Tampereen yliopisto

Seela Nissinen

KVANTTITIETOKONEET JA KVANTTILASKENNAN PERUSTEET

Kandidaatin tutkielma
Informaatioteknologian ja viestinnän tiedekunta
Tarkastajat: Yliopistonlehtori Erja Sipilä ja professori Teemu Ojanen
Heinäkuu 2022

TIIVISTELMÄ

Seela Nissinen: Kvanttitietokoneet ja kvanttilaskennan perusteet
Kandidaatin tutkielma
Tampereen yliopisto
Tieto- ja sähkötekniikan TkK-tutkinto-ohjelma
Heinäkuu 2022

Kvanttimekaniikka on kummastuttanut fyysikoita jo vuosisadan ajan. Silti kiinnostus sen tutkimiseen ei ole laantunut. Nykypäivänä kvanttimekaanisiin ilmiöihin perustuvia kvanttitietokoneita on kehitteillä ympäri maailman, vaikka niiden rakentaminen onkin osoittautunut erittäin haastavaksi. Kvantti-ilmiöt ovat äärimmäisen herkkiä ulkoisille häiriöille, minkä takia ne vaativat erityiset olosuhteet, jotta laskentaa voidaan ylipäätään suorittaa. Tässä työssä perehdytään siihen, miksi halutaan rakentaa jotain niin vaikeaa ja monimutkaista.

Kvanttilaskenta perustuu moderniin tietojenkäsittelytieteeseen, joka syntyi 1900-luvun alkupuolella, kun laskentaprosesseja alettiin mallintaa matemaattisesti. Laskentatehtävää suoritettaessa on aluksi selvitettävä tehtävän laskettavuus, mikä niihin aikoihin aiheutti päänvaivaa matemaatikoille. Vuonna 1936 Alan Turing kehitteli laskettavuuden ongelmaan Turingin koneen, joka on teoreettinen tietokoneen malli. Turingin kone oli suunniteltu simuloimaan tiettyä algoritmia. Turingin koneesta kehittyi aikojen saatossa erilaisia versioita, joilla pystyttiin ratkaisemaan yhä monimutkaisempia laskentatehtäviä. Myöhemmin 1980-luvulla fyysikoiden työn tuloksena syntyi kvanttimekaanisia systeemejä simuloiva malli, joka nykyään tunnetaan kvanttitietokoneena.

Kvanttilaskennan luonne poikkeaa perustavanlaatuisesti klassisesta tietojenkäsittelystä. Niiden välillä on kuitenkin tietty analogia, jota tässä työssä havainnollistetaan. Kvanttimekaaniset systeemit, kubitit, toimivat informaation yksikköinä kvanttipiireissä aivan kuten bitit digitaalisissa piireissä. Kubitilla on kvanttimekaanisen luonteensa vuoksi erikoisia ominaispiirteitä, jotka erottavat sen tavallisesta bitistä ja tarjoavat mahdollisuuksia monimutkaisempaan tiedonkäsittelyyn. Kvanttitietokoneet suorittavat kvanttialgoritmeja. Tärkein niistä on Peter Shorin vuonna 1994 julkaisema algoritmi, jonka avulla suuriakin kokonaislukuja voidaan jakaa tekijöihin lyhyessä ajassa.

Kvanttitietokoneiden fyysiselle toteutukselle on erilaisia vaihtoehtoja. Työssä tutustutaan yhteen niistä, joka on suprajohtava kvanttitietokone. Suprajohtavaa toteutusta tarkastellaan kvanttitietokoneelle annettujen kriteerien valossa: mitkä niistä toteutuvat ja millaisia ongelmia on ratkaistava, jotta kvanttitietokone täyttäisi loputkin niistä. Kvanttiteknologia on uusi tutkimusala, johon investoidaan valtavasti. Kvanttimaailman ihmeet ja niiden mahdollisuudet käytännön sovelluksissa ovat kiehtovia, ja teknisiin ongelmiin haetaan kuumeisesti ratkaisuja. Kvanttitietokone on todiste siitä, kuinka häviävän pienistä, omituisesti käyttäytyvistä kvanteista voidaan rakentaa suuri kompleksinen kokonaisuus, jolla on mahdollista laskea vaikeitakin ongelmia äärimmäisen nopeasti.

Avainsanat: laskenta, Turingin kone, kvanttilaskenta, kvanttitietokone, kubitti, kvanttialgoritmi

SISÄLLYSLUETTELO

LYHENTEET JA MERKINNÄT

AES	Advanced Encryption Standard
MIT	Massachusetts Institute of Technology, Massachusettsin teknillinen korkeakoulu
NMR	Nuclear Magnetic Resonance, ydinmagneettinen resonanssi
PTM	Probabilistic Turing machine, probabilistinen Turingin kone
QD	Quantum Dot, kvanttipiste
QEC	Quantum Error Correction, kvanttivirheenkorjaus
QED	Quantum Electrodynamics, kvanttielektrodynamiikka
QTM	Quantum Turing Machine, Turingin kvanttitietokone
UQTM	Universal Quantum Turing Machine, universaali Turingin kvanttitietokone
UTM	Universal Turing Machine, universaali Turingin kone

1 JOHDANTO

Kvanttitietokoneiden toiminta perustuu kvanttimekaniikan ilmiöihin. Kvanttimekaaniset hiukkaset käyttäytyvät tavalla, joka poikkeaa perusteellisesti klassisista, makroskooppisista ilmiöistä. Siksi ne voivatkin vaikuttaa melko kummallisilta ja herättää epäluuloa. Kuitenkin niin epäintuitiiviselta kuin kvanttimaailma näyttääkin, on olemassa suuri määrä kokeita, jotka osoittavat lopullisesti, että maailmankaikkeus todella toimii kvanttimekaniikan lakien mukaan pienimmässä mittakaavassa. Tätä saattaa olla vaikea ymmärtää klassisesta näkökulmasta, koska emme yleensä näe kvanttimaailman ilmiöitä ihmissilmällämme.

Kvanttitietokoneet toimivat kubiteilla, jotka ovat pieniä kvanttijärjestelmiä. Kubittina voi toimia elektroni, fotoni tai mikä tahansa hiukkanen, jolla havaitaan aalto-hiukkasduaalisuutta ja muita ei-klassisia ominaisuuksia. Kvanttijärjestelmillä on erityisiä ominaisuuksia, joista yksi on superpositiotila. Kvanttijärjestelmän mittaaminen kuitenkin romuttaa superpositiotilan yhdeksi määrätyksi klassiseksi tilaksi. Tämä piirre vaivasi Albert Einsteinia. Hänen ystävänsä Abraham Pais kirjoittaa: ”Muistan, että yhden kävelyn aikana Einstein yhtäkkiä pysähtyi, kääntyi puoleeni ja kysyi, uskoinko todella, että kuu on olemassa vain katsoessani sitä.” [1, s. 4]

Kubiteilla on myös muita ainutlaatuisia ominaisuuksia, joita hyödynnetään kvanttilaskennassa. Niin kutsuttu lomittumisilmiö kytkee kubitit toisiinsa, jolloin niiden väliset korrelaatiot välittyvät nopeasti. Lomittuneet kubitit vuorovaikuttavat keskenään tavalla, jota Einstein kutsui ”aavemaiseksi”. Näihin arkijärjen vastaisiin ilmiöihin perustuvat monet kvanttialgoritmit. Mitä suuremmassa mittakaavassa näitä ilmiöitä pystytään käytännössä toteuttamaan, sitä enemmän kvanttitietokoneelle saadaan tehoa. Kubittien määrää halutaan siis kasvattaa. Kuitenkin mitä enemmän kubitteja lisätään, sitä todennäköisemmin kubitit ovat vuorovaikutuksessa ympäristön kanssa. Ympäristön aiheuttama dekoherenssi tuhoaa järjestelmän kvanttiominaisuuksia, ja onkin yksi suurimmista haasteista toimivan kvanttitietokoneen rakentamisessa. [1, s. 59-60, 90]

Viimeisten vuosikymmenten ajan kvanttilaskennan tutkimuksessa on etsitty vastauksia seuraavaan kysymykseen: voidaanko saada jotakin etua siitä, että tallennetaan, siirretään ja prosessoidaan tietoa järjestelmissä, joilla on ainutlaatuisia kvanttiominaisuuksia? Tänä päivänä on ymmärretty, että vastaus on kyllä: useat tutkimusryhmät ympäri maailman työskentelevät saavuttaakseen erittäin kunnianhimoisen teknologisen tavoitteen, kvanttitietokoneen rakentamisen. Kvanttitietokone voi dramaattisesti parantaa laskentatehoa tietyissä laskentatehtävissä. Useita fyysisiä järjestelmiä, jotka kattavat suuren osan

nykyaikaisesta fysiikasta, kehitetään kvanttilaskentaa varten. On kuitenkin edelleen epäselvää, mikä tekniikka, jos sellainen on, lopulta osoittautuu menestyksekkääksi. Tässä työssä kuvailemme yhden johtavimmista lähestymistavoista, suprajohteisiin perustuvan kvanttitietokoneen, periaatteen, ja pohdimme sen mahdollisuuksia. [2, s. 45]

Kandidaatintyön toisessa luvussa tarkastellaan kvanttilaskennan historiaa. Kolmannessa luvussa syvennytään kvanttimekaanisiin ilmiöihin ja selvitetään, kuinka niitä voidaan hyödyntää kvanttilaskennassa. Neljännessä luvussa tarkastellaan kvanttitietokoneiden arkkitehtuureja ja käsitellään kvanttitietokoneen rakentamiseen liittyviä haasteita. Viimeisessä luvussa pohditaan myös kvanttitietokoneiden tutkimuksen tulevaisuuden näkymiä. Lopuksi esitetään yhteenveto tutkielman aiheista ja työn pohjalta tehdyistä johtopäätöksistä.

2 KVANTTILASKENNAN HISTORIAA

Tässä luvussa käsitellään kvanttilaskennan historiaa. Aloitetaan tarkastelu sadan vuoden takaisesta modernin klassisen laskennan synnystä, ja tutustutaan Turingin koneeseen. Lopuksi tarkastellaan sitä, kuinka Turingin koneesta kehittyi myöhemmin kvanttitietokoneen teoreettinen malli.

2.1 Klassisen laskennan malleista

Kvanttilaskennan paradigma perustuu pitkälti moderniin klassiseen laskentateoriaan, jonka voidaan sanoa pohjautuvan brittiläisen matemaatikko Alan Turingin saavutuksiin tietojenkäsittelytieteessä 1930-luvulla. Turingin sekä muiden 1900-luvun matemaatikkojen ponnistusten ansiosta laskentaprosesseja alettiin mallintaa matemaattisesti. Laskentaprosessista kyettiin siten erottelemaan perusominaisuuksia riippumatta alustasta, jolla se suoritettiin. [3, s. 101] Tutustutaan tarkemmin siihen, miten klassisen laskennan mallit kehittyivät viime vuosisadalla.

2.1.1 Turingin kone

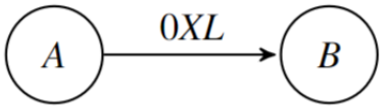
1900-luvun matemaatikoita ja logiikan tutkijoita vaivasi niin kutsuttu *laskettavuusongelma*. Laskentatehtävää suoritettaessa on tärkeää aluksi selvittää, onko tehtävä ylipäätään ratkaistavissa tietokoneella. Tätä kutsutaan *laskettavuudeksi*. Jos haluttaisiin selvittää funktion laskettavuus, olisi tarkasteltava erikseen jokaista funktion laskemiseen suunniteltua algoritmia, mikä olisi ilmeisen työlästä. Ratkaisuna laskettavuuden ongelmaan Alan Turing kehitti vuonna 1936 teoreettisen tietokoneen mallin, joka tunnetaan *Turingin koneena*. [3, s.101]

Turingin kone *M* on äärellinen tilakone, joka lukee symbolisen syötteen nauhalta, suorittaa sen perusteella toimintoja vaiheittain ja antaa tuloksen. Turingin kone koostuu seuraavista osista:

1. *Nauha*, joka pituus on rajaton molempiin suuntiin. Nauha koostuu peräkkäisistä ruuduista, joista kukin sisältää yhden symbolin äärellisestä symbolien joukosta $\Gamma = \{s_i\}$. Symboli voi olla binääriluku 0,1 tai tyhjä $(\emptyset)$.
2. *Lukupää*, joka lukee syötteen ruudusta tai kirjoittaa ruutuun. Nauhalle kirjoittamisen etuna on, että Turingin kone voi tallentaa välituloksia, joita voidaan tarvita myöhemmissä laskutoimituksissa, sekä tulostaa lopullisen laskentatuloksen.

3. *Rekisteri*, joka tallentaa koneen senhetkisen tilan, joka kuuluu äärelliseen tilojen joukkoon $Q = \{q_i\}$. Alkutilaa merkitään symbolilla *S* ja lopputilaa symbolilla *H*.
4. *Siirtymäfunktio*, joka asettaa Turingin koneen seuraavaan tilaan. Siirtymäfunktio määrittää ruudun uuden symbolin ja antaa käskyn lukupäälle joko pysyä paikallaan tai siirtyä nauhalla yhden ruudun vasemmalle tai oikealle. Siirtymäfunktion määräämä tilasiirtymä riippuu sen hetkisestä syötteestä ja edellisestä tilasta.

