

Lomittajalle töitä

Jukka Liukkonen

Mat. yo. evp.

Lomituspalvelulain muuttuminen vuoden 2016 alussa on aiheuttanut harmaita hiuksia lomittajille. Monet heistä ovat hyvinkin käärmeissään työtuntien vähentymisestä. Syyttävät sormet osoittavat Suomen hallitukseen ja Euroopan komissioon. Yhä useampi lomittaja harkitsee siirtymistä maataloilta kvanttitilojen lomittajaksi. Mitä ovat kvanttitilat? Mistä kvanttitilojen lomittamisessa on oikein kysymys? Mikä on superpositio? Tieteen termipankin mukaan positio on “ajattelun tai päättelyn lähtökohdaksi otettu oletus”. Ottaako superälykkö ajattelunsa lähtökohdaksi superposition? Voisiko kvanttietokone olla superälykkö?

Suhteellisuusteoria ja kvanttiteoria ovat viime vuosisadan alkupuolella syntyneitä fysiikan suuria kehityslinjoja. Kvanttifysiikan legenda, fysiikan nobelisti Richard Feynman (1918–1988) oivalsi, että kvanttiteorian soveltaminen uudella tavalla saattaisi olla perustana perinteistä huomattavasti tehokkaampien tietokoneiden suunnittelulle. Näissä pienikokoisissa kvanttietokoneissa valtava määrä eri vaihtoehtoja voitaisiin prosessoida samanaikaisesti. Vuonna 1985 fyysikko David Deutsch (1953–) julkaisi yksinkertaisen esimerkin kvanttilaskennasta. Siinä suoritetaan yhdellä funktio-kutsulla tehtävä, joka klassisessa laskennassa vaatisi kaksi funktio-kutsua. Deutschin pieni ja sievä esimerkki hämää vaatimattomuudellaan. Vuonna 1994 matemaatikko Peter Shor (1959–) esitti tavan jakaa nopeasti suuria kokonaislukuja tekijöihin kvanttietokoneella, ja viimeistään tuolloin kvanttilaskennan mahdollisuudet alkoivat selvitä. Shorin algoritmilla pystyttäisiin

siin murtamaan RSA-salaus, joka on tätä nykyä laajalti käytetty tietoliikenteessä.

Kvanttietokone oli kuuma puheenaihe siis jo kolmisen vuosikymmentä sitten. Moni varmaan ehti kyllästyä koko aiheeseen, kun ainuttakaan toimivaa kvanttietokoneetta ei pitkiin aikoihin saatu naputeltua kasaan. Kvanttietokoneiksi kutsuttuja härveleitä on kuitenkin pikkuhiljaa alkanut ilmaantua maailmalle. Epäilevät tuomaat silti jaksavat mutista, että tokkopa nuo ihan ehtoja kvanttikoneita ovat. Mene, tiedä. Jari epäilee ihmisen kuussakäyntiäkin huijaukseksi. Joka tapauksessa Googlella on kvanttietokoneeksi väitetty laite. Kuvassa se näyttää mustalta laatikolta. Joku on spreijannut hohtavanvalkoisen tägin laatikon kylkeen. Mikä sitten on se homman juju, joka tekee kvanttilaskennasta (ainakin teoriassa) niin moninkertaisesti tehokkaampaa kuin perinteisellä vanhan ajan bittikoneella suoritettu laskenta? Deutschin pelkistetty esimerkki antaa mielestäni oivan vastauksen kysymykseen, ja siksi käyn esimerkin valmisteluineen yksityiskohtia myöten läpi. Muuta ei tähän artikkeliin sitten mahdukaan.

