Tarinoita kvanttilaskennasta

Mika Hirvensalo
Matematiikan laitos
Turun yliopisto
mikhirve@utu.fi

1 Hieman historiaa

Kvanttilaskennan, sen syntyhistorian ja merkityksen ymmärtämiseksi on syytä aluksi perehtyä ainakin pintapuolisesti kvanttifysiikan kehitykseen.

1.1 Kvanttifysiikan kehitys

Suunnilleen 1800-luvun puolivälissä käsitys valosta (ja yleisemmin *sähkömagneettisesta säteilystä*) näytti vakiintuneen: valo ymmärrettiin Huygensin mallin mukaiseksi *aaltoliikkeeksi*, jossa aaltoilevat toisiaan vastaan kohtisuorassa olevat sähkö- ja magneettikentät. Samalla Newtonin malli, jossa valo etenee *hiukkasvirtana*, näytti osoittautuneen vääräksi. Kuitenkin 1800-luvun loppupuolella nk. *mustan kappaleen*[1] säteily osoittautui ilmiöksi, jossa teoria ja koetulokset olivat selvästi ristiriidassa. Mustan kappaleen säteilyn voimakkuutta eri aallonpituuksilla ja eri lämpötiloissa yritettiin selittää ainakin kahden toisensa pois sulkevan teorian avulla, mutta vasta vuonna 1900 Max Planck julkaisi ensimmäisen havaintoihin yhtyvän teoreettisen selityksen mustan kappaleen säteilylle.

Planckin säteilylain erikoinen piirre oli se, että lakia johtaessaan Planck turvautui seuraavaan oletukseen: mustan kappaleen säteily erittyy "säteilypaketteina", joiden energia E on verrannollinen säteilyn taajuuteen ν, siis $E = h\nu$. Nykyisin verrannollisuuskerrointa h kutsutaan *Planckin vakioksi*. Planckin olettamus oli varsin erikoinen sillä jos sähkömagneettinen säteily olisikin aaltoliikkeen sijasta pienten hiukkasten virtaa, ei koko olettamusta tarvittaisi, vaan se olisi suora seuraus säteilyn olemuksesta. Toisaalta taas fyysikot olivat jo miltei puoli vuosisataa aiemmin omaksuneet sen näkemyksen,

[1] Musta kappale on kuvitteellinen esine, joka pystyy sekä vastaanottamaan että lähettämään sähkömagneettista säteilyä kaikilla aallonpituuksilla. Pieni aukko sisältä noetussa ontossa kappaleessa on varsin hyvä mustan kappaleen likimääräistys kokeellisia tarkoituksia varten.

että sähkömagneettinen säteily on aaltoliikettä. Planckin säteilylaki herätti täten epäilyksen, että sähkömagneettisella säteilyllä voisi olla *aaltoluonteen* lisäksi *hiukkasluonne*.

Vuonna 1905 Albert Einstein selitti nk. *valosähköisen ilmiön* Planckin otaksumaan perustuen. Einsteinin menestyksekäs selitys tuki edelleen hiukkasluonteen olemassaoloa. Tässä yhteydessä on syytä mainita, että Einsteinille myönnettiin Nobelin palkinto vuonna 1921 valosähköisen ilmiön selittämisestä; suhteellisuusteoriaa ei mainittu syynä Nobelin palkinnon myöntämiseen.

Niels Bohr toi vuonna 1912 esille toisentyyppisen, vetyatomiin liittyvän ilmiön: varattuna hiukkasena ydintä kiertävän elektronin tulisi Maxwellin säteilylakien mukaan jatkuvasti lähettää sähkömagneettista säteilyä. Jos näin todella tapahtuisi, tulisi sen myös jatkuvasti menettää energiaa ja lopulta syöksyä atomin ytimeen. Niels Bohr selitti atomin stabiilisuuden otaksumalla, että elektroneilla, joita perinteisesti pidettiin hiukkasina, on myös aaltoluonne. Elektronien aaltoluonne sai vahvistusta Davidssonin ja Germerin interferenssikokeessa vuonna 1927, mutta jo 1924 Louis de Broglie esitti ajatuksen, että kaikilla hiukkasilla on myös aaltoluonne.

Edellä on lueteltu esimerkkejä ilmiöistä (ja niiden selityksistä), jotka saivat fyysikot 1900-luvun alkupuoliskolla vakuuttuneiksi siitä, että on tarpeen kehittää uudentyyppistä hiukkas- ja säteilyfysiikkaa. Luetelluista ilmiöistä käy myös ilmi, että tämän uudentyyppisen teorian tulisi pystyä kuvailemaan ja selittämään sellaisten objektien käyttäytymistä, joilla on sekä hiukkas- että aaltoluonne. Tätä uudentyyppistä fysiikka kutsutaan nykyisin kvanttifysiikaksi. Kvanttifysiikkaa on halki 1900-luvun hahmoteltu nykyiseen muotoonsa, mutta yhä useat perustavanlaatuiset ongelmat ovat ratkaisematta.

1.2 Kvanttilaskennan varhaisvaiheet

Usein katsotaan kvanttilaskennan syntyneen Richard Feynmanin artikkelin [15] myötä vuonna 1982. Kyseisessä artikkelissa Feynman tarkasteli suljettua fysikaalista systeemiä, jossa on R hiukkasta, ja keskittyi tämän systeemin simulointiin tietokoneella. Feynmanin tarkastelemassa simulaatiossa kunkin hiukkasen paikka ja liikemäärä ovat tiedossa tietyllä tarkkuudella. Feynman oli heti oivaltanut, että mikäli systeemi on klassisen fysiikan mukainen, ei simulointi tuota suuria ongelmia. Tällöin nimittäin kunkin hiukkasen kuvaamiseksi riittää paikka ja liikemäärä, ja simuloiva (deterministinen) ohjelma voi käsitellä kutakin hiukkasta yksitellen. Täten siis systeemiä, jossa on R hiukkasta, voidaan tietokoneella simuloida *lineaarisessa* ajassa hiukkasten lukumäärään R nähden (paikka- ja liikemääräkoordinaatteja käsitellään kiinteällä tark-

kuudella, joten aritmeettisten operaatioiden suorittamiseen kuluva aika voidaan katsoa vakioksi).

Toisin kuitenkin käy, jos oletetaan, että edellä mainittu systeemi onkin kvanttifysiikan mukaan käyttäytyvä. Tällöin hiukkasten käyttäytymistä kuvaa aaltofunktio, joka riippuu *kaikista* hiukkasista, ja tällaisen systeemin simulointi (ilmeisellä tavalla) veisi eksponentiaalisen ajan hiukkasten määrään nähden. Feynman ei nähnyt mitään keinoa kiertää tätä eksponentiaalista hidastumista, ei edes siinä tapauksessa, että simuloiva deterministinen algoritmi korvattaisiin *todennäköisyysalgoritmilla*. Lopulta Feynman päätyi otaksumaan, että perinteisillä tietokoneilla ei kvanttifysikaalista systeemiä voida simuloida ilman, että simulaatioaika kasvaa eksponentiaalisesti.[2]

Feynman tarkasteli myös sitä mahdollisuutta, että simuloiva tietokone itse toimisi kvanttifysiikan periaatteiden mukaisesti ja tuli siihen tulokseen, että tällaisella koneella voitaisiin varsin hyvin simuloida edellä kuvattua kvanttifysikaalista hiukkassysteemiä ilman eksponentiaalista viivettä. Yhdistettynä "klassisen" simuloinnin vaikeuksiin tämä johtopäätös sisältää, joskin hieman peiteltynä, kvanttilaskennan kannalta mitä oleellisimman huomion: vaikuttaa siltä, että joissain tehtävissä kvanttifysiikan erikoispiirteitä hyödyntävä tietokone, *kvanttitietokone*, olisi eksponentiaalisesti tehokkaampi kuin perinteiset tietokoneet.

Feynmanin työn jälkeen merkittävin kvanttilaskennan kehittäjä lienee David Deutsch. Artikkeleissaan [12] (1985) ja [13] (1989) Deutsch määritteli *Turingin kvanttikoneen* ja *kvanttipiirit* sekä osoitti, että on olemassa *universaali* Turingin kvanttikone, joka käytännnössä merkitsee ohjelmoitavaa kvanttitietokonetta.

Jo ensimmäisessä kvanttilaskentaa käsittelevässä työssään [12] Deutsch antoi esimerkin siitä, että kvanttitietokone voi säästää laskenta-aikaa. Tämän esimerkin yleistys löytyy artikkelista [14]. Kyseinen Deutschin ja Richard Jozsan artikkeli [14] (1992) on historiallisesti merkittävä, sillä mainitussa työssä esitettiin ensimmäistä kertaa laskennallinen ongelma, joka voidaan ratkaista kvanttitietokoneella lineaarisessa ajassa, mutta joka vaatii eksponentiaalisen ajan perinteisiltä tietokoneilta (todennäköisyysalgoritmeja ei tässä sallittu). Deutschin ja Jozsan ongelma on varsin helppo kuvata: on luvattu, että tarkasteltava funktio $f : \{0,1\}^n \to \{0,1\}$ on joko vakiofunktio tai tasapainotettu (nollia ja ykkösiä tulee arvoiksi sama määrä). Syötteen suurudeksi katsotaan n ja tehtävänä on selvittää, onko f vakio vai tasapainotettu.

[2] Toisin kuin kirjallisuudessa toisinaan mainitaan, ei Feynman tätä otaksumaa todistanut. Feynmanin otaksuma on yhä nykyään yksi tärkeimmistä avoimista ongelmista kvanttilaskennan alalla.