Havainnollistetaan Turingin koneen toimintaa yksinkertaisen esimerkin avulla. Oletetaan, että kone on tilassa *A* ja nauhalta luetaan symboli 0. Sen jälkeen siirrytään tilaan *B*, korvataan 0 kirjoittamalla ruutuun symboli *X* ja siirretään lukupää yhden ruudun verran vasemmalle. Kuvassa 1 on esitetty esimerkin mukainen Turingin koneen tilakaavio. [3, s. 102][4, s. 50]



Kuva 2.1. *Turingin koneen toimintaa voidaan havainnollistaa tilakaaviolla. [4, s. 50]*

Turingin koneen tilakaavion nuolet merkitään kolmella symbolilla; ensimmäinen on nauhalta luettava symboli, toinen on nauhalle kirjoitettava symboli ja viimeinen kertoo, siirretäänkö lukupäätä vasemmalle (L) vai oikealle (R), vai pidetäänkö se paikallaan (0). [4, s. 50]

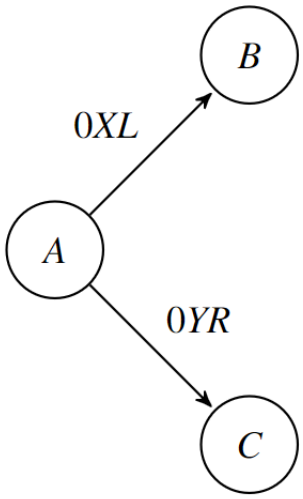
Jokainen Turingin kone on määritelty tietyn symbolijoukon Γ, tilojen joukon Q ja toiminnallisuuden perustella. Tämä tarkoittaa sitä, että tietylle algoritmille määritellään tietty Turingin kone. On kuitenkin mahdollista ohjelmoida kone suorittamaan erilaisia algoritmeja, mikäli ohjelma annetaan koneelle osana syötettä. Tällaista Turingin konetta, joka voi simuloida mitä tahansa muuta Turingin konetta, kutsutaan *universaaliksi Turingin koneeksi* (eng. Universal Turing Machine, UTM). Turing ja Alonso Church, joka samoihin aikoihin työskenteli laskettavuuden ongelman parissa, olivat itsenäisesti päätyneet samaan hypoteesiin funktioiden laskettavuudesta. Tämä myöhemmin julkaistu *Churchin-Turingin teesi* kuuluu seuraavasti:

"Jokainen funktio, jota pidetään laskettavana luonnollisella tavalla, voidaan laskea universaalilla Turingin koneella."

Tarkemmin sanottuna päädyttiin siihen hypoteesiin, että ongelma on laskettavissa, mikäli universaali Turingin kone lopulta pysähtyy. Mielenkiintoista kuitenkin oli, että sitä, pysähtyykö tietty Turingin koneen algoritmi, ei voida laskea. Tätä kutsutaan *pysähtymisongelmaksi*. Voidaanko tietystä ongelmasta, jota UTM ei voi laskea, tehdä laskettava eri laskentaparadigmalla? Tähän ratkaisuna oli Turingin koneen konseptin laajentaminen *probabilistiseen Turingin koneeseen*. [4, s.62] [3, s. 104]

2.1.2 Probabilistinen Turingin kone

Churchin-Turingin teesin haasteena olivat probabilistiset algoritmit, joilla voidaan ratkaista ongelmia tehokkaasti mutta tietyllä epäonnistumisen todennäköisyydellä. Esimerkki tällaisesta algoritmista on Solovayn ja Strassenin testi (1977), jota ei voida ratkaista yllä kuvatulla *deterministisellä* Turingin koneella. Siispä Churchin-Turingin teesiä haluttiin laajentaa päteväksi myös probabilististen algoritmien tapauksessa eli suunniteltiin probabilistinen Turingin kone (eng. Probablistic Turing Machine, PTM). [3, s. 104] Koska probabilistinen Turingin kone voi olla useammassa kuin yhdessä tilassa samanaikaisesti, eli se voi suorittaa rinnakkaisia operaatioita, se on nopeampi kuin aiemmin kuvattu deterministinen Turingin kone. PTM valitsee jokaisen toimintonsa sattumanvaraisesti mahdollisten vaihtoehtojen joukosta jollakin tietyllä todennäköisyydellä. PTM tarvitse siis lisäksi toisen nauhan, joka sisältää satunnaislukuja, jotka valitsevat suoritettavat operaatiot. Kuvassa 2.2 nähdään PTM, joka on tilassa A ja joka lukee nauhalta syötteen 0. Tällöin sillä on kaksi vaihtoehtoa: siirtyä tilaan B, korvata syöte symbolilla X ja siirtää lukupäätä vasemmalle; tai siirtyä tilaan C, korvata syöte symbolilla Y ja siirtää lukupäätä oikealle. Laskennassa on siis monia vaihtoehtoja eli haaroja. Jos jokin haaroista saavuttaa lopputilan, kone pysähtyy ja syötejono hyväksytään. [3, s. 104][4, s.65]



Kuva 2.2. *Probabilistisella Turingin koneella voi olla enemmän kuin yksi mahdollinen tilasiirtymä tietyllä syötteellä. [4, s. 65]*

2.2 Kohti kvanttitietokonetta

"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."

Nämä kuuluisat sanat lausui Richard Feynman vuonna 1981 Massachusettsin teknillisen korkeakoulun (Massachusetts Institute of Technology, MIT) järjestämässä ensimmäisessä laskennallisen fysiikan konferenssissa (The Physics of Computation Conference). [5,

s. 486] Hän havaitsi, että probabilistisella Turingin koneella ei voida tehokkaasti simuloida kvanttimekaanisen systeemin aikaevoluutiota. Tapa, jolla kvanttisysteemi kehittyy ja käsittelee informaatiota, eroaa olennaisesti klassisesta tiedonkäsittelystä. Tämä haastoi Churchin-Turingin teesin, sillä sen mukaan mikä tahansa laskettavissa oleva funktio on mahdollista laskea Turingin koneella. [3, s. 104] Tarkastellaan seuraavaksi sitä, kuinka Turingin koneen pohjalta kehitettiin kvanttimekaanista systeemiä kuvaava teoreettinen kvanttitietokoneen malli.

2.2.1 Turingin kvanttitietokone

Kvanttimekaanisen systeemin tilan kuvaamiseen tarvitaan huomattavan suuri määrä klassista informaatiota verrattuna vastaavan klassisen tilan kuvaamiseen. Feynman kuitenkin oivalsi, että kvanttimekaniikan lait mahdollistavat monimutkaisemman tietojenkäsittelyn, jota voitaisiin toteuttaa *kvanttitietokoneella*. (Feynman itse käytti termiä "kvanttimekaaninen tietokone") [6, s.268] Myöhemmin vuonna 1985 David Deutsch muotoili *Turingin kvanttitietokoneen* (eng. Quantum Turing Machine, QTM) mallin. Merkittävä oivallus QTM:n taustalla oli, että se on sekä probabilistinen että lisäksi *reversiibeli*, eli laskentaoperaatioita voidaan ajaa käänteisesti palauttamalla kone lopputilasta takaisin alkutilaan. Tämä oli olennaista siksi, että myös kvanttimekaanisen systeemin aikaevoluutio on reversiibeli prosessi. [3, s. 104]

Turingin kvanttitietokoneen toimintaperiaate on samankaltainen kuin probabilistisella Turingin koneella, jolla ajetaan todennäköisyyksiin perustuvia algoritmeja. QTM nimittäin suorittaa laskentaa kompleksisilla siirtymäamplitudeilla, joiden neliöt ilmaisevat todennäköisyyttä. [7, s. 123] Klassisen Turingin koneen komponentit, kuten äärettömän pitkä nauha, lukupään paikka, prosessori, siirtymäjoukko ja pysäytystoiminto ovat Turingin kvanttitietokoneessa niiden kvanttiversioita. QTM:n nauha koostuu kvanttimekaanisista informaation yksiköistä, *kubiteista*. Lukupää voi siirtyä nauhalla vain yhden askeleen ruudusta toiseen. Useiden laskentavaiheiden jälkeen lukupää asettuu superpositioon, eli se on useassa kohdassa nauhalla yhtä aikaa, eikä sen sijaintia voida tarkasti määrittää. Kun QTM pysähtyy, suoritetaan mittaus. Mittauksen tulos on jollakin siirtymäamplitudin määräämällä todennäköisyydellä valittu satunnainen superposition konfiguraatio (nauhan ruutu). [8, s. 1 ja 5]

QTM:n määrittelyssä käytetään *Hilbertin avaruuksia*, joilla kuvataan kvanttimekaanisia tiloja. Klassisen Turingin koneen tilajoukko korvataan QTM:ssä Hilbertin avaruuden vektoreina, ja siirtymäfunktio korvataan unitaarisella operaattorilla U, jolla kuvataan kvanttimekaanisen systeemin muutosta ja joka on Hilbertin avaruuden operaattori. Hilbertin avaruuden hyödyntämistä kvanttilaskennassa käsitellään tarkemmin luvussa 3.1.

QTM määritellään kompleksisten lukujen joukolla $\langle Q, F, H, P, \Gamma, \sum, \delta_{QTM} \rangle$:

1. Q: QTM:n mahdollisten tilojen Hilbertin avaruus.
2. $F \subseteq Q$: prosessorin alku- ja lopputilojen aliavaruus Hilbertin avaruudessa Q.

3. H: pysäytyskubitin (eng. halting qubit) Hilbertin avaruus. Pysäytyskubitti kertoo, milloin laskennan tulos voidaan lukea nauhalta.
4. P: Lukupään sijainnin Hilbertin avaruus $P = \{|p\rangle\}$.
5. Γ: Kvanttinauhojen symbolien Hilbertin avaruus. ”Tyhjä” -symboli vastaa nollavektoria.
6. $\sum \subseteq \Gamma$: Kvanttinauhan alkutilojen joukko.
7. δ_{QTM}: tilasiirtymien joukko on $Q \times \Gamma \times P \times H \longrightarrow Q \times \Gamma \times P \times H$. Tietty tilasiirtymä vastaa unitaarista operaattoria U.

QTM:llä voidaan myös suorittaa monia laskentaoperaatioita yhtäaikaisesti. Tätä ominaisuutta kutsutaan *kvanttirinnakkaisuudeksi*, ja siihen perustuvat monet *kvanttialgoritmit*, joiden tarkoitus on nopeuttaa laskentaa. [8, s. 4-5][9, s. 67]

Jokaiselle unitaariselle operaattorille U voidaan määrittää tietty Turingin kvanttitietokone. Toisin sanoen jokainen QTM vastaa tiettyä algoritmia. QTM:llä voidaan tuottaa lineaarisessa ajassa eksponentiaalinen määrä tuloksia, mutta valitettavasti niitä kaikkia ei voida määrittää. Tilasiirtymien unitaarisuus kuitenkin mahdollistaa sen, että QTM:llä voidaan suorittaa reversiibeliä eli käännettävää laskentaa. [10, s. 2] Tiedetään, että mikä tahansa funktio, joka voidaan laskea Turingin koneella, voidaan laskea myös reversiibelillä Turingin koneella, johon QTM lukeutuu. Turingin kvanttitietokone on siis ainakin yhtä tehokas kuin klassinen Turingin kone. [11, s. 33]

2.2.2 Uusia kvanttilaskennan malleja

David Deutsch osoitti, että on olemassa teoreettinen *universaalin Turingin kvanttitietokoneen* (eng. Universal Quantum Turing Machine, UQTM) malli, jolla voidaan simuloida mitä tahansa toista Turingin kvanttitietokonetta jollain satunnaisella tarkkuudella. Hän ei kuitenkaan käsitellyt sitä, kuinka tehokas UQTM todellisuudessa on. Vuonna 1997 Bernstein ja Vazirani julkaisivat UQTM:n mallin, joka simuloi mitä tahansa Turingin kvanttitietokonetta millä tahansa halutulla tarkkuudella $\epsilon > 0$. Kun aika-askelten T (aika, joka kuluu yhteen tilasiirtymään) lukumäärä annetaan sille syötteenä, UQTM laskee tuloksen ja pysähtyy. Deutschin mukaan jaksollisilla mittauksilla voitaisiin määrittää, milloin kvanttitietokoneen laskenta oli pysäytettävä, kun taas Bernstein ja Vazirani tarkastelivat laskentaa, jonka vaiheiden lukumäärä on ennalta määrätty. [11, s. 33] [12, s.8]

Toinen hyödyllinen konventio kvanttilaskennan kuvaamiseen on *kvanttipiirimalli*. Samoin kuin klassisessa logiikkapiirissä bittejä operoidaan loogisilla porteilla, myös kvanttipiirissä *kvanttiportit* muuntavat johtimia pitkin kulkevia kvanttibittejä eli kubitteja loogisilla operaatioilla. Vuonna 1993 Yao esitti kvanttisimulaatiota käsittelevän julkaisun, jonka mukaan Turingin kvanttitietokonetta, jonka aika-askelten pituus on T ja syötteen pituus *n* ja jolle pätee $T > n$, voidaan simuloida tietyillä kvanttipiireillä, joiden koko on T^2. [13, s. 61] [12, s. 1]

