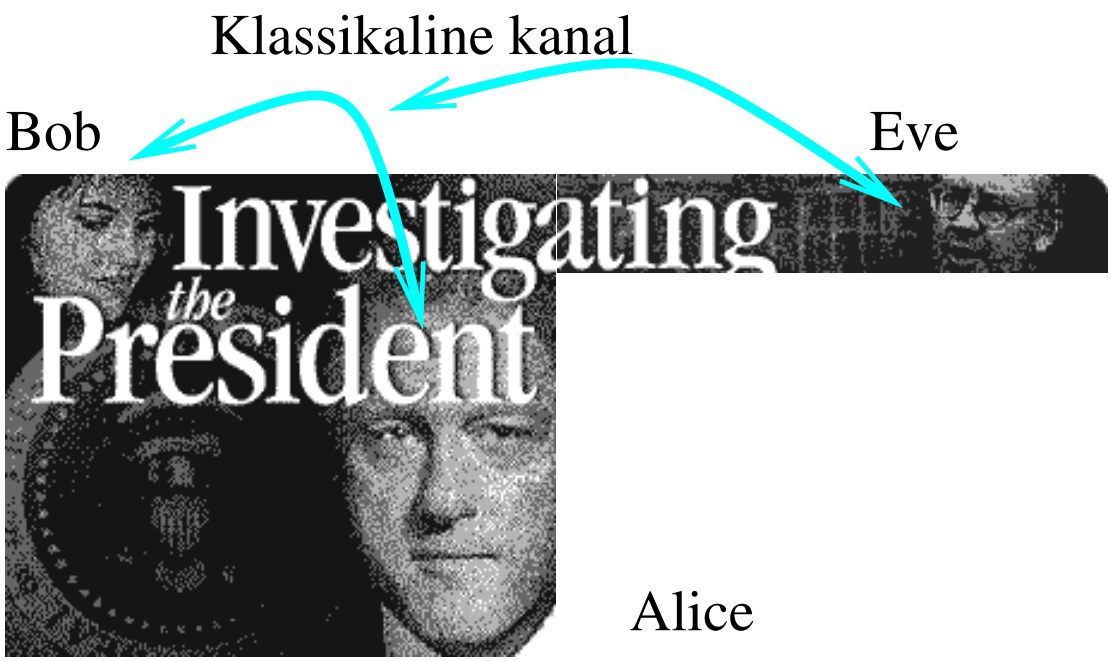
Superpositsioon

Erinevalt klassikalistest bittidest võivad kvantbitid olla superpositsioonis, st kvantbiti iga väärtus kujul $a|0\rangle + b|1\rangle$, $a^2 + b^2 = 1$, on lubatud. Superpositsiooni *mõõtmisel* fikseeritud baasi $\{|0\rangle, |1\rangle\}$ järgi, saadakse tõenäosusega a^2 tulemuseks vektor $|0\rangle$ ning tõenäosusega b^2 tulemuseks vektor $|1\rangle$.

Ühes kvantbitis on võimalik kodeerida vaid ühte klassikalist bitti, st informatsiooniteooria vaatenurgast sisaldub ühes kvantbitis täpselt sama palju informatsiooni kui ühes klassikalises bitis.

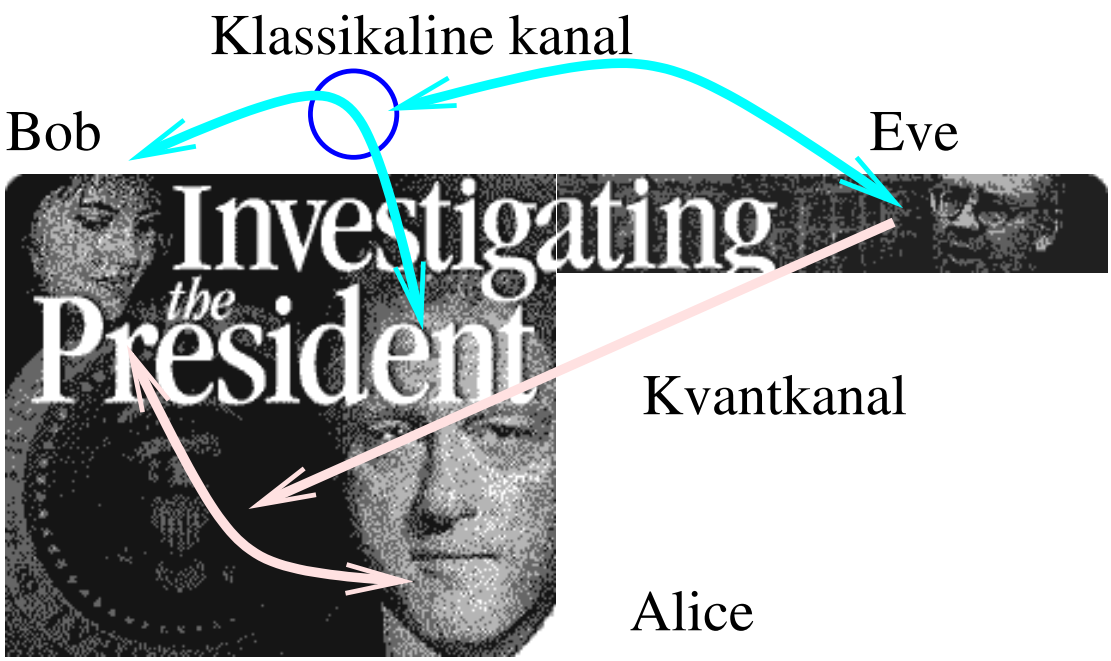
Tõestus: esimest mõõtmist kollapseerub kvantbitt üheks kahest vektorist, järelikult on mõõtmise tulemus väärt täpselt ühte bitti. Järgmistel mõõtmistel saadakse aga täpselt sama tulemus, mis esimesel.

Klassikaline võtmekehtestus



Eesmärgiks on genereerida salajane võti, mida edasises suhtluses kasutada andmete krüptimiseks. Võimatu, kui ei toetu arvutuslikele eeldustele (ntks et faktoriseerimine on raske).

Kvantvõtmekehtestus



Eesmärk sama. Salajane võtmekehtestus on nüüd võimalik, kasutades kvantkanalit.

Kvantvõtmekehtestuse protokoll

Protokoll. Alice genereerib juhuslikult n bitti ning saadab need kvantkanalil Bobile, valides iga biti kodeerimiseks juhuslikult ühe kahest baasist $\mathcal{B}(0) := \{|\uparrow\rangle, |\rightarrow\rangle\}$ ja $\mathcal{B}(1) := \{|\nwarrow\rangle, |\nearrow\rangle\}$. Kodeerigu footoni polarisatsioonid $|\uparrow\rangle$ ning $|\nwarrow\rangle$ bitti 0 ning polarisatsioonid $|\rightarrow\rangle$ ning $|\nearrow\rangle$ bitti 1.

Iga footoni saabumisel valib Bob juhuslikult kas baasi $\mathcal{B}(0)$ või $\mathcal{B}(1)$, mille järgi seda footonit mõõta. Pärast bittide edastamist avalikustavad Alice ning Bob oma baasidevalikud.

Kui n-nda baasi valik ühtis (tõenäosus $\frac{1}{2}$), võetakse n-is bitt kasutusele, vastasel juhul mitte.

Kvantvõtmekehtestuse protokoll, II

Kui Eve soovib lugeda protokolli i-ndat bitti, peab ta seda tegema mingi baasi $\mathcal{B}(E_i)$ järgi. Kuna Alice valis baasid juhuslikult, on Eve'i jaoks parim strateegia ka ise baasid juhuslikult valida. Sellisel juhul valib Eve õige baasi tõenäosusega $\frac{1}{2}$ ning saab teada biti tegeliku väärtuse.

Tõenäosusega $\frac{1}{2}$ valib Eve vale baasi ning seega on mõõtmise tulemuseks juhuslik suurus hulgast $\{|0\rangle, |1\rangle\}$. Vale baasi järgi mõõtmine muudab footoni ning seega on "nuhitud" footonil erinev polarisatsioon kui mittenuhitud footonil.

Lisaprotokollide ("salastuse võimendamine") abil saavad Alice ja Bob hiljem klassikalist kanalit pidi informatsiooni vahetades ligikaudse hinnangu sellele, kas ja kuipalju bitte on keegi vahepeal pealt kuulanud.