Funktiota f ei kuitenkaan anneta syötteenä perinteisessä mielessä, vaan sen arvoja voidaan kysellä yksi kerrallaan. Lisäksi katsotaan, että yhden arvon kysymiseen käytetään yksi laskenta-askel. Voidaan siis ajatella, että funktion f määrittely on taulukoidussa muodossa jonkin toisen osapuolen hallussa ja että algoritmi voi ainoastaan kysellä funktion arvoja yksi kerrallaan.

Kuvatunkaltaista funktiota kutsutaan yleensä *oraakkeliksi* [27] tai tarkemmin sanoen, oraakkelin rajoittumaksi tietyn pituisille sanoille. Kvanttilaskennan yhteydessä tämänkaltaista funktiota kutsutaan kuitenkin yleensä *mustaksi laatikoksi.*

Jos sallitaan todennäköisyysalgoritmit, ei ole vaikeaa selvittää, onko f vakiofunktio vaiko tasapainotettu. Tällöin on nimittäin voidaan arpoa kaksi eri bittijonoa ja kysyä, minkä arvon funktio näillä saa. Jos f saa saman arvon valituilla jonoilla, päätetään, että funktio f on vakio. Muussa tapauksessa päätetään, että f on tasapainotettu. On helppo todeta, että tällä tavoin toimien päätös on oikea vähintään viidenkymmenen prosentin todennäköisyydellä, mikäli f todella täyttää luvatut ehdot (on joko vakio tai tasapainotettu). Jos taas vaaditaan *varmaa* vastausta, on välttämätöntä kysyä funktion arvoa yli puolella mahdollisista bittijonoista ($2^{n-1}+1$ kysymystä riittää). Deutsch ja Jozsa esittivät kvanttialgoritmin, joka antaa varman tuloksen kysymällä funktion f arvoa *yhden* kerran (ja joka käyttää lineaarisen määrän muita kvanttioperaatioita).

Deutschin ja Jozsan tulos ei kuitenkaan anna mitään osviittaa siitä, miten aiemmin mainittu Feynmanin otaksuma voitaisiin todistaa, sillä kyseinen tulos ei ollut absoluuttinen, vaan sidottu tietyntyyppiseen mustaan laatikkoon. Yleisesti ottaen Deutschin työt ovat keskittyneet kuitenkin pääasiassa kvanttilaskennan periaatteellisiin kysymyksiin, eivät niinkään laskennan kompleksisuuteen.

Artikkelissa [32] Daniel Simon esitti ensimmäisenä (1994) laskennallisen tehtävän, joka voidaan ratkaista kvanttitietokoneella suurella todennäköisyydellä polynomiaalisessa ajassa, mutta joka vaatii eksponentiaalisen ajan perinteisillä tietokoneilla, vaikka sallittaisiin todennäköisyysalgoritmit. Simonin tulos ei myöskään ratkaise Feynmanin otaksumaa sillä siinäkin esiintyy "musta laatikko".

Varsinaiseksi kuuluisuudeksi kvanttilaskenta nousi Peter Shorin artikkelin [30] myötä vuonna 1994. Kyseisessä työssään Shor esitti kvanttitietokoneelle suunnitellun algoritmin, jonka avulla annettu kokonaisluku voitaisiin jakaa tekijöihin polynomiaalisessa[3]

[3]Shorin algoritmi toimii ajassa $O(n^3 \log n)$, missä n jaettavan luvun pituus. O-merkintään liittyvä vakio riippuu siitä, kuinka suurella todennäköisyydellä halutaan algoritmin löytävän tekijät.

ajassa (samaisessa artikkelissa oli myös polynomiajassa toimiva algoritmi diskreetin logaritmin laskemiseen, mutta tämä algoritmi jäi aluksi vähäisemmälle huomiolle). Tekijöihinjaon merkitys on varsin laajalti tunnettu: niin kutsutun RSA-salakirjoitusmenetelmän turvallisuus perustuu otaksumaan, että suuria lukuja ei voida jakaa alkutekijöihinsä "mielekkäässä" ajassa. Shorin työ osoitti, että tämä ei kuitenkaan pidä paikkaansa, jos on mahdollista rakentaa kvanttitietokone.

Yhtenä tärkeimmistä merkkipaaluista kvanttilaskennan teoreettisella puolella pidetään myös Lov Groverin algoritmia [17], jolla voidaan kvanttitietokoneella hakea tietokannasta *kvadraattisesti nopeammin* kuin perinteisillä tietokoneilla.

Kvanttitietokoneen toteuttaminen ei kuitenkaan ole mikään yksinkertainen asia. Periaatteessa mikä tahansa fysikaalinen systeemi, joka voi olla kahdessa eri tilassa, voisi toimia *kvanttibittinä*, kvanttitietokoneen perusosasena. Ydinhiukkasten spiniin perustuvalla tekniikalla on kyetty toteuttamaan seitsemän kvanttibitin systeemi (katso [23] ja [36]), ja kvanttibittien määrässä tämä lienee yhä ennätys.

Kvanttitietokoneen käytännön toteuttamisen edellytyksenä on se, että bitit esitetään erittäin pienillä fysikaalisilla systeemeillä. Tämä taas aiheuttaa ainakin kaksi, osittain toisensa poissulkevaa vaatimusta: systeemin, jossa bitit esitetään, tulee olla hyvin eristetty, jotta ympäristön satunnaiset häiriöt voitaisiin minimoida. Toisaalta taas bitit eivät voi kokonaan olla eristettyjä, tuleehan niiden arvoja voida muuttaa ja laskennallisia operaatioita on voitava suorittaa. Peter Shor esitteli artikkelissaan [31] (1995) periaatteen, jolla satunnaisia kvanttibiteissä tapahtuvia virheitä voidaan korjata, mutta joka tapauksessa kvanttitietokoneen kehittely käytännössä vaikuttaa erittäin hankalalta.

2 Kvanttilaskentaa keveästi

Toisin kuin Newtonin fysiikka, kvanttifysiikka on luonteeltaan *epädeterminististä*. Tämä merkitsee sitä, että suureiden arvojen sijasta kvanttifysiikassa käsitellään näiden arvojen *todennäköisyysjakaumia*. Tämä on kvanttifysiikan rakenteellinen ominaisuus eikä näitä jakaumia yleensä voida tarkentaa mielivaltaisen kapeiksi esim. olosuhteita tai koejärjestelyjä parantamalla.

Kvanttifysiikkaa pidetään usein hankalana. Tämä johtuu luultavasti lähinnä siitä, että kvanttifysikaalisten objektien kuvailuun todennäköisyysjakaumina ja näiden jakaumien *dynamiikan* esittämiseen tarvitaan usein varsin pitkälle kehitettyä matematiikkaa: siinä missä klassisen mekaniikan *Hamiltonin liikeyhtälöt* olivat kohtuullisen helposti hallittavissa, on kvanttimekaniikan *Schrödingerin liikeyhtälö* usein varsin hankala.

Itse asiassa kvanttifysikaalisia objekteja ei suoranaisesti esitetä todennäköisyysjakaumina vaan *amplitudijakaumina*, joista sitten vastaavat todennäköisyysjakaumat määräytyvät. Ero näiden jakaumatyyppien välillä on siinä, että todennäköisyydet eivät voi olla negatiivisia, kun taas amplitudit voivat. Tällöin esimerkiksi positiiviset ja negatiiviset amplitudit voivat kumota toisiaan; tämä on juuri se piirre kvanttifysiikassa, jossa aaltoluonne tulee esille! Tästä tulemme näkemään esimerkkejä myöhemmin.

Tämän artikkelin näkökulmasta suurin osa matemaattisesta koneistosta voidaan kuitenkin karsia: kvanttilaskentaan voi aivan hyvin perehtyä, kunhan hallitsee hieman aivan tavallista lineaarialgebraa. Kvanttilaskennan erikoisuuksia on varsin vaikea kuvata ja niihin on hankalaa perehtyä edes pinnallisesti käyttämättä minkäänlaista formalismia. Tämän vuoksi seuraavassa pykälässä käsitellään kvanttibittien esittämistä, käyttämättä kuitenkaan juuri lainkaan matemaattista koneistoa. Enemmän tietoa Kvanttiinformaation matemaattisesta esityksestä löytyy kirjasta [19].

2.1 Kvanttibitit

Informaation perusyksikkönä käytetään usein *bittiä*. Bitti tarkoittaa suuretta, joka voi saada kaksi arvoa ja perinteisesti näitä arvoja on merkitty symboleilla 0 ja 1. Kvanttilaskennassa bitin vastine on *kvanttibitti* ja periaatteessa mikä hyvänsä kaksiarvoinen kvanttifysiikan suure voi toimia kvanttibittinä. Tässä artikkelissa emme kuitenkaan perehdy kvanttibittien käytännön toteuttamiseen, vaan ainoastaan niiden matemaattiseen esitykseen.

Kvanttibittien arvoja on tapana esittää P. Diracilta periytyvillä merkinnöillä $|0\rangle$ ja $|1\rangle$. Siinä missä tavalliset bitit saavat vain arvoja 0 ja 1, voivat kvanttibitit olla sekä nollan että ykkösen *superpositiossa*, josta käytetään merkintää

$$a\,|0\rangle + b\,|1\rangle\,. \tag{1}$$

Yleisesti merkintöjä $|0\rangle$, $|1\rangle$ ja (1) kutsutaan kvanttibitin *tiloiksi*. Lisäksi tiloja $|0\rangle$ ja $|1\rangle$ sanotaan *perustiloiksi*. Ylläolevassa merkinnässä a ja b ovat (kompleksi)lukuja, joita kutsutaan amplitudeiksi ja jotka toteuttavat ehdon $|a|^2 + |b|^2 = 1$.