1900-luvulla tapahtui kvanttilaskennan kehityksen läpimurto, kun Peter Shor esitti, että

suurten kokonaislukujen jako tekijöihin olisi mahdollista kvanttitietokonella. *Shorin algoritmilla* olisi mahdollista murtaa nykyisin käytössä olevia kryptografisia järjestelmiä. Toinen kvanttilaskennan kehitykselle tärkeä löydös oli *Groverin hakualgoritmi*, jolla voidaan tehokkaasti hakea alkioita suurista tietokannoista. Näitä kahta kvanttialgoritmia tarkastellaan tarkemmin luvussa 3.4.2. [14, s. 3]

Kvanttihakualgoritmeista on mahdollista määrittää sellaisia jatkuva-aikaisia versioita, joiden laskennallisia malleja voidaan simuloida tehokkaasti kvanttipiirimallin avulla. Toinen mielenkiintoinen ehdotus kvanttialgoritmiksi on *Kvanttikulku* (eng. quantum walk), joka on vastine klassiselle satunnaiskululle (eng. random walk). Satunnaiskulku on stokastinen prosessi, joka kuvaa satunnaismuuttujien askelista muodostuvaa polkua. [15, s. 205-206]. Kvanttikulkualgoritmilla voidaan löytää optimaalisia algoritmeja niin kutsutun kvanttikompleksisuusteorian ongelmien, kuten osien erotusongelman (eng. element distinctness) ratkaisemiseksi (ks. [16]). [13, s. 178]

Puoli vuosisataa kestäneen teoreettisen kvanttilaskennan tutkimustyön tuloksena on löydetty kuitenkin vain vähän kvanttialgoritmeja. Yksinkertaisen kvanttitietokoneen ohjelman ymmärtäminen, saati edistyneiden ohjelmistotyökalujen suunnittelu ja kehittäminen vaatii niin suuren määrän taustatietoa kvanttilaskentajärjestelmistä, että useimmilla ohjelmistotekniikan osaajilla sitä ei ole. [17, s. 258] Siispä kvanttilaskennan tutkimuksessa tarvitaan eri alojen asiantuntijoiden yhteistyötä.

3 KVANTTILASKENNAN PERIAATTEITA

Tämä luku on lyhyt johdatus kvanttilaskentaan ja kvanttimekaniikan formalismiin. Perehdytään siihen, kuinka kvanttitilojen ominaisuuksia hyödynnetään kvanttilaskennassa. Lopuksi esitellään kvanttipiirien komponentteja ja tutustutaan kvanttialgoritmeihin.

3.1 Notaatioita ja Hilbertin avaruus

Kvanttilaskennassa käytetään lineaarialgebran notaatiota, Paul Diracin kehittelemää Diracin bra-ket-merkintätapaa, kuvaamaan kvanttimekaanisia tiloja. Diracin notaatiossa vektori *v* esitetään ”ket”-merkinnällä $|v\rangle$. Vektori $|v\rangle$ kuuluu kompleksiseen vektoriavaruuteen *V*. [13, s. 21] Ket-vektorin konjugaattitranspoosia *f* esitetään ”bra”-merkinnällä $\langle f|$ [18, s. 2725]. Bra-vektori kuuluu duaaliavaruuteen $V^\dagger$ [13, s. 21]. Duaaliavaruuden [$V^\dagger$, $\langle f|$] ja lineaarisen avaruuden [*V*, $|v\rangle$] välillä vallitsee relaatio

$$|v\rangle \equiv \langle f|^\dagger ,$$

jossa notaatio $R^\dagger$ merkitsee Hermiten konjugointia. Vektorien *f* ja *v* sisätulo $\langle f|v\rangle$ on niin kutsuttu "bra-ket". [19, s. 30 ja s. 40]

Kvanttimekaniikan ensimmäisen postulaatin, tila-avaruuspostulaatin (State Space postulate), mukaan tarkastelemamme kompleksiset ja äärelliset vektoriavaruudet kuuluvat niin sanottuihin Hilbertin avaruuksiin $\mathcal{H}$, jotka sisältävät kvanttimekaanisia tiloja edustavia tilavektoreita $|\psi\rangle$. Hilbertin avaruudella tarkoitetaan täydellistä kompleksista vektorien sisätuloavaruutta, ja sitä merkitään symbolilla $\mathcal{H}$. Tietyillä systeemin vapausasteilla $\mathcal{H}$:n dimensio voi olla ääretön. Funktioanalyysin kirjallisuudessa käsitellään usein ääretönulotteisia avaruuksia matemaattisesti eksaktisti, mutta tämä tarkastelutapa on kuitenkin hyvin monimutkainen. Sen takia kvanttilaskennan mallien kuvaamiseksi ollaan lähinnä kiinnostuneita sellaisista vapausasteista, joiden tiloja kuvataan vektoreilla äärellisulotteisessa Hilbert-avaruudessa. [13, s. 21 ja s.39] [19, s. 4] Kuten klassisessa tiedonkäsittelyssä, myös kvanttitietokoneiden yhteydessä käytetään tyypillisesti Hilbertin avaruuden dimensiona 2^n, missä *n* on jokin positiivinen kokonaisluku. Yhdistelemällä näitä pienempiä systeemejä saavutetaan suurempia tila-avaruuksia. [13, s. 21-22]

3.2 Informaatio digitaali- ja kvanttipiireissä

Kvantti-informaatio on perimmäiseltä luonteeltaan hyvin erilaista kuin klassinen informaatio, mutta niiden välillä on myös tiettyjä yhtäläisyyksiä. Digitaalisessa piirissä tietoalkion pienin osa on binäärisiä arvoja saava bitti, kun taas kvanttipiirissä kvanttimekaaninen kaksitilasysteemi, kubitti. Seuraavissa alaluvuissa määritellään tarkemmin bitin ja kubitin käsitteet.

3.2.1 Bitti

Klassiset tietokoneet toimivat biteillä, informaation pienimmillä yksiköillä, jotka voivat esittää kahta toisensa poissulkevaa loogista arvoa 0 tai 1. Digitaalisissa tietokoneissa bitti voidaan muodostaa esimerkiksi johtimen jännitteestä osoittamalla binääriarvo 0 tilaan, jossa johtimen jännite on 0 V ja arvo 1 tilaan, jossa johtimella on jokin positiivinen jännite, kuten +5 V. [13, s. 39][20, s. 222-223].

Niin kutsutussa deterministisessä piirissä (deterministic circuit) johtimien bittien arvot määrittelevät piirin tilan tietyssä pisteessä. Tarkastellaan yksittäistä bittiä, joka saa arvon 0 todennäköisyydellä p_0 ja arvon 1 todennäköisyydellä p_1. Näistä arvoista voidaan luoda kaksiulotteinen vektori

$$\begin{bmatrix} p_0 \\ p_1 \end{bmatrix}. \tag{3.1}$$

Deterministisessä piirissä oleva johdin, jonka tila on 0, voidaan määritellä vektorilla

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}. \tag{3.2}$$

Samalla periaatteella johdin, jonka tila on 1, voidaan ilmoittaa muodossa

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{3.3}$$

Todennäköisyyspiirin (probabilistic circuit) kuvaus on hieman monimutkaisempi. Todennäköisyyspiirin bitistä arvoja p_0 ja p_1 ei voida määrittää tarkasti. Voidaan kuitenkin kerätä tilastoja riippumattomien todennäköisyysbitin kopioiden arvoista p_0 ja p_1, joissa p_0 merkitsee todennäköisyyttä bitin arvolle 0 ja p_1 arvolle 1. Ehto p_0 + p_1 = 1 pätee aina. [13, s. 8 ja s. 39-42]

3.2.2 Kubitti

Kvanttibitti eli kubitti on kvanttimekaaninen kaksitilasysteemi. Kaksitilasysteemi voidaan muodostaa esimerkiksi polarisoituneesta fotonista. Muodostetaan yksikkövektori $|0\rangle$ kubitin tilalle, jossa fotoni on vaakapolarisoitunut ja ortogonaalinen yksikkövektori $|1\rangle$ kubitin tilalle, jossa fotoni on pystypolarisoitunut. Toisin kuin bitti, joka voi saada joko arvon 0 tai 1, kubitti voi olla myös näiden tilojen superpositiossa eli fotonin tapauksessa jossakin näiden kahden polarisaation välisessä tilassa. Kubitin superpositiota esitetään vektoreina kaksiulotteisessa Hilbertin avaruudessa. [18, s. 2724]

Merkitään avaruuden kahta kantavektoria Diracin merkintätavan mukaan $|0\rangle$ ja $|1\rangle$. Tällöin systeemin tila voidaan ilmaista yleisesti muodossa

$$\alpha_0 |0\rangle + \alpha_1 |1\rangle ,$$

jossa α_0 ja α_1 ovat kompleksisia kertoimia, joita usein kutsutaan myös tilojen $|0\rangle$ ja $|1\rangle$ amplitudeiksi. Kompleksinen amplitudi α voidaan ilmoittaa muodossa $e^{i\theta}|\alpha|$, missä $|\alpha|$ on ei-negatiivinen reaaliluku ja θ on α:n argumentti. [13, s.39-40]

Kubitin superpositiotiloja ei voida yhdellä mittauksella erottaa tiloista $|0\rangle$ ja $|1\rangle$. Kuitenkin jos sama tila preparoidaan monta kertaa, voidaan tehdä joukko mittauksia. Näistä mittauksista saadaan selville tilojen $|0\rangle$ ja $|1\rangle$ todennäköisyydet, eli $|\alpha_0|^2$ ja $|\alpha_1|^2$. Yleensä kaksi kvanttitilaa ovat luotettavasti erotettavissa, jos ja vain jos niiden vektoriesitykset ovat ortogonaalisia. Tätä tarkastellaan yksityiskohtaisemmin luvussa 3.1. Yksikkövektoreilla kuvatulle tilalle pätee mittauspostulaattiin perustuva ehto $|\alpha_0|^2$ + $|\alpha_1|^2$ = 1. Tätä ehtoa kutsutaan joskus normalisointirajoitukseksi (normalization constraint). [18, s. 2725] [13, s.39]

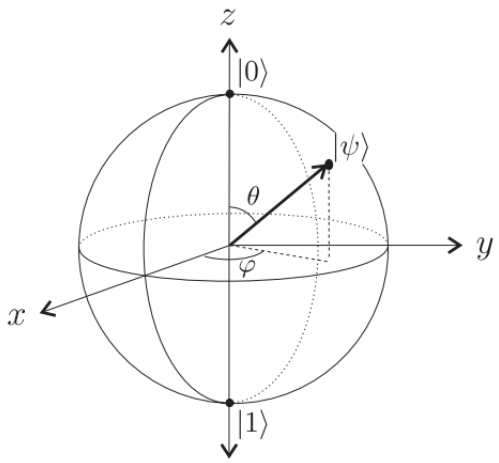
Tila-avaruuspostulaatin ja kompleksisen amplitudin määritelmän nojalla voidaan esittää kubitin yleistä tilaa $|\psi\rangle$ vektorilla

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\vartheta}|\alpha|\sin\left(\frac{\theta}{2}\right)|1\rangle ,$$

jossa $e^{i\vartheta}$ on kubitin aaltovektorin suhteellinen vaihe sekä $0 \leq \theta \leq \pi$ ja $0 \leq \vartheta \leq 2\pi$. Kubitin tilavektoria usein kuvataan pisteenä kolmeulotteisen Blochin pallon pinnalla, kuten kuvassa 3.1 nähdään. Kaksi reaalista parametria θ ja ϑ riittävät kuvaamaan tilavektoria, sillä vektorien normille asetetaan arvo 1. [13, s. 42]

3.3 Kvanttimekaanisten tilojen ominaisuuksia

Edellisessä luvussa nähtiin, että yksittäinen kubitti on jo itsessään kiehtova ja monimutkainen systeemi. Kvanttilaskennassa ollaan kuitenkin kiinnostuneita useamman kuin yhden kubitin systeemeistä. Kahdella kubitilla voidaan esittää tiloja $|00\rangle$, $|01\rangle$, $|10\rangle$ ja $|11\rangle$ neliulotteisessa Hilbertin avaruudessa. Kun kasvatetaan kubittien määrää kolmeen, saa-



Kuva 3.1. *Kubitin tila Blochin pallolla. [13]*

vutetaan 8-ulotteisen Hilbertin avaruuden kanta. Suuren Hilbertin avaruuden dimension hyödyntäminen laskennassa on kvanttitietokoneelle merkittävä etu. [21, s. 48] Seuraavaksi tarkastellaan kvanttimekaanisille systeemeille ominaisia piirteitä.