Kubitti

Tavallisen tietokoneen bitti on muuttuja, joka voi olla jommassa kummassa tiloista $\mathbf{0}$ ja $\mathbf{1}$. Kvanttietokoneessa bitin korvaa **kubitti**. Sen tilat ovat muotoa $\alpha\mathbf{0} + \beta\mathbf{1}$, missä α ja β ovat ehdon $|\alpha|^2 + |\beta|^2 = 1$ toteuttavia kompleksilukuja. Mahdollisia tiloja on siis äärettömän

monta. Kubitin tila on hyvä ajatella vektorisummana, jonka termeinä ovat kaksi keskenään kohtisuoraa yksikkövektoria $\mathbf{0}$ ja $\mathbf{1}$ kompleksiluvuilla α ja β kerrottuina.¹ Tuttuun reaaliseseen tasovektoriin nähden erona on vain omituinen tapa merkitä kantavektoreita ja se, että kertoimet ovat kompleksilukuja. Luultavasti geometrisen mielikuvan luominen kompleksikertoimisista vektoreista on hankalaa. Jos näin on, lukijaa kehoitetaan ajattelemaan algebrallisesti, ei geometrisesti. Kubitti pystytään toteuttamaan reaalimaailmassa, mutta tässä artikkelissa tarkastellaan ainoastaan kvanttilaskennan matemaattista mallia.

Kubitin **arvo** on skalaari. Täten se on eri asia kuin tila. Arvon määrittämistä kutsutaan mittaamiseksi, ja arvona voi olla ainoastaan joko 0 tai 1. Kubitin sisäisen tilan kertoimia α ja β ei pystytä saamaan selville mittauksella, vaan niiden merkitys on seuraava: mitaustulos eli kubitin arvo on 0 todennäköisyydellä $|\alpha|^2$ ja 1 todennäköisyydellä $|\beta|^2$. Arvo on siis satunnaisluku. Jos kuitenkin $\beta = 0$ eli kubitin tila on muotoa $\alpha\mathbf{0} + \mathbf{01} = \alpha\mathbf{0}$, missä $|\alpha| = 1$, mittauksen tulos on 0 todennäköisyydellä 1. Samoin jos $\alpha = 0$ eli kubitti on tilassa $\mathbf{00} + \beta\mathbf{1} = \beta\mathbf{1}$, $|\beta| = 1$, mittauksen tulos on 1 todennäköisyydellä 1. Tiloja $\mathbf{0}$ ja $\mathbf{1}$ sanotaan **ominaistiloiksi**,² tilat $\alpha\mathbf{0} + \beta\mathbf{1}$, $\alpha\beta \neq 0$, ovat **superpositiotiloja**. Ominaitilat vastaavat klassisen bitin tiloja. Mittauksessa kubitti ns. romahtaa jompaan kumpaan ominaitilaan: välittömästi mittauksen jälkeen kubitin tila on $\mathbf{0}$ (mitaustulos 0) tai $\mathbf{1}$ (mitaustulos 1). Kvanttifiysiikassa on hyväksytty ajatus, että havainto edellyttää havaittavan kohteen häiritsemistä tavalla, joka yleensä muuttaa kohteen tilaa.

Kvanttirekisteri

Yhden tai useamman kubitin jonoja kutsutaan **rekistereiksi**. Kahden kubitin rekisterin tila Ψ yleisessä muodossaan ominaitilojen avulla esitettynä on

$$\Psi = \gamma_0\mathbf{00} + \gamma_1\mathbf{01} + \gamma_2\mathbf{10} + \gamma_3\mathbf{11},$$

$$|\gamma_0|^2 + |\gamma_1|^2 + |\gamma_2|^2 + |\gamma_3|^2 = 1.$$

Kertoimien todennäköisyystulkinta on luonnollisesti sellainen, että rekisterin mittausta johtaa esim. tilaan $\mathbf{10}$ todennäköisyydellä $|\gamma_2|^2$. Rekisterin kubitit voidaan mitata erikseen. Esim. oikeanpuoleisen kubitin arvo on 0 todennäköisyydellä $|\gamma_0|^2 + |\gamma_2|^2$. Rekisterin tila noudattaa ristiinkertomissääntöä

$$(\alpha_0\mathbf{0} + \beta_0\mathbf{1})(\alpha_1\mathbf{0} + \beta_1\mathbf{1}) =$$

$$\alpha_0\alpha_1\mathbf{00} + \alpha_0\beta_1\mathbf{01} + \beta_0\alpha_1\mathbf{10} + \beta_0\beta_1\mathbf{11}.$$