Superpositio merkitsee käytännössä seuraavaa: jos yllä kuvatussa tilassa (1) olevaa kvanttibittiä *havainnoidaan*, saadaan todennäköisyydellä $|a|^2$ tulokseksi, että kvanttibitti esitti nollaa, ja todennäköisyydellä $|b|^2$ tulokseksi, että se kvanttibitti esitti ykköstä.[4] Lisäksi havainnointi "tuhoaa" superposition (1) seuraavassa mielessä: jos havainnon tuloksena oli, että kvanttibitti esitti nollaa, on havannoinnin jälkei-

[4] Matemaattisesti kvanttibitti merkitsee yksikkövektoria kaksiulotteisessa Hilbertin avaruudessa H_2. Vektorit $|0\rangle$ ja $|1\rangle$ valitaan ortonormaalikannaksi.

nen tila $|0\rangle$. Vastaavasti jos kvanttibitin nähtiin esittävän ykköstä, on havainnoinnin jälkeinen tila $|1\rangle$.

Esimerkkinä kvanttibitin tilasta toimii vaikkapa *tasapainotettu* superpositio

$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,, \qquad (2)$$

jossa todennäköisyys nähdä nolla on $\left|1/\sqrt{2}\right|^2 = \frac{1}{2}$ ja samoin on ykkösen todennäköisyyden laita. Huomaa että myös tila

$$\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle \qquad (3)$$

on tasapainotettu: ykkösen todennäköisyys tilassa (3) on $\left|-1/\sqrt{2}\right|^2 = \frac{1}{2}$.

Kahden kvanttibitin arvoista käytetään merkintöjä $|0\rangle\,|0\rangle$, $|0\rangle\,|1\rangle$, $|1\rangle\,|0\rangle$ ja $|1\rangle\,|1\rangle$, tai lyhyemmin $|00\rangle$, $|01\rangle$, $|10\rangle$ ja $|11\rangle$. Myös kaksi kvanttibittiä voivat näiden perustilojen lisäksi olla superpositiossa; yleisestä kahden kvanttibitin tilasta käytetään merkintää

$$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle\,. \qquad (4)$$

Samoin kuin yhden kvanttibitin tapauksessa, ovat a, b, c ja d amplitudeiksi kutsuttuja lukuja, jotka toteuttavat ehdon $|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$.

Tilaa (4) tulkitaan ilmeisellä tavalla: jos tilassa (4) olevaa kvanttibittiparia havainnoidaan, saadaan tulokseksi 00, 01, 10 ja 11 todennäköisyyksillä $|a|^2$, $|b|^2$, $|c|^2$ ja $|d|^2$ (tässä järjestyksessä).[5]

Kahden kvanttibitin tila

$$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \qquad (5)$$

on tasapainotettu: tilaa (5) havainnoimalla minkä tahansa kahden bitin yhdistelmän näkeminen onnistuu nimittäin todennäköisyydellä $\left|\frac{1}{2}\right|^2 = \frac{1}{4}$. Yllä esitetyllä tilalla (5) on myös eräs toinen varsin mielenkiintoinen piirre: kahden kvanttibitin tilasta voidaan nimittäin muodostaa nk. *tulo*. [6] Jos esimerkiksi kaksi kvanttibittiä ovat kummatkin tilassa (2), on niiden tulona muodostettu yhteinen tila

$$\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big)\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big),$$

joka auki kertomalla voidaan kirjoittaa muotoon

$$\begin{aligned} & \frac{1}{\sqrt{2}}|0\rangle\,\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|0\rangle\,\frac{1}{\sqrt{2}}|1\rangle \\ + \;& \frac{1}{\sqrt{2}}|1\rangle\,\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\,\frac{1}{\sqrt{2}}|1\rangle \\ = \;& \frac{1}{2}|0\rangle\,|0\rangle + \frac{1}{2}|0\rangle\,|1\rangle \\ + \;& \frac{1}{2}|1\rangle\,|0\rangle + \frac{1}{2}|1\rangle\,|1\rangle\,. \end{aligned}$$

Näin saatu tila voidaan lyhennysmerkintöjä käyttäen kirjoittaa muotoon

$$\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle\,.$$

[5] Kvanttibittipari merkitsee yksikkövektoria neliulotteisessa Hilbertin avaruudessa H_4. Tämä voidaan esittää tensoritulona $H_4 = H_2 \otimes H_2$.

[6] Kyseessä on kahden avaruuden H_2 vektorin tensoritulo avaruudessa $H_4 = H_2 \otimes H_2$.

Kyseessä on siis täsmälleen sama kuin tila (5). [7] Superposition (5) kaltaisia tiloja, jotka voidaan esittää kahden superposition tulona, kutsutaan *hajoaviksi*.

On melko helppoa havaita, että kahden kvanttibitin muodostama tila

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \qquad (6)$$

ei ole hajoava (katso [19]). Tämänkaltaisia tiloja kutsutaan *limittyneiksi*. Myös tilassa (6) piilee mielenkiintoisia ominaisuuksia. Huomautettakoon ensiksi, että tässä tilassa olevaa kvanttibittiparia havainnoitaessa voidaan nähdä molempien bittien esittävän nollaa todennäköisyydellä $\left|1/\sqrt{2}\right|^2 = 1/2$ ja samalla todennäköisyydellä nähdään kummankin bitin esittävän ykköstä. Toisaalta todennäköisyys sille, että toisen bitin nähtäisiin esittävän nollaa ja toisen ykköstä, on nolla. Tämä merkitsee sitä, että kvanttibitit ovat *täydellisesti korreloituneet*: bittiparia havainnoitaessa nähdään näillä kummallakin olevan sama arvo, joka on nolla todennäköisyydellä $\frac{1}{2}$ ja ykkönen täsmälleen samalla todennäköisyydellä.

Tilaa (6) kutsutaan EPR-tilaksi Einsteinin, Podolskyn ja Rosenin mukaan (mainitut fyysikot pitivät aluksi tilan (6) olemassaoloa perustavanlaatuisena paradoksina kvanttifysiikassa). Erityisen kiintoisaa on se, että edellämainittu korrelaatio EPR-tilassa olevien kvanttibittien välillä voi säilyä, vaikka kvanttibitit olisivat hyvinkin kaukana toisistaan! Teoreettista ylärajaa kvanttibittien väliselle etäisyydelle ei ole, ja käytännön kokeissakin [34] EPR-tilan on havaittu säilyvän vaikka kvanttibitit olisivat yli kymmenen kilometrin etäisyydellä toisistaan. EPR-tiloja ja niiden käyttöä kvanttilaskennassa käsitellään myöhemmin enemmän.

2.2 Kvanttiportit

Sen lisäksi, että tunnetaan kvanttibittien matemaattinen esitystapa, on tiedettävä miten kvanttibittejä käsitellään. Toisin sanoen on tiedettävä mitä operaatioita kvanttibiteillä voidaan suorittaa. Analogiana *loogisille porteille* näitä kvanttibittien operaatioita kutsutaan *kvanttiporteiksi*.

Kyseiset operaatiot ovat varsin helposti määriteltävissä matematiikan kielellä: kun käsiteltävänä on n kpl kvanttibittejä, ovat näille sallitut operaatiot tarkalleen kaikki unitaarimuunnokset bittien esitysavaruudessa H_{2^n}. Tätä määritelmää ei kuitenkaan jatkossa tarvita vaan asiaa käsitellään esimerkkien valossa.

Ennen kvanttiportteihin siirtymistä käsitellään kuitenkin erästä periaatteellista kysymystä: kvanttiporttien määritelmästä unitaarimuunnoksina seuraa, että kvanttioperaatiot

[7] Tuloa laskettaessa on huomioitava, että tulo ei ole *kommutatiivinen*, siis tekijöiden järjestystä ei voi vaihtaa. Esimerkiksi $|0\rangle|1\rangle$ on erisuuri kuin $|1\rangle|0\rangle$.

ovat *kääntyviä*. Tämä merkitsee sitä, että operaation tuloksesta voidaan aina päätellä syöte, kun taas perinteisessä laskennassa näin ei aina ole; klassiset bittioperaatiot eivät välttämättä ole kääntyviä (informaation säilyttäviä). Tällöin tietysti herää kysymys, voidaanko kvanttitietokoneella laskea aivan kaikkea mitä tavanomaisilla tietokoneilla voidaan.

Laskennan kääntyvyyttä tutkineet Yves Lecerf [24] (1963) ja Charles Bennett [2] (1973) olivat päätyneet kvanttilaskennan kannalta positiiviseen tulokseen: kaikki laskenta tavanomaisella tietokoneella voidaan tehdä myös kääntyvällä tavalla. Toisin sanoen, kaikkea laskentaa voidaan aina simuloida kääntyvällä laskennalla. Bennettin tulos oli hieman Lecerfin tulosta vahvempi, sillä Bennett osoitti, että (simuloiva) kääntyvä laskenta voidaan tehdä myös oleellisesti yhtä nopeasti kuin alkuperäinenkin, tosin laskennan vaatimaa tilaa lisäämällä.

Kvanttiportteihin siirtyäksemme todettakoon ensin, että kaikki kvanttiportit voidaan määritellä selostamalla, miten ne vaikuttavat perustiloihin. Täten yhden bitin kvanttiportti määritellään kertomalla, miten se vaikuttaa tiloihin $|0\rangle$ ja $|1\rangle$, kahden bitin kvanttiportti taas selostamalla sen vaikutus tiloihin $|00\rangle$, $|01\rangle$, $|10\rangle$ ja $|11\rangle$, jne.