Näide. Alice soovib edastada võtit $K := 011101010001$. Selleks genereerib ta juhuslikult teise bitijada A (olgu ntks $A := 110010110011$), mis määrab ära baasid. Seega edastab Alice 12 footonit:

K	0	1	1	1	0	1	0	1	0	0	0	1
A	1	1	0	0	1	0	1	1	0	0	1	1
Footon	$\lvert\nwarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\nearrow\rangle$

Saades footonid kätte, genereerib Bob bitijada $B := 111000011010$). Mõõtes i-ndat footonit baasi $\mathcal{B}(B_i)$ järgi, saab Bob järgmised tulemused:

Footon	$\lvert\nwarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\rightarrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\nearrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\uparrow\rangle$	$\lvert\nwarrow\rangle$	$\lvert\nearrow\rangle$
B	1	1	1	0	0	0	0	1	1	0	1	0
K	0	1	?	1	?	1	?	1	?	0	0	?

Küsimärkidega tähistatud väljades võib olla võrdse tõenäosusega nii 0 kui 1. Seejärel avalikustavad Alice ja Bob oma valitud baasid ning loevad ühiseks võtmeks $K' := 0111100$.

Kvantregistrid

Klassikalistes arvutusmudelites (ja klassikalises füüsikas) moodustab n osakesest koosnev süsteem, mille iga osake on vektor kahemõõtmelises vektorruumis, kokku $2n$-mõõtmelise vektorruumi: $\dim(U \times V) = \dim U + \dim V$. Kvantsüsteemis on saadava vektorruumi dimensioon ent 2^n:

$$\dim(U \otimes V) = \dim U \cdot \dim V \ .$$

Nii on näiteks kolmest kvantbitist koosneva süsteemi baasiks

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle \ ,$$

kus kokkuleppeliselt tähistatakse $|xy\rangle := |x\rangle \otimes |y\rangle$.

Kvantparallelism

Paralleelsuse eksponentsiaalne kasv tuleneb sellest, et kõik $n+m$-mõõtmelised vektorid ei avaldu n- ja m-mõõtmeliste vektorite tensorkorrutisena. Tõestame, et olek $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ ei avaldu kahe vektori tensorkorrutisena.

Tõestus. Väide on, et ei leidu selliseid kompleksarve a_1, a_2, b_1, b_2, nii et $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Lahti kirjutades, $(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) = a_1a_2|00\rangle + a_1b_2|01\rangle + a_2b_1|10\rangle + a_2b_2|11\rangle$. Kui kehtiks võrdus $a_1b_2 = 0$, siis ka $a_1a_2 = 0$ või $b_1b_2 = 0$.

Selliseid olekuid nimetatakse *sasiolekuks* (ka sidusolek, *entangled state*); ainult logaritmiline osa kõikidest olekutest ei ole sasiolekud; neil olekutel ei ole klassikalises füüsikas analoogi ning just nende tõttu tekib kvantparallelism. Eelnevast tuleneb ka see, et isegi väikese kvantsüsteemi simuleerimine klassikalistel arvutitel nõuab eksponentsiaalse arvu olekute jälgimist.

Kvantarvutite potentsiaali põhjuseks on kvantolekute evolutsiooni kasutamine arvutusmehhanismina.

Mõõtmine

Kvantsüsteemi parameetri(te) mõõtmise tulemuseks on süsteemi normaalprojektsioon olekuruumi alamruumi, mis on ühilduv mõõdetud väärtustega (“Von Neumanni projektsioonihüpotees”). Normaalprojektsioon — pärast mõõtmist saadud süsteemi olekuvektor on endiselt üks.

Näide. Suvaline kahest kvantbitist koosneva süsteemi olek väljendub kui summa $a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$, kus $a^2 + b^2 + c^2 + d^2 = 1$. Kui esimest kvantbitti mõõta baasi $\{|0\rangle, |1\rangle\}$ järgi, on tulemuseks väärtus $|0\rangle$ tõenäosusega $a^2 + b^2$. Seejärel projekteerub olek alamruumi, mis on ühilduv mõõdetud tulemusega ($|0\rangle$), uus olekuvektor normeeritakse ning seega saadakse tulemuseks uus olek

$$\frac{1}{\sqrt{a^2 + b^2}}(a|00\rangle + b|11\rangle) \ .$$

Einstein-Podelsky-Rosen paradoks

Saab tõestada, et osakesed ei ole sasiolekus kui ühe osakese mõõtmine ei mõjuta teist osakest (sasioleku teine, ekvivalentne definitsioon). Nii näiteks on olek $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ sasiolek, kuna enne teise osakese mõõtmist on esimese osakese mõõtmise tulemuseks tõenäosusega $\frac{1}{2}$ vektor $|0\rangle$. *Pärast* teise osakese mõõtmist on aga esimese osakese mõõtmise tulemuseks $|0\rangle$ või $|1\rangle$ tõenäosusega 1 sõltuvalt sellest, kas teise osakese mõõtmisel saadi tulemuseks $|0\rangle$ või $|1\rangle$.

