Kvanttilaskenta

LuK-tutkielma
Jere Lotvonen
2627973
Matemaattisten tieteiden laitos
Oulun yliopisto
Kevät 2022

Sisällys

1 Johdanto **2**

2 Matematiikkaa **3**
2.1 Hilbertin avaruudet 3
2.2 Bra-ket formalismi 4
2.3 Operaattorit 5
2.4 Tensoritulo 7

3 Kvantti-informaatio **8**
3.1 Kubitit 8
3.2 Kvanttisysteemit 8
3.3 Kvanttiportit 9
3.4 kvanttipiirit 11

4 Systeemeistä ja niiden ominaisuuksista **12**
4.1 Lomittuminen 12
4.2 Mittauksesta 13
4.3 Yhdistesysteemit 13

5 Sovelluksia ja tuloksia **14**
5.1 Kvanttitietokoneet 14
5.2 Kvanttialgoritmit 15

1 Johdanto

Kvanttilaskennan teorian rakentamisen voidaan sanoa alkaneen vuonna 1980, kun Paul Benioff julkaisi muotoilunsa kvanttimekaanisesta turingin koneesta. Yhteydessä algoritmien kompleksisuus teoriaan fyysikko *Richard P. Feynman* ehdotti vuonna 1982 julkaistussa artikkelissaan *"Simulating physics with computers"*, että kvanttimekaanista systeemiä, mikä koostuu N-kappaleesta partikkeleita ei pystytä simuloimaan tavallisilla tietokoneilla ilman exponentiaalista laskua laskennan nopeudessa. Feynman ehdotti myös, että tämä hidastuminen olisi mahdollista kiertää käyttämällä tietokonetta, joka noudattaisi kvanttifysiikan lakeja. Tutkielmassani käsittelen matemaattista teoriaa näille kvanttitietokoneille ja käyn läpi hieman esimerkkejä laskuista sekä sovelluksia kvanttilaskennalle. Lukijan olisi hyvä tietää perusteet lineaarialgebrasta, koska sitä käytetään kielenä kvanttilaskennassa.[1] (kirjoitetaan tähän perään sitten myöhemminmitä asioita tutkielma käsittelee, kun se on valmis)

[1] Hyväksi onnekseni suurempi osa tarvittavaa lineaarialgebraa perustuu vektoreihin, jotka käydään läpi lukiotason matematiikassa.

2 Matematiikkaa

2.1 Hilbertin avaruudet

Äärellisuloitteinen Hilbertin avaruus H on täydellinen vektoriavaruus, jolle on määritelty sisätulo $H \times H \to \mathbb{C}, (x, y) \mapsto \langle x|y\rangle$. Sisätulon tulee täyttää seuraavat ominaisuudet kaikille $\mathbf{x}, \mathbf{y}, \mathbf{z} \in H$ sekä $c_1, c_2 \in \mathbb{K}$[2]

$$\langle x|y\rangle = \langle y|x\rangle^* . \tag{1}$$
$$\langle x|x\rangle \geq 0. \tag{2}$$
$$\langle x|x\rangle = 0 \text{ jos ja vain jos } \mathbf{x} = 0. \tag{3}$$
$$\langle x|c_1 y + c_2 z\rangle = c_1 \langle x|y\rangle + c_2 \langle x|z\rangle \tag{4}$$

Merkinnällä $\langle x|y\rangle^*$ tarkoitetaan sisätulon kompleksikonjugaattia. Jos $U = \{u_1, u_2, \ldots, u_n\}$ on Hilbertin avaruuden H ortonormaali kanta, jokainen vektori $\mathbf{x} \in H$ voidaan esittää muodossa $\mathbf{x} = x_1 u_1 + x_2 u_2 + \cdots + x_n u_n$. Kertoimet $(x_1, x_2, \ldots, x_n)$ määräävät vektorin $\mathbf{x}$ *koordinaatit* kanssa U. Sisätulo määritellään Seuraavasti:

$$\langle x|y\rangle = x_1^* y_1 + x_2^* y_2 + \cdots + x_n^* y_n. \tag{5}$$

Määritelmä 2.1. Vektoriavaruus V on *täydellinen*, jos jokaiselle vektorijonolle $\{x_i\}_{i\in\mathbb{N}}$ jolle pätee

$$\lim_{n,m\to\infty} \|x_m - x_n\| = 0,$$

On olemassa vektori $\mathbf{x} \in V$ siten, että

$$\lim_{n,m\to\infty} \|x_m - x\| = 0.$$

Käyttämällä hyväksi sisätulon indusoimaa normia voimme todistaa avaruuksien täydellisyyden osoittamalla, että vektorijono, joka konvergoi absoluuttisesti (normi) konvergoi myös tavallisesti.

Hilbertin avaruuden käsite on olennainen kvanttilaskennan yhteydessä, sillä kaikki kubitit pystytään ilmaisemaan Hilbertin avaruuden vektoreina. Kubittien fyysinen tulkinta on myös yhteydessä Hilbertin avaruuteen, sillä kaikki fyysisesti hahmoteltavissa olevat aaltofunktion tilafunktio ovat neliöllisesti integroituvia funktiota. Neliöllisesti integroituvat funktiot muodostavat hilbertin avaruuden käyttämällä (määrättyä)integraalia sisätulona.

[2] merkintä $\mathbb{K}$ tarkoittaa kerroinkuntaa

2.2 Bra-ket formalismi

Tulen käyttämään vektoreille Bra-ket merkintää jatkossa, missä $|x\rangle \in H$ on *ket* ja $\langle y| \in H$ on *bra*. Tästä lähtien Hilbertin avaruuden vektorit erottaa siis Bra-ket merkinnän avulla yleisesti muista vektoreista. bra- ja ket-vektorit määritellään seuraavanlaisesti[3].

$$|x\rangle = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad \langle y| = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}^\dagger = [y_1^*, y_2^*, \cdots, y_n^*].$$

Bra-ket merkintä helpottaa joidenkin laskujen tarkasteluja, sillä työskentelemme yleensä ortonormaaleissa kannoissa. Huomataan lisäksi, että Bra-ket merkintätapa muodostaa sisätulon.[4]

$$\langle y| \left(|x\rangle\right) = \langle y|x\rangle = \sum_{k=1}^{n} y_k^* x_k.$$

Normaali vektoreiden yhteenlasku ja skalaarilla kertominen määritellään tavanomaisesti seuraamalla annettuja merkintätapoja.

Esimerkki 2.2. Olkoon

$$|x\rangle = \begin{bmatrix} 1 \\ i \end{bmatrix}, |y\rangle = \begin{bmatrix} 1 \\ -i \end{bmatrix}$$

määrää vektoreiden bra-esitykset ja niiden sisätulo. Virittävätkö vektorit jonkin avaruuden, kun kerroinkuntana käytetään joukkoa $K = \mathbb{C}$?
Nyt

$$\langle x| = \begin{bmatrix} 1 \\ i \end{bmatrix}^\dagger = [1, -i] \quad ja \quad \langle y| = \begin{bmatrix} 1 \\ -i \end{bmatrix}^\dagger = [1, i].$$

[3] merkinnällä † tarkoitetaan kompleksikonjugaatin transpoosia.

[4] Asia ei tietenkään ole näin yksinkertainen, mutta se vaatii perinpohjaisempaa tarkastelua Hilbertin avaruuksista. Tyypillisesti Hilbertin avaruuden ket-vektoreita $|x\rangle$ vastaavat bra-vektorit $\langle x|$ ovat Hilbertin avaruuden H *duaali avaruuden* $H*$ vektoreita. Duaali avaruus on myös Hilbertin avaruus ja kaikki Hilbertin avaruudet ovat keskenään isomorfisia. Tämä oikeuttaa bra-ket notaation sisätulo tulkinnan, koska voidaan ajatella bra-vektoreiden toimivan lineaarikuvauksina Hilbertin avaruudelta kerroinkunnalle.

Tarkastellaan seuraavaksi vektorien sisätuloa.

$$\langle x|y\rangle = \langle y|x\rangle^* = [1, -i]\begin{bmatrix}1\\-i\end{bmatrix} = 1 + i^2 = 1 - 1 = 0.$$

Koska vektorit ovat ortogonaaliset ja niiden kerroinkuntana toimii $\mathbb{C}$ ne toimivat kantaektoreina avaruudessa $\mathbb{C}^2$ ja täten virittävät sen.

Huomautus 2.3. jos valitaan kerroinkunnaksi $\mathbb{R}$, tämä ei enää toimisi. Olkoon $\mathbf{x} \in \mathbb{C}^2$ tästä seuraa, että

$$\mathbf{x} = \begin{bmatrix}a+ib\\c+id\end{bmatrix} = a_x\,|x\rangle + a_y\,|y\rangle = a_x\begin{bmatrix}1\\i\end{bmatrix} + a_y\begin{bmatrix}1\\-i\end{bmatrix}$$

silloin kun

$$a_x = \frac{a-d+i(c+b)}{2} \quad a_y = \frac{a+d+i(b-c)}{2}.$$

Vektorit $|x\rangle$ ja $|y\rangle$ eivät ole ortonormaaleja, mutta ne voidaan normalisoida rakentaaksemme ortonormaalin kannan. Vektorin normi saadaan kaavalla

$$\|x\| = \sqrt{\langle x|x\rangle}.$$

2.3 Operaattorit

Määritelmä 2.4. Vektoriavaruuksien U ja V välistä kuvausta $L : U \mapsto V$ kutsutaan lineaarikuvaukseksi, jos $L(ax+by) = aL(x)+bL(y)$ kaikille $x, y \in U$ sekä kaikille $a, b \in \mathbb{K}$.

Määritelmä 2.5. Lineaarikuvausta $\hat{T} : H \mapsto H$ kutsutaan operaattoriksi.

Operaattorit ovat siis muunnoksia, jotka muokkaavat Hilbertin avaruuden vektoreita. Loogisia portteja havainnoidaan operaattorien avulla.

Lause 2.6. *Jokainen vektoriavaruuden V alkio $x \in V$ voidaan esittää yksikäsitteisesti kantavektorien $\{v_i\}_{i=1}^n$ lineaarikombinaationa*

$$x = \sum_{k=1}^{n} x_1 v_1.$$

Todistus. Olkoon V vektoriavaruus kantanaan $\{v_i\}_{i=1}^n$ ja $x \in V$. Nyt

$$x = \sum_{k=1}^{n} a_k v_k$$

Oletetaan, että vektorilla $x \in V$ on toinen esitys kannassa $\{v_i\}_{i=1}^n$

$$x = \sum_{k=1}^{n} a_k^{'} v_k.$$

Tästä seuraa, että

$$\begin{aligned} x - x &= \sum_{k=1}^{n} a_k v_k - \sum_{k=1}^{n} a_k^{'} v_k = 0 \\ &\sum_{k=1}^{n} (a_k - a_k^{'}) v_k = 0. \end{aligned}$$

Vektorit $\{v_i\}_{i=1}^n$ ovat kantavektoreina lineaarisestiriippumattomia toisistaan, joten

$$\begin{aligned} a_k - a_k^{'} &= 0 \\ a_k &= a_k^{'}. \end{aligned}$$

□

Seuraus 2.7. *Lineaarikuvaus $L : X \mapsto Y$ voidaan aina esittää matriisina, joten operaattoreiden tarkasteluun voidaan käyttää matriisien laskusääntöjä.*

Määritelmä 2.8. Operaattorille T sen *viereinen operaattori* $T^\dagger$ on määritelty kaikille $x, y \in H$ seuraavanlaisesti

$$\langle Tx|y\rangle = \langle x|T^\dagger y\rangle\,, \quad \textit{missä}$$

$$T^\dagger = (T^T)^* = \left(\begin{bmatrix} t_{11} & t_{12} & \cdots & t_{1m} \\ t_{21} & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ t_{n1} & \cdots & \cdots & t_{nm} \end{bmatrix}^T \right)^* = \begin{bmatrix} t_{11}^* & t_{21}^* & \cdots & t_{n1}^* \\ t_{12}^* & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ t_{1m}^* & \cdots & \cdots & t_{nm}^* \end{bmatrix}$$

Määritelmä 2.9. Operaattori T on *itsensä-viereinen*, jos $T = T^\dagger$. Operaattori on *unitaarinen*, jos $T^\dagger = T^{-1}$.

Määritelmä 2.10. Yhtälöä $Tx = \lambda x$, missä $x \in H, x \neq 0$ sekä $\lambda \in \mathbb{C}$. kutsutaan *ominaisarvoyhtälöksi* ja sen vastauksina saadaan *ominaisarvoja* λ sekä *ominaisvektoreita* x.

Ominaisarvoyhtälöt ovat tärkeitä suhteessa Hilbertin avaruuksiin, sillä operaattorin ominaisarvoista ja -vektoreista voidaan konstruktoida Hilbertin avaruuden ortonormaalikanta. Ominaisarvot ovat myös yhteydessä mitattaviin suureisiin.

Lause 2.11. *Olkoon T itsensä-viereinen operaattori $T = T^\dagger$. Nyt seuraavat asiat pätevät operaattorille T.*

1. *Operaattorilla T on reaaliset ominaisarvot $\lambda \in \mathbb{R}$.*
2. *Operaattorin T ominaisvektorit $x_k \in H$, joilla on erisuuret ominaisarvot ovat ortogonaaliset.*
3. *jos $T : H_n \mapsto H_n$[5] On olemassa Hilbertin avaruuden H_n ortonormaalikanta, joka koostuu operaattorin T ominaisarvoista.*

Todistetaan seuraavaksi vain kohdat (1) ja (2). Kohta (3) jätetään todistamatta, koska se vaatii suurempaa tarkastelua.

Lause 2.12. *Olkoot A itsensä-viereinen operaattori, jolle $Ax = \lambda x$.*

1. *Nyt*[6]

$$\lambda^* \langle x|x\rangle = \langle \lambda^* x|x\rangle = \langle x|\lambda x\rangle = \langle x|Ax\rangle = \langle Ax|x\rangle = \lambda \langle x|x\rangle$$

   , koska $\langle x|x\rangle \neq 0$ niin $\lambda^* = \lambda$. Tämä implikoi, että $\lambda \in \mathbb{R}$. $\square$

2. *Olkoot $\lambda \neq \lambda'$, $Ax = \lambda x$ sekä $Ax' = \lambda' x'$. Edellisen kohdan perusteella*

$$\lambda' \langle x'|x\rangle = \langle Ax'|x\rangle = \langle x'|Ax\rangle = \lambda \langle x'|x\rangle$$

   , koska $\lambda \neq \lambda'$ niin $\langle x'|x\rangle = 0$. $\square$

2.4 Tensoritulo

Määritellään tensoritulo $\otimes$ kahden $r \times s$ ja $t \times u$ matriisin A ja B välillä kaavalla.

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1s}B \\ a_{21}B & a_{22}B & \cdots & a_{2s}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1}B & a_{r2}B & \cdots & a_{rs}B \end{bmatrix}$$

[5] H_n tarkoittaa, että $\dim(H_n) = n$.
[6] $\langle x|y\rangle = \langle y|x\rangle^* \Rightarrow \langle x|x\rangle = \langle x|x\rangle^*$.

3 Kvantti-informaatio

Tässä osiossa käydään läpi matematiikan avulla kvanttilaskennan perusteita

3.1 Kubitit

Kubitit ovat kvantti-informaation perusyksikkö ja niitä hahmotetaan Hilbertin avaruuden vektoreilla. Kubitit muodostavat kvanttisysteemejä, jotka ovat lineaarikombinaatioita kubiteista.
Kubitit ovat tietyllä tasolla analogisia verrattuina klassisiin bitteihin. Kubitit niin kuin klassiset bititkin voivat olla tilassa 0 ja 1, mutta erona klassisiin bitteihin kubitit voivat olla superpositiotilassa niin kuin tilojen 1 ja 0 "välillä"[7]. Merkitsemme tätä superpositio tilaa vektorilla $|\psi\rangle \in H_2$

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,\ \text{missä } \alpha, \beta \in \mathbb{C}.$$

3.2 Kvanttisysteemit

Luetellaan tähän tärkeimpiä äärellisten kvanttisysteemien ominaisuuksia

1 n-ulotteisen kvanttisysteemin kanta muodostaa ortonormaalin Hilbertin avaruuden kannan. Tämä kanta on valittavissa mielivaltaisesti, joka tarkoittaa sitä, että voimme määrätä mitä kubittien mitattavat tilat esittävät.[8]

2 Kvanttisysteemien tilaa esitetään yksikkövektorilla
$|\psi\rangle = \alpha_1\,|x_1\rangle + \alpha_2\,|x_2\rangle + \cdots + \alpha_n\,|x_n\rangle$. Tätä yksikkövektoria kutsutaan tilavektