Kvanttitietokoneet, kvanttilaskenta ja kvanttikryptografia

Kvanttimekaniikka

- Kvanttimekaniikka: Aineen käyttäytymistä kuvaava fysiikan perusteoria.
- Mikroskooppisella tasolla ilmenee erityisiä kvantti-ilmiöitä, joita klassinen fysiikka ei tunne.
- Kun järjestelmät suurenevat, kvantti-ilmiöt käyvät yhä huomaamattomammiksi.
- Makroskooppisella tasolla kvantti-ilmiöitä ei juurikaan havaita; poikkeuksena suprajohtavuus ja suprajuoksevuus.

Kvanttimekaniikan perusperiaatteet

- Aineen ominaisuudet, kuten energia, eivät ole jatkuvia, vaan kvantittuneita.
- Kaikki kappaleet käyttäytyvät niin kuin ne olisivat sekä hiukkasia että aaltoja.
- Hiukkasen kaikkia ominaisuuksia ei voida mitata samanaikaisesti mielivaltaisen tarkasti.
- Yksittäisen mittauksen tulos voidaan ennustaa vain jollain tietyllä todennäköisyydellä.

Kvanttimekaniikan sovelluksia

- Kvanttiteleportaatio: Järjestelmän kvanttitila siirretään paikasta toiseen ilman fyysisen materian siirtoa.
- Kvanttikryptografia: Salakirjoitus koodilla, jota ei voi murtaa; tiedonvälitys linjalla, jota ei voi salakuunnella paljastumatta.
- Kvanttilaskenta: Kvantti-ilmiöihin perustuva, uudenlainen tapa käsitellä informaatiota.

Kvanttilaskenta

- Klassisessa laskennassa suoritetaan loogisia operaatioita biteille.
- Kvanttilaskennassa suoritetaan loogisia operaatioita kvanttibiteille eli kubiteille (engl. quantum bit, qubit).
- Kubiteille on olemassa operaatioita, joille ei ole vastinetta klassisessa laskennassa; esimerkiksi negaation neliöjuuri $\sqrt{NOT}$.
- Kvanttitietokone: Fyysinen järjestelmä, jossa voidaan toteuttaa kvanttilaskentaa.

Kvanttilaskennan historiaa (1)

- 1978:
  - Ajatus kvanttitietokoneesta (David Deutsch).
- 1980:
  - Ensimmäinen kvanttimekaanisiin osiin perustuvan tietokoneen malli (Paul Benioff).
- 1981:
  - Ajatus universaalista kvanttisimulaattorista (Richard Feynman).
- 1985:
  - Universaalin kvanttitietokoneen malli (Deutsch).
  - Ensimmäinen algoritmi kvanttitietokoneelle (Deutsch).

Kvanttilaskennan historiaa (2)

- 1987:
  - Ensimmäinen kvanttivirheenkorjausalgoritmi (Deutsch).
- 1989:
  - Ensimmäinen toimiva kvanttikryptojärjestelmä (Charles Bennet ja Gilles Brassard).
- 1994:
  - Ensimmäinen suurten etäisyyksien (30 km) jakelu kvanttiavaimille (Paul Townsend ja Christophe Marand).
  - Algoritmi, joka laskee suurten lukujen tekijät nopeasti kvanttitietokoneella (Peter Shor).

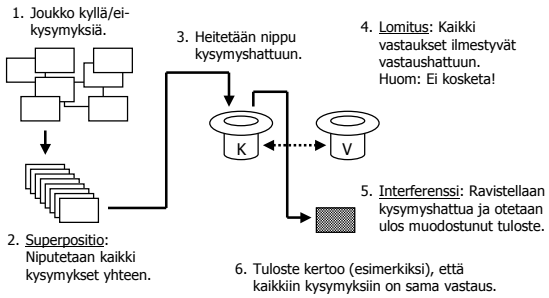
Kvanttilaskennan historiaa (3)

- 1995:
  - Menetelmä korjata kvanttivirheet bitti bitiltä (Shor).
  - Kvanttioperaatioiden fyysinen toteutus ioniloukulla (Ignazio Cirac ja Peter Zoller).
- 1997:
  - Ensimmäiset onnistuneet kvanttiteleportaatio-kokeet (Francesco De Martini, Anton Zeilinger).
- 1998:
  - Ensimmäinen toimiva kvanttimekaniikkaan perustuva tietokone (MIT, IBM, Oxford, Berkeley).