Anname Alice'ile ning Bobile ühe osakese sasiosakeste paarist, ning laseme neil liikuda teineteisest kuitahes kaugele (näiteks mõned valgusaastad). Seejärel teostab Alice oma osakesel mõõtmise. Kohe seejärel mõõdab Bob oma osakest ning saab vastuseks sama tulemuse, mis Alice. Tundub, et tegu on paradoksiga (informatsiooni liikumine valgusest kiiremini). On siiski võimalik näidata, et Alice'il ja Bobil ei ole nii võimalik valgusest kiiremini informatsiooni vahetada. /* Füüsikas paradoks: lokaalsuse printsiip, kvantmehaanika interpretatsioonid */

Unitaarteisendused

Eelnevalt vaatlesime, kuidas muutub kvantsüsteem selle mõõtmisel; mittemõõdetud kvantsüsteem areneb vastavalt Schrödingeri võrrandile, olekud muutuvad olekuteks, säilitades ortogonaalsust.

Vektorruumis üle korpuse $\mathbb{C}$ on ortogonaalsust säilitavateks lineaarteisendusteks unitaarteisendused. Lineaarteisendused on esitatavad maatriksitena. Maatriks M on *unitaarne* (vastab unitaarteisendusele) kui $MM^* = 1$, kus M^* on maatriksi M konjugeeritud maatriksi transponeeritud maatriks. Kvantolekute ruumi unitaarsed teisendused vastavad (üksüheselt) legaalsetele kvantteisendustele.

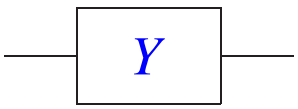
- Unitaarteisendusi saab esitada kompleksse vektorruumi rotatsioonidena.

- Kõik kvantteisendused on pööratavad.

Kvantlülid (*Quantum Gates*)

Samasusteisendus	I	$\|0\rangle\langle 0\| + \|1\rangle\langle 1\|$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
Eitus	X	$\|0\rangle\langle 1\| + \|1\rangle\langle 0\|$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Faasinihe	Z	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
Faasinihke eitus	$Y(=Z\cdot X)$	$\|0\rangle\langle 0\| - \|1\rangle\langle 1\|$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

Ühebitiseid kvantoperatsioone kujutatakse graafiliselt operatsiooni nimega märgendatud kastina:

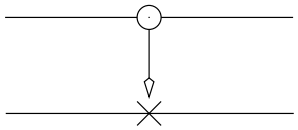


Juhitav eitus

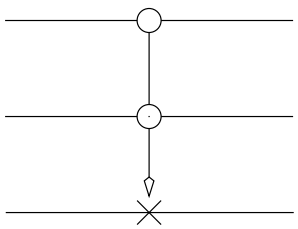
Olgu

$$CNOT := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} .$$

Kontrollige, et $CNOT$ ei avaldu kahe ühebitise teisenduse tensorkorrutisena! Teisendust $CNOT$ tähistatakse graafiliselt tavaliselt järgmiselt:



Joonisel on kujutatud kahe kvantbitine lüli, kus esimese biti väärtusest sõltuvalt teise biti väärtus muutub või mitte. Lüliti *juhitav-juhitav-eitus* (Toffoli lüli), kus kolmanda biti väärtus muutub vaid siis kui esimese kahe biti väärtused on mõlemad 1, kujutatakse järgmiselt:



Walsh-Hadamard'i teisendus

Hadamard'i teisendus:

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

Kui rakendada Hadamard'i teisendust ühele kvantbitile $|0\rangle$, saab tulemuseks superpositsiooni $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Kui rakendada teisendus H paralleelselt n erinevale kvantbitile, on tulemuseks süsteemi kõigi 2^n võimaliku oleku superpositsioon:

$$W|00\ldots0\rangle = (H \otimes H \otimes \cdots \otimes H)|00\ldots0\rangle$$
$$= \frac{1}{\sqrt{2^n}}(|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes \cdots \otimes (|0\rangle + |1\rangle)$$
$$= \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \ .$$

Kloonimise võimatus

Tõestame, et kvantinformatsiooni ei saa kloonida. Olgu U — klooniv unitaarteisendus, st $U(|x0\rangle) = |xx\rangle$ iga kvantoleku x jaoks. Olgu a ning b kaks ortogonaalset kvantolekut. Siis $U(|a0\rangle) = |aa\rangle$, $U(|b0\rangle) = |bb\rangle$. Olgu $c := \frac{1}{\sqrt{2}}(|a\rangle + |b\rangle)$. Lineaarsusest

$$U(|c0\rangle = \frac{1}{\sqrt{2}}(U(|a0\rangle) + U(|b0\rangle)) = \frac{1}{\sqrt{2}}(|aa\rangle + |bb\rangle) \ ,$$

kuid samas

$$U(|c0\rangle = |cc\rangle = \frac{1}{2}(|aa\rangle + |ab\rangle + |ba\rangle + |bb\rangle) \ .$$

Vastuolu.

Teadaoleva kvantoleku kloonimine on võimalik, tundmatu kvantoleku kloonimine on võimatu. Sh on võimatu tundmatust kvantolekust $a|0\rangle + b|1\rangle$ alustades lõpetada olekutes $a|0\ldots0\rangle + b|1\ldots1\rangle$ või $(a|0\rangle + b|1\rangle) \otimes \cdots \otimes (a|0\rangle + b|1\rangle)$.

Tihe kodeerimine

Tihe kodeerimine (*dense coding*) kasutab ühte kvantbitti koos EPR-paariga kahe klassikalise biti kodeerimiseks ning edastamiseks. Kuna EPR-paari võib edastada millal iganes, kulub kahe klassikalise biti edastamiseks vaid üks tavaline bitt. Üllatav (vt lk 9), kuid teostatav! Enne kodeerimist antakse Alice'ile esimene ning Bobile teine sasiosake EPR-paarist $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.

Alice: Alice'il on kaks bitti ehk suurus vahemikus $0 \ldots 3$. Sõltuvalt sellest suurusest rakendab Alice ühe teisendustest $\{I, X, Y, Z\}$ oma osakesele. EPR-paari ühe osakese teisendusega kaasneb samasusteisendus teisel osakesel. EPR-paari uued olekud on toodud järgmises tabelis.

Väärtus	Teisendus	EPR-paari uus olek
0	$\psi_0 = (I \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
1	$\psi_1 = (X \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
2	$\psi_2 = (Y \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$
3	$\psi_3 = (Z \otimes I)\psi_0$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$

Alice saadab enda osakese (1 kvantbitt) Bobile.

Tihe kodeerimine, II

Bob: Bob rakendab $CNOT$ lüli EPR-paari kahele kvantbitile.

Algolek	Juhitav eitus	1. bitt	2. bitt
$\psi_0 = \frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle + \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
$\psi_1 = \frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|1\rangle$
$\psi_2 = \frac{1}{\sqrt{2}}(-\|10\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(-\|11\rangle + \|01\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|1\rangle$
$\psi_3 = \frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$	$\frac{1}{\sqrt{2}}(\|00\rangle - \|10\rangle)$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|0\rangle$

Seejärel mõõdab Bob teise kvantbiti väärtuse (kvantolek ei kollapseeru!). Kui mõõtmise tulemus on $|0\rangle$, siis kodeeritud väärtus oli 0 või 3, kui mõõtmise tulemus on $|1\rangle$, siis kodeeritud väärtus oli 1 või 2.

Tihe kodeerimine, III

Lõpuks rakendab Bob esimesele osakesele teisenduse H.

Algolek	1. bitt	H(1. bitt)
ψ_0	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
ψ_1	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$	$\|0\rangle$
ψ_2	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|1\rangle$
ψ_3	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|1\rangle$

Nüüd mõõdab Bob esimese biti väärtuse ning suudab eristada väärtusi 0 ja 3, 1 ja 2.