2.2.1 Yhden kvanttibitin portit

Aloitetaan esimerkillä yhden bitin kvanttiportista. Kutsutaan sitä nimellä N ja määritellään se seuraavasti:

$$\begin{cases} N|0\rangle = |1\rangle \\ N|1\rangle = |0\rangle \end{cases}$$

(portti N muuttaa tilan $|0\rangle$ tilaksi $|1\rangle$ ja päinvastoin). Selvästikin N on tavanomaisista loogisista piireistä tuttu NOT-portti. Portin N vaikutus tasapainotettuun tilaan (2) saadaan yksinkertaisesti:

$$\begin{aligned} & N\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big) \\ = \; & \frac{1}{\sqrt{2}}N|0\rangle + \frac{1}{\sqrt{2}}N|1\rangle \\ = \; & \frac{1}{\sqrt{2}}|1\rangle + \frac{1}{\sqrt{2}}|0\rangle, \end{aligned}$$

siis N ei muuta tilaa (2) lainkaan!

Määritellään seuraavaksi yhden kvanttibitin portti W ehdoilla

$$\begin{cases} W|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \\ W|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle, \end{cases}$$

siis portti W muuntaa perustilan $|0\rangle$ tasapainotetuksi tilaksi (2) ja perustilan $|1\rangle$ myös tasapainotetuksi tilaksi (3). Portti W, jota kutsutaan *Walshin muunnokseksi* (tai *Hadamardin-Walshin munnokseksi*), on kvanttilaskennan kannalta erittäin tärkeä.

Katsotaan seuraavaksi mitä tapahtuu, kun porttia W sovelletaan tasapainotettuun tilaan (2). Suora lasku

osoittaa, että

$$\begin{aligned} & W\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\Big) \\ = \; & \frac{1}{\sqrt{2}}W|0\rangle + \frac{1}{\sqrt{2}}W|1\rangle \\ = \; & \frac{1}{\sqrt{2}}\big(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\big) \\ + \; & \frac{1}{\sqrt{2}}\big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\big) \\ = \; & \frac{1}{2}|0\rangle + \frac{1}{2}|1\rangle + \frac{1}{2}|0\rangle - \frac{1}{2}|1\rangle \\ = \; & |0\rangle\,. \end{aligned}$$

Samoin nähdään, että

$$W\Big(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\Big) = |1\rangle\,.$$

Edellä havaitut muunnokset voidaan kirjoittaa portin W määritelmän muistaen seuraavaan muotoon:

$$\begin{aligned} WW|0\rangle &= |0\rangle \\ WW|1\rangle &= |1\rangle\,. \end{aligned}$$

Toisin sanoen, kaksi W-porttia peräkkäin ei aiheuta mitään muutosta kvanttibittiin. Tämän asian läheisempi tarkastelu paljastaa ilmiön, joka erottaa kvanttilaskennan perinteisistä laskennan muodoista. Seuraavassa pykälässä keskitytään tähän ilmiöön tarkemmin.

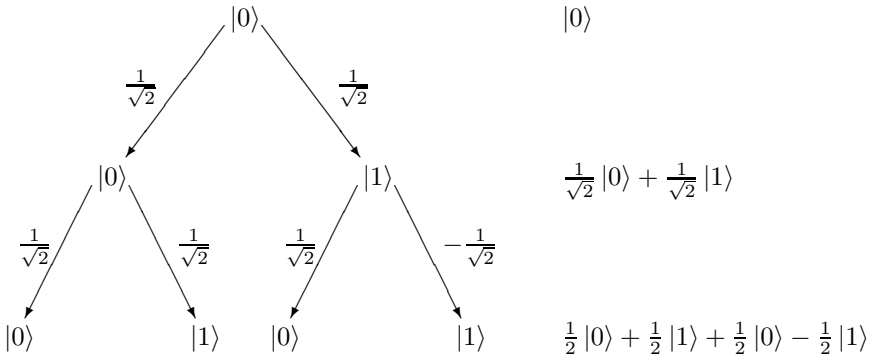
2.2.2 Interferenssi

Interferenssi-ilmiö esiintyy jo silloin kun tarkastellaan vain yhtä kvanttibittiä ja lieneekin helpointa tutustua tähän ilmiöön Walshin muunnoksen avulla.

Kuva 1 esittää Walshin muunnoksen suorittamista kahteen kertaan. Vasemmalla on kaavio joka esittää tilojen kehittymistä ja oikealla laidalla ovat taas vastaavat tilat. Ylinnä on lähtötila $|0\rangle$ ja ensimmäinen Walshin muunnos "halkaisee" tämän superpositioksi, jossa esiintyvät sekä $|0\rangle$ että $|1\rangle$, kummatkin amplitudeilla $1/\sqrt{2}$. Kuvassa toinen taso esittää tilannetta, jossa Walshin muunnos on suoritettu kertaalleen.

Toinen Walshin muunnoksen suorituskerta aiheuttaa muutoksen kumpaankin superposition perustilaan. Tila $|0\rangle$ muuntuu kuten edellä ja myös tila $|1\rangle$ muuntuu Walshin muunnoksen määritelmän mukaisesti, siis "halkeaa" tilojen $|0\rangle$ ja $|1\rangle$ superpositioksi amplitudeilla $1/\sqrt{2}$ ja $-1/\sqrt{2}$. Lopulliset amplitudit alimmaisessa rivissä esiintyville tiloille saadaan seuraamalla polkua ylhäältä alas ja kertomalla polun varrella esiintyvät amplitudit keskenään. Esimerkiksi kuvan 1 vasemmanpuolimmaisen $|0\rangle$:n amplitudi on $\frac{1}{\sqrt{2}}\cdot\frac{1}{\sqrt{2}} = \frac{1}{2}$, kun taas oikeanpuolimmaisen $|1\rangle$:n amplitudiksi saadaan $\frac{1}{\sqrt{2}}\cdot(-\frac{1}{\sqrt{2}}) = -\frac{1}{2}$.

Alimmalla rivillä kuitenkin esiintyy kahteen kertaan sekä $|0\rangle$ että $|1\rangle$, ja tällöin näiden amplitudit summautuvat yhteen. Tilojen $|0\rangle$ amplitudien summaksi saadaan $\frac{1}{2}+\frac{1}{2} = 1$ mutta tilojen $|1\rangle$ amplitudien summaksi $\frac{1}{2}-\frac{1}{2} = 0$. Tällöin sanotaan, että alimmalla rivillä olevat tilat $|0\rangle$ interferoivat *positiivi-*



Kuva 1: Walshin muunnos kaksi kertaa.

sesti (toisiaan vahvistavasti) ja että tilat $|1\rangle$ interferoivat *negatiivisesti* (toisiaan heikentävästi).

Nähdäksemme vielä selvemmin eron kvantti-informaation ja klassisen informaation välillä, esitetään kaksinkertainen Walshin muunnos edelleen hieman eri tavoin. Ajatellaan, että Walshin muunnos kuvaa "kolikonheittoa". Tällä tarkoitetaan sitä, että aloitetaanpa sitten tilasta $|0\rangle$ tai $|1\rangle$, on Walshin muunnoksen jälkeen todennäköisyys nähdä nolla tai ykkönen tarkalleen $\frac{1}{2}$.

Kaksi kertaa tehdyssä Walshin muunnoksessa, tilasta $|0\rangle$ aloittaen, käy seuraavasti: ensimmäisen Walshin muunnoksen jälkeen todennäköisyys nähdä 0 ja 1 ovat tasan, molemmat $\frac{1}{2}$. Tehdään kuitenkin niin, että *ei katsota tulosta*, vaan "heitetään kolikkoa" (= suoritetaan Walshin muunnos) toiseen kertaan. Tällöin nähdäänkin aivan varmasti 0. Tämänkaltaista interferenssiin perustuvaa ilmiötä ei esiinny perinteisessä informaationkäsittelyssä.

Kvanttitietokoneiden teho perustuukin nimenomaan interferenssiin eikä siihen, että ne olisivat oleellisesti nopeampia kuin perinteiset tietokoneet. Siinä missä perinteinen tietokone joutuu suorittamaan suuren laskentaurakan, kvanttitietokone saattaa päästä oikotietä paljon helpommalla samaan lopputulokseen.

Periaatteellisella tasolla tämä tapahtuu seuraavasti: kuvitellaan, että jossakin laskentatehtävässä tietokoneen tulisi etsiä valtavasta joukosta jokin tietyn ehdon täyttävä alkio. Oletetaan vielä, että on varsin helppoa *tarkistaa* täyttääkö jokin annettu alkio ehdon vai ei, mutta ehdon täyttäviä alkiota on vaikea löytää, koska niitä on harvassa ja joukko, josta nii-

tä etsitään on suuri.[8] Kyseistä tehtävää varten voidaan ajatella todennäköisyysalgoritmia, jossa kone aluksi arpoisi jonkin alkion etsittävien joukosta ja sen jälkeen tarkistaisi täyttääkö arvottu alkio määrätyn ehdon. Oletusten mukaan tämänkaltainen algoritmi toimisi nopeasti, mutta todennäköisyys, että tällä tavoin haluttu alkio löydetään, jäisi häviävän pieneksi. Näin ollen tästä todennäköisyysalgoritmista ei olisi vastaavaa hyötyä, sillä "arvottaessa" ei voida ohjailla arpaonnea suosimaan haluttuja alkioita.

Kvanttitietokoneella sen sijaan näin voidaan joskus tehdä. Tarkemmin sanoen, suunnittelemalla kvanttialgoritmi hyvin on mahdollista että "huonot" arvonnat interferoivat toisiaan heikentävästi ja "hyvät" toisiaan vahvistavasti. Sitä, mille ongelmille tämänkaltainen "hyviä" valintoja suosiva kvanttialgoritmi voidaan laatia (siten että saadaan lähes eksponentiaalinen nopeutus), ei tarkasti tiedetä. Sellainen voidaan tehdä ainakin niissä tapauksissa, joissa hakujoukolla on tietyntyyppinen algebrallinen rakenne ja haettavat alkiot liittyvät tähän rakenteeseen sopivasti. Tähän liittyviä tarkempia yksityiskohtia löytyy kirjasta [19].

