Kvantarvutid

Helger Lipmaa*

17. detsember 1998. a.

Kokkuvõte

Käesolev ülevaade tutvustab konspektiivses vormis viimase kümne aasta jooksul loodud kvantarvutusmudelit. Lühidalt kirjeldatakse kvantinformatsiooniteooria olulisemaid tulemusi ning kahte olulisimat, praktikas väga oluliste probleemide lahendamiseks mõeldud kvantalgoritmi: Groveri otsialgoritmi ning Shori faktoriseerimisalgoritmi. Ülevaade baseerub autori poolt 1998. Noorte Füüsikute Sügiskoolis ning 1998. sügisel toimunud kvantloogika seminaride ajal peetud ettekannete kiledel. Täpsustavaks lugemiseks soovitab autor raamatut [WC97] ning õppematerjali [Pre98]. Eestikeelse lühikese ülevaate võib leida raamatust [HML$^+$98].

1 Sissejuhatus

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.

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

Öeldakse, et (determineeritud, stohhastiline) algoritm töötab (determineeritud, stohhastilises) *polünomiaalses ajas* (DPA, SPA), kui leidub selline polünoom p, nii algoritmi tööks kuluv aeg on väiksem kui $p(|x|)$ suvalise sisendi x jaoks.

Kui ülesande X jaoks leidub determineeritud (stohhastiline) polünomiaalse keerukusega algoritm, öeldakse, et see ülesanne on lahenduv determineeritud (stohhastilises) polünomiaalses ajas ning kirjutatakse $X \in \mathcal{P}$ ($X \in \mathcal{BPP}$).

Keerukusklassi $\mathcal{BPP}$ kuuluvaid ülesandeid samastatakse tavaliselt "lihtsate" ehk "efektiivselt lahenduvate" ülesannetega.

1.1 Näiteid

1. Kahe arvu korrutamine on keerukusklassist $\mathcal{P}$.
2. Algarvutest on keerukusklassist $\mathcal{BPP}$.
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. Salajase ühisteadmise tekkimine kahe osapoole vahele ilma eelnevat ühist salajast informatsiooni omamata on *põhimõtteliselt* võimatu klassikalistes arvutusmudelites.

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

1.2 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.

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: andmete kustutamisega kaasneb energiakulu. Andmeid 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".

2 Olekuruum

Hulka X nimetatakse *meetriliseks ruumiks*, kui igale tema elementide paarile $x, y \in X$ on vastavusse seatud reaalarv $\rho(x, y)$ nii, et on täidetud tingimused:

1. $\rho(x, y) = 0 \iff x = y$;
2. $\rho(x, y) = \rho(y, x)$;
3. $\rho(x, y) \leq \rho(x, z) + \rho(z, y)$.

Arvu $\rho(x, y)$ nimetatakse elementide x ja y vaheliseks *kauguseks*.

Meetrilist ruumi nimetatakse *täielikuks*, kui temas iga Cauchy jada koondub.

Olgu $\mathbb{K} = \mathbb{R}$ või $\mathbb{K} = \mathbb{C}$. Suvalise $a + bi \in \mathbb{C}$ korral $\overline{x} = a - bi$ on arvu x *kaaskompleksarv*. Kui $\mathbb{K} = \mathbb{R}$, siis $\overline{x} = x$, $\forall x$.

Vektorruumi H üle korpuse $\mathbb{K}$ nimetatakse *skalaarkorrutisega ruumiks*, kui igale elemendipaarile $x, y \in H$ on vastavusse seatud kindel arv $\langle x|y\rangle \in \mathbb{K}$, mida nimetatakse elementide x ja y *skalaarkorrutiseks*, nii, et on täidetud järgmised tingimused:

1. kui $\langle x|x\rangle \geq 0$ ja $\langle x|x\rangle = 0$, siis $x = 0$;
2. $\langle x|y\rangle = \overline{\langle y|x\rangle}$;
3. $\langle x_1 + x_2|y\rangle = \langle x_1|y\rangle + \langle x_2|y\rangle$;
4. $\langle \lambda x|y\rangle = \lambda\langle x|y\rangle$.

Definitsioon. Hilberti ruum on täielik skalaarkorrutisega ruum.

Kvantsüsteemi olekuruumi saab kirjeldada lainefunktsioonide Hilberti ruumina. Kvantarvutuste jaoks on vaja vaid *lõplikumõõtmelisi* vektorruume üle korpuse $\mathbb{C}$. Sellistel olekuruumidel leiduvad (Gram-Schmidti ortogonaliseerimisprotsess) 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 $\left\{\binom{1}{0}, \binom{0}{1}\right\}$ võib tähistada kui $\{|0\rangle, |1\rangle\}$.

Vektorruumi suvaline element $|x\rangle$ avaldub baasivektorite $|0\rangle$ ja $|1\rangle$ lineaarse kombinatsioonina $a|0\rangle + b|1\rangle = \binom{a}{b}$, 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

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

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

3 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 $|\rightarrow\rangle$ ja $|\uparrow\rangle$, 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.

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.

4 Võtmekehtestus

Võtmekehtestusprotokolli eesmärgiks on genereerida salajane võti, mida edasises suhtluses kaks osapoolt saaksid kasutada andmete krüptimiseks. Võimatu ilma eelneva ühisteadmuseta (eelnevalt vahetatud salajane võti, mida kasutades vahetatakse uus võti), kui ei toetu arvutuslikele eeldustele (näiteks: faktoriseerimine on raske). Põhjuseks on tõestatavalt turvaliste kanalite mitteleidumine "klassikalises maailmas." Ehk: kõik on põhimõtteliselt pealtkuulatav. Kvantkanali lisamisel muutub salajane võtmekehtestus võimalikuks.

4.1 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.

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 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 baasijadade valikuid määrava jada A (olgu näiteks $A := 110010110011$). 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	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$

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

Footon	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\rightarrow\rangle$	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\rightarrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$	$\|\uparrow\rangle$	$\|\uparrow\rangle$	$\|\nwarrow\rangle$	$\|\nearrow\rangle$
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 $K' := 0111100$.

5 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 $|xy\rangle := |x\rangle \otimes |y\rangle$.

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,

$$(a_1|0\rangle + b_1|1\rangle) \otimes (a_2|0\rangle + b_2|1\rangle) =$$
$$a_1a_2|00\rangle + a_1b_2|01\rangle + a_2b_1|10\rangle + b_1b_2|11\rangle \ .$$

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.

6 Mõõtmine. EPR paradoks

Kvantsüsteemi parameetri(te) mõõtmise tulemuseks on süsteemi normaalprojektsioon olekuruumi mõõdetud väärtustega ühilduvasse alamruumi ("Von Neumanni projektsioonihüpotees"). Normaalprojektsioon — pärast mõõtmist saadud süsteemi olekuvektor on endiselt üks. Öeldakse, et mõõtmisel olek *kollapseerub*.

Näide. Suvalise 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

$$\frac{1}{\sqrt{a^2+b^2}}(a|00\rangle + b|01\rangle) \ .$$

Saab tõestada, et osakesed ei ole sasiolekus $\iff$ ühe osakese mõõtmine ei mõjuta teist osakest (teine, ekvivalentne definitsioon). Nii on $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ 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. Seejärel teostab Alice oma osakesel mõõtmise. Seejärel mõõdab Bob oma osakest ning saab *hetkeliselt* vastuseks sama tulemuse, mis Alice, sõltumatult Alice'i ja Bobi vaheliselt kauguselt. 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.

Seega, ehkki füüsikas on EPR-paradoks tunnetuslikult väga oluline (lokaalsuse printsiip, kvantmehaanika interpretatsioonid), ei ole kvantarvutite seisukohalt tegemist paradoksiga.

7 Unitaarteisendused

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. Vastavalt unitaarteisenduste definitsioonile,

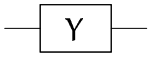
- Unitaarteisendusi saab esitada kompleksse vektorruumi rotatsioonidena.
- Kõik unitaarteisendused on pööratavad.

8 Kvantlülid

Esitame järgnevas tabelis neli kõige elementaarsemat kvantlüli (*quantum gates*) koos nende alternatiivsete definitsioonidega.

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	$Y = Z \cdot X$	$\|0\rangle\langle 1\| - \|1\rangle\langle 0\|$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

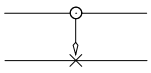
Ühebitiseid kvantoperatsioone kujutatakse graafiliselt operatsiooni nimega märgendatud kastina:



Olgu

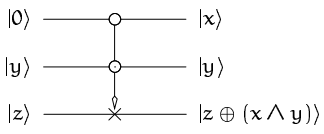
$$C_{\text{not}} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \ .$$

(kontrollige, et C_{not} ei avaldu kahe ühebitise teisenduse tensorkorrutisena). Teisendust C_{not} (*juhitac eitus*) tähistatakse graafiliselt tavaliselt järgmiselt:



Joonisel on kujutatud kahe kvantbitine lüli, kus esimese biti väärtusest sõltuvalt teise biti väärtus muutub või mitte.

Lüli *juhitav-juhitav-eitus* (Toffoli lüli), kus kolmanda biti väärtus muutub vaid siis kui esimesed kaks bitti on mõlemad 1, kujutatakse järgmiselt:



Hadamard'i teisendus on järgmine:

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

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, mida nimetatakse Walsh-Hadamard'i teisenduseks:

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

9 Kvantinformatsioon

9.1 Kloonimise võimatus

Olgu U — klooniv unitaarteisendus: $U(|x0\rangle) = |xx\rangle$ iga 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 $(a|0\rangle + b|1\rangle) \otimes \cdots \otimes (a|0\rangle + b|1\rangle)$.