Teleportimine

Vastand tihedale kodeerimisele — ühe kvantbiti edastamiseks kasutatakse kaks klassikalist bitti. Üllatav, kuna võimaldab teisaldada tundmatu kvantbiti väärtust (kloonimise võimatus, lk 22). On realiseeritud eksperimentaalselt.

Enne protokolli algust on Alice'il esimene ning Bobil teine osake EPR-paarist. Alice soovib edastada kvantbitti

$$\phi := a|0\rangle + b|1\rangle \quad ,$$

kasutades klassikalisi kanaleid.

Teleportimine, II

Kvantsüsteemi algolek on

$$\begin{aligned}\phi \otimes \psi_0 &= \frac{1}{\sqrt{2}}(a|0\rangle \otimes (|00\rangle + |11\rangle) + b|1\rangle \otimes (|00\rangle + |11\rangle)) \\ &= \frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) \ ,\end{aligned}$$

millest Alice kontrollib esimest ning teist bitti, Bob kontrollib kolmandat bitti.

Teleportimine, III

Alice rakendab algolekule järjestikku teisendusi $CNOT \otimes I$ ja $H \otimes I \otimes I$ (ehk tiheda kodeerimise dekodeerimissammu):

$$
\begin{aligned}
&(H \otimes I \otimes I)(CNOT \otimes I)(\phi \otimes \psi_0) \\
&\quad = (H \otimes I \otimes I)(CNOT \otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) \\
&\quad = (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle) \\
&\quad = \frac{1}{2}(a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\
&\quad = \frac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|1\rangle)) \ .
\end{aligned}
$$

Teleportimine, IV

Alice mõõdab esimesed kaks kvantbitti, saades ühe neljast väärtusest $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$ tõenäosusega $\frac{1}{4}$. Vastavalt Alice'i mõõtmise tulemustele projekteerub Bobi kvantbitt üheks neljast väärtusest $a|0\rangle + b|1\rangle$, $a|1\rangle + b|0\rangle$, $a|0\rangle - b|1\rangle$ või $a|1\rangle - b|1\rangle$. Alice saadab oma mõõtmise tulemused kui kaks klassikalist bitti Bobile.

NB! Oma kvantbitte mõõtes muutis Alice taastamatult kvantbiti ϕ väärtust, mistõttu biti teleporteerimine Bobile ei räägi vastu kloonimise mittevõimalikkusele.

Bob: Kui Bob saab Alice'ilt kaks bitti, saab ta teada millises seoses on EPR-paari teise osakese (mis on Bobi käes) olek Alice'i kvantbiti algolekuga. Algoleku saab Bob kätte kui rakendab tollele osakesele õige teisenduse (vastab tiheda kodeerimise kodeerimissammule):

Bitid	Olek	Dekodeerimine
00	$a\|0\rangle + b\|1\rangle$	I
01	$a\|1\rangle + b\|0\rangle$	X
10	$a\|0\rangle - b\|1\rangle$	Y
11	$a\|1\rangle - b\|0\rangle$	Z

NOT ning AND tehete simuleerimine

Tuletagem esmalt meelde, et kõik kvantoleku teisendused peavad olema pööratavad. Kuigi klassikaline NOT tehe on pööratav, pole seda AND ega NAND tehted. Seega pole sugugi selge, et kvantteisenduste abil saab läbi viia kõik klassikalised arvutused. Seega tuleb esmalt täielikult kirjeldada pööratavad lülid, mille abil saab kvantarvutil teostada suvalisi klassikalisi arvutusoperatsioone.

Suvalise kahe unitaarteisenduse U ja V korral on unitaarne ka "tingimuslik" teisendus $|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes V$. $CNOT$ teisendust võib defineerida järgmiselt: $CNOT := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$.