3.3.1 Lomittuminen

Lomittumisen käsitteen esitteli Erwin Schrödinger jo vuonna 1935. Selittäessään kvanttiteoriaa Schrödinger muotoili, että kvanttimekaanisen systeemin aaltofunktio eli ”informaatiopaketti” antaa tietyllä todennäköisyydellä tietyn tuloksen, kun systeemin tila mitataan. Schrödinger piti kuitenkin omituisena sitä, että tieto kahden tunnetun ja erillään olevan hiukkasen systeemistä ei kuitenkaan sisällä tietoa yksittäisistä hiukkasista, vaikka niiden välillä ei ole vuorovaikutusta. Kuten edellisessä luvussa todettiin, yksittäisten hiukkasten tiloja ei voida kuvata riippumatta muiden hiukkasten tiloista. Tätä klassiselle mekaniikalle vierasta ilmiötä alettiin kutsua lomittumiseksi. [22, s. 256]

Kvanttimekaniikan formalismin mukaan Hilbertin avaruus *H* on alisysteemiavaruuksien tensoritulo $H = \otimes_{L=1}^{n} H_l$. Koko systeemin tila voidaan siis kirjoittaa superpositiona

$$|\psi\rangle = \sum_{i_1,\ldots,i_n} c_{i_1 \ldots i_n} |i_1\rangle \otimes |i_2\rangle \otimes \ldots \otimes |i_n\rangle \,, \tag{3.4}$$

jota ei voida yleisesti kuvata yksittäisten alisysteemien tilojen tulona $|\psi\rangle \neq |\psi_1\rangle \otimes |\psi_2\rangle \otimes \ldots \otimes |\psi_n\rangle$. Tämä on formaalinen kuvaus lomittumisilmiöstä. Siinä missä klassinen superpositio on lineaarista, kvanttimekaanisten systeemien lukumäärän kasvaessa tilojen määrä kasvaa eksponentiaalisesti. Näin ollen lomittuminen mahdollistaa Hilbertin avaruuden suuren koon hyväksikäytön ja on täten keskeinen resurssi kvanttilaskennassa. [23]

Kuvitellaan koejärjestely, jossa otetaan tarkasteluun kaksi kubittia *a* ja *b*. Kullekin kubitille muodostetaan erilliset kahden tilan tasapainotetut superpositiot. Toisessa näistä kahdesta tilasta kubitit saavat arvon $|1\rangle$ ja toisessa $|0\rangle$. Mitataan kubitin *a* tilaa, jolloin se saa

satunnaisesti ja yhtä suurella todennäköisyydellä joko arvon $|1\rangle$ tai $|0\rangle$. Sen jälkeen mitataan kubitin *b* tilaa, ja se saa myös arvon $|1\rangle$ tai $|0\rangle$, kuitenkin riippuen kubitin *a* arvosta. Kun näitä mittauksia toistetaan uudelleen ja uudelleen, huomataan, että kubittien *a* ja *b* arvot ovat aina mittaushetkellä korreloituneita. Ensin mitatun kubitin tila määrää toisen kubitin tilan eli kubitit ovat lomittuneita. Yksi esimerkki tällaisista lomittuneesta tiloista ovat niin kutsutut Bellin tilat eli *maksimaalisesti lomittuneet* tilat:

$$\left|\psi^{\pm}\right\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2} \qquad \left|\phi^{\pm}\right\rangle = (|00\rangle \pm |11\rangle)/\sqrt{2}. \tag{3.5}$$

Huomataan, että neljä Bellin tilaa muodostavat ortonormaalin kannan kahden kubitin Hilbertin avaruudelle. Siis $H = \mathcal{H}_1 \otimes \mathcal{H}_2$, jossa $\mathcal{H}_1$:n ja $\mathcal{H}_2$:n dimensiot ovat 2. [21, s.53][23, s. 873]

3.3.2 Aikaevoluutio

Fysikaalinen järjestelmä muuttuu ajan kuluessa, joten järjestelmän tilavektori $|\psi\rangle$ on ajan funktio $|\psi(t)\rangle$. Kvanttimekaniikassa oletus on, että suljetun kvanttijärjestelmän tilavektorin aikaevoluutio on lineaarinen. Kuten luvussa 3.2.2 mainittiin, mittauspostulaatin mukaan tilavektorin kertoimet α_i toteuttavat ehdon $\sum_i |\alpha_i|^2 = 1$. Ainoat lineaarioperaattorit, jotka toteuttavat tämän ehdon, ovat niin kutsuttuja *unitaarioperaattoreita*. Kvanttimekaniikan aikakehityspostulaatin (Evolution Postulate) mukaan suljetun järjestelmän mille tahansa evoluutiolle on olemassa unitaarioperaattori *U* siten, että jos järjestelmän alkutila on $|\psi_1\rangle$, niin järjestelmän tila evoluution jälkeen on

$$|\psi_2\rangle = U\,|\psi_1\rangle\,. \tag{3.6}$$

Unitaarioperaattorilla manipulointi voidaan visualisoida Blochin pallolla kubitin tilaa kuvaavan origoon kiinnitetyn yksikkövektorin $|\psi\rangle$ rotaationa vektoriksi $U\,|\psi\rangle$. [13, s. 43-44]

3.3.3 Dekoherenssi

Kvanttisysteemi on alati vuorovaikutuksessa ympäristönsä kanssa, minkä takia sitä kutsutaan *avoimeksi systeemiksi*. Avoimen kvanttisysteemin vuorovaikutus ympäristönsä kanssa aiheuttaa systeemin tilojen ja ympäristön tilojen lomittumisen. Informaatio kulkee lomittuneiden tilojen kautta ympäristön ja avoimen systeemin välillä. Vuorovaikutus ympäristön kanssa väistämättä muuttaa kvanttisysteemin tilaa, minkä seurauksena systeemiin koodattu informaatio saatetaan menettää. Tämä *dekoherenssiksi* kutsuttu prosessi ilmenee systeemissä ei-toivottuna häiriönä. [24, s. 26] [25, s. 219]

Dekoherenssia voidaan kuvata kuuluisalla Schrödingerin kissa -ajatuskokeella (ks. [9, s. 53-54], jolla havainnollistetaan makroskooppisen maailman vertauskuvan avulla sitä, kuinka omituisesti kvanttimekaaninen systeemi käyttäytyy: systeemin havaitsijalla on vaikutusta sen tilaan (eng. the observer effect). Superpositioperiaatteen mukaan kubitti voi olla tiloissa $|0\rangle$ ja $|1\rangle$ samanaikaisesti. Ympäristö kuitenkin toimii kvanttimekaanisen sys-

teemin "havaitsijana", jonka vaikutuksesta kubitin superpositiotila romahtaa joko tilaan $|0\rangle$ tai tilaan $|1\rangle$. [26, s. 2]

Ajan kuluessa dekoherenssi tuhoaa kubittien superpositiotilojen sisältävää tietoa kvanttitietokoneessa, minkä takia pitkiä laskentaprosesseja on mahdotonta suorittaa. Tämä onkin yksi suurimmista nykypäivän kvanttilaskennan haasteista. Dekoherenssin vaikutuksia kvanttimuistiin tallennettuun tietoon voidaan kuitenkin vähentää olettaen, että dekoherenssiprosessi vaikuttaa erikseen jokaiseen muistiin tallennettuun bittiin. Esimerkkejä tällaisista menetelmistä, joilla lievennetään dekoherenssin vaikutusta, ovat erilaiset virheenkorjausmenetelmien kvanttiversiot (eng. quantum error correction). [27, s. 1]

3.4 Kvanttipiirit

Digitaaliset tietokoneet tallentavat ja käsittelevät binääristä dataa Boolen algebran operaattoreilla (kuten NOT, AND ja OR) eli loogisilla porteilla. Vastaavasti kvanttitietokoneilla laskentaa suoritetaan unitaarisilla operaatioilla *U* eli yhden ja kahden kubitin kvanttiporttien sekvensseillä. Tutustutaan tarkemmin siihen, miten kvanttiporteilla manipuloidaan kubitteja. [18, s. 2725]

3.4.1 Kvanttiportit

Mikä tahansa klassinen logiikkaportti, kuten summain tai kertoja, voidaan muodostaa yhdistelemällä perusportteja, kuten AND-, NOT- ja XOR-portteja, keskenään. Tällainen porttijoukko, jolla voidaan kuvata mitä tahansa loogista operaatiota, on *universaali*. *Kvanttiporttien* joukko on huomattavasti suurempi kuin klassinen porttijoukko. Universaalisuusteoreeman mukaan yhden kubitin portit ja CNOT-portti (tai lähes mikä tahansa kahden kubitin portti) muodostaa universaalin kvanttiporttien joukon. [24, s.23]

Yleisin yhden kubitin portti esitetään 2x2 -unitaarimatriisilla

$$\begin{pmatrix} \alpha & \beta^* \\ \beta & \delta \end{pmatrix},$$

joka muuntaa kubitin arvolla $|0\rangle$ muotoon $\alpha|0\rangle + \beta|1\rangle$ ja kubitin arvolla $|1\rangle$ muotoon $\beta^*|0\rangle + \delta|1\rangle$. Yhden kubitin portit ovat helposti toteutettavissa fyysisesti, esimerkiksi polarisoituihin fotoneihin vaikuttavilla neljännes- ja puoliaaltolevyillä tai radiotaajuisilla pulsseilla, jotka aiheuttavat ydinmagneettista resonanssia (eng. nuclear magnetic resonance, NMR). [18, s. 2725]

Esimerkki yhden kubitin kvanttiportista on NOT-portti, joka muuntaa kubitin arvon $|0\rangle$ arvoon $|1\rangle$ sekä käänteisesti arvon $|1\rangle$ arvoon $|0\rangle$. Koska NOT on lineaarioperaattori, se muuntaa sisäänmenon lineaarikombinaation vastaavaan ulostulon lineaarikombinaatioon. NOT-portti muuntaa siis kubitin yleisen tilan

$$\alpha_0|0\rangle + \alpha_1|1\rangle$$

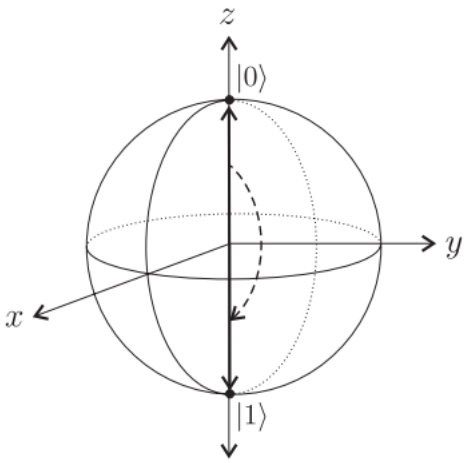
muotoon

$$\alpha_0 |1\rangle + \alpha_1 |0\rangle .$$

NOT-portin lineaarikuvauksen matriisi on muotoa

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} . \tag{3.7}$$

Blochin pallolla NOT-portin operaatio esitetään kulman π kiertona x-akselin suhteen. Kuvassa 3.2 visualisoidaan punaisella yhtenäisellä viivalla NOT-portin rotaatiota tilasta $|1\rangle$ tilaan $|0\rangle$ ja katkoviivalla tilasta $|0\rangle$ tilaan $|1\rangle$. [13, s. 44 ja 63]



Kuva 3.2. *NOT-portin kierto Blochin pallolla. [13]*

NOT-porttia merkitään usein symbolilla *X*, ja se on yksi neljästä Pauli-portista:

$$I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \quad Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} .$$

Pauli-portit ovat tärkeitä kvanttilaskennassa, sillä ne kattavat kaikkien yhden kubitin operaattoreiden muodostaman vektoriavaruuden. Siispä mikä tahansa yhden kubitin unitaarioperaattori voidaan ilmaista Paulin porttien lineaarikombinaationa. [13, s. 63-64]

Yleisin kahden kubitin portti on controlled-NOT eli CNOT-portti, joka toimii ohjausbitillä *c* ja kohdebitillä *t*. Portin tehtävänä on soveltaa NOT-operaatiota kohdebittiin, jos ohjausbitti

on $|1\rangle$ ja olla tekemättä mitään, jos ohjausbitti on $|0\rangle$. CNOT-porttia esitetään matriisilla

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{3.8}$$

CNOT suorittaa siis operaation $t \oplus c$, jossa $\oplus$ esittää loogista eksklusiivista disjunktiota, XOR. [18, s. 2725] [13, s. 10]

3.4.2 Kvanttialgoritmit

Kvanttilaskentaa suoritetaan ajamalla *kvanttialgoritmeja* kvanttitietokoneella, ja se koostuu kolmesta elementistä:

1. Rekisteri tai rekistereiden joukko (kvanttitietokone)
2. Unitaarimatriisi U, jolla kvanttialgoritmi suoritetaan ja
3. Lopputilan mittaus

Formaalisti ilmaistuna kvanttilaskenta koostuu joukosta $\{\mathcal{H}, U, \{M_m\}\}$, jossa $\mathcal{H} = \mathbb{C}^{2^n}$ on Hilbertin avaruus n:n kubitin rekisterille, $U \in U(2^n)$ esittää kvanttialgoritmia ja M_m on mittausoperaattoreiden joukko. [24, s. 20]

Laskenta aloitetaan asettamalla rekisteri alkutilaan $|\psi_{in}\rangle$. Unitaarimatriisilla U_{alg} toteutetaan haluttu algoritmi. Operoimalla alkutilaa $|\psi_{in}\rangle$ matriisilla U_{alg} saavutetaan lopputila $|\psi_{out}\rangle = U_{alg}\,|\psi_{in}\rangle$. Informaatio määritetään lopputilasta sopivilla mittauksilla. Tyypillisesti sisäänmenon arvolla $x \in \mathbb{Z}$ kvanttitietokone laskee funktion $f(x)$ seuraavasti:

$$U_f : |x\rangle\,|0\rangle \rightarrow |x\rangle\,|f(x)\rangle\,,$$

jossa unitaarimatriisi U_f toteuttaa annetun funktion f. [24, s. 20 ja 23]