Huomaa, että yhtälön vasemmalla puolella rekisterin tila on esitetty liittämällä kaksi kubitin tilaa pariaksi, kun taas oikealla puolella esiintyy vain ominaitilapareja, so. kahden kubitin rekisterin ominaitiloja, skalaareilla kerrottuna.³ Kvanttitietokoneen kummallisiin piirteisiin kuuluu rekisteritilojen superpositioon liittyvä mahdollisuus **lomittuneisiin** (engl. *entangled*) tiloihin, joita ei voida esittää vasemmanpuoleisessa "tulomuodossa". Esimerkiksi

$$\Psi_0 = (\mathbf{00} + \mathbf{11})/\sqrt{2} = \frac{1}{\sqrt{2}}\mathbf{00} + \frac{1}{\sqrt{2}}\mathbf{11}$$

on lomittunut tila. Sen sijaan

$$\Psi_1 = (\mathbf{00} + \mathbf{01} + \mathbf{10} + \mathbf{11})/2 = (\mathbf{0} + \mathbf{1})(\mathbf{0} + \mathbf{1})/2$$

ei ole lomittunut. Kummassakin tiloista Ψ_0 ja Ψ_1 yksittäiseen kubittiin liittyvät todennäköisyydet ovat samat. Esim. vasemmanpuoleinen kubitti saa mittauksessa arvon 0 todennäköisyydellä 1/2 siitä riippumatta, onko rekisteri tilassa Ψ_0 vai Ψ_1 . Lomittuneisuus ilmenee kubittien arvojen korrelaationa: tilassa Ψ_0 vasemmanpuoleiselle kubitille saatu arvo eli mitaustulos määrää täysin oikeanpuoleisen kubitin arvon ja päinvastoin.

Portit

Kubittien tiloja muunnetaan kvanttitietokoneessa **porteiksi** kutsuttujen komponenttien avulla. Voidaan ajatella, että kubitti laitetaan menemään portista läpi, jolloin sen tila muuttuu toiseksi. Matemaattisessa mielessä portti on funktio, jolle syötetään tila, ja joka palauttaa arvonaan muunnetun tilan. Yksinkertainen esimerkki portista on **EI-portti**. Sen vaikutus kubittiin ilmaistaan yläviivan avulla: tila ψ muuttuu portin läpi kulkiessaan tilaksi $\bar{\psi}$. Ominaitiloille

$$\bar{\mathbf{0}} = \mathbf{1}, \quad \bar{\mathbf{1}} = \mathbf{0}.$$

Toinen esimerkki on **Hadamard-portti** H , jolle

$$H(\mathbf{0}) = \frac{1}{\sqrt{2}}(\mathbf{0} + \mathbf{1}), \quad H(\mathbf{1}) = \frac{1}{\sqrt{2}}(\mathbf{0} - \mathbf{1}).$$

Kun ominaitilojen muuntuminen portissa G tiedetään, muiden tilojen muuntuminen nähdään säännöllä

$$G(\alpha\mathbf{0} + \beta\mathbf{1}) = \alpha G(\mathbf{0}) + \beta G(\mathbf{1}).$$

¹Lihavoidut symbolit $\mathbf{0}, \mathbf{1}, \mathbf{x}, \mathbf{y}, \mathbf{f}, \boldsymbol{\psi}, \dots$ tarkoittavat vektoreita, lihavoimattomat $0, 1, \alpha, \beta, \gamma, \dots$ skalaareita (so. kompleksilukuja). Korostettakoon sitä, että $\mathbf{0}$ ei ole vektorilaskennan nollavektori hämäävästä merkinnästä huolimatta.

²Tilojen $\mathbf{0}$ ja $\mathbf{1}$ kutsuminen ominaitiloiksi saattaa häiritä valistunutta lukijaa (myös $\alpha\mathbf{0}$ ja $\beta\mathbf{1}$ ovat ominaitiloja; lisäksi herää kysymys, minkä operaattorin ominaitiloja). Usein käytetään niimityksiä *kantatila* tai *laskennallinen kantatila* (vektoriavaruuden kantakaan ei ole yksikäsitteisesti määrätty).