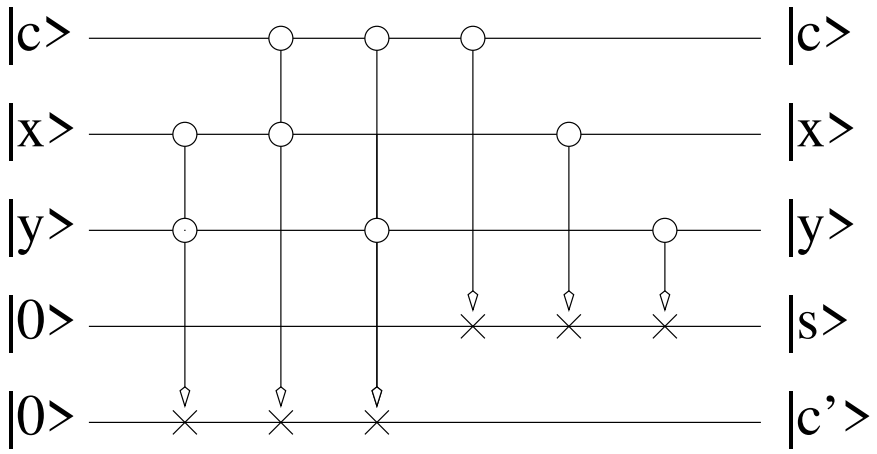
Kolmebitine *juhitav-juhitav-eitus* (ehk *Toffoli lüli*):

$$T := |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes CNOT \quad .$$

Toffoli lülist piisab kõigi Boole'i funktsioonide konstrueerimiseks, kuna Toffoli lüliga saab arvutada NOT-i ja AND-i: $T|1,1,x\rangle := |1,1,\neg x\rangle$ ning $T|x,y,0\rangle := |x,y,x \wedge y\rangle$.

Näide: liitja

Järgmisel joonisel on toodud ühebitist liitjat implementeeriv kvantskeem, mis kasutab Toffoli lüli ning juhitavat eitust. Siin on x ning y liidetavad bitid, c on sisendülekanne, s on saadav summa (mod 2) ning c' on väljundülekanne.



Fredkini lüli

Olgu $S := |00\rangle\langle 00| + |01\rangle\langle 10| + |10\rangle\langle 01| + |11\rangle\langle 11|$ — *vahetusoperaator*. *Fredkini lüli* on "juhitav vahetus":

$$F := |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes S \ .$$

Kuna

$$F|x,0,1\rangle = |x,x,\neg x\rangle \ ,$$
$$F|x,y,1\rangle = |x,y \vee x,y \vee \neg x\rangle$$

ja

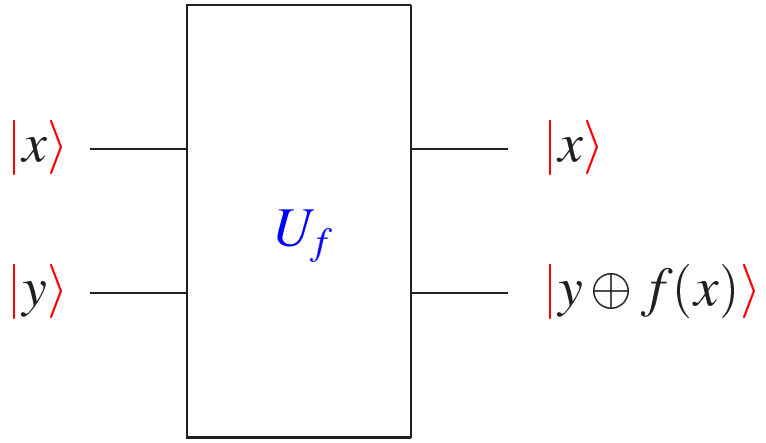
$$F|x,0,y\rangle = |x,y \wedge x,y \wedge \neg x\rangle \ ,$$

piisab ka Fredkini lülist Boole'i funktsioonide arvutamiseks.

Seega pööratavate kvantlülide abil saab arvutada suvalist klassikaliselt arvutatavat funktsiooni, järelikult on võimalik konstrueerida universaalne kvant-Turingi masin.

Kvantskeemid

Kuna suvalist klassikalist funktsiooni f saab arvutada kvantarvutil, võime eeldada seda funktsiooni arvutava *kvantskeemi* $U_f : |x,y\rangle \to |x, y \oplus f(x)\rangle$ olemasolu.



Sedasi defineeritud skeem U_f on unitaarne suvalise funktsiooni f jaoks. Väärtuse $f(x)$ leidmiseks rakendame skeemi U_f sisendile $|x, 0\rangle$.

Kuna $f(x) \oplus f(x) = 0$, siis $U_f U_f = I$ ning seega U_f on pööratav.