Oletetaan, että U_f on alkutilassa $\sum_x |x\rangle\,|0\rangle$. Lineaarioperaattorina U_f operoi kaikkia vektoreja samanaikaisesti, jolloin ulostulo on kaikkien laskutulosten superpositio;

$$U_f : \sum_x |x\rangle\,|0\rangle \rightarrow \sum_x |x\rangle\,|f(x)\rangle\,.$$

Tätä kutsutaan *kvanttirinnakkaisuudeksi* (engl. quantum parallelism), joka mahdollistaa kvanttitietokoneiden huomattavan suuren laskentanopeuden. [24, s. 23-24]

Monissa kvanttialgoritmeissa unitaarimuunnos generoi kaikkien mahdollisten ominaistilojen superposition. Tämä toteutetaan operoimalla alkutilassa $|00...0\rangle$ olevaa n:n kubitin rekisteriä Walsh-Hadamard-muunnoksella, jolloin saadaan tulokseksi $\sum_{x=0}^{2^n-1} |x\rangle / \sqrt{2^n}$. Operaattorin U_f lineaarisuuden ansioista saadaan superpositioksi

$$U_f\left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|0\rangle\right)=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}U_f|x\rangle|0\rangle=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle|f(x)\rangle. \tag{3.9}$$

Huomataan, että superpositio koostuu $2^n = e^{nln2}$ tilasta ja U_f operoi e^{nln2} vektoria samanaikaisesti. [24, s. 24]

Oletetaan, että halutaan löytää, mitä saadaan ulostulon funktion $|f(x_0)\rangle$ arvoksi tietyllä sisäänmenon arvolla x_0. Kun mitataan tilan ensimmäisen rekisterin arvo kaavalla 3.9, saadaan hyvin pienellä todennäköisyydellä $1/\{2^n\}$ arvo $|x_0\rangle$. Jotta saataisiin määritettyä $|x_0\rangle|f(x_0)\rangle$, mittausta täytyisi toistaa niin monta kertaa, että kvanttitietokone ei olisi enää erityisasemassa klassiseen tietokoneeseen nähden. Tästä syystä kvanttialgoritmi tulee suunnitella niin, että vektorilla, joka halutaan havaita, on suurempi todennäköisyys tulla havaituksi. Tämä on voitu toteuttaa esimerkiksi

1. Shorin algoritmilla (v. 1994); operoimalla superpositiota käänteisellä kvanttifourier'n muunnoksella ja etsimällä funktion$f(x)$ arvolle alkutekijät.
2. Groverin hakualgoritmilla; kasvattamalla vektorin amplitudia ja samalla sen todennäköisyyttä tulla havaituksi.

Näitä kahta käytetään muiden kvanttialgoritmien ohella tosielämän sovellusten kehittämiseen. Groverin algortimi antaa huomattavasti suuremman hakunopeuden klassisiin hakualgoritmeihin verrattuna. Shorin algoritmilla taas on mahdollista murtaa nykyisiä kryptografisia tietojärjestelmiä. Tarkastellaan vielä lähemmin näitä kahta algoritmia. [24, s. 24][6, s. 269]

Shorin algoritmi

Yksinkertainen tekijöihin jako voidaan suorittaa tarkastamalla kokonaisluvun N jakojäännös jollakin luvulla $p < \sqrt{N}$. Mikäli jakojäännös on 0, tiedämme luvun p olevan kokonaisluvun N tekijä. Tämä metodi on kuitenkin varsin tehoton, sillä sen avulla nopeinkaan klassinen tietokone ei kykene jakamaan 80-numeroista lukua tekijöihin universumin ikää lyhyemmässä ajassa. [6, s. 275]

Vuonna 1994 Peter Shor kehitti kvanttilomittumiseen perustuvan kokonaislukujen tekijöihinjakoalgoritmin, joka osoittautui huomattavasti paremmaksi kuin edeltäjänsä. Tekijöihinjaon ongelmaa voidaan verrata jaksollisen funktion $f(N)$ jakson määrittämiseen. Klassisella tietokoneella tämä metodi ei ole lainkaan tehokkaampi kuin perinteinen tekijöihin jako, mutta kvanttitietokoneessa useiden kubittien interferenssillä voidaan saada funktion jakson arvo nopeasti määritettyä ilman tietoa yksittäisistä funktion arvoista $f(0), f(1), f(2), ...$ Funktion arvojen superpositiosta voidaan määrittää funktion jakso kvanttifourier'n muunnoksen avulla. Merkittävää on, että siinä missä kokonaisluvun N tekijöihin jaon laskenta-aika kasvaa klassisella tietokoneella eksponentiaalisesti luvun N numeroiden kasvaessa, Shorin algoritmilla se on ratkaistavissa polynomiaalisessa ajassa. [6, s. 277]

Groverin hakualgoritmi

AT&T:n Bellin laboratoriossa New Jerseyssä vuonna 1996 Lov Grover löysi algoritmin, joka etsii N:n alkion järjestämättömästä listasta tietyn alkion suurella todennäköisyydellä. Groverin algoritmilla haluttu alkio voidaan löytää vain $\sqrt{N}$ askeleella, kun taas klassisella hakualgoritmilla vastaavaan ongelmaan saadaan ratkaisu keskimäärin $N/2$ askeleella. [6, s. 276]

Kuvitellaan, että halutaan löytää tietty puhelinnumero puhelinluettelosta, joka sisältää miljoona aakkosjärjestyksessä tallennettua alkiota (nimeä). Klassisella algoritmilla hakua ei voida toteuttaa muilla järkevillä tavoilla kuin käymällä luetteloa läpi ja tarkastelemalla erikseen jokaista alkiota, kunnes haluttu numero löytyy. Kvanttitietokoneella voidaan käydä läpi kaikki alkiot yhtäaikaisesti samassa ajassa, joka klassisella algoritmilla kuluu yhden alkion tarkasteluun. Hakutulosta ei voida kuitenkaan tulostaa heti, sillä muuten tietokoneen tilasta mitatun tiedon saavuttamisen todennäköisyys olisi vain yksi miljoonasta. Siispä hakutulos jätetään aluksi mittaamatta, ja toistetaan haku $\sqrt{N}$ kertaa. Tällöin saavutetaan 50% todennäköisyys, että tieto halutun numeron sisältävästä alkiosta on mitattavissa. [6, s. 276]

Yksi Groverin algoritmin sovelluskohteista on kryptografia. Se voisi tuoda vaihtoehdon klassisille salausjärjestelmille, esimerkiksi maailman käytetyimmälle symmetrisen avaimen salausmenetelmälle AES (Advanced Encryption Standard). Jotta AES- koodi voidaan murtaa, täytyy suorittaa haku 2^{128} salausavaimen joukosta. Jos avaimia tarkistetaan nopeudella 10^{18} avainta per sekunti, klassisella tietokoneella oikean avaimen löytäminen kestää kauemmin kuin universumillamme on ikää. Kvanttitietokoneella Groverin algoritmilla hakutulos saavutetaan alle 20 sekunnissa. [6, s. 276]

4 KVANTTITIETOKONEET NYKYPÄIVÄNÄ

Tässä luvussa tarkastellaan, millaisia edellytyksiä on kvanttitietokoneen rakentamiselle. Tutustutaan myös kvanttitietokoneiden arkkitehtuureihin ja tarkemmin yhteen niistä, suprajohtaviin kubitteihin. Kartoitetaan myös suprajohtavan toteutuksen potentiaalia kvanttitietokoneelle annettujen kriteerien pohjalta. Lopuksi esitetään kvanttitietokoneiden sovelluskohteita.

4.1 Kvanttitietokoneen rakentaminen

Klassisessa tietokoneessa bitit 0 ja 1 edustavat kahta sallittua johtimen jännitettä klassisessa piirissä, ja näitä jännitteitä kontrolloidaan transistoreilla. Mistä kubitit on sitten tehty? Kvanttitietokoneiden rakennuspalikat ovat hyvin erilaisia kuin klassisten tietokoneiden, joten ne on rakennettava täysin eri menetelmällä. Tästä esimerkkinä on klassinen sähkövirta, jonka ei ole mahdollista olla kvanttimekaanisten tilojen tavoin superpositiossa, eli samanaikaisesti sekä virrata että olla virtaamatta johtimen läpi. Kvanttitietokoneiden fyysiseksi toteutukseksi on olemassa erilaisia tapoja. Jotkut tekniikat perustuvat optiikkaan, toiset suprajohteisiin tai molekyyleihin. [1, s. 13] Fyysisille kubiteille on kuitenkin olemassa tiettyjä kriteerejä, joita tarkastellaan seuraavaksi.

4.1.1 DiVincenzon kriteerit

Kvanttilaitteistoehdokkaiden tunnistaminen on ensimmäinen askel kohti kvanttitietokoneen fyysistä toteutusta. Kvanttialgoritmien rakenteen ja ensimmäisten kokeellisten tutkimusten perusteella vuonna 2000 David P.DiVincenzo laati joukon vaatimuksia kvanttitietokoneen toiminnallisuuksille, jotta kvanttilaskentaa voidaan onnistuneesti suorittaa. [28, s. 16] Kriteerit ovat seuraavat [24, s. 36-40][9, s. 105-107]:

1. *Skaalautuva fysikaalinen systeemi, jossa kubitit ovat tarkasti karakterisoituja.*
   Tarvitaan fyysinen kubitti, jonka parametrit tiedetään tarkasti. Tällainen on tavallisesti kvanttimekaaninen kaksitilasysteemi. Tarvitaan myös usean kubitin kvanttirekisteri, johon voidaan tallettaa informaatiota. Lisäksi systeemin tulee olla skaalautuva eli yhä vakaammin käsiteltävissä kubittien määrän kasvaessa.
2. *Kubitit on mahdollista alustaa tunnettuun tilaan, esim.* $|00...0\rangle$.
   Kvanttirekisterin alustaminen on välttämätöntä ennen laskennan aloittamista. Alustaminen toteutetaan usein jäähdyttämällä systeemiä, jotta se saadaan asetettua

perustilaansa. Jos tarpeeksi matalan lämpötilan saavuttaminen ei ole mahdollista, voidaan käyttää alkutilana myös miehitettyä energiatilaa. Kubittien alustaminen on tärkeää myös *kvanttivirheenkorjauksen* (eng. quantum error correction, QEC) kannalta. QEC:llä tarkoitetaan kvantti-informaation suojelua dekoherenssin eli ulkoisten häiriöiden aiheuttamilta virheiltä.

3. *Dekoherenssiajat, jotka ovat selvästi pidemmät kuin kvanttiporttien toiminta-ajat.*
   Klassisen tietokoneen laitteisto voi kestää jopa 10 vuotta. Kvanttitietokone sen sijaan on erittäin herkkä dekoherenssille, mikä aiheuttaa kvanttitilojen heikkenemistä. Dekoherenssi määrää maksimiajan laskentaoperaatioille, joka voi olla hyvin lyhyt, mikrosekuntien luokkaa. Sen jälkeen kubittien superpositiotila romahtaa. Esimerkiksi jos tyypillisen kvanttiportin operointiaika on pikosekuntin luokkaa, systeemillä voidaan suorittaa 10^6 operaatiota ennen kvanttitilan romahtamista. Tarvitaan noin 10^5 kvanttiporttia, jotta voidaan Shorin algoritmia hyödyntäen jakaa luku 21 tekijöihin 3 ja 7.
4. *Universaali kvanttiporttien joukko.*
   Tarvitaan universaaleja kvanttiportteja, jotka esitetään unitaarimuunnoksilla. Kvanttialgoritmia voidaan näin kuvata unitaarimuunnosten sekvenssillä. Jokaisella unitaarimuunnoksella operoidaan suurta joukkoa kubitteja, mutta tyypillisesti enintään kolmea kerrallaan. Kvanttiporttien toteutus on kuitenkin harvoin virheetöntä, sillä dekoherenssin ehkäiseminen on haastavaa. Näin ollen luotettavat laskentaprosessit edellyttävät tehokkaita virheenkorjausmenetelmiä.
5. *Yksittäisten kubittien tilat on kyettävä mittaamaan.*
   Kvanttialgoritmin suorituksen päätyttyä tulee laskennan tuloksen olla mitattavissa. Dekoherenssin, kvanttiporttien epäideaalisuuksien ja monien muiden laskentaa heikentävien seikkojen vuoksi mittauksen hyötysuhde on tavallisesti alle 100 prosenttia. Siispä laskentaprosessi täytyy suorittaa niin monta kertaa, että saavutetaan riittävän luotettavia tuloksia.