Kvanttilaskennan perusperiaatteet

- Superpositio: Kvanttitilat esiintyvät puhtaiden perustilojen sekoituksina – kubitti voi olla samanaikaisesti sekä 0 että 1.
- Lomittuminen: Eri kvanttitilat eivät ole täysin erillisiä, vaan korreloivat keskenään – yhden kubitin arvon tutkiminen voi vaikuttaa muiden kubittien arvoihin.
- Interferenssi: Kvanttitilojen aalto-ominaisuudet vahvistavat ja vaimentavat toisiaan – yhden kubitin arvosta voidaan päätellä jotain muiden kubittien arvoista.

Kvanttilaskennan perus-periaatteet: Taikahattuanalogia



Kvanttibitit eli kubitit

- Klassinen bitti voi olla vain kahdessa eri tilassa: 0 tai 1.
- Kubitti voi myös olla kahdessa eri tilassa: $|0\rangle$ tai $|1\rangle$.
- Kubitti voi lisäksi olla missä tahansa tilojen $|0\rangle$ ja $|1\rangle$ välisessä superpositiossa: $\alpha|0\rangle+\beta|1\rangle$, missä $|\alpha|^2+|\beta|^2=1$.
- Kertoimia α ja β ei aina merkitä näkyviin.

Kubitin mittaus

- Superpositiossa $\alpha|0\rangle+\beta|1\rangle$ olevan kubitin mittaus antaa todennäköisyydellä $|\alpha|^2$ tuloksen 0 ja todennäköisyydellä $|\beta|^2$ tuloksen 1.
- Esimerkkejä:

$$\pm|0\rangle \xrightarrow{\text{Mittaus}} 0 \quad \text{(Tod.näk. 100 \%)}$$

$$\pm|1\rangle \xrightarrow{\text{Mittaus}} 1 \quad \text{(Tod.näk. 100 \%)}$$

$$\pm\frac{1}{\sqrt{2}}|0\rangle \pm \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{\text{Mittaus}} \begin{cases} 0 & \text{(Tod.näk. 50 \%)} \\ 1 & \text{(Tod.näk. 50 \%)} \end{cases}$$

Kvanttirekisterit

- Klassisista biteistä muodostettu n:n bitin rekisteri voi sisältää yhden luvuista $0,1,\ldots,2^n-1$.
- Kubiteista muodostettu n:n kubitin rekisteri voi sisältää kaikki nämä luvut samanaikaisesti.
- Esimerkiksi kolme kubittia:

$$\underbrace{(|0\rangle+|1\rangle)}_{\text{Kubitti 1}}\underbrace{(|0\rangle+|1\rangle)}_{\text{Kubitti 2}}\underbrace{(|0\rangle+|1\rangle)}_{\text{Kubitti 3}}=|000\rangle+|001\rangle+|010\rangle+|011\rangle+|100\rangle+|101\rangle+|110\rangle+|111\rangle$$

Yhden kubitin kvanttiportteja

- Hadamardin portti:

$$\alpha|0\rangle+\beta|1\rangle \;\text{—}\boxed{H}\text{—}\; \frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle+\frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle$$

- Esimerkkejä:

$$|0\rangle \text{—}\boxed{H}\text{—} |0\rangle+|1\rangle \qquad |0\rangle+|1\rangle \text{—}\boxed{H}\text{—} |0\rangle$$
$$|1\rangle \text{—}\boxed{H}\text{—} |0\rangle-|1\rangle \qquad |0\rangle-|1\rangle \text{—}\boxed{H}\text{—} |1\rangle$$

- Vaihesiirtoportti:

$$\alpha|0\rangle+\beta|1\rangle \;\overset{\phi}{\text{—}\bullet\text{—}}\; \alpha|0\rangle+e^{i\phi}\beta|1\rangle$$

- Hadamardin portin ja vaihesiirtoporttien avulla voidaan muodostaa mikä tahansa superpositiotila.