Kvantarvutused kvantarvutil

Kuigi T- ja F-lülid on täielikud klassikaliste arvutuste jaoks, ei ole vaid nende abil võimalik teostada suvalisi kvantarvutusi. Viimaste jaoks tuleb primitiivsete skeemide hulka lisada ka ühebitised rotatsioonid. On tõestatud, et kõik kvantarvutused saab sooritada, kui $CNOT$ skeemile lisada järgnevad rotatsioonid ning faasinihketeisendused iga α jaoks:

$$\begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}, \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{-i\alpha} \end{pmatrix}, \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}.$$

Kvantparallelismi kasutamine

Rakendame skeemi U_f sisendite superpositsioonile. Kuna U_f on lineaarteisendus, "rakendub" U_f simultaanselt kõigile superpositsioonis olevatele sisenditele. Seetõttu on võimalik välja arvutada funktsiooni f väärtused kõikvõimalikel sisenditel, rakendades skeemi U_f sisendite superpositsioonile üksainus kord.

Kvantparallelismist kasu lõikamiseks peavad kvantalgoritmid järgima fikseeritud plokkskeemi. Alustatakse n-kvantbitisest olekust $|00\ldots0\rangle$. Algolekule rakendatakse teisendust W, misjärel saadakse olek $W|0\rangle = \frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$. Lineaarsuse tõttu

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

Seega nagu juba teada, tähendab kvantparallelism eksponentsiaalset parallelismi lineaarses ruumis.

Näide

Vaatleme juhtu $f = T$. Superpositsiooni arvutamine:

$$H|0\rangle \otimes H|0\rangle \otimes |0\rangle = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |110\rangle) \ .$$

Saadud olekule Toffoli lüli rakendades saame

$$T(H|0\rangle \otimes H|0\rangle \otimes |0\rangle) = \frac{1}{2}(|000\rangle + |010\rangle + |100\rangle + |111\rangle) \ .$$

Kvantparallelism, III

Saadud tulemust võib vaadata kui funktsiooni tõeväärtuste tabelit ehk kui funktsiooni graafikut. Väärtused x, y ja $x \wedge y$ on seotud sellisel moel, et tulemuse mõõtmine annab teada tõeväärtuste tabeli ühe rea ehk funktsiooni graafiku ühe punkti. Funktsiooni väärtuse mõõtmine projekteerib oleku kõigi selliste sisendväärtuste y superpositsiooni, mil $f(y) = f(x)$.

Kaks tuntumat kvantparallelismi kasutamise meetodit on:

1. Soovitavate tulemuste amplifitseerimine. Teisendada olekut nii, et soovitava tulemuse amplituud suureneks teiste tulemuste amplituudide arvel. N: Groveri algoritm.

2. Leida mõõtmisega väärtuste $f(x)$ ühiseid omadusi, näiteks selle funktsiooni perioodi. N: Shori faktoriseerimisalgoritm.

Deutsch'i algoritm

Probleem. (Musta kastina) antud funktsioonile $f : \{0,1\} \to \{0,1\}$ vastav kvantskeem $U_f : |xy\rangle \to |x, y \oplus f(x)\rangle$, mille tööaeg on 24 tundi. Leida suurus $f(0) \oplus f(1)$ 24 tunni jooksul!

Klassikaliselt võimatu, kuid kvantarvutitel teostatav. Nimelt olgu $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ning $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$,

$$\begin{aligned} U_f|xy\rangle &= U_f\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \\ &= \frac{1}{\sqrt{2}}(|f(0)\rangle + |f(1)\rangle) \otimes \frac{1}{\sqrt{2}}(|f(x)\rangle - |1 \oplus f(x)\rangle) \\ &= \frac{1}{\sqrt{2}}(|f(0)\rangle + |f(1)\rangle) \otimes \frac{1}{\sqrt{2}}(-1)^{f(x)}(|0\rangle - |1\rangle) \quad . \end{aligned}$$

Mõõtes esimest kvantbitti baasi $\{\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$ järgi, saame vastuseks $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ parajasti siis kui $f(0) \neq f(1)$.

Shori faktoriseerimisalgoritm

Kiire faktoriseerimine.

Piiiiiiiiiiiiiiiiiiiik kirjeldus.

Groveri otsialgoritm

Otsing struktureerimata andmebaasis ajas $O(\sqrt{N})$, kus N on andmebaasi suurus. Klassikalisel arvutil: $O(N)$.

Piiiiiiiiiiiiiiiiiiiiik kirjeldus.