Osa näistä edellä käsitellyistä kriteereistä näyttää olevan ristiriidassa. Esimerkiksi ne järjestelmän osat, joilla suoritetaan mittausta, on kytkettävä päälle virheenkorjausta ja tuloksen lukemista varten. Kuitenkin heti kun järjestelmä kytketään päälle, alkaa systeemi menettää koherenssiaan. Systeemin kytkeminen vuorotellen päälle ja pois on vaikea toteuttaa. Suunniteltaessa skaalautuvaa kvanttitietokonearkkitehtuuria tätä ongelmaa helpottavat usein kvanttiviestinnän tekniikat, minkä takia DiVincenzo myöhemmin täydensi kriteerejään. Kaksi uutta vaatimusta koskien tiedonvälitystä kvanttitietokoneessa ovat:

6. *Paikallaan olevia ja liikkuvia kubitteja on kyettävä muuntamaan toisikseen.*
   Jotkut kvanttitietokoneiden realisaatiot pystyvät vaivatta tallettamaan kvantti-informaatiota, mutta silti niiltä puuttuu sellaisia resursseja, joita tiedonsiirto pitkien välimatkojen päähän edellyttää. Kykyä muuntaa paikallaan olevia kubitteja "lentäviksi kubiteiksi", kuten fotoneiksi tarvitaan kvanttiteleportaatiossa.

7. *Liikkuvia kubitteja on kyettävä siirtämään tarkasti tiettyjen paikkojen välillä.* Kvanttitietokoneen tiedonsiirron tulee olla luotettavaa, jotta kvanttiteleportaatiota tai turvallista kvanttisalausta voidaan ylipäätään toteuttaa. Kvanttitiedonsiirto mahdollistaa pienten kvanttitietokoneiden yhdistämistä osaksi suurempia systeemejä, jolloin mittauslaitteisto voidaan sijoittaa etäälle herkistä kvanttimuistikomponenteista ja vikasietojärjestelmien vaatima vahva kubittien yhteys on helpompi toteuttaa.

Kubittien toteutusmahdollisuuksia on tutkittu paljon viime aikoina. On löydetty arvokasta tietoa yksittäisten kvanttisysteemien manipuloinnista sekä lomittuneiden tilojen luomisesta ja havaitsemisesta. Lisäksi tutkimuksissa on keskitytty fyysisiin prosesseihin, erityisesti dekoherenssiin, joka nähdään suurimpana esteenä toimivan kvanttitietokoneen arkkitehtuurin rakentamiselle. Monet kvanttilaitteistoehdokkaat toteuttavat osan vaatimuksista, mutta kaikkien DiVincenzon kriteerien täyttäminen on haastavaa. DiVincenzon sanoja lainaten:

"On vielä epävarmaa, kuinka kaikki yllä olevat vaatimukset täytettäisiin ja ovatko ne kaikki ylipäätään täytettävissä. On myös mahdollista, että kriteereille löydetään uusia kompromisseja, jotka vievät tutkimusta aivan uuteen suuntaan." [28, s. 17]

4.1.2 Kvanttitietokoneiden arkkitehtuureja

Kvanttitietokoneiden tutkimus on tähän mennessä osoittanut, että kvanttijärjestelmiin koodatun tiedon tallentamisesta, siirtämisestä ja käsittelemisestä on hyötyä. Keskeinen ja edelleen avoin kysymys on, millainen on paras vaihtoehto kvanttitietokoneen laitteistolle. [28, s. 21] Kvanttitietokoneiden rakentamisessa suuri haaste on samanaikaisesti ohjata ja mitata kvanttisysteemejä sekä pitää ne ympäristön vaikutuspiirin ulkopuolella. Seuraavilla teknologioilla on pyritty vastaamaan tähän haasteeseen [24, s. 40] [1, s. 47] [29, s. 6]:

- **Ydinmagneettinen resonanssispektroskopia** käyttää molekyylien ytimien spintiloja kubitteina. Molekyylien ytimiä voidaan kontrolloida säteilyttämällä niitä resonoivilla radiotaajuuspulsseilla. Tässä toteutuksessa käytetään yksittäisten kvanttien sijaan molekyylejä, minkä takia kubittien tilojen alustaminen ja lopputilojen mittaaminen on haastavaa.
- **Ioniloukut**: Kubitti muodostetaan sähkö- ja magneettikentän avulla eristetystä ionista, jonka energiatiloja manipuloidaan laserilla. Eristetyn ionin koherenssiaika on pitkä, mutta haasteena on ionien tarkan ohjauksen säilyttäminen suuremmissa arkkitehtuureissa.
- **Fotonin polarisaatiosta** voidaan aaltolevyn avulla muodostaa kubitti. Dekoherenssilla on suhteellisen mitätön vaikutus fotoneihin, mutta fotonien välinen vuorovaikutus on erittäin heikkoa, minkä takia ne eivät sovellu yksinään monimutkaisimpiin laskentatehtäviin.
- **Kvanttipisteet (QD)** ovat nanokokoisia puolijohderakenteita, joita voidaan pitää

eräänlaisina kontrolloitavissa olevina keinotekoisina atomeina. Kvanttipisteiden pareista luodaan kubitti. Kvanttipisteiden välinen vuorovaikutus toimii vain erittäin lyhyellä kantamalla.

- **Suprajohtavia kubitteja** kuljettaa suprajohtava piiri. Matalassa lämpötilassa suprajohteella ei ole resistiivisyyttä ja kvantti-ilmiöt tulevat näkyviksi.

Edellä on kuvattu vain muutama kubitin mahdollinen toteutustapa. Todellisuudessa on olemassa valtava määrä muitakin teknologioita, joilla pyritään pienentämään dekoherenssin vaikutuksia kvanttilaitteistossa. Vielä on kiistaa siitä, millainen kubitin toteutus on lupaavin, sillä kvanttitietokoneet ovat vasta kehityksensä alkutaipaleella. Eri teknologiat on usein optimoitu tietyntyyppisten ongelmien ratkaisemiseen. Tavoitteena on kuitenkin rakentaa kvanttitietokone, jolla on mahdollisimman monia eri toimintoja. On vaikeaa ennustaa, mitkä vaihtoehdot johtavat parhaisiin tuloksiin tulevaisuudessa, kun tavoitellaan universaalia kvanttitietokonetta. Tällaiselta kvanttitietokoneelta, jolla olisi mahdollista simuloida mitä tahansa kvanttisysteemiä, vaadittaisiin kaikkien DiVincenzon kriteerien toteutumista.

Tällä hetkellä yksi johtavista teknologioista on suprajohtavat kvanttipiirit, joilla monet kehittyneimmät kvanttitietokoneet toimivat. Tarkastellaan seuraavaksi suprajohtavaa toteutusta yksityiskohtaisemmin.

4.2 Suprajohteisiin perustuva kvanttitietokone

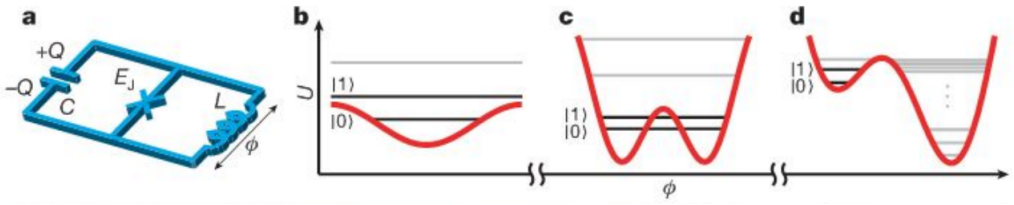
Suprajohtava piiri on yksi nykypäivän lupaavimmista vaihtoehdoista kvanttitietokoneen fyysiseksi toteutukseksi. Seuraavaksi tutustutaan suprajohtavien piirien toimintaan ja siihen, millaisilla erilaisilla tavoilla suprajohtava kubitti voidaan luoda. Sen jälkeen tarkastellaan suprajohtavaa toteutusta DiVincenzon kriteerien valossa, ja analysoidaan toteutuksen etuja sekä siihen liittyviä haasteita.

4.2.1 Suprajohtavat kubitit

Klassisista sähköpiireistä valmistetut kubitit menettäisivät koherenssinsa nopeasti resistiivisten häviöiden vuoksi. Suprajohteissa puolestaan alhaisissa lämpötiloissa kidehilan muodostavien positiivisten ionien hilavärähtelyt saavat kaksi vastakkaisen spinin elektronia muodostamaan *Cooperin parin*. Cooperin parin elektronit käyttäytyvät bosonien tavoin ja pyrkivät tiivistymään kvanttitilaan, jolloin materiaali menettää resistiivisyytensä ja kvantti-ilmiötä ilmenee makroskooppisella tasolla. Suprajohtavuuden ansioista sähkövirran on mahdollista kulkea piirissä häviöttömästi. Sähkökenttä värähtelee ominaistaajuudella, joka riippuu sähköpiirin induktanssin ja kapasitanssin tulosta. Sähkökentän värähtely on häviötöntä, ja piirin virtaa kutsutaan *supravirraksi*. [2, s. 50] [30, s. 1-2] [31, s. 8]

Suprajohtavan kubitin toimintaa voidaan havainnollistaa kvanttimekaanisen hiukkasen potentiaalin avulla. Tavallinen LC-värähtelypiiri toimii kvanttimekaanisena harmonisena

värähtelijänä. Kelan magneettivuon $\hat{\phi}$ ja levykondensaattorin varauksen $\hat{Q}$ kommutaattori on muotoa $[\hat{\phi}, \hat{Q}] = i\hbar$ (ks. [32, s. 217]), ja näin ollen $\hat{\phi}$ ja $\hat{Q}$ ovat analogisia yksittäisen hiukkasen paikan $\hat{x}$ ja liikemäärän $\hat{p}$ kanssa, jotka toteuttavat relaation $[\hat{x}, \hat{p}] = i\hbar$. Harmonisen värähtelijän liike määräytyy ”potentiaalienergian” ϕ^2/L ja ”kineettisen energian” $Q^2/2C$ perusteella. [2, s. 50] Magneettivuo ϕ saa vain kvantittuneita arvoja, ja koska kyseessä on harmoninen systeemi, sen energiaspektri on tasavälinen. [31, s. 8].



***Kuva 4.1. Suprajohtavat kubitit. a**, Suprajohtavien kubittien yksinkertainen piirimalli. Josephsonin liitos on merkitty sinisellä ”X” -merkinnällä. **b**-**d**, eri kubittityyppien, varaus- (**b**), vuo- (**c**) ja vaihekubitin (**d**) potentiaalienergiaa $U(\phi)$ merkitään punaisella viivalla ja energiatasoja eli kubitin tiloja mustilla viivoilla. [2]*

Jotta kvanttijärjestelmä voi toimia kubittina, on energiatasojen oltava epäharmonisia. Epäharmonisuuden tulee olla sellaista, että sen spektrissä on kaksi hyvin muista tiloista eristettyä tilaa, ja tämä kaksitilasysteemi voidaan käytännössä muodostaa lisäämällä piiriin *Josephsonin liitos* (Kuva 4.1.a). Josephsonin liitos koostuu kahdesta suprajohtavasta materiaalista, joiden välillä on ohut eristekerros. Silmukassa kiertävä supravirta kohtaa potentiaalivallin Josephsonin liitoksen kohdalla, mikä muuttaa harmonisen supravirran värähtelyn epäharmoniseksi. Josephsonin liitos käyttäytyy samankaltaisesti kuin epälineaarinen induktanssi, eli kun liitoksen läpi kulkee supravirta, siihen varastoituu energia, jota kutsutaan Josephsonin energiaksi E_J. [31, s. 8]

Kolme tavallisinta suprajohtavan kubitin tyyppiä ovat vuo-, varaus- ja vaihekubitti, joiden potentiaalit on esitetty kuvassa 4.1. Jokaiselle kubittityypille on määritelty energioiden suhde E_J/E_C, jossa $E_C = e^2/2C$ on yksittäisen elektronin varausenergia. Jokaista Josephsonin liitoksen muodostavaa suprajohdetta kuvataan makroskooppisella aaltofunktiolla. Energioiden suhde E_J/E_C vaikuttaa aaltofunktion herkkyyteen varauksen ja vuon muutoksille. [2, s. 50]

Varauskubitti (kuva 4.1.b) luodaan silmukan supravirrasta, ja se tunnetaan myös *Cooperin parin laatikkona* (eng. Cooper pair box). Kubitin tila määräytyy Josephsonin liitoksen läpi tunneloituneiden Cooperin elektroniparien lukumäärän mukaan. Cooperin parin laatikon paranneltua versiota kutsutaan *transmoniksi*. Transmonissa Josephsonin liitoksen energian suhde varausenergiaan on suurempi ($E_J/E_C \gg 1$), mikä vähentää varauskohinan haitallisia vaikutuksia. [31, s. 9] [2, s. 1]

Piirissä myötäpäivään kulkeva supravirta tuottaa alaspäin suuntautuvan magneettivuon ja vastapäivään kulkeva virta ylöspäin suuntautuvan magneettivuon. Josephsonin liitoksen aiheuttaman epäharmonisuuden vuoksi magneettivuon arvot eivät ole tasaisin välein kvantittuneita. Kaksi matalinta vuon arvoa muodostavat *vuokubitin* (kuva 4.1.c) tilat. Alas-

päin suuntautuva magneettivuo toimii vuokubitin tilana $|0\rangle$ ja ylöspäin suuntautuva tilana $|1\rangle$. [31, s. 8-9] Vuokubitissa induktanssi usein korvataan Josephsonin liitoksilla, ja energioiden suhde on $E_J/E_C \gg 1$. [2, s. 51]