9.2 Tihe kodeerimine (*dense coding*)

Olgu Alice'il esimene ning Bobil teine sasiosake EPR-paarist $1/2(|00\rangle + |11\rangle)$. Tihe kodeerimine kasutab ühte kvantbitti koos eelnevalt "vahetatud" EPR-paariga kahe klassikalise biti kodeerimiseks ning edastamiseks. Seega kulub hiljem kahe klassikalise biti edastamiseks vaid üks tavaline bitt. Üllatav, kuna teame, et informatsiooniteoreetiliselt kvantbitt=bitt!

Alice'il on kaks bitti ($\phi \in \{0\ldots3\}$). Sõltuvalt ϕ väärtusest rakendab Alice ühe teisendustest $\{I, X, Y, Z\}$ oma osakesele. EPR-paari uued olekud:

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.

Bob: Bob rakendab C_{not} 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.

Bob rakendab 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	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$	$\|1\rangle$

Mõõtes esimese biti väärtuse, suudab Bob eristada väärtusi 0 ja 3, 1 ja 2.

9.3 Teleportimine

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

Enne protokolli algust on Alice'il esimene ning Bobil teine osake EPR-paarist. Alice soovib edastada kvantbitti $\phi := a|0\rangle + b|1\rangle$, kasutades klassikalisi kanaleid. 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 ja Bob kolmandat bitti.

Alice rakendab algolekule järjestikku teisendusi $C_{not} \otimes I$ ja $H \otimes I \otimes I$ (ehk tiheda kodeerimise dekodeerimissammu):

$$\begin{aligned}&(H \otimes I \otimes I)(C_{not} \otimes I)(\phi \otimes \psi_0) \\ &= (H \otimes I \otimes I)(C_{not} \otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|100\rangle + b|111\rangle) \\ &= (H \otimes I \otimes I)\frac{1}{\sqrt{2}}(a|000\rangle + a|011\rangle + b|110\rangle + b|101\rangle) \\ &= \frac{1}{2}(a(|000\rangle + |011\rangle + |100\rangle + |111\rangle) + b(|010\rangle + |001\rangle - |110\rangle - |101\rangle)) \\ &= \frac{1}{2}(|00\rangle(a|0\rangle + b|1\rangle) + |01\rangle(a|1\rangle + b|0\rangle) + |10\rangle(a|0\rangle - b|1\rangle) + |11\rangle(a|1\rangle - b|0\rangle)) \ .\end{aligned}$$

Alice mõõdab esimesed kaks kvantbitti, saades väärtuse $|\alpha\rangle$, $\alpha \in \{0, \ldots, 3\}$. Alice saadab mõõtmise tulemused kui kaks klassikalist bitti Bobile. Vastavalt Alice'i mõõtmise tulemustele projekteerub Bobi kvantbitt üheks neljast väärtusest $a|0\rangle \pm b|1\rangle$, $a|1\rangle \pm b|0\rangle$.

Kvantbitte mõõtes muutis Alice taastamatult kvantbiti ϕ väärtust, mistõttu biti teleportimine 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

10 Universaalne kvantarvuti

10.1 NOT ning AND tehete simuleerimine

Teame, et kõik kvantteisendused on pööratavad. Kuigi klassikaline NOT tehe on pööratav, pole seda AND ega NAND tehted: teades, et lause "A ja B" on väär, pole võimalik teada saada, kumb komponentidest tegelikult väär oli. See probleem lahendatakse nn *prügibittide* kasutusele võtmisega.

Suvalise kahe unitaarteisenduse U ja V korral on unitaarne ka *tingimuslik* teisendus $|0\rangle\langle 0| \otimes U + |1\rangle\langle 1| \otimes V$.

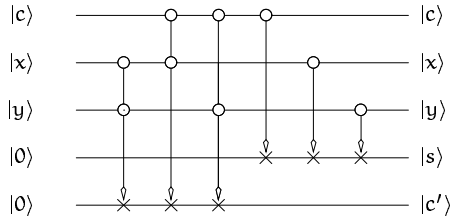
$C_{\text{not}} := |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$.

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

$$T := |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes C_{\text{not}} \ .$$

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 $T|x,y,0\rangle := |x,y,x \wedge y\rangle$.

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.



