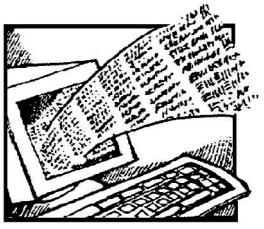


Lomittajalle töitä

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 maatiloilta 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 kvanttitietokone 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 kvanttitietokoneissa valtava määrä eri vaihtoehtoja voitaisiin prosessoida samanaikaisesti. Vuonna 1985 fyysikko David Deutsch (1953−) julkaisi yksinkertaisen esimerkin kvanttilaskennasta. Siinä suoritetaan yhdellä funktiokutsulla tehtävä, joka klassisessa laskennassa vaatisi kaksi funktiokutsua. Deutschin pieni ja sievä esimerkki hämää vaatimattomuudellaan. Vuonna 1994 matemaatikko Peter Shor (1959−) esitti tavan jakaa nopeasti suuria kokonaislukuja tekijöihin kvanttitietokoneella, ja viimeistään tuolloin kvanttilaskennan mahdollisuudet alkoivat selvitä. Shorin algoritmilla pystyttäisiin murtamaan RSA-salaus, joka on tätä nykyä laajalti käytetty tietoliikenteessä.

Kvanttitietokone oli kuuma puheenaihe siis jo kolmisen vuosikymmentä sitten. Moni varmaan ehti kyllästyä koko aiheeseen, kun ainuttakaan toimivaa kvanttitietokonetta ei pitkiin aikoihin saatu naputeltua kasaan. Kvanttitietokoneiksi 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 kvanttitietokoneeksi 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 wanhan 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 **0** ja **1**. Kvanttitietokoneessa 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 reaaliseen 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 kehotetaan 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: mittaustulos 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 $\alpha\mathbf{0} + 0\mathbf{1} = \alpha\mathbf{0}$, missä $|\alpha| = 1$, mittauksen tulos on 0 todennäköisyydellä 1. Samoin jos $\alpha = 0$ eli kubitti on tilassa $0\mathbf{0} + \beta\mathbf{1} = \beta\mathbf{1}$, $|\beta| = 1$, 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**. Ominaistilat vastaavat klassisen bitin tiloja. Mittauksessa kubitti ns. romahtaa jompaan kumpaan ominaistilaan: välittömästi mittauksen jälkeen kubitin tila on $\mathbf{0}$ (mittaustulos 0) tai $\mathbf{1}$ (mittaustulos 1). Kvanttifysiikassa 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 $\boldsymbol{\Psi}$ yleisessä muodossaan ominaistilojen avulla esitettynä on

$$\boldsymbol{\Psi} = \gamma_0\mathbf{00} + \gamma_1\mathbf{01} + \gamma_2\mathbf{10} + \gamma_3\mathbf{11},$$
$$|\gamma_0|^2 + |\gamma_1|^2 + |\gamma_2|^2 + |\gamma_3|^2 = 1.$$

Kertoimien todennäköisyystulkinta on luonnollisesti sellainen, että rekisterin mittaus 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 pariksi, kun taas oikealla puolella esiintyy vain ominaistilapareja, so. kahden kubitin rekisterin ominaistiloja, skalaareilla kerrottuina.[3] Kvanttitietokoneen kummallisiin piirteisiin kuuluu rekisteritilojen superpositioon liittyvä mahdollisuus **lomittuneisiin** (engl. *entangled*) tiloihin, joita ei voida esittää vasemmanpuoleisessa "tulomuodossa". Esimerkiksi

$$\boldsymbol{\Psi}_0 = (\mathbf{00} + \mathbf{11})/\sqrt{2} = \frac{1}{\sqrt{2}}\mathbf{00} + \frac{1}{\sqrt{2}}\mathbf{11}$$

on lomittunut tila. Sen sijaan

$$\boldsymbol{\Psi}_1 = (\mathbf{00} + \mathbf{01} + \mathbf{10} + \mathbf{11})/2 = (\mathbf{0} + \mathbf{1})(\mathbf{0} + \mathbf{1})/2$$

ei ole lomittunut. Kummassakin tiloista $\boldsymbol{\Psi}_0$ ja $\boldsymbol{\Psi}_1$ yksittäiseen kubittiin liittyvät todennäköisyydet ovat samat. Esim. vasemmanpuoleinen kubitti saa mittauksessa arvon 0 todennäköisyydellä 1/2 siitä riippumatta, onko rekisteri tilassa $\boldsymbol{\Psi}_0$ vai $\boldsymbol{\Psi}_1$. Lomittuneisuus ilmenee kubittien arvojen korrelaationa: tilassa $\boldsymbol{\Psi}_0$ vasemmanpuoleiselle kubitille saatu arvo eli mittaustulos 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 $\boldsymbol{\psi}$ muuttuu portin läpi kulkiessaan tilaksi $\overline{\boldsymbol{\psi}}$. Ominaistiloille