Vaihekubitti (kuva 4.1.d) muodostuu yhdestä Josephsonin liitoksen läpi kulkevasta supravirrasta, ja energioiden suhde on edelleen $E_J/E_C \gg 1$. Josephsonin liitoksessa on useita potentiaalikaivoja, ja vaihekubitilla on käytössään kaivon kaksi alinta energiatilaa. Josephsonin liitoksessa suprajohteiden aaltofunktioilla on kompleksinen vaihe-ero. Vaihekubitin tilat määräytyvät tämän vaihe-eron aiheuttamien kvanttivärähtelyiden perusteella. [33, s. 1036]

Suprajohtavat kubitit ovat ainutlaatuinen lähestymistapa kvanttilaskentaan. Verrattuna muihin kubittien toteutuksiin ne ovat fyysisesti suurikokoisia, noin 1-100 µm. Vierekkäiset kubitit voivat kytkeytyä toisiinsa joko kapasitiivisesti tai induktiivisesti, mikä muodostaa yksinkertaisen kvanttiportin. Kubitteja voidaan myös kytkeä toisiinsa mikroaaltofotoneilla resonaattoripiirien siirtolinjoissa, mikä mahdollistaa kahden kubitin porttioperaation muutamassa kymmenessä nanosekunnissa. Tällaisia järjestelmiä on käytetty kvanttialgoritmien toteutuksessa ja millimetrien etäisyydellä toisistaan olevien lomittuneiden kubittien kvanttikorrelaatioiden mittaamisessa. Suprajohtavien kubittien etuna on skaalautuvuus, sillä monimutkaisiakin suprajohtavia piirejä voidaan rakentaa käyttämällä tavanomaista integroitujen piirien valmistustekniikkaa. [33, s. 81][2, s. 51]

4.2.2 Suprajohtavien kvanttipiirien potentiaali

Suprajohtava kubitti voidaan muodostaa Josephsonin liitoksesta, mutta voidaanko suprajohtavista kubiteista valmistaa toimiva kvanttitietokone? Kvanttitietokoneen tulisi kyetä suorittamaan laskentaa monilla kubiteilla, jotta laskenta olisi hyödyllistä. Kääntöpuolena on, että virheiden esiintymisen mahdollisuus kasvaa käsi kädessä kubittien lukumäärän kanssa. Arvioidaan Divincenzon viiden ensimmäisen kriteerin avulla suprajohteisiin perustuvan kvanttitietokoneen potentiaalia.

1. *Skaalautuva fysikaalinen systeemi, jossa kubitit ovat tarkasti karakterisoituja.*
   Edellisessä alaluvussa tutkittiin suprajohtavaa järjestelmää, jossa on kolme vaihtoehtoa kubitille, varaus-, vuo- ja vaihekubitti. Skaalautuvuus on taas mahdollista toteuttaa kytkemällä kubitteja samaan elementtiin, jota kutsutaan *kvanttiväyläksi*, ja taajuutta muuttamalla voidaan valita tietyt kytkettävät kubitit [33, s. 1039]. Vaikka kovin tarkkaa kubittien karakterisointia ei tässä työssä tehty, voidaan selvityksen perusteella todeta, että suprajohtava piiri on mahdollinen kvanttitietokoneen rakennuspalikka.
2. *Kubitit on mahdollista alustaa tunnettuun tilaan, esim.* $|00...0\rangle$.
   Ennen laskennan aloittamista kvanttirekistereillä tulisi olla tiedossa kaikkien kubittien arvot, ja kubittien tilat tulisi alustaa. Tavallisesti alustaminen toteutetaan jäähdyttämällä järjestelmä perustilaan, joka toimii vertailutilana. Kaikki kolme edellä mainittua suprajohtavaa kubittia voivat saavuttaa alkutilansa pitkän relaksaatioajan

jälkeen. Digitaalinen takaisinkytketty ohjaus tekee suprajohtavien kubittien alustamisesta nopeampaa ja kontrolloidumpaa. [30, s.2-3]

3. *Dekoherenssiajat, jotka ovat selvästi pidemmät kuin kvanttiporttien toiminta-ajat.*
   Suprajohtavissa piireissä induktiivisten elementtien, mukaan lukien Josephsonin liitosten, energiahäviöt ovat hyvin pieniä, sillä Cooperin parien elektronit bosonien tavoin muodostavat yhteisen koherentin tilan matalissa lämpötiloissa. Kuitenkin samat kytkennät, jotka mahdollistavat skaalauksen monien kubittien arkkitehtuureiksi, tarjoavat myös kubiteille reitin vuorovaikutukseen ympäristön sähkömagneettisten häiriöiden kanssa. Kytkennät piiristä ulkoisiin laitteisiin lisäävät dekoherenssia ja kubittien tilojen hajoamisen riskiä [33, s. 90-91]. Näin ollen mittauksia ja systeemin parempaa kontrollointia tehdään aina koherenssin kustannuksella. Suprajohtavissa piireissä dekoherenssiaikaa voidaan kuitenkin pidentää esimerkiksi sopivilla kubitti- ja materiaalivalinnoilla, Josephsonin liitosten aloja pienentämällä ja niiden laatua parantamalla sekä lisäämällä oksidikerroksia liitoksiin [33, s. 1039]. Dekoherenssia aiheuttavat lukuisat tekijät, ja niiden kaikkien tunnistaminen on haastavaa. Dekoherenssilähteiden löytäminen on kuitenkin tärkeää, jotta uusia koherenssia lisääviä elementtejä voidaan kehittää.
4. *Universaali kvanttiporttien joukko.*
   Kvanttitietokoneen laskentaa voidaan yksinkertaistaa niin, että mikä tahansa laskutoimitus voidaan suorittaa universaalilla porttijoukolla: yhden kubitin porteilla (AND, NOT, XOR) ja CNOT-portilla. Suprajohtavien piirien kvanttiportit eivät kuitenkaan ole ideaalisia, jonka takia tarvitaan kvanttivirheenkorjausta. [30, s. 3] Kuitenkin vuonna 2014 esitettiin merkittäviä tutkimustuloksia: universaali kvanttiporttien joukko toteutettiin suprajohtavassa monen kubitin prosessorissa, jossa yhden kubitin portin keskimääräinen tarkkuus on 99,92 % ja kahden kubitin portin tarkkuus jopa 99,4 % [34]. Tulokset osoittavat, että suprajohtavat kubitit voivat toimia erittäin tarkasti.
5. *Yksittäisten kubittien tilat on kyettävä mittaamaan.*
   Laskennan tulosten lukeminen edellyttää erittäin tarkkaa suprajohtavien kubittien tilojen mittauskykyä. Mittauksessa on myös kiinnitettävä huomiota ympäristön systeemiä heikentäviin vaikutuksiin. Vain todella tarkasti mitatun suprajohtavan järjestelmän antamia tuloksia voidaan pitää valideina. [30, s. 3-4] Vuonna 2015 julkaistussa tutkimuksessa hyödynnettiin parametrista vahvistustekniikkaa, Josephsonin liitoksen siirtolinjaan perustuvaa suprajohtavaa vahvistinta, jolla saatiin luettua suprajohtavien kubittien tiloja jopa 99 % tarkkuudella [35].

Ylläolevan tarkastelu osoittaa, että suprajohtavalla toteutuksella on jo monia ominaisuuksia, joita kvanttitietokoneelta vaaditaan. Suprajohteisiin perustuvan kvanttitietokoneen olennaisin etu on, että varauskubittien, vuokubittien ja vaihekubittien piirit ovat täysin yhteensopivia nykyisin käytössä olevan mikroelektroniikan valmistustekniikan kanssa. Suprajohtava toteutus on myös skaalautuvuutensa vuoksi kärkisijoilla kvanttitietokoneiden kilvassa, sillä vikasietoinen kvanttilaskenta vaatii suuren määrän kubitteja. [30, s. 4].

Vaikka suprajohtavat kubitit ovat lupaava löydös, monia esteitä on vielä edessä. Erityisesti dekoherenssiajan pidentäminen ja mittaustuloksen parantaminen ovat keskeisiä haasteita. Kvanttitilat ovat erittäin herkkiä, ja ne reagoivat vähäiseenkin ympäristön vaikutukseen. Suurten tavoitteiden saavuttaminen vaatii teknisten seikkojen parantelua, kuten ympäristön matalataajuisen kohinan poistamista, tai ainakin sen vähentämistä [33, s. 1034]. On olemassa monia menetelmiä, joista mainittakoon kvanttielektrodynamiikan (eng. quantum electrodynamics, QED) teoria, jolla pyritään vastaamaan näihin dekoherenssin tuomiin haasteisiin. Myös uusia virheenkorjausmalleja tarvitaan. [30, s. 4]. Mitä enemmän tiedetään fysikaalisista prosesseista, sitä enemmän voidaan kehittää uusia menetelmiä ongelmien korjaamiseksi. Näin ollen suprajohtavien kvanttipiirien tutkimusta tulisi jatkaa.

4.3 Tulevaisuuden näkymät

Kvanttilaskenta on haastanut traditionaalisen teknologian, joka on toistaiseksi seurannut Mooren lakia. Viime vuosina teollisuuden ja akateemisen yhteisön kiinnostus kvanttiteknologiaan on kasvanut, ja suuria investointeja on suunnattu kvanttitietokoneiden tutkimukseen ja kehitykseen. [17, s. 258] Alalla tarvitaan laajaa tietotaitoa: niin kvanttimekaniikan ilmiöiden syvällistä ymmärrystä kuin käytännön toteutuksen tuntemista. Kvanttitietokoneen suunnittelussa tulee olla fyysikoiden lisäksi mukana ohjelmoinnin, elektroniikan sekä materiaalitekniikan osaajia. Universaali kvanttitietokone häämöttää tulevaisuudessa, mutta ennen sen rakentamista lukuisia fyysisiä esteitä on ylitettävä. Nykypäivän kvanttitietokoneet ovat lähinnä tutkimuskäytössä, eivätkä luultavasti tule olemaan lähitulevaisuudessa tavallisten ihmisten saatavilla.

Vaikka kvanttitietokoneiden kehitys on kohdannut monia teknisiä haasteita, kvanttilaskentaa on edistyksellisesti onnistuttu käyttämään moniin kaupallisiin tarkoituksiin. Kvanttilaskennalle on kysyntää esimerkiksi näillä toimialoilla [36][37]:

- kemiantekniikka
- rahoitus
- lääketeollisuus
- koneoppiminen
- kyberturvallisuus
- kvanttikryptografia
- materiaalitiede

Vuodesta 2018 lähtien suuret yritykset, kuten IBM ja Google, ovat rakentaneet erilaisia kvanttitietokoneita, joista suurimmat toimivat parhaimmillaan jopa 72:lla kubitilla. Kubittien määrä ei ole kuitenkaan vielä riittävä: 1024-bittisen nykyaikaisen salausavaimen murtamiseen Shorin algoritmilla tarvittaisiin yli 5 000 kubittia. Vuonna 2019 Google väitti suorittaneensa ensimmäisen kvanttilaskentaoperaation, jota klassisella tietokoneella ei käytännössä pystytä tekemään. Tämä virstanpylväs tunnetaan *kvanttiherruutena* (eng.

quantum supremacy). Klassiselle tietokoneelle mahdottomien tehtävien ratkaisemisesta ei kuitenkaan välttämättä ole käytännön hyötyä. On siis tärkeää huomata, että kvanttiherruus ei tarkoita välttämättä *kvanttietua* (eng. quantum advantage), jonka saavuttaakseen kvanttitietokoneen tulisi kyetä ratkaisemaan jokin ennalta määritelty ja käytännön kannalta hyödyllinen laskutehtävä klassista tietokonetta nopeammin. [1, s. 90]

Klassiset tietokoneet ovat muuttuneet huoneen kokoisista kännykän kokoisiksi vain muutamassa vuosikymmenessä, joten myös kvanttitietokoneiden kehitys saattaa olla yllättävän nopeaa. Niin ainakin uskotaan, nimittäin kvanttitietokoneisiin investoidaan miljardeja euroja. [1, s. 90-91] Suuret yritykset kilpailevat kvanttiherruudesta, ja ennätyksiä kubittien määrästä rikotaan jatkuvasti. Mediassa puhutaan kvanttitietokoneiden ylivallasta, ja yleisön odotukset ovat korkealla. Kvanttitietokoneet eivät tarjoa nopeutusta suureen osaan nykyisten tietokoneiden suorittamista toiminnoista. Ne kuitenkin potentiaalisesti tarjoavat mullistavaa tapaa ratkaista tiettyjä ongelmia, jotka ovat periaatteessakin ylivoimaisia klassisille tietokoneille.

5 YHTEENVETO

Tämä työ on kirjallisuuskatsaus kvanttiteknologian kiinnostavaan sovellukseen, kvanttitietokoneeseen. Kvanttitietokoneella suoritetaan kvanttilaskentaa, jonka valttina on kvanttimekaanisten tilojen poikkeuksellisten ominaisuuksien hyödyntäminen suuremman laskentanopeuden saavuttamiseksi.