10.2 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":

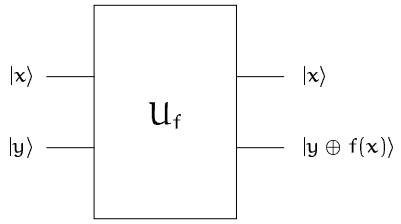
$$F := |0\rangle\langle 0| \otimes I \otimes I + |1\rangle\langle 1| \otimes S \ .$$

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.

Pööratavate kvantlülide abil saab arvutada kõiki klassikaliselt arvutatavaid funktsioone, järelikult on võimalik konstrueerida universaalne kvant-Turingi masin.

10.3 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.

10.4 Kvantarvutused kvantarvutil

Kuigi T- ja F-lülid on täielikud klassikaliste arvutuste jaoks, ei piisa neist suvaliste kvantarvutuste teisendamiseks. Viimaste jaoks tuleb primitiivsete skeemide hulka lisada ka ühebitised rotatsioonid.

Olgu $R_y(\alpha) := \begin{pmatrix} \cos\frac{\alpha}{2} & \sin\frac{\alpha}{2} \\ -\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$ (rotatsioon θ radiaani ümber y-telje), $R_z(\alpha) := \begin{pmatrix} e^{i\frac{\alpha}{2}} & 0 \\ 0 & e^{-i\frac{\alpha}{2}} \end{pmatrix}$ (rotatsioon θ radiaani ümber z-telje), $Ph(\alpha) := \begin{pmatrix} e^{i\alpha} & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$ (faasinihe α võrra).

Lemma. Iga unitaarset 2×2 maatriksit $M \in U(2)$ saab avaldada kujul $Ph(\delta)R_z(\alpha)R_y(\theta)R_z(\beta)$, δ, α, θ ja $\beta \in \mathbb{R}$. Iga unitaarset maatriksit M, $\det M = 1$ (st $M \in SU(2)$), saab avaldada kujul $R_z(\alpha)R_y(\theta)R_z(\beta)$.

Tõestus. Kuna maatriks on unitaarne $\iff$ maatriks rea- ja veeruvektorid on ortonormaalsed, siis avaldub iga $M \in U(2)$ kujul

$$\begin{pmatrix} e^{i(\delta+\frac{\alpha}{2}+\frac{\beta}{2})}\cos\frac{\theta}{2} & e^{i(\delta+\frac{\alpha}{2}-\frac{\beta}{2})}\cos\frac{\theta}{2} \\ -e^{i(\delta-\frac{\alpha}{2}+\frac{\beta}{2})}\sin\frac{\theta}{2} & e^{i(\delta-\frac{\alpha}{2}-\frac{\beta}{2})}\cos\frac{\theta}{2} \end{pmatrix} = Ph(\delta)R_z(\alpha)R_y(\theta)R_z(\beta) \ .$$

Kui $M \in SU(2)$, siis $\det Ph(\delta) = 1$ ehk $e^{i\delta} = \pm 1$ ehk korrutise esimest maatriksi saab võrrandist maha taandada.

Seega saab kõiki ühekvantbitiseid kvantarvuteid emuleerida, kasutades vaid rotatsioone ning faasinihkeid. On näidatud, et mitmekvantbitiste arvutite korral piisab, kui lisada tehetele juhitav-eitus.

10.5 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.

Kõik kvantparallelismi kasutavad kvantalgoritmid peavad järgima fikseeritud plokkskeemi. Alustatakse n-kvantbitisest olekust $|00\ldots0\rangle$. Algolekule rakendatakse teisendust W, misjärel saadakse olek

$$W|0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle \ .$$

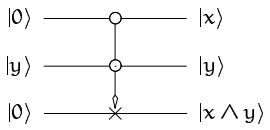
Lineaarsuse tõttu

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

Seega tähendab kvantparallelism eksponentsiaalset parallelismi lineaarses ruumis.

10.6 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 uue oleku

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

11 Kvantparallelism, III

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. 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.

12 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).

Olgu $|x\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ ning $|y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$,

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

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

13 Otsialgoritmid

Paljusid probleeme saab formuleerida kui otsiprobleeme kujul “leida selline x, et $P(x)$ oleks tõene” (ülesanded andmebaasi päringutest kuni graafi värvimiseni).

Teatud tüüpi probleemide korral on teada mingi abistav lisainformatsioon, mida saab kasutada tõhusa lahendusalgoritmi leidmiseks: paljude otsiülesannete (graafi värvitavus, elemendi otsing järjestatud listis) on otsinguruum struktureeritud, sellistel juhtudel saab ülesande täislahendi kätte teatud alamprobleemide lahendite kombineerimisel.

Üldjuhul, lisastruktuuride puudumisel, puudub täielikust läbivaatusest parem algoritm: kui otsinguruumi suurus on N, kulub struktureerimata otsinguks $O(N)$ sammu.