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

Toinen esimerkki on **Hadamard-portti** $\boldsymbol{H}$, jolle

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

Kun ominaistilojen muuntuminen portissa $\boldsymbol{G}$ tiedetään, muiden tilojen muuntuminen nähdään säännöllä

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

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

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

[3] Kvanttitietokoneen ominaistiloille $\mathbf{0}$ ja $\mathbf{1}$ käytetään tavallisesti merkintöjä $|0\rangle$ ja $|1\rangle$, ja rekisterin ominaistilat 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

$$\boldsymbol{H}\big(\tfrac{1}{2}\mathbf{0}+\tfrac{\sqrt{3}}{2}\mathbf{1}\big)=\tfrac{1}{2}\boldsymbol{H}(\mathbf{0})+\tfrac{\sqrt{3}}{2}\boldsymbol{H}(\mathbf{1})=\tfrac{1+\sqrt{3}}{2\sqrt{2}}\mathbf{0}+\tfrac{1-\sqrt{3}}{2\sqrt{2}}\mathbf{1}.$$

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

David Deutschin esimerkki

Miten kvanttitietokone 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 kvanttitietokoneen 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 **unitaarioperaattoreilla**. Tässä yhteydessä ei tarvitse tarkkaan tietää, mitä unitaarisuus tarkoittaa. Unitaarisuuden 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.

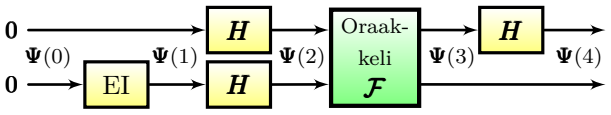
Deutsch on artikkelissaan [2] esittänyt minimalistisen esimerkin, miten kvanttilaskentaa hyväksikäyttäen selvitetään, onko binäärinen funktio $f:\{0,1\}\to\{0,1\}$ vakio vai ei. Tehtävä on hyvin pelkistetty, sillä tällaisia funktioita on olemassa vain neljä erilaista. Erinomaisessa luennossaan [1] Deutsch 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 selittelyjen välttämiseksi funktio f tulkitaan ominaistilojen funktioksi

$$\boldsymbol{f}:\{\mathbf{0},\mathbf{1}\}\to\{\mathbf{0},\mathbf{1}\},\quad \boldsymbol{x}\mapsto\boldsymbol{f}(\boldsymbol{x}).$$

Bijektiivisyysvaatimuksesta johtuen $\boldsymbol{f}$ sellaisenaan ei kelpaa oraakkeliksi, mutta kubittipareille muunnettu operaattori

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

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



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

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

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

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

Kumpaankin kubittiin tehtävän Hadamardin jälkeen saadaan

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

jolloin oraakkeli tuottaa tilan

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

Alunperin piti selvittää, onko $\boldsymbol{f}$ vakiofunktio $\big(\boldsymbol{f}(\mathbf{0})=\boldsymbol{f}(\mathbf{1})\big)$ vai ei $\big(\boldsymbol{f}(\mathbf{0})=\overline{\boldsymbol{f}(\mathbf{1})}\big)$. Tapaukset käsitellään erik-

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

[5] Myös vastaavuus $\boldsymbol{f}\mapsto\boldsymbol{\mathcal{F}}$, joka liittää funktioon $\boldsymbol{f}$ bijektion $\boldsymbol{\mathcal{F}}$, on bijektiivinen.

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

$$\begin{aligned}\boldsymbol{f}(\mathbf{0}) = \boldsymbol{f}(\mathbf{1}) \;\Rightarrow\; \boldsymbol{\Psi}(3) &= \tfrac{1}{2}\big(\mathbf{0}\boldsymbol{\psi} + \mathbf{1}\boldsymbol{\psi} - \mathbf{0}\overline{\boldsymbol{\psi}} - \mathbf{1}\overline{\boldsymbol{\psi}}\big)\\ &= \tfrac{1}{2}\big(\mathbf{0}+\mathbf{1}\big)\big(\boldsymbol{\psi} - \overline{\boldsymbol{\psi}}\big),\\ \boldsymbol{f}(\mathbf{0}) = \overline{\boldsymbol{f}(\mathbf{1})} \;\Rightarrow\; \boldsymbol{\Psi}(3) &= \tfrac{1}{2}\big(\mathbf{0}\boldsymbol{\psi} + \mathbf{1}\overline{\boldsymbol{\psi}} - \mathbf{0}\overline{\boldsymbol{\psi}} - \mathbf{1}\boldsymbol{\psi}\big)\\ &= \tfrac{1}{2}\big(\mathbf{0}-\mathbf{1}\big)\big(\boldsymbol{\psi} - \overline{\boldsymbol{\psi}}\big).\end{aligned}$$

Siis

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

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

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

Alkuperäiseen ongelmaan saadaan ratkaisu mittaamalla lopuksi vasemmanpuoleinen kubitti.

Kannattaa panna merkille, että kvanttilaskennassa ei ole sijaa satunnaisuudelle. Jokainen laskennan vaihe suoritetaan deterministisellä unitaarioperaattorilla. Päätösvaihe eli kvanttitietokoneen 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/`