2.2.3 Useamman kvanttibitin portit

Matemaattisesti useamman kvanttibitin portit määritellään samoin kuin yhden kvanttibitin tapauksessa. Tarkkaa matemaattista määritelmää emme kuitenkaan käytä, joten tässäkin yhteydessä tyydymme vain esimerkkeihin. On kuitenkin huomattava, että koska kvanttiportit ovat aina kääntyviä, on niissä pakko olla yhtä monta ulostuloa kuin sisääntuloa.

Määritellään kahden kvanttibitin portti CN seuraavasti:

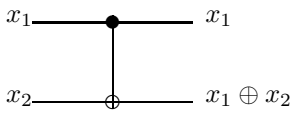
$$\begin{cases} CN\,|00\rangle = |00\rangle \\ CN\,|01\rangle = |01\rangle \\ CN\,|10\rangle = |11\rangle \\ CN\,|11\rangle = |10\rangle \end{cases}$$

Määritelmän perusteella portti CN kääntää toisen bitin arvon, jos ensimmäisen arvo on 1, muussa tapauksessa CN jättää toisen bitin koskemattomaksi. Joka tapauksessa CN jättää ensimmäisen bitin koskemattomaksi. Portti CN onkin varsin hyvin tunnettu ja perinteisesti sitä kutsutaan nimellä *kontrolloitu not*. Tässä siis ensimmäinen bitti on "kontrollibitti" joka määrää, suoritetaanko toiselle bitille NOT-operaatio vai ei.

Kontrolloitua NOT-porttia merkitään yleensä kuvan 2 mukaisella symbolilla. Kuvassa x_1 on kontrollibitti ja bitin x_2 arvo vaihtuu mikäli kontrollibitin x_1 arvo on 1. Toisin sanoen, laskettavaksi tulee nk. *exclusive or* (XOR, josta käytetään symbolia $\oplus$) bittien x_1 ja x_2 välillä.

Loogisia piirejä tuntevat tietävät varsin hyvin, että kaikki loogiset piirit voidaan rakentaa käyttäen portte-

[8] Tässä yhteydessä tarkoitetaan lähinnä **NP**-luokan ongelmia.



Kuva 2: Kontrolloitu not-portti

ja AND, OR ja NOT (mainituista ainoastaan NOT on kääntyvä, kaksi muuta eivät). Portilla CN on tärkeä asema kvanttilaskennassa, nimittäin *kaikki kvanttipiirit* voidaan rakentaa käyttäen ainoastaan yhden kvanttibitin portteja ja porttia CN [1]. Porttijoukkoa, jolla on tämä ominaisuus, sanotaan *universaaliksi*. [9]

Deutsch oli jo tosin aiemmin osoittanut että on olemassa *yksi ainoa* kolmen kvanttibitin portti, josta kaikki kvanttipiirit voidaan rakentaa [13], mutta tietysti on miellyttävämpää jos voidaan kolmen bitin porteista siirtyä kahden bitin portteihin. Artikkelin [1] tuloksessa on vielä eräs merkillinen piirre: voidaan kohtuullisen helposti osoittaa, että pelkästään kahden bitin kääntyviä klassisia portteja käyttäen ei voida saada aikaan kaikkia kääntyviä klassisia piirejä vaan tähän tarvitaan myös kolmen bitin portteja (katso [19]). Kuitenkin artikkelin [1] tuloksen mukaan kvanttilaskennassa vastaava on mahdollista!

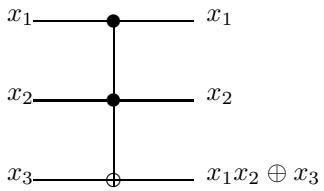
Käsitellään vielä hieman kolmen kvanttibitin portteja. Määritellään portti T seuraavasti:

$$\begin{cases} T|000\rangle = |000\rangle \\ T|001\rangle = |001\rangle \\ T|010\rangle = |010\rangle \\ T|011\rangle = |011\rangle \\ T|100\rangle = |100\rangle \\ T|101\rangle = |101\rangle \\ T|110\rangle = |111\rangle \\ T|111\rangle = |110\rangle \end{cases}$$

Toisin sanoen, portti T säilyttää kahden ensimmäisen bitin arvon sellaisenaan ja vaihtaa kolmannen bitin arvon tarkalleen silloin kun kaksi ensimmäistä bittiä ovat molemmat ykkösiä. Porttia T, jota kutsutaan *Toffolin portiksi*, voidaankin pitää portin CN yleistyksenä.

Toffolin portilla, jota merkitään kuvan 3 piirrossymbolilla, on suuri merki-

[9] Mainittaessa, että kaikki kvanttipiirit voidaan rakentaa käyttäen tiettyä joukkoa kvanttiportteja, tarkoitetaan yleensä, että ko. joukolla voidaan *approksimoida* mitä hyvänsä kvanttipiiriä. Lisäksi usein tarkoitetaan, että sallitaan lisättävän ns. joutilaita bittejä, jotka alkutilassa asetetaan kaikki nolliksi ja joiden arvosta ei lopuksi välitetä.



Kuva 3: Toffolin portti

tys myös perinteisessä laskennassa. Tätä porttia käyttäen voidaan nimittäin rakentaa kaikki loogiset piirit, jos myös vakiobitit 0 ja 1 ovat käytössä [35]. Tämä on kohtalaisen helppo nähdä myös suoraan [19].

Koska Toffolin portti on myös kääntyvä, voidaan sanoa, että Toffolin portti (vakiobittien kanssa) on universaali kääntyvän laskennan portti. Se, että kaikki loogiset piirit voidaan rakentaa käyttäen ainoastaan Toffolin porttia (sekä vakiobittejä) osoittaa uudella tavalla todeksi sen, että kaikki laskenta voidaan tehdä myös kääntyvällä tavalla.

2.2.4 Kvanttilaskenta analogista?

Toffolin portit esiintyvät myös Yaoyun Shin tuloksessa [29], joka kertoo hyvin paljon kvanttilaskennan luonteesta. Voitaisiin nimittäin ajatella, että kvanttilaskenta ei ole "diskreettiä" vaan sen voima piilisi pikemminkin "analogiselle laskennalle" tyypillisissä piirteissä. Esimerkiksi artikkelin [1] tuloksessa esiintyivät yhden kvanttibitin portit, ja näiden ulostuloissa saattaa esiintyä tiloja $a\,|0\rangle + b\,|1\rangle$, missä esim. a voi olla mikä tahansa reaaliluku nollan ja ykkösen väliltä.

Tällöin herää tietysti kysymys, piileekö kvanttilaskennan voima juuri tässä mahdollisuudessa käyttää mielivaltaisia reaalilukuja. Tähän kysymykseen on jo aiemmin löydetty vastaus [7], mutta Shin tulos esittää vastauksen erityisen selkeällä tavalla.

Shin tuloksen mukaan *kaikki kvanttipiirit voidaan rakentaa käyttäen ainoastaan Toffolin porttia, Walshin muunnosta (porttia W) ja vakiobittejä.* Tämä tulos siis "diskretisoi" kvanttilaskennan täysin. Tarvittavien kvanttiporttien määrä ei myöskään kasva räjähdysmäisesti: Solovay-Kitaevin lauseena tunnetusta vahvasta tuloksesta [22] seuraa, että tarvitaan vain $O(n \log^c(\frac{n}{\epsilon}))$ porttia *mistä hyvänsä* universaalista kvanttiporttien joukosta simuloimaan kvanttipiiriä, jossa aluksi oli n kvanttiporttia. Kaavassa esiintyvä $c \approx 4$ on vakio, ja ϵ on haluttu simulaatiotarkkuus.

Tämän lisäksi Shin tuloksesta seuraa, että ei ole tarpeen käyttää kompleksilukuja kvanttitilojen superpositioissa; reaaliluvut riittävät aivan hyvin (myös tämä oli jo aiemmin tunnettu [7]). On kuitenkin huomautettava, että jotkin kvanttilaskennan kannalta keskeiset asiat, kuten Shorin algoritmit, ovat paljon informatiivisemmin esitettävissä, mikäli käytetään kompleksilukuja.

2.3 Kvanttilaskenta ja XOR

Tässä pykälässä käsitellään yksinkertaisinta versiota Deutschin-Jozsan ongelmasta [14], joka tapauksessa $n = 1$ kutistuu funktion XOR (exclusive or) laskemiseksi. Tässä yhteydessä käytetään myös matematiikkaa hieman enemmän kuin ennen, mutta tämän pykälän matemaattisen osuuden ymmärtäminen ei ole edellytyksenä jatkossa esiintyvien asioiden seuraamiselle.

Funktio XOR (jonka symbolina toimii $\oplus$) määritellään siten, että

$$\begin{cases} 0 \oplus 0 = 0 \\ 0 \oplus 1 = 1 \\ 1 \oplus 0 = 1 \\ 1 \oplus 1 = 0 \end{cases}$$

Toisin sanoen, XOR kahdesta bitistä saa arvon 1 tarkalleen silloin kun toinen niistä (mutta ei molemmat) saa arvon 1.