14 Otsialgoritmid kvantarvutitel

Grover, 1997: stohhastiline kvantalgoritm, mis kulutab struktureerimata otsinguks $O(\sqrt{N})$ sammu (tõestatud, et parim võimalik algoritm).

Hogg: Groveri algoritmi saab kiirendada struktureeritud otsinguruumide jaoks. Hoggi algoritmid on juba nii keerukad, et nende õnnestustõenäosust pole siiamaani suudetud määrata ja seega pole ka teada Hoggi algoritmi täpne keerukus.

Tavaliselt leitakse heurilistiliste algoritmide efektiivsus empiiriliste meetodite arvutil testides. Kvantarvutide puhul võimatu — simuleerimiseks kulub eksponentsiaalne aeg. Väikeste sisendite puhul on Hoggi algoritm Groveri algoritmist kiirem (polünomiaalselt). Kuni pole ehitatud kvantarvuteid või pole leitud paremaid matemaatilisi meetodeid selliste algoritmide analüüsimiseks, ei ole seega täpse keerukuse määramine võimalik.

15 Groveri algoritm

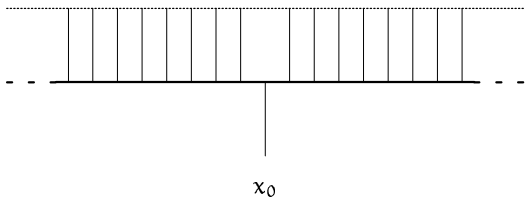
Groveri algoritm teostab otsingut struktureerimata listis võimsusega N. Olgu n naturaalarv, $2^n > N$. Olgu n-bitine predikaat P teostatud kvantskeemina $U_p : |x, 0\rangle \to |x, P(x)\rangle$, kus viimase biti väärtus on $1 \iff P(x)$ on tõene. Groveri algoritmi esimene samm on standarne: sisendile $|0 \ldots 0\rangle$ rakendatakse Walshi teisendust ning seejärel skeemi U_p, saades tulemuseks summma $A(P) = (1/2)^{n/2} \sum_{x=0}^{2^n-1} |x, P(x)\rangle$.

Suvalise sellise x_0 korral, mille jaoks $P(x_0)$ on tõene, kuulub $|x_0, 1\rangle$ superpositsiooni $A(P)$, kuid kuna selle oleku amplituud on $1/2^{n/2}$, on tõenäosus superpositsiooni mõõtmise järel suuruse x_0 saamiseks $(1/2)^{n/2}$.

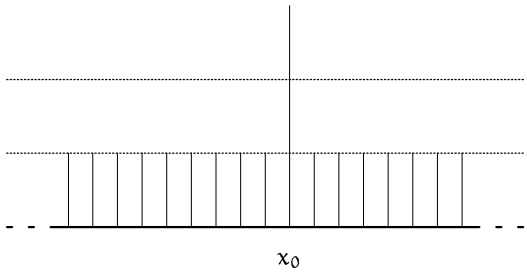
Groveri algoritmi järgmised sammud muudavad kvantolekut $A(P)$ nii, et olekute $|x, 1\rangle$ (olekute, mille puhul $P(x)$ on tõene) amplituud suureneks oluliselt olekute $|x, 0\rangle$ amplituudide arvel.

15.1 Amplituudi võimendamine

1. Muuta olekute $|x_j, 1\rangle$ amplituude $a_j \to -a_j$. Uus olek on graafiliselt kujutatud järgmisel joonisel:



2. Teostada inversiooni ümber keskmise (suurendab olekute $|x, 1\rangle$ amplituude oluliselt, olekute $|x, 0\rangle$ amplituudid kahanevad tühiselt). Uus olek:



3. Korrata eelmisi samme $\pi/4\sqrt{2^n}$ korda.

4. Mõõta tulemi viimast bitti.

Tänu amplituudi muutustele on tõenäosus, et mõõtmisel saadakse 1, suur. Sellisel juhul projitseerub olek $A(P)$ alamruumile $2^{-k/2}\sum_{i=1}^{k}|x_i,1\rangle$, kus k on lahendite arv. Esimese n biti mõõtmine väljastab tulemuseks ühe nendest olekutest. Kui viimase biti mõõtmisel saadakse tulemuseks 0, alustatakse kogu protsessi algusest peale.

On tõestatud, et GA ja optimaalse algoritmi vahe ei ole suurem kui konstant struktureerimata listide korral. Kui vaid ühe x_0 korral on $P(x_0)$ tõene, on $\pi/8\sqrt{2^n}$ sammu järel algoritmi õnnestumistõenäosus 0.5. Pärast $\pi/4\sqrt{2^n}$ sammu on õ.t. $1-2^{-n}$. Huvitaval kombel väheneb õ.t. pärast lisasamme: peale $\pi/2\sqrt{2^n}$ sammu on õ.t. 2^{-n}.