Lomittuneet tilat

- Kvanttirekisteri voi olla lomittuneessa tilassa, jolloin kubittien tiloja ei voi erotella toisistaan.
- Kahden kubitin rekisteri, joka ei ole lomittunut:

$$|00\rangle+|01\rangle=\underbrace{|0\rangle}_{\text{Kubitti 1}}\underbrace{(|0\rangle+|1\rangle)}_{\text{Kubitti 2}}$$

- Kahden kubitin rekisteri, joka on lomittunut:

$$|00\rangle+|11\rangle\neq(\ \ldots\ )(\ \ldots\ )$$

Ei voi erotella

- Lomittuneita tiloja voidaan muodostaa erityisillä kahden kubitin porteilla.

Lomittuneiden kubittien mittaus

- Kubitin mittaus vaikuttaa muiden, sen kanssa lomittuneiden kubittien mittausten tuloksiin.
- Esimerkkejä:

$$|00\rangle+|11\rangle \xrightarrow{\text{Kubitin 1 mittaus}} \begin{cases} 0 \ (50\ \%) \xrightarrow{\text{Kubitin 2 mittaus}} 0 \ (100\ \%) \\ 1 \ (50\ \%) \xrightarrow{\text{Kubitin 2 mittaus}} 1 \ (100\ \%) \end{cases}$$

$$|00\rangle+|11\rangle \xrightarrow{\text{Kubitin 2 mittaus}} \begin{cases} 0 \ (50\ \%) \xrightarrow{\text{Kubitin 1 mittaus}} 0 \ (100\ \%) \\ 1 \ (50\ \%) \xrightarrow{\text{Kubitin 1 mittaus}} 1 \ (100\ \%) \end{cases}$$

- Siis mittausjärjestys voi vaikuttaa tuloksiin!

Kahden kubitin kvanttiportteja (1)

- Säädetty NOT-portti:

$$\left.\begin{array}{l}\alpha|0\rangle+\beta|1\rangle \\ \gamma|0\rangle+\delta|1\rangle\end{array}\right\} \alpha\gamma|00\rangle+\alpha\delta|01\rangle+\beta\delta|10\rangle+\beta\gamma|11\rangle$$

- Esimerkkejä:

$$|0\rangle \text{—}\bullet\text{—} |0\rangle \qquad |1\rangle \text{—}\bullet\text{—} |1\rangle$$
$$|0\rangle-|1\rangle \text{—}\oplus\text{—} |0\rangle-|1\rangle \qquad |0\rangle-|1\rangle \text{—}\oplus\text{—} |1\rangle-|0\rangle$$

Ei muutu — Vaihtuu $0\leftrightarrow 1$

$$\left.\begin{array}{l}|0\rangle+|1\rangle \\ |0\rangle\end{array}\right\} |00\rangle+|11\rangle$$

Lomittunut tila

Kahden kubitin kvanttiportteja (2)

- Säädetty U-portti (periaate):

$$|0\rangle \text{—}\bullet\text{—} |0\rangle \qquad |1\rangle \text{—}\bullet\text{—} |1\rangle$$
$$|y\rangle \text{—}\boxed{U}\text{—} |y\rangle \qquad |y\rangle \text{—}\boxed{U}\text{—} U|y\rangle$$

Ei muutu — Muuttuu kuvauksen U mukaisesti

- Kvanttifunktiolla säädetty portti (periaate):

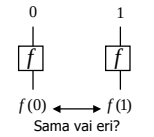
$$|x\rangle \text{—}\bullet\text{—} |x\rangle$$
$$|y\rangle \text{—}\boxed{f}\text{—} |(y+f(x))\bmod 2\rangle$$

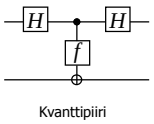
$f(x)=0$: Ei muutu
$f(x)=1$: Vaihtuu $0\leftrightarrow 1$

missä $f:\{0,1\}\rightarrow\{0,1\}$ on jokin looginen funktio.