1930-luvulla löydettiin uusia matemaattisia malleja kuvaamaan klassisia laskentaprosesseja, ja myöhemmin 1980-luvulla Richard Feynmanin oivallusten pohjalta näitä malleja alettiin soveltaa myös kvanttilaskennassa. Kun tarkastellaan historian kehitystä sadan vuoden takaisesta modernin tietojenkäsittelytieteiden synnystä nykypäivän kvanttilaskentaan, voidaan nähdä yhteys klassisen laskennan ja kvanttilaskennan välillä. Klassisten Turingin koneen mallien pohjalta kehitettiin Turingin kvanttitietokone, jolla voidaan simuloida kvanttimekaanisia systeemejä. Kuitenkin kvanttitietokoneen ja tavallisten tietokoneiden rakennuspalikat poikkeavat toisistaan olennaisella tavalla. Klassisen tietojenkäsittelyn pienin yksikkö on bitti, kun taas kvanttilaskentaa suoritetaan kubiteilla, joilla on erikoisia kvanttimekaanisia ominaisuuksia. Nämä ominaisuudet tarjoavat kvanttitietokoneille mahdollisuuden ratkoa klassisen tietokoneen kykyjä ylittäviä ongelmia, joskin niihin liittyy monia ratkaisemattomia haasteita.

Toimivan kvanttitietokoneen rakentaminen ei ole suoraviivaista. Kvanttitietokoneen laitteistolle on useita ehdokkaita, joista yksi, suprajohtava piiri, esiteltiin tässä työssä. Riittävän laskentatarkkuuden saavuttaminen edellyttää kvanttilaitteistolta tiettyjä ominaisuuksia. Haasteellista on täyttää monia edellytyksiä yhtäaikaisesti, ja usein joudutaankin tekemään kompromisseja niiden välillä. Suprajohtavaa toteutusta tarkasteltiin Divincenzon kriteerien valossa, ja voidaan todeta, että se on skaalautuvuutensa takia edullisessa asemassa kvanttitietokonemarkkinoilla. Suurella kubittimäärällä saadaan suoritettua vikasietoista kvanttilaskentaa. Toteutuksen etuna on myös se, että suprajohtavien piirien valmistuksessa hyödynnetään jo käytössä olevia mikroelektroniikan valmistustekniikoita.

Lähtökohtaisesti kvanttitietokonetta ei suunnitella laskemaan laajasti erilaisia ongelmia, vaan keskitytään kohentamaan sen soveltuvuutta tiettyyn erityistehtävään. Näin ollen klassisten tietokoneiden ja kvanttitietokoneiden keskinäinen vertailu on mielekästä vain siinä tapauksessa, jos mitataan soveltuvuutta yksittäisen ongelman ratkaisemiseen. Nykyiset kvanttitietokoneet ovat lähinnä tutkimuskäytössä, ja niiden tulevaisuuden mahdollisuuksia voidaan toistaiseksi vain spekuloida. Kvanttitietokoneiden tutkimukseen investoidaan valtavasti, eikä syyttä: lupaavia sovelluskohteita on lukuisilla tieteen- ja teollisuudenaloilla, kuten lääketieteessä, koneoppimisessa ja kryptografiassa.

LÄHTEET

[1] C. Hughes, J. Isaacson, A. Perry, R. F. Sun ja J. Turner. *Quantum Computing for the Quantum Curious*. Springer, 2021. Saatavissa (viitattu 12.5.2022): https://library.oapen.org/handle/20.500.12657/48236.

[2] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, J. L. O'Brien ja C. Monroe. Quantum computers. *Nature (London)* (2010). Saatavissa (viitattu 15.5.2022): https://www-nature-com.libproxy.tuni.fi/articles/nature08812.

[3] R. Vathsan. *Introduction to quantum physics and information processing*. CRC Press, 2016. Saatavissa (viitattu 12.4.2022): https://learning.oreilly.com/library/view/introduction-to-quantum/9781482238129/?sso_link=yes&sso_link_from=tampere-university.

[4] C. Bernhardt. *Turing's vision : the birth of computer science*. MIT Press, 2016. Saatavissa (viitattu 12.4.2022): http://libproxy.tuni.fi/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=cookie,ip,uid&db=e000xww&AN=1239109&site=ehost-live&scope=site.

[5] R. Feynman. Simulating physics with computers. *International journal of theoretical physics* (1982). Saatavissa (viitattu 5.4.2022): http://physics.whu.edu.cn/dfiles/wenjian/1_00_QIC_Feynman.pdf.

[6] G. Fraser. *The New Physics: For the Twenty-First Century*. Cambridge University Press, 2006.

[7] W. Fouché, J. Heidema, G. Jones ja P. H. Potgieter. Universality and programmability of quantum computers. *Theoretical computer science* (2008). Saatavissa (viitattu 21.4.2022): https://www-sciencedirect-com.libproxy.tuni.fi/science/article/pii/S0304397508003885?via%3Dihub.

[8] D.-S. Wang. A local model of quantum Turing machines. *Quantum information computation* (2020). Saatavissa (viitattu 19.4.2022): https://arxiv.org/pdf/1912.03767.pdf.

[9] S. Akama. *Elements of Quantum Computing: History, Theories and Engineering Applications*. Springer, 2014.

[10] A. A. Lagana, M. A. Lohe ja L. von Smekal. Construction of a universal quantum computer. *Physical Review A* (2009). Saatavissa (viitattu 25.4.2022): https://journals-aps-org.libproxy.tuni.fi/pra/issues.

[11] M. Hirvensalo. *Quantum computing*. Springer, 2001. Saatavissa (viitattu 25.4.2022): https://ebookcentral.proquest.com/lib/tampere/reader.action?docID=3098466.

[12] A. Molina ja J. Watrous. Revisiting the simulation of quantum Turing machines by quantum circuits. *Proceedings of the Royal Society. A, Mathematical, phy-*

sical, and engineering sciences (2019). Saatavissa (viitattu 30.4.2022): https://royalsocietypublishing.org/doi/10.1098/rspa.2018.0767.

[13] P. Kaye, R. Laflamme ja M. Mosca. *An introduction to quantum computing*. Oxford University Press, 2007. Saatavissa (viitattu 5.2.2022): https://ebookcentral.proquest.com/lib/tampere/detail.action?docID=415080&pq-origsite=primo.

[14] S. Heinrich. From Monte Carlo to quantum computation. *Mathematics and computers in simulation* (2003). Saatavissa (viitattu 30.4.2022): https://www.sciencedirect.com/science/article/abs/pii/S0378475402002392?via%3Dihub.

[15] O. C. Ibe. *Markov processes for stochastic modeling*. Elsevier, 2013. Saatavissa (viitattu 2.5.2022): https://www.sciencedirect.com/book/9780124077959/markov-processes-for-stochastic-modeling.

[16] A. Ambainis. Quantum Walk Algorithm for Element Distinctness. *SIAM journal on computing* (2007). Saatavissa (viitattu 2.5.2022): https://www-proquest-com.libproxy.tuni.fi/docview/918788698?pq-origsite=primo&accountid=14242.

[17] S. Hu, P. Liu, C.-F. Chen ja M. Pistoia. Automatically solving NP-complete problems on a quantum computer. ACM, 2018. Saatavissa (viitattu 2.5.2022): https://dl-acm-org.libproxy.tuni.fi/doi/abs/10.1145/3183440.3194959.

[18] C. H. Bennett ja P. W. Shor. Quantum Information Theory. *IEEE transactions on information theory* (1998). Saatavissa (viitattu 5.2.2022): https://ieeexplore-ieee-org.libproxy.tuni.fi/stamp/stamp.jsp?tp=&arnumber=720553.

[19] R. Griffiths. *Consistent Quantum Theory*. Cambridge University Press, 2002. Saatavissa (viitattu 7.2.2022): https://ebookcentral.proquest.com/lib/tampere/detail.action?docID=202015&pq-origsite=primo.

[20] I. Grout. *Digital systems design with FPGAs and CPLDs*. Elsevier, 2008. Saatavissa (viitattu 8.3.2022): https://www-sciencedirect-com.libproxy.tuni.fi/book/9780750683975/digital-systems-design-with-fpgas-and-cplds.

[21] J. A. Jones ja D. Jaksch. *Quantum information, computation and communication*. Cambridge University Press, 2012. Saatavissa (viitattu 9.3.2022): http://libproxy.tuni.fi/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=cookie,ip,uid&db=e000xww&AN=862338&site=ehost-live&scope=site.

[22] V. Vedral. Quantum entanglement. *Nature physics* (2014). Saatavissa (viitattu 9.3.2022): https://web-p-ebscohost-com.libproxy.tuni.fi/ehost/pdfviewer/pdfviewer?vid=0&sid=1b9df5bf-4188-40b0-94a0-720bd2739117%40redis.

[23] R. H. et al. Quantum entanglement. *Reviews of Modern Physics* (2009). Saatavissa (viitattu 10.2.2022): https://journals-aps-org.libproxy.tuni.fi/rmp/pdf/10.1103/RevModPhys.81.865.

[24] M. Nakahara ja Y. Sasaki. *Quantum information and quantum computing*. World Scientific, 2013. Saatavissa (viitattu 10.3.2022): https://ebookcentral.proquest.com/lib/tampere/reader.action?docID=10698293.

[25] H.-P. Breuer ja F. Petruccione. *The Theory of Open Quantum Systems*. Oxford University Press, 2007. Saatavissa (viitattu 27.5.2022): https://ochicken.top/Library/Physics/Quantum_Computation_and_Quantum_Information/Heinz-Peter%20Breuer,%20Francesco%20Petruccione%20-%20The%20Theory%20of%20Open%20Quantum%20Systems.pdf.

[26] P. Ball. How decoherence killed Schrödinger's cat. *Nature* (2000). Saatavissa (viitattu 27.5.2022): https://www-nature-com.libproxy.tuni.fi/articles/news000120-10.

[27] P. Shor. Scheme for reducing decoherence in quantum computer memory. *Physical Review A* (1995). Saatavissa (viitattu 27.5.2022): https://journals-aps-org.libproxy.tuni.fi/pra/pdf/10.1103/PhysRevA.52.R2493.

[28] T. M. Nieuwenhuizen. *Quantum foundations and open quantum systems : lecture notes of the advanced school*. World Scientific, 2015. Saatavissa (viitattu 9.5.2022): http://libproxy.tuni.fi/login?url=https://search.ebscohost.com/login.aspx?direct=true&AuthType=cookie,ip,uid&db=e000xww&AN=862338&site=ehost-live&scope=site&ebv=EB&ppid=pp_C.

[29] J. A. Jones. Quantum computing and nuclear magnetic resonance. *PhysChemComm* (2001). Saatavissa (viitattu 12.5.2022): https://pubs-rsc-org.libproxy.tuni.fi/en/content/articlelanding/2001/QU/b103231n.

[30] Y. Wang. Analysis on the Mechanism of Superconducting Quantum Computer. *Journal of Physics Conference Series* (2020). Saatavissa (viitattu 20.5.2022): https://www-proquest-com.libproxy.tuni.fi/docview/2570977311?pq-origsite=primo.

[31] B. C. Sanders. *How to build a quantum computer*. Institute Of Physics Publishing, 2017. Saatavissa (viitattu 17.5.2022): https://iopscience.iop.org/book/978-0-7503-1536-4.

[32] E. Stefanovich. *Elementary particle theory*. De Gruyter, 2019. Saatavissa (viitattu 17.5.2022): https://ebookcentral.proquest.com/lib/tampere/reader.action?docID=5574727#.

[33] J. Clarke ja F. K. Wilhelm. Superconducting quantum bits. *Nature (London)* (2008). Saatavissa (viitattu 17.5.2022): https://www-nature-com.libproxy.tuni.fi/articles/nature07128.pdf.

[34] R. Barends, J. Kelly, A. Megrant, A. Veitia, D. Sank, E. Jeffrey, T. C. White, J. Mutus, A. G. Fowler, B. Campbell, Y. Chen, Z. Chen, B. Chiaro, A. Dunsworth, C. Neill, P. O'Malley, P. Roushan, A. Vainsencher, J. Wenner, A. N. Korotkov, A. N. Cleland ja J. M. Martinis. Superconducting quantum circuits at the surface code threshold for fault tolerance. *Nature (London)* (2014). Saatavissa (viitattu 20.5.2022): https://www-nature-com.libproxy.tuni.fi/articles/nature13171.

[35] C. Macklin, K. O'Brien, D. Hover, M. E. Schwartz, V. Bolkhovsky, X. Zhang, W. D. Oliver ja I. Siddiqi. A near-quantum-limited Josephson traveling-wave parametric amplifier. *Science (American Association for the Advancement of Science)* (2015).

Saatavissa (viitattu 20.5.2022): https://www.science.org/doi/10.1126/science.aaa8525.

[36] F. Bova, A. Goldfarb ja R. G. Melko. Commercial applications of quantum computing. *EPJ quantum technology* (2021). Saatavissa (viitattu 27.5.2022): https://www-proquest-com.libproxy.tuni.fi/docview/2483412648?pq-origsite=primo.

[37] M. Brooks. Beyond quantum supremacy: the hunt for useful quantum computers. *Nature (London)* (2019). Saatavissa (viitattu 27.5.2022): https://www-nature-com.libproxy.tuni.fi/articles/d41586-019-02936-3.