³Kvanttitietokoneen ominaitiloille $\mathbf{0}$ ja $\mathbf{1}$ käytetään tavallisesti merkintöjä $|0\rangle$ ja $|1\rangle$, ja rekisterin ominaitilat ovat tensorituloja, esimerkiksi $\mathbf{01}$ on tensoritulo $|0\rangle \otimes |1\rangle$, lyhyemmin merkittynä $|0, 1\rangle$ tai $|01\rangle$. Ristiinkertomissääntö tulee tensoritulon bilineaarisuudesta. Lukijan ei tarvitse tuntea tässä mainittuja, kenties outoja käsitteitä.

Esimerkiksi

$$\mathbf{H}\left(\frac{1}{2}\mathbf{0} + \frac{\sqrt{3}}{2}\mathbf{1}\right) = \frac{1}{2}\mathbf{H}(\mathbf{0}) + \frac{\sqrt{3}}{2}\mathbf{H}(\mathbf{1}) = \frac{1+\sqrt{3}}{2\sqrt{2}}\mathbf{0} + \frac{1-\sqrt{3}}{2\sqrt{2}}\mathbf{1}.$$

Vastaava sääntö pätee ominaistilapareille.⁴ Lukijalle jätetään harjoitustehtäväksi osoittaa, että kubitin tila palautuu ennalleen sen kulkiessa kahden perättäisen Hadamard-portin lävitse, ts. $\mathbf{H}(\mathbf{H}(\psi)) = \psi$. Siinä mielessä Hadamard-portti muistuttaa EI-porttia.

David Deutschin esimerkki

Miten kvanttietokone nopeuttaa laskentaa verrattuna tavalliseen tietokoneeseen? Kahden kubitin rekisterin tapauksessa ideana on muodostaa alkutilasta $\mathbf{00}$ kvanttiporteilla superpositiotila

$$(\mathbf{00} + \mathbf{01} + \mathbf{10} + \mathbf{11})/2,$$

joka on siis yhden ainoan kubittiparin tila. Siinä ovat mukana kaikki neljä mahdollista kubitin ominaistilaparia, jotka vastaavat neljää bittiparia. Tämän jälkeen suoritetaan haluttu laskenta kerran tälle ainokaiselle kahden kubitin rekisteritilalle. Klassisella tietokoneella laskenta jouduttaisiin suorittamaan tyypillisesti jokaiselle neljälle bittiparille erikseen. Laskennan suorittavaa komponenttia sanotaan **oraakkeliksi**. Nopeusero klassisen ja kvanttilaskennan välillä tulee selvemmäksi n kubittia käsittävän rekisterin yhteydessä, kun n on suuri luku. Silloin kvanttietokoneen oraakkelin kertakutsua vastaa klassisessa laskennassa 2^n kutsua. Esimerkiksi tapauksessa $n = 20$ on $2^n = 1048576$. Lopuksi oraakkelin antama tulos pitää osata tulkita. Tulkinta onnistuu, jos tulos kyetään muuntamaan kvanttiporteilla sellaiseksi tilaksi, josta haluttu tieto saadaan mitattua.

Kvanttilaskennan vaiheita kuvataan **unitaariopeeraattoreilla**. Tässä yhteydessä ei tarvitse tarkkaan tietää, mitä unitaarisuus tarkoittaa. Unitarisuuden vaatimuksesta kuitenkin johtuu, että kvanttilaskennassa jokaisen operaation tulee olla bijektiivinen. Operaatio on matemaattisessa mielessä kuvaus, joka liittää rekisterin jokaiseen mahdolliseen tilaan (tila ennen operaatiota) yksikäsitteisen lopputilan (tila operaation suorittamisen jälkeen), ja tuon kuvauksen tulee olla bijektio. Siitä johtuen mikä tahansa tiloja toisikseen muuntava funktio ei kelpaa oraakkeliksi.