Esimerkki: Kvanttilaskentaa kvanttipiirillä

- Olkoon käytössä ”musta laatikko”, joka laskee loogisen funktion $f:\{0,1\}\to\{0,1\}$ arvon.
- Tehtävänä on päätellä, onko $f(0)=f(1)$ vai $f(0)\neq f(1)$.
- Klassisesti vastaus saadaan laskemalla funktion arvo kahdesti.
- Kvanttilaskennalla vastaus saadaan laskemalla funktion arvo vain kerran!

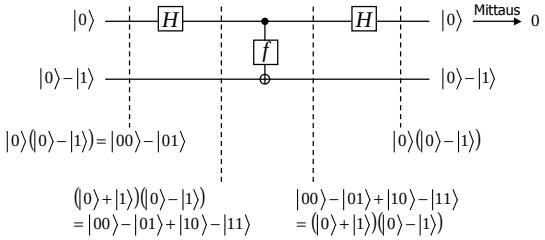




Kvanttipiiri

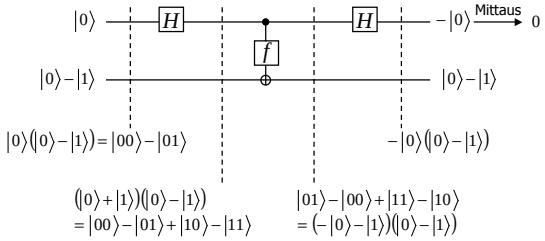
Esimerkki: Kvanttipiirin toiminta (1)

- Tapaus (a) $f(0)=f(1)=0$



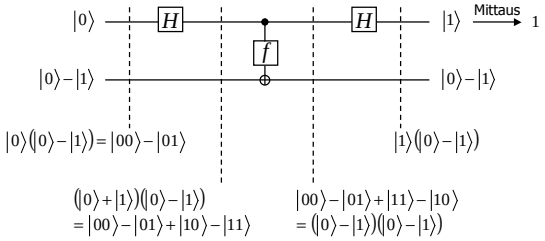
Esimerkki: Kvanttipiirin toiminta (2)

- Tapaus (b) $f(0)=f(1)=1$



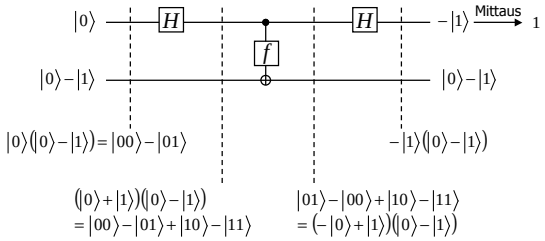
Esimerkki: Kvanttipiirin toiminta (3)

- Tapaus (c) $f(0)=0,\ f(1)=1$



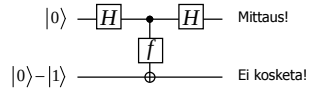
Esimerkki: Kvanttipiirin toiminta (4)

- Tapaus (d) $f(0)=1,\ f(1)=0$



Esimerkki: Yhteenveto

- Tapaus (a) $f(0)=f(1)=0$ Mittaus ⟶ 0
- Tapaus (b) $f(0)=f(1)=1$ Mittaus ⟶ 0
- Tapaus (c) $f(0)=0,\ f(1)=1$ Mittaus ⟶ 1
- Tapaus (d) $f(0)=1,\ f(1)=0$ Mittaus ⟶ 1



- Mittaamalla ylemmän kubitin arvo saadaan selville, onko $f(0)=f(1)$ vai $f(0)\neq f(1)$.