Põhjendus: kvantalgoritmid on rotatsioonid kompleksruumis. Liiga suur pöördenurk kaugendab tulemust oodatust. Järelikult: itereeritud kvantteisenduste kasutamisel peab olema täpselt teada, millal lõpetada.

15.2 Inversioon ümber keskmise

Olgu $A=\sum a_i$. Teisendust $\sum a_i|x_i\rangle \to \sum(2A-a_i)|x_i\rangle$ teostab $N\times N$ maatriks

$$D=\begin{pmatrix} 2/N-1 & 2/N & \cdots & 2/N \\ 2/N & 2/N-1 & \cdots & 2/N \\ \vdots & \vdots & \ddots & \vdots \\ 2/N & 2/N & \cdots & 2/N-1 \end{pmatrix} .$$

Kuna $DD^*=I$, siis on D unitaarmaatriks (ja seega lubatud kvantteisendus). D dekomponeerimisel saame $D=WRW$, kus W on Walsh-Hadamardi teisendus ning

$$R=\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & -1 \end{pmatrix} = \begin{pmatrix} 2 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix} - I = R' - I .$$

Tõepoolest, $WRW = W(R'-I)W = WR'W - I$, ning

$$WR'W=\begin{pmatrix} 2/N & 2/N & \cdots & 2/N \\ 2/N & 2/N & \cdots & 2/N \\ \vdots & \vdots & \ddots & \vdots \\ 2/N & 2/N & \cdots & 2/N \end{pmatrix} .$$

R-i saab leida $O(\log N)$ sammuga.

16 Märgimuutmine

(Üldistus) Olgu P — suvaline predikaat, $U_p : |x,b\rangle \to |b\oplus P(x)\rangle$. Olgu $|\phi\rangle = 2^{-n/2}\sum|x\rangle$. Rakendame lüli U_p superpositsioonile $|\phi,b\rangle$, kus $b=2^{-1/2}(|0\rangle-|1\rangle)$. Olgu $X_i=\{x : P(x)=i\}$.

$$
\begin{aligned}
U_p(|\psi, b\rangle) &= 2^{-(n+1)/2} U_p\Big(\sum_{x\in X_0}|x,0\rangle + \sum_{x\in X_1}|x,0\rangle - \sum_{x\in X_0}|x,1\rangle - \sum_{x\in X_1}|x,1\rangle\Big)\\
&= 2^{-(n+1)/2}\Big(\sum_{x\in X_0}|x,0\rangle + \sum_{x\in X_1}|x,1\rangle - \sum_{x\in X_0}|x,1\rangle - \sum_{x\in X_1}|x,0\rangle\Big)\\
&= 2^{-(n+1)/2}\Big(\sum_{x\in X_0}|x\rangle - \sum_{x\in X_1}|x,0\rangle\Big)\otimes b \ .
\end{aligned}
$$

17 Shori faktoriseerimisalgoritm

Kvantarvutite vastu tõusnud huvi üks peapõhjuseid oli kiire faktoriseerimisalgoritmi avastamine Peter Shori poolt 1994 aastal. Shori algoritm töötab randomiseeritud polünomiaalses ajas, olles järelikult sama keerukusastmega kui parimad (teadaolevad) algarvutestid. Veelgi enam — Shori algoritmi keerukus (kui kõrvale jätta randomiseeritus) on täpselt sama, mis modulaareksponendi arvutamisel).

Arvestades sellega, et Shori algoritmi kordamisel suureneb tema õ.t. eksponentsiaalselt, võib pisut üldistades siiski öelda, et kvantarvutitel on ründed RSA-tüüpi krüptosüsteemi vastu täpselt niisama efektiivsed kui RSA-ga krüptimine; enamiku tänapäeva asümmeetriliste krüptosüsteemide kasutamine kaotab mõtte kvantarvutite saabumisel.

17.1 Kõrvalepõik krüptograafiasse

Asümmeetriline krüptograafia: kolm algoritmi — võtmegeneraator G, krüptimisalgoritm e, dekrüptimisalgoritm d. Fikseeritud turvaparameeter k.

Alice genereerib võtmepaari (E_A, D_A), kus E_A on avalik ning D_A salajane võti ning avalikustab võtme E_A (peab olema efektiivne).

Bob krüptib teate M, kasutades Alice'i avalikku võtit E_A ning saadab teate $C := e(E_A, M)$ Alice'ile (peab olema efektiivne).

Alice dekrüptib teate C, kasutades salajast võtit D_A ning saab tulemuseks bitistringi $d(D_A, e(E_A, C)) = M$ (peab olema efektiivne).

Ründaja soovib leida salajast võtit D_A, teades võtit E_A ning polünomiaalset paaride hulka $(M, e(E_A, M))$ (peab olema ebaefektiivne).

Vaatleme konkreetselt RSA krüptosüsteemi. Olgu $\phi(x) = \{y < x : \gcd(y,x) = 1\}$. Alice genereerib kaks suurt algarvu p ja q, ning leiab korrutise n. Seejärel genereerib Alice avaliku eksponendi e, nii et $\gcd(e, \phi(n))$=1 ning leiab (Eukleidese algoritmi kasutades) salajase eksponendi d, nii et $ed \equiv 1 \pmod{\phi(n)}$. Alice'i avalik võti on $E_A = (n, e)$, Alice'i salajane võti on (n, p, q, e, d) (algarvutest $\in \mathcal{BPP}$, Eukleidese algoritm $\in \mathcal{P}$).

Avateksti M krüptogramm $e(E_A, M) := x^e \mod n$, krüptogrammile M vastav avatekst $d(D_A, M) := x^d \mod n$ (modulaareksponent $\in \mathcal{P}$).

Kuna $\phi(n) = (p-1)(q-1)$, siis võimaldab n-i faktoriseerimine ründajal leida suuruse $\phi(n)$ ning seejärel leida d, kasutades Eukleidese algoritmi. Järelikult, kui faktoriseerimine on lihtne, on lihtne ka RSA lahtimurdmine.

17.2 Shori algoritm: idee

Algoritmi alguses kasutatakse standardsel moel kvantparallelismi, leides funktsiooni f väärtused kõikvõimalikel sisenditel vastava kvantskeemi U_f ühekordse rakendamisega.

Seejärel leitakse funktsiooni f nn kvant-Fourier' teisendus (KFT). Pärast KFT rakendamist saab mõõtmisel suure tõenäosusega kätte funktsiooni f perioodi, mida kasutatakse järgnevas "tava-algoritmi" kasutades faktoriseerimiseks.

17.3 Kvant-Fourier' teisendus

Diskreetne Fourier' teisendus teisendab väärtustehulgaga $0, \ldots, N-1$ funktsiooni g funktsiooniks F_g, piltlikult öeldes "ajafunktsioon" "sagedusfunktsiooniks," mille väärtuste hulgaks on lõigus $[0, 2\pi)$ asetsevad suuruse $2\pi/N$ kordsed.

Muuhulgas, kui funktsiooni g periood on r, on tulemfunktsiooni F_g väärtus nullist erinev vaid sageduse $1/r$ kordsetel sisenditel.

KFT opereerib kvantoleku amplituudidega, teisendades oleku $\sum_{x=0}^{N-1} g(x)|x\rangle$ olekuks $\sum_{c=0}^{N-1} F_g(c)|c\rangle$. Kui kvantolekut mõõta pärast KFT rakendamist, saadakse tulem $|c\rangle$ tõenäosusega $|F_g(c)|^2$. Sealjuures on $F_g(c)$ nullist erinev vaid suuruse N/r kordsetel punktidel ning seega jagub mõõtmistulemus suurusega N/r.

Kuna KFT on variant kahe astmetel baseeruvast kiirest Fourier' teisendusest, mis annab täpsed vastused vaid kahe astmele vastaval perioodil, on ka KFT tulemus ligikaudne, kui funktsiooni g periood ei ole kahe aste. KFT täpsus suureneb koos baasiks kasutatud kahe astme kasvuga, kvantskeem U_{KFT} baasil 2^m defineeritakse järgnevalt:

$$U_{KFT} : |x\rangle \rightarrow \frac{1}{\sqrt{2^m}} \sum e^{2\pi c x/2^m} |c\rangle \ .$$

KFT arvutamiseks kulub $m(m+1)/2$ kvantskeemi. Konstruktsioon kasutab Hadamardi teisendust ning teisendusi kujul

$$S_{j,k} = \begin{pmatrix} 1 & 0 & 0 & & 0 \\ 0 & 1 & 0 & & 0 \\ 0 & 0 & 1 & & 0 \\ 0 & 0 & 0 & e^{i\pi/2^{k-j}} & \end{pmatrix}$$

(mõjub k-ndale elemendile vastavalt j-nda elemendi väärtusele).

17.4 Shori algoritmi raamkava

1. Genereeritakse arv a juhuslikult. Kui $\gcd(a, M) > 1$, on arv M faktoriseeritud. Vastasel juhul jätkata algoritmi täitmist.

2. Olgu m selline, et $M^2 \leq 2^m < 2M^2$. Olgu $f(x) \equiv a^x \mod M$. Kvantparallelism, olekusse $2^{-m/2} \sum_x |x, f(x)\rangle$.

3. Konstrueeritakse olek, mille amplituudifunktsioonil $g(x)$ on sama periood kui funktsioonil $f(x)$. Selleks mõõdetakse sammu 2 lõppolekut, saades tulemuseks juhusliku suuruse u. Mõõtmine projitseerib olekuruumi alamruumi, mis on ühilduv mõõdetud väärtusega. Seega on uueks olekuks $C \sum_x g(x)|x, u\rangle$, mingi normeerimisfaktori C jaoks, kus $g(x) = 1$, kui $f(x) = u$, ja $g(x) = 0$ vastasel juhul. Kuna summas esinevad x-i väärtused erinevad teineteisest perioodi kordsete võrra, oleme leidnud otsitava funktsiooni. Edasises ei kasutata enam oleku viimast poolt u.

4. KFT-d rakendades jõutakse olekusse $C \sum_c F_g(c)|c\rangle$. Üldisest FT teooriast on teada, et kui $g(x)$ periood on kahe aste, on KFT tulemuseks olek $D \sum_j \rho_j |j2^m/r\rangle$, kus $|\rho_j| = 1$. Kui $r \not| 2^m$, aproksimeerib teisendus täpset juhtu nii, et enamik amplituude on täisarvud, mis paiknevad suuruse $2^m/r$ kordsete läheduses.

5. Olekut mõõdetakse baasis $\{|0\rangle, |1\rangle\}$, saades tulemuseks väärtuse v. Kui periood on kahe aste (KFT väljastab skaleeritud sageduse täpsed kordajad), on $v = j2^m/r$, kus j on täisarv. Enamasti $\gcd(j, r) = 1$, sellisel juhul saab murrust $v/2^m = j/r$ leida r-i. Kui v ei ole kahe aste, annab KFT ainult ligikaudselt skaleeritud sageduse kordsed. Sellisel juhul arvatakse perioodi väärtus ära, saades tulemuseks arvu q.

6. Kui q on paarisarv, kasutatakse Eukleidese algoritmi, et kontrollida, kas ühel kahest suurusest $a^{q/2} \pm 1$ on mittetriviaalseid ühistegureid arvuga M. Kui q on funktsiooni $f(x)$ periood, siis $a^q \mod M = 1$, kuna $a^q a^x = a^x \mod M$, suvalise x korral. Kuna q on paarisarv, siis $(a^{q/2}+1)(a^{q/2}-1) = 0 \mod M$. Seega, kui kumbki teguritest pole M kordne, on ühel neist teguritest arvuga M mittetriviaalne ühistegur.

7. Korrata algoritmi, kui vaja. Vajadus võib tekkida, kui (a) v pole $2^m/r$ kordaja, (b) perioodil $\gcd(r, j) > 1$ (siis q pole periood, vaid perioodi tegur), (c) samm 6 annab tegurina arvu M, (d) funktsiooni $f(x)$ periood on paaritu. Algoritmi mõned korrad korrates saadakse suure tõenäosusega õige tulem.

18 Kvantveaparandus

Kvantarvutite ehitamisel on fundamentaalseks probleemiks vajadus isoleerida kvantolek. Kvantbitte kandvate osakeste interaktsioon välise keskkonnaga rikub kvantolekut, põhjustades selle dekoherentsi (mitteunitaarseid teisendusi). Suvalise ehitatava kvantarvuti dekoherents on arvatavalt vähemalt 10^7 korda liiga suur, et rakendada Shori algoritmi 130-kohalistel arvudel.

Veaparandusalgoritmide lisamisel Shori algoritmile väheneb dekoherentsiefekt, mis teeb (teoreetiliselt) võimalikumaks piisavalt suurte süsteemide ehitamise.

Kvantveaparandus on väliselt sarnane klassikalise veaparandusega — "teksti" lisatakse liiasust, mis võimaldab vigu avastada ja kõrvaldada. KVP on siiski keerulisem kui VP, kuna me ei tegele mitte kahendandmete, vaid kvantolekutega: KVP peab täpselt rekonstrueerima kodeeritud kvantoleku.

Kuna kvantolekut on võimatu kloonida ehk kopeerida, tundub rekonstruktsioon olevat keerulisem, kui klassikalisel juhul. Siiski, klassikalised tehnikad töötavad (modifitseeritult) kvantjuhul.

Viited

[HML+98] Vello Hanson, Tarvi Martens, Helger Lipmaa, Arne Ansper, and Viljar Tulit. *Infosüsteemide turve II. Turbetehnoloogia*. Küberneetika AS, 1998.

[Pre98] John Preskill. Lecture Notes for Physics 229: Quantum Information and Computation. Available at `http://www.theory.caltech.edu/people/preskill/ph229/`, October 1998.

[WC97] Colin P. Williams and Scott H. Clearwater. *Explorations in Quantum Computing*. Springer-Verlag, 1997. ISBN: 0-387-94768-X.