Deutsch on artikkelissaan [2] esittänyt minimalistisen esimerkin, miten kvanttilaskentaa hyväksikäyttäneen selvitetään, onko binäärinen funktio $f : \{0, 1\} \rightarrow \{0, 1\}$ vakio vai ei. Tehtävä on hyvin pelkistetty, sillä tällaisia

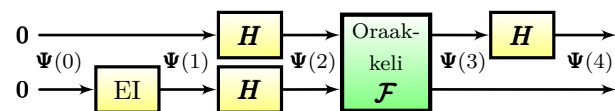
funktioita on olemassa vain neljä erilaista. Erinomaisessa luennoissaan [1] Deutsch esittelee parannellun version esimerkistään. Klassista laskentaa käyttäen ongelman ratkaisu vaatii funktion arvojen $f(0)$ ja $f(1)$ määrittämisen, jolloin funktion f arvon laskevaa oraakkelia kutsutaan kahteen kertaan. Kvanttilaskennassa pärjätään yhdellä kutsulla. Yksinkertaisuuden vuoksi ja sellittelyjen välttämiseksi funktio f tulkitaan ominaistilojen funktioksi

$$f : \{0, 1\} \rightarrow \{0, 1\}, \quad x \mapsto f(x).$$

Bijektiivisyysvaatimuksesta johtuen f sellaisenaan ei kelpaa oraakkeliksi, mutta kubittipareille muunnettu operaattori

$$\mathcal{F} : xy \mapsto \begin{cases} xf(x), & y = 0, \\ x\overline{f(x)}, & y = 1, \end{cases} \quad x, y \in \{0, 1\},$$

kelpaa. Jos esim. $f(0) = f(1) = 1$, operaation \mathcal{F} jälkeen saadaan $\mathcal{F}(\mathbf{10}) = \mathbf{1f(1)} = \mathbf{11}$ ja $\mathcal{F}(\mathbf{01}) = \mathbf{0f(0)} = \mathbf{0\bar{1}} = \mathbf{00}$. Bijektiivisyyden varmistamiseksi lukijaa kehoitetaan etsimään kuvaukselle \mathcal{F} käänteiskuvaus \mathcal{F}^{-1} kiinteällä f . Riittää, kun käänteiskuvaus lauseke lausutaan ominaistilapareille samaan tapaan kuin kuvauksen \mathcal{F} lauseke edellä.⁵ Oheiseen kuvaan on piirretty Deutschin ratkaisua vastaava lohkokaaevio. Symboli $\Psi(t)$ tarkoittaa rekisterin tilaa hetkellä t , missä "aikamuuttuja" t kasvaa jokaisen operaation jälkeen yhdellä.



Laskennan aluksi rekisterin tila alustetaan pariaksi $\mathbf{00}$:

$$\Psi(0) = \mathbf{00}.$$

Seuraavaksi oikeanpuoleiseen (kuvassa alempaan) kubittiin sovelletaan EI-operaatiota:

$$\Psi(1) = \mathbf{01}.$$

Kumpaankin kubitin tehtävän Hadamardin jälkeen saadaan

$$\Psi(2) = \frac{1}{2}(\mathbf{0} + \mathbf{1})(\mathbf{0} - \mathbf{1}) = \frac{1}{2}(\mathbf{00} + \mathbf{10} - \mathbf{01} - \mathbf{11}),$$

jolloin oraakkeli tuottaa tilan

$$\Psi(3) = \frac{1}{2}(\mathbf{0}f(\mathbf{0}) + \mathbf{1}f(\mathbf{1}) - \mathbf{0}\overline{f(\mathbf{0})} - \mathbf{1}\overline{f(\mathbf{1})}).$$

Alunperin piti selvittää, onko f vakiofunktio ($f(0) = f(1)$) vai ei ($f(0) \neq f(1)$). Tapaukset käsitellään erik-

⁴Lineaarialgebraa tuntevalle lukijalle muistutetaan, että kysymys on lineaarisen kuvauksen yksikäsitteisestä laajentamisesta koko vektoriaruuteen tiedettäessä kuinka kanta kuvautuu.