On täysin selvää, että kummankin bitin x_0 ja x_1 arvo on kysyttävä, ennen kuin funktion $x_0 \oplus x_1$ arvo voidaan saada selville; on siis tehtävä kaksi kysymystä. Näin ei kuitenkaan ole kvanttilaskennassa, yksi kysymys riittää! Ensin on kuitenkin selvennettävä, mitä tarkoitetaan "bitin arvon kysymisellä" kvanttilaskennassa. Aiemminhan oli jo mainittu, että kaikki kvanttilaskennan operaatiot ovat kääntyviä, mutta bitin kirjoittaminen aiemman tilalle (aiempaa kysymättä) ei välttämättä ole kääntyvä operaatio — tällöinhän voidaan hävittää aiempaa informaatiota.

Tämän vuoksi on sovittu, että bitin kysyminen kvanttilaskennassa merkitsee seuraavaa (tässä esimerkissä kysytään vain kahta eri bittiä x_0 ja x_1, yleistys on suoraviivainen): kysyttävän bitin numero asetetaan ensimmäiseen kvanttibittiin, kun taas toinen bitti voi olla nolla tai ykkönen. Tämän jälkeen kahden kvanttibitin "kysymysoperaattori" (tai "kysymysportti") Q tekee seuraavan:

$$\begin{cases} Q\,|0\rangle\,|0\rangle &= |0\rangle\,|0 \oplus x_0\rangle \\ Q\,|0\rangle\,|1\rangle &= |0\rangle\,|1 \oplus x_0\rangle \\ Q\,|1\rangle\,|0\rangle &= |1\rangle\,|0 \oplus x_1\rangle \\ Q\,|1\rangle\,|1\rangle &= |1\rangle\,|1 \oplus x_1\rangle \end{cases}$$

Edelleen eri tavoin sanottuna, portti Q katsoo ensimmäisestä kvanttibitistä sen bitin *numeron*, jota on kysyttävä, ja toiseen kvanttibittiin Q asettaa kysytyn bitin *arvon* (jos toinen bitti oli alunperin nolla) tai *arvon negaation* (jos toinen bitti oli alunperin ykkönen).

Seuraava, kaksi bittiä käyttävä kvanttialgoritmi laskee funktion $x_0 \oplus x_1$ kysymällä bittien arvon vain kerran.

1. Aloitetaan tilasta

$$|0\rangle\,|1\rangle$$

2. Suoritetaan kummallekin kvanttibitille Walshin muunnos. Näin päästään tilaan

$$\frac{1}{\sqrt{2}}\big(\,|0\rangle + |1\rangle\,\big)\frac{1}{\sqrt{2}}\big(\,|0\rangle - |1\rangle\,\big),$$

joka saadaan sulkeet auki kertomalla muotoon

$$\frac{1}{2}\big(\,|0\rangle\,|0\rangle - |0\rangle\,|1\rangle + |1\rangle\,|0\rangle - |1\rangle\,|1\rangle\,\big).$$

3. Nyt kysytään, siis käytetään "kysymysporttia" Q. Tulos on

$$\begin{aligned} & \frac{1}{2}\big(\,|0\rangle\,|x_0\rangle - |0\rangle\,|1 \oplus x_0\rangle \\ + \;& |1\rangle\,|x_1\rangle - |1\rangle\,|1 \oplus x_1\rangle\,\big) \\ = \;& \frac{1}{2}\big(\,|0\rangle\,(|x_0\rangle - |1 \oplus x_0\rangle) \\ + \;& |1\rangle\,(|x_1\rangle - |1 \oplus x_1\rangle)\big) \end{aligned}$$

Käymällä läpi esim. bitin x_0 arvot huomataan, että ylläoleva lauseke voidaan kirjoittaa muotoon

$$\begin{aligned} & \frac{1}{2}\big((-1)^{x_0}\,|0\rangle\,(|0\rangle - |1\rangle) \\ + \;& (-1)^{x_1}\,|1\rangle\,(|0\rangle - |1\rangle)\big) \\ = \;& \frac{1}{2}\big((-1)^{x_0}\,|0\rangle \\ + \;& (-1)^{x_1}\,|1\rangle\,\big)(|0\rangle - |1\rangle). \end{aligned}$$

4. Walshin muunnosta toiseen bittiin käyttäen saadaan aikaan tila

$$\frac{1}{\sqrt{2}}\big((-1)^{x_0}\,|0\rangle + (-1)^{x_1}\,|1\rangle\,\big)\,|1\rangle$$

5. Samaista muunnosta ensimmäiseen bittiin käyttäen saadaan tila

$$\begin{aligned} & \frac{1}{2}\big((-1)^{x_0}(|0\rangle + |1\rangle) \\ + \;& (-1)^{x_1}(|0\rangle - |1\rangle)\big)\,|1\rangle \\ = \;& \frac{1}{2}\Big(\big((-1)^{x_0} + (-1)^{x_1}\big)\,|0\rangle \\ + \;& \big((-1)^{x_0} - (-1)^{x_1}\big)\,|1\rangle\,\Big)\,|1\rangle \end{aligned}$$

Nyt voidaan bittien x_0 ja x_1 eri arvoille kirjoittaa seuraava taulukko:

x_0	x_1	yllä oleva superpositio
0	0	$\|0\rangle\,\|1\rangle$
0	1	$\|1\rangle\,\|1\rangle$
1	0	$-\,\|1\rangle\,\|1\rangle$
1	1	$-\,\|0\rangle\,\|1\rangle$

6. Havainnoidaan ensimmäisen bitin arvo. Mikäli havainnoitu arvo on 0, päätellään että $x_0 \oplus x_1 = 0$, muutoin päätellään päinvastoin. Yllä olevasta taulukosta nähdään, että tällä tavoin saadaan aina oikea tulos.

Tässä kvanttialgoritmissa funktiota XOR varten tehtiin todellakin vain yksi kysymys muuttujien arvosta. Tämä kysymys tapahtui kuitenkin sillä

tavoin että kysyttävän muuttujan numero oli tasapainotetussa superpositiossa: intuitiivisesti sanottuna kysyttiin siis kumpaakin muuttujaa x_0 ja x_1 "yhtäaikaa". Toisaalta myös "vastausbitti" oli tasapainotetussa superpositiossa. Jälleen intuitiivisesti katsoen voidaan sanoa, että vastauksen tallentaminen suoraan (nolla vastausbitin paikalla) ja bitin kääntäen (ykkönen vastausbitin paikalla) tapahtuivat molemmat "yhtäaikaa". Koska tämä algoritmi oli interferenssin kannalta suunniteltu optimaalisesti, nähdään algoritmin tuloksena $x_0 \oplus x_1$ todennäköisyydellä 1, siis aina oikein.

2.4 Kvanttilaskennan rajoitukset

Nykyisin tiedetään varsin hyvin, että kvanttitietokoneella voitaisiin jakaa suuria lukuja tekijöihin kohtalaisen nopeasti. Tällä tarkoitetaan sitä, että tekijöihinjako voitaisiin suorittaa *polynomiaalisessa ajassa* lukujen pituuteen nähden, siis resursseja ei tarvitsisi käyttää oleellisesti enemmän kuin kertolaskuunkaan.

Ei ole tiedossa miten tekijöihinjako suoritettaisiin nopeasti perinteisillä tietokoneilla; nykyisin ei tunneta mitään menetelmää, jolla suuren luvun tekijät voitaisiin saada selville suurella todennäköisyydellä *polynomiajassa* luvun pituuteen nähden, ja niinpä tekijöihinjakoa pidetäänkin erittäin vaikeana ongelmana. Kuitenkaan ei tiedetä, onko tekijöihinjako loppujen lopuksi "vaikea" ongelma perinteisilläkään tietokoneilla; toisin sanoen, ei tiedetä, *onko mahdotonta* keksiä "nopeaa" tekijöihinjakomenetelmää perinteisille tietokoneille. Tällaista menetelmää ei kuitenkaan ole toistaiseksi löydetty.

Samoin kuin perinteisessä laskennan teoriassa, myöskin kvanttilaskennassa tiedetään aivan liian vähän *laskennan rajoituksista* (tässä yhteydessä rajoituksilla tarkoitetaan alarajoja). Perinteisen laskennan parissa on hankalaa löytää todellisia rajoituksia laskennan *kompleksisuuteen*. Esimerkkinä tästä toimii hyvin tunnettu avoin kysymys **P** vs. **NP**; tämän ongelman ratkaisusta Clay Mathematics institute on tarjonnut miljoonan dollarin palkkion [11]. Kvanttilaskennan rajoituksia koskevat kysymykset näyttävät ainakin yhtä vaikeilta kuin **P** vs. **NP** - ongelma.

Toisaalta on kuitenkin huomautettava, että kvanttilaskennan ns. *suhteellisista* rajoituksista tiedetään jonkin verran ja näiden etsimisessä menetelmät ovat melko hyviä. Suhteellisista rajoituksista puhuttaessa tarkoitetaan rajoituksista laskennalle, jossa esiintyy "musta laatikko". Näitä rajoituksia käsitellään enemmän kirjoissa [27] (klassinen laskenta[10]) ja [19] (kvanttilaskenta).

[10]Kirjassa [27] ei käytetä termiä "musta laatikko", vaan tämän yleisempää muotoa "oraakkeli".

3 Lyhyesti kvantti-informaatiosta

Kvanttifysiikan ja teoreettisen tietojenkäsittelytieteen risteymäkohdan katsotaan nykyisin jakautuvan ainakin kahteen osaan: kvanttilaskentaan ja kvantti-informaatioteoriaan. Tässä luvussa tarkastellaan joitakin esimerkkejä kvantti-informaation käsittelystä. Kvantti-informaatioteoriasta enemmän kiinnostuneen kannattaa perehtyä kirjoihin [18] ja [26]. Lisäksi artikkeli [33] tarjoaa mainion johdannon limittyneiden kvanttitilojen ominaisuuksiin ja [37] kvanttikommunikaatioteoriaan. Artikkeli [10] on perustavaa laatua oleva tutkielma kvantti-informaatiosta.