Julkisen avaimen salausmenetelmät

- Viestin välitys: Lähettäjä koodaa viestin vastaanottajan julkisella avaimella; vastaanottaja purkaa koodauksen omalla yksityisellä avaimellaan.
- Digitaalinen allekirjoitus: Lähettäjä koodaa allekirjoituksen omalla yksityisellä avaimellaan; vastaanottaja purkaa koodauksen lähettäjän julkisella avaimella.
- RSA: Tunnetuin julkisen avaimen salausmenetelmä.

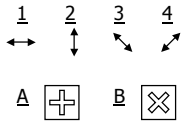
Salauksen murtaminen

- RSA-järjestelmässä julkisesta avaimesta voi laskea vastaavan yksityisen avaimen, jos osaa jakaa suuren kokonaisluvun alkutekijöihinsä.
- Ei tunneta yhtään klassista algoritmia, jolla tekijöihin jako voitaisiin suorittaa polynomisessa ajassa.
- Sen sijaan on olemassa kvanttialgoritmi, jolla tekijöihin jako voidaan suorittaa erittäin nopeasti.
- Vaatimattoman kokoinen kvanttitietokone romuttaisi nykyiset salausjärjestelmät.

Kvanttikryptografian perusperiaatteet

- Kvanttikryptografiassa viesti välitetään kvanttitiloiksi koodattuna, esimerkiksi eri polarisaatiotiloissa olevina fotoneina.
- Yksittäistä kvanttitilaa ei voi selvittää täydellisesti yhdellä mittauksella.
- Mittaus tuhoaa aina kvanttitilan.
- Yksittäistä kvanttitilaa ei voi kopioida täydellisesti tuhoamatta alkuperäistä tilaa.
- Salakuuntelu muuttaa tai tuhoaa välttämättä viestin siirtoon käytettyjä kvanttitiloja, jolloin salakuuntelu paljastuu.

Esimerkki: Kvantti-kryptografian toteutus (1)



- Käytetään fotoneja, joilla voi olla neljä erilaista polarisaatiotilaa.
- Polarisaation voi mitata kahdella eri tavalla.
- Mittaustapa A tunnistaa tilat 1 ja 2 varmasti (”oikea tapa”), mutta tilat 3 ja 4 muuttuvat satunnaisesti tiloiksi 1 tai 2 (”väärä tapa”).
- Mittaustapa B tunnistaa tilat 3 ja 4 varmasti (”oikea tapa”), mutta tilat 1 ja 2 muuttuvat satunnaisesti tiloiksi 3 tai 4 (”väärä tapa”).

Esimerkki: Kvantti-kryptografian toteutus (2)

- Lähettäjä lähettää jonon fotoneja, joiden polarisaatiot on valittu satunnaisesti.
- Vastaanottaja mittaa jokaisen fotonin satunnaisesti valitsemallaan tavalla.
- Vastaanottaja kertoo lähettäjälle kunkin fotonin mittaustavan (mutta ei itse mittaustulosta).
- Lähettäjä ilmoittaa vastaanottajalle, mitkä mittaukset tehtiin oikealla tavalla (mutta ei itse polarisaatiotilaa).
- Molemmat hylkäävät kaikki tapaukset, joissa mittaus tehtiin väärällä tavalla.

Esimerkki: Kvantti-kryptografian toteutus (3)

- Molemmilla on nyt jäljellä sama fotonien polarisaatioiden jono, jota he voivat käyttää salakirjoitusavaimen muodostamiseen.
- Tietoa polarisaatiotiloista tai mittaustuloksista ei välitetty, joten kukaan ulkopuolinen ei voi tietää avainta.
- Fotonien mittaaminen salaa on hyödytöntä, sillä salakuuntelija ei tiedä mikä on kunkin fotonin oikea mittaustapa.
- Lisäksi salakuuntelu muuttaa fotonien polarisaatiotiloja, minkä lähettäjä ja vastaanottaja voivat havaita helposti.