⁵Myös vastaavuus $f \mapsto \mathcal{F}$, joka liittää funktion f bijektion \mathcal{F} , on bijektiivinen.

seen ottamalla käyttöön lyhennysmerkintä $\mathbf{f}(\mathbf{0}) = \psi$:

$$\begin{aligned} \mathbf{f}(\mathbf{0}) = \mathbf{f}(\mathbf{1}) &\Rightarrow \Psi(3) = \frac{1}{2}(\mathbf{0}\psi + \mathbf{1}\psi - \mathbf{0}\bar{\psi} - \mathbf{1}\bar{\psi}) \\ &= \frac{1}{2}(\mathbf{0} + \mathbf{1})(\psi - \bar{\psi}), \end{aligned}$$

$$\begin{aligned} \mathbf{f}(\mathbf{0}) = \overline{\mathbf{f}(\mathbf{1})} &\Rightarrow \Psi(3) = \frac{1}{2}(\mathbf{0}\psi + \mathbf{1}\bar{\psi} - \mathbf{0}\bar{\psi} - \mathbf{1}\psi) \\ &= \frac{1}{2}(\mathbf{0} - \mathbf{1})(\psi - \bar{\psi}). \end{aligned}$$

Siis

$$\Psi(3) = \begin{cases} \frac{1}{\sqrt{2}}\mathbf{H}(\mathbf{0})(\psi - \bar{\psi}), & \mathbf{f}(\mathbf{0}) = \mathbf{f}(\mathbf{1}), \\ \frac{1}{\sqrt{2}}\mathbf{H}(\mathbf{1})(\psi - \bar{\psi}), & \mathbf{f}(\mathbf{0}) \neq \mathbf{f}(\mathbf{1}). \end{cases}$$

Kun muistetaan, että Hadamard on oma käänteisoperaattorinsa eli $\mathbf{H}(\mathbf{H}(\mathbf{x})) = \mathbf{x}$, vasemmanpuoleiseen kubittiin sovellettuna Hadamard antaa viimeisessä vaiheessa

$$\Psi(4) = \begin{cases} \frac{1}{\sqrt{2}}\mathbf{0}(\psi - \bar{\psi}), & \mathbf{f}(\mathbf{0}) = \mathbf{f}(\mathbf{1}), \\ \frac{1}{\sqrt{2}}\mathbf{1}(\psi - \bar{\psi}), & \mathbf{f}(\mathbf{0}) \neq \mathbf{f}(\mathbf{1}). \end{cases}$$

Alkuperäiseen ongelmaan saadaan ratkaisu mittamalla lopuksi vasemmanpuoleinen kubitti.

Kannattaa panna merkeille, että kvanttilaskennassa ei ole sijaa satunnaisuudelle. Jokainen laskennan vaihe suoritetaan deterministisellä unitaarioperaattorilla. Päätösvaihe eli kvanttietokoneen antaman tuloksen mittaus on ainoa paikka, missä satunnaisuutta voisi esiintyä. Deutschin esimerkissä satunnaisuus on eliminoitu muuntamalla oraakkelin antama tulos tulomuotoon, jossa vastauksen sisältävä ensimmäinen kubitti on ominaistilassa.

Viitteet

- [1] Deutsch, D.: *Lectures on Quantum Computation. Lecture 5: A Quantum Algorithm*. Videotallenne. Katsottavana (viittauspäivä 18.7.2017): http://www.quiprocone.org/Protected/DD_lectures.htm
- [2] Deutsch, D.: *Quantum theory, the Church-Turing principle and the universal quantum computer*. Proceedings of the Royal Society of London A **400**, ss. 97-117 (1985).

Verkko-Solmussa on ilmestynyt 100 matematiikan ylioppilastehtävää itsenäisyyden ajalta

Tehtävien keräämiseen on osallistunut kymmenen matemaatikkoa. Tehtävät on jaoteltu kymmenen vuoden jaksoihin, ratkaisut ovat eri tiedostoissa. Sekä tehtävät että ratkaisut ovat luettavissa ja tulostettavissa osoitteessa

matematiikkalehtisolmu.fi/100yo.html

Tehtävät antavat käsityksen siitä, miten matematiikan opetus koulussa on muuttunut ajan myötä. Varmaan on monillekin mielenkiintoista yrittää ratkoa näitä tehtäviä.

Valtioneuvoston kanslia on 19.6.2017 liittänyt hankkeen Suomen itsenäisyyden satavuotisjuhlavuoden 2017 ohjelmaan:

suomifinland100.fi/project/100-matematiikan-ylioppilastehtavaa-itsenaisyyden-ajalta/