3.1 Kvanttikopiokoneet

Kvanttikopiokoneella tarkoitetaan sellaista sallittua kvantti-operaatiota (unitaarimuunnosta), joka suorittaa operaation

$$\begin{aligned} & (a\,|0\rangle + b\,|1\rangle)\,|0\rangle \\ \mapsto\ & (a\,|0\rangle + b\,|1\rangle)(a\,|0\rangle + b\,|1\rangle). \end{aligned}$$

Kvanttikopiokone siis kopioisi ensimmäisen kvanttibitin tilan toiseen kvanttibittiin, jonka aluksi oletettaisiin olevan tilassa $|0\rangle$. Kopiointi ei klassisen informaationkäsittelyn kannalta ole mikään ongelma, mutta kvantti-informaation kannalta kopiointi on mahdoton tehtävä. Tunnettu tulos [38] kertoo, että kvanttikopiokonetta *ei ole olemassa*, siis kvantti-informaatiota ei voida kopioida. Tämä tulos ei kuitenkaan merkitse sitä etteikö *joissakin kvanttitiloissa olevia* kvanttibittejä voisi kopioida; esimerkiksi perustiloissa olevien kvanttibittien kopiointi onnistuu aivan hyvin. Kvanttitiloja ei yleisesti ottaen kuitenkaan voida kopioida.

Tämän varsin tunnetun "no-cloning" -periaatteen vastineeksi on esitetty sittemmin myös käänteinen tulos, niin sanottu "no-deleting" -periaate [28], jonka mukaan kvanttitilaa ei voida noin vain tuhota. Richard Jozsa yhdisti nämä kaksi asiaa artikkelissaan [21].

3.2 Kvanttikryptografiaa

EPR-tiloja (pykälä 2.1) käyttämällä kahden kommunikoivan osapuolen on mahdollista suorittaa tehtävä, joka on miltei mahdoton klassisen fysiikan puitteissa: osapuolet voivat toisiaan tapaamatta arpoa yhteisen jonon satunnaisia bittejä ja vieläpä huomaavat, mikäli jokin kolmas osapuoli yrittää saada selville informaatiota tästä satunnaisjonosta! (Viimeksi mainittu johtuu siitä, että havainnointi häiritsee aina kvanttibittejä.)

Jos kaksi kommunikoivaa osapuolta voisivat aina halutessaan saada yhteisen, kaikille muille tuntemattoman bittijonon, ei heillä olisi mitään ongelmaa salata viestintäänsä. Tällöinhän osapuolet voisivat käyttää ns. *one-time pad* -salausmenetelmää, joka tie-

detään ehdottoman varmaksi. Tämänkaltainen protokolla esitettiin artikkelissa [4] ja yksinkertaisempi myöhemmin artikkelissa [3]. Nykyisin kvanttikryptografia on jo kaupallisessa käytössä [20]. Kvanttikryptografian "perusturvallisuutta" käsittelevä ensimmäinen laajamittainen artikkeli ilmeisestikin kuuluu D. Mayersin ansioihin [25].

3.3 Teleportaatio

Kvanttibittien *teleportaatio* esitettiin ensimmäiseksi artikkelissa [5] ja merkitsee seuraavaa: Kvanttibitin omistava henkilö siirtää kvanttibittinsä vastaanottajalle hyödyntäen EPR-paria ja siirtämällä ***kaksi*** klassista bittiä. Kokeellisesti suoritetusta teleportaatiosta kertovat artikkelit [9], [8] ja [16].

Kutsutaan perinteen mukaisesti kommunikoivia osapuolia nimillä Alice ja Bob. Oletuksena on siis että Alice ja Bob ovat toisistaan ehkä hyvinkin kaukana, mutta heillä kummallakin on kvanttibitti. Lisäksi heidän kvanttibittinsä ovat EPR-tilassa

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

Tämän lisäksi Alicella on siirrettävä kvanttibitti jossakin tilassa

$$a\,|0\rangle + b\,|1\rangle\,.$$

Merkitään kaikkien kolmen kvanttibitin yhteistilaa seuraavasti:

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

Ylläolevasta merkinnästä pitää muistaa, että kaksi ensimmäistä bittiä kuuluvat Alicelle ja että hän pystyy näille biteille suorittamaan operaatiota, mutta kolmas kvanttibitti on Bobin hallussa ja tähän bittiin Alice ei voi kajota.

Aluksi Alice suorittaa *CN*-operaation toiselle bitille käyttäen ensimmäistä bittiä kontrollibittinä. Tuloksena on tila

$$\begin{aligned}
& \frac{a}{\sqrt{2}}\,|000\rangle + \frac{a}{\sqrt{2}}\,|011\rangle \\
+ \;& \frac{b}{\sqrt{2}}\,|110\rangle + \frac{b}{\sqrt{2}}\,|101\rangle\,. \qquad (7)
\end{aligned}$$

Tämän jälkeen Alice suorittaa Walshin muunnoksen tilan (7) ensimmäiselle kvanttibitille. Tuloksena saadaan tila

$$
\begin{aligned}
& \frac{a}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|00\rangle \\
+ \quad & \frac{a}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\,|11\rangle \\
+ \quad & \frac{b}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|10\rangle \\
+ \quad & \frac{b}{\sqrt{2}}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\,|01\rangle\,,
\end{aligned}
$$

joka voidaan myös kirjoittaa muotoon

$$
\begin{aligned}
& \frac{a}{2}\,|000\rangle + \frac{a}{2}\,|100\rangle \\
+ \quad & \frac{a}{2}\,|011\rangle + \frac{a}{2}\,|111\rangle \\
+ \quad & \frac{b}{2}\,|010\rangle - \frac{b}{2}\,|110\rangle \\
+ \quad & \frac{b}{2}\,|001\rangle - \frac{b}{2}\,|101\rangle\,.
\end{aligned}
$$

Siirtämällä vakioita ylläolevassa lausekkeessa saadaan muoto

$$
\begin{aligned}
& \frac{1}{2}\,|00\rangle\,a\,|0\rangle + \frac{1}{2}\,|10\rangle\,a\,|0\rangle \\
+ \quad & \frac{1}{2}\,|01\rangle\,a\,|1\rangle + \frac{1}{2}\,|11\rangle\,a\,|1\rangle \\
+ \quad & \frac{1}{2}\,|01\rangle\,b\,|0\rangle - \frac{1}{2}\,|11\rangle\,b\,|0\rangle \\
+ \quad & \frac{1}{2}\,|00\rangle\,b\,|1\rangle - \frac{1}{2}\,|10\rangle\,b\,|1\rangle\,,
\end{aligned}
$$

joka ryhmittelemällä muuntuu muotoon

$$
\begin{aligned}
= \quad & \frac{1}{2}\,|00\rangle\,(a\,|0\rangle + b\,|1\rangle) \\
+ \quad & \frac{1}{2}\,|01\rangle\,(a\,|1\rangle + b\,|0\rangle) \\
+ \quad & \frac{1}{2}\,|10\rangle\,(a\,|0\rangle - b\,|1\rangle) \\
+ \quad & \frac{1}{2}\,|11\rangle\,(a\,|1\rangle - b\,|0\rangle).
\end{aligned}
$$

Tämän jälkeen Alice havainnoi molempien kvanttibittiensä arvot. Hän saa neljäsosan todennäköisyydellä jonkin arvoista 00, 01, 10 ja 11. Tila muuntuu vastaavasti seuraavan taulukon mukaan:

Alicen havainto	tila havainnon jälkeen
00	$\|00\rangle\,(a\,\|0\rangle + b\,\|1\rangle)$
01	$\|01\rangle\,(a\,\|1\rangle + b\,\|0\rangle)$
10	$\|10\rangle\,(a\,\|0\rangle - b\,\|1\rangle)$
11	$\|11\rangle\,(a\,\|1\rangle - b\,\|0\rangle)$

Seuraavaksi Alice lähettää havaitsemansa bittien arvot Bobille käyttäen jotakin perinteistä tiedonsiirtomenetelmää.

Mikäli Alicen lähettämät bitit ovat 00, ei Bobin tarvitse tehdä mitään; tällöin hänen kvanttibittinsä on jo valmiiksi tilassa $a\,|0\rangle + b\,|1\rangle$ ja teleportaatio on suoritettu. Mikäli Alicen lähettämät bitit ovat 01, suorittaa Bob NOT-operaation omalla kvanttibitillään, ja tuloksena on jälleen tila $a\,|0\rangle + b\,|1\rangle$. Jos taas Alice lähetti bitit 10, on Bobin suoritettava *vaihesiirto-operaatio*

b_1	b_2	tila Alicen operaatioiden jälkeen	tila Bobin operaation jälkeen
0	0	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$	$\|00\rangle$
0	1	$\frac{1}{\sqrt{2}}\|10\rangle + \frac{1}{\sqrt{2}}\|01\rangle$	$\|01\rangle$
1	0	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$	$\|10\rangle$
1	1	$\frac{1}{\sqrt{2}}\|10\rangle - \frac{1}{\sqrt{2}}\|01\rangle$	$\|11\rangle$

Kuva 4: Tilat Alicen ja Bobin operaatioiden jälkeen ylitiheässä koodauksessa

$$\begin{cases} |0\rangle & \mapsto & |0\rangle \\ |1\rangle & \mapsto & -|1\rangle\,, \end{cases}$$

jonka jälkeen Bobin bitti on halutussa tilassa. Lopuksi, jos Alicen lähettämät bitit ovat 11, on Bobin suoritettava ensin NOT-operaatio ja sitten vaihesiirto.