Dekoherenssi

- Dekoherenssi: Järjestelmän ja sen ympäristön kvanttitilat lomittuvat.
- Kvantti-ilmiöt häviävät, superpositiot romahtavat klassisiksi tiloiksi ja interferenssi heikkenee.
- Vaikutus kasvaa eksponentiaalisesti sekä järjestelmän koon että ajan suhteen.
- Dekoherenssin vuoksi makroskooppisia kvanttisysteemejä on vaikea havaita.
- Dekoherenssi on kvanttitietokoneen rakentamisen suurin este.

Kvanttitietokoneen fyysinen toteutus: Ioniloukut

- Ionisoituja atomeja tai muita hiukkasia pidetään tyhjiökammiossa sähkö- ja magneettikenttien avulla.
- Ioneja siirretään viritystilasta toiseen laservalolla.
- Sähköisesti varatut ionit vuorovaikuttavat toistensa kanssa värähtelemällä.
- Kvantti-informaatio koodautuu ionien sisäisiin viritystiloihin ja niiden välisiin värähdystiloihin.

Kvanttitietokoneen fyysinen toteutus: Kaviteetti-QED

- Atomeja ja fotoneja lähetetään kaviteettiin eli onkaloon, jossa on erittäin heijastavat seinät.
- Kaviteetin resonanssitaajuus ja fotonien taajuudet valitaan siten, että fotonit vuorovaikuttavat voimakkaasti atomien kanssa.
- Kvantti-informaatio koodautuu fotonien polarisaatiotiloihin.
- Kaviteetti-QED –teknologiaa voidaan käyttää myös kvantti-informaation siirtoon.

Kvanttitietokoneen fyysinen toteutus: NMR

- NMR (ydinmagneettinen resonanssispektropia) on sama kuin lääketieteessä käytetty MRI (magneettinen resonanssikuvaus).
- Atomiytimien spinejä (”pyörähdystiloja”) muutetaan voimakkailla magneettikentillä ja radiopulsseilla.
- Kvantti-informaatio koodautuu atomien ydinspineihin.
- Kvanttilaskenta tapahtuu nesteessä (”Kvanttitietokone toimii kahvikupissa”, Science, 1997).

Kvanttitietokoneen fyysinen toteutus: Kvanttipisteet

- Puolijohdemateriaalille muodostetaan sähkökentillä alueita, joissa on vain yksi elektroni.
- Elektroneja siirretään viritystilasta toiseen laservalolla.
- Elektronit vuorovaikuttavat muuntamalla toistensa resonanssitaajuuksia.
- Kvantti-informaatio koodautuu elektronien viritystiloihin.
- Kvantti-informaatio voidaan koodata myös elektronien spinien suuntiin.

Kvanttitietokoneen fyysinen toteutus: Vertailua

Teknologia	Kytkentä-aika	Dekohe-renssiaika	Hyvyys-suhde	Skaalau-tuvuus
Ioniloukut	10^{-7}	10^{-1}	10^{6}	50
Kaviteetti-QED	10^{-14}	10^{-5}	10^{9}	2–5
NMR	10^{-3}	10^{4}	10^{7}	10–50
Kvanttipisteet	10^{-9}	10^{-6}	10^{3}	1000

Kytkentäaika: Yhden kvanttioperaation vaatima aika.
Dekoherenssiaika: Aika, jonka jälkeen dekoherenssi tuhoaa laskennan.
Hyvyyssuhde: Edellisten osamäärä; montako kvanttioperaatiota ehditään tehdä.
Skaalautuvuus: Montako kubittia voidaan liittää yhteen.

(*Lähde: Julian Brown, Kvanttitietokone, 2001*)