Tässä yhteydessä on syytä huomauttaa, että teleportaatiossa kvanttibitti ei *fyysisesti* siirry, ainoastaan kvantti-informaatio. Lisäksi on syytä painottaa sanaa "siirtyä"; kvanttiinformaatio ei kopioidu, vaan alkuperäinen Alicella oleva kvanttiinformaatio tuhoutuu (kopiointihan olisi mahdotonta).

3.4 Ylitiheä koodaus

Ylitiheä koodaus [6] on teleportaatiolle käänteinen operaatio: siinä Alice ja Bob jakavat EPR-parin ja Alice lähettää Bobille yhden kvanttibitin, mutta informaatiota siirtyy *kahden* tavallisen bitin verran.

Teoriassa ylitiheä koodaus tapahtuu seuraavasti: Alice ja Bob jakavat jälleen EPR-tilan

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\,. \qquad (8)$$

Olkoon kvanttibiteistä ensimmäinen Alicen ja toinen Bobin hallussa ja Alice tahtoo lähettää kaksi bittiä b_1 ja b_2 Bobille. Mikäli $b_1 = 1$, Alice suorittaa kvanttibitilleen vaihesiirron ja mikäli $b_2 = 1$, Alice suorittaa bitilleen NOT-operaation. Tämän jälkeen tila on seuraavan taulukon mukainen.

b_1	b_2	tila Alicen operaatioiden jälkeen
0	0	$\frac{1}{\sqrt{2}}\|00\rangle + \frac{1}{\sqrt{2}}\|11\rangle$
0	1	$\frac{1}{\sqrt{2}}\|10\rangle + \frac{1}{\sqrt{2}}\|01\rangle$
1	0	$\frac{1}{\sqrt{2}}\|00\rangle - \frac{1}{\sqrt{2}}\|11\rangle$
1	1	$\frac{1}{\sqrt{2}}\|10\rangle - \frac{1}{\sqrt{2}}\|01\rangle$

Seuraavaksi Alice lähettää oman kvanttibittinsä Bobille, joka puolestaan suorittaa kvanttibiteillään seuraavalla tavalla määritellyn operaation (kahden kvanttibitin portti):

$$\begin{cases} |00\rangle & \mapsto & \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \\ |01\rangle & \mapsto & \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle \\ |10\rangle & \mapsto & \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle \\ |11\rangle & \mapsto & \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle \end{cases}$$

Kuvassa 4, joka on yllä olevan taulukon laajennus, on viimeisessä sarakkeessa esitetty miten Bobin operaatio vaikuttaa. Viimeinen sarake on saatu suoralla laskulla, esimerkiksi tilan $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ operaatio muuntaa tilaksi

$$\begin{aligned} & \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle\Big) \\ + \quad & \frac{1}{\sqrt{2}}\Big(\frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle\Big) \\ = \quad & \frac{1}{2}|00\rangle + \frac{1}{2}|10\rangle \\ + \quad & \frac{1}{2}|00\rangle - \frac{1}{2}|10\rangle = |00\rangle\,. \end{aligned}$$

Lopuksi Bobin tarvitsee vain havainnoida omat kvanttibittinsä; tällöin hän saa ylläolevan taulukon mukaan suoraan selville Alicen bitit b_1 ja b_2.

Viitteet

[1] Adriano Barenco, Charles H. Bennett, Richard Cleve, David P. DiVincenzo, Norman Margolus, Peter Shor, Tycho Sleator, John Smolin, Harald Weinfurter: *Elementary gates for quantum computation*, Physical Review A 52:5, 3457–3467 (1995). quant-ph/9503016.[11]

[2] Charles H. Bennett: *Logical reversibility of computation*, IBM Journal of Research and Development 17, 525–532 (1973). http://www.research.ibm.com/people/b/bennetc/bennettc19734c533842.pdf

[3] Charles H. Bennett: *Quantum cryptography using any two nonorthogonal states*, Physical Review Letters 68:21, 3121 – 3124 (1992). http://www.research.ibm.com/people/b/bennetc/qc2nos.pdf

[4] Charles H. Bennett, Gilles Brassard: *Quantum cryptography: public key distribution and coin tossing*, Proceedings of IEEE conference on Computers, Systems, and Signal processing. Bangalore (India), 175–179 (1984). http://www.research.ibm.com/people/b/bennetc/bennettc198469790513.pdf

[5] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Ahsher Peres, William K. Wootters: *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Physical Rewiev Letters 70, 1895–1899 (1993).

[11] quant-ph/9503016 viittaa osoitteeseen http://xxx.lanl.gov/abs/quant-ph/9503016.

http://www.research.ibm.com/people/b/bennetc/BBCJPW.pdf

[6] Charles H. Bennett, Stephen J. Wiesner: *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Physical Review Letters, 69(20): 2881–2884 (1992). http://www.research.ibm.com/people/b/bennetc/bennettc19926c731103.pdf

[7] Ethan Bernstein, Umesh Vazirani: *Quantum complexity theory*, SIAM Journal of Computing 26:5, 1411–1473 (1997).

[8] D. Boschi, S. Branca, F. De Martini, L. Hardy, S. Popescu: *Experimental realization of teleporting an unknown pure quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Physical Review Letters 80:6, 1121–1125 (1998). quant-ph/9710013.

[9] Dik Bouwmeester, Jian-Wei Pan, Klaus Mattle, Manfred Eibl, Harald Weinfurter, Anton Zeilinger: *Experimental quantum teleportation*, Nature 390, 575–579 (1997).

[10] Nicolas J. Cerf, Chris Adami: *Quantum information theory of entanglement and measurement*, Physica D 120:1–2, 62–81, (1998). quant-ph/9605039.

[11] Clay Mathematics Institute, http://www.claymath.org/

[12] David Deutsch: *Quantum theory, the Church-Turing principle and the universal quantum computer*, Proceedings of the Royal Society of London A 400, 97–117 (1985).

[13] David Deutsch: *Quantum computational networks*, Proceedings of the Royal Society of London A 425, 73–90 (1989).

[14] David Deutsch, Richard Jozsa: *Rapid solutions of problems by quantum computation*, Proceedings of the Royal Society of London A 439, 553–558 (1992).

[15] Richard P. Feynman: *Simulating physics with computers*, International Journal of Theoretical Physics 21:6/7, 467–488 (1982).

[16] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, E. S. Polzik: *Unconditional quantum teleportation*, Science 282, 706–709 (1998).

[17] Lov K. Grover: *A fast quantum-mechanical algorithm for database search*, Proceedings of the 28th Annual ACM Symposium on the Theory of Computing – STOC, 212–219 (1996). quant-ph/9605043

[18] Jozef Gruska: *Quantum Computing*, McGraw Hill (1999).

[19] Mika Hirvensalo: *Quantum Computing*, Springer (2001).

[20] http://www.idquantique.com/

[21] Richard Jozsa: *A stronger no-cloning theorem*, quant-ph/0204153.

[22] A. Y. Kitaev: *Quantum computation: algorithms and error correction*, Russian Mathematical surveys 52:1991 (1997).

[23] E. Knill, R. Laflamme, R. Martinez, C.-H. Tseng: *An algorithmic benchmark for quantum information processing*, Nature 404: 368–370 (2000). quant-ph/9908051

[24] Yves Lecerf: *Récursive insolubilité de l'équation générale de diagonalisation de deux monomorphismes de monoïdes libres* $\phi x = \psi x$, Comptes Rendus de l'Académie se Sciences 257, 2940–2943 (1963).

[25] Dominic Mayers: *Unconditional security in quantum cryptography*, quant-ph/9802025.

[26] Michael A. Nielsen, Isaac L. Chuang: *Quantum Computation and Quantum Information*, Cambridge University Press (2001).

[27] Christos H. Papadimitriou: *Computational Complexity*, Addison-Wesley (1994).

[28] A.K. Pati, S. L. Braunstein: *Impossibility of deleting an unknown quantum state*, Nature 404, 164–165 (2000). quant-ph/9911090.

[29] Yaoyun Shi: *Both Toffoli and controlled-NOT need little help to do universal quantum computation*, quant-ph/0205115.

[30] Peter W. Shor: *Algorithms for quantum computation: discrete log and factoring*, Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science – FOCS, 20–22 (1994). quant-ph/9508027

[31] Peter W. Shor: *Scheme for reducing decoherence in quantum computer memory*, Physical Review A 52:4, 2493–2496 (1995).

[32] Daniel R. Simon: *On the power of quantum computation*, Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science – FOCS, 116–123 (1994).

[33] Barbara M. Terhal: *Detecting quantum entanglement*, Theoretical Computer Science 287:1, 313–335 (2002). quant-ph/0101032.

[34] W. Tittel, J. Brendel, H. Zbinden, N. Gisin: *Violation of Bell inequalities by photons more than 10 km apart*, Physical Review Letters 81:17, 3563–3566, (1998). quant-ph/9806043.

[35] Tommaso Toffoli: *Bicontinuous extensions of invertible combinatorial functions*, Mathematical Systems Theory 14, 13–23 (1981).

[36] Lieven M. K. Vandersypen, Matthias Steffen, Gregory Breyta, Costantino S. Yannoni, Mark H. Sherwood, Isaac L. Chuang: *Experimental realization of Shor's quantum factoring algorithm using nuclear magnetic resonance*, Nature 414: 883–887 (2001). quant-ph/0112176

[37] Ronald de Wolf: *Quantum communication and complexity*, Theoretical Computer Science 287:1, 337–353 (2002).

[38] William K. Wootters, Wojciech H. Zurek: *A single quantum cannot be cloned*, Nature 299, 802–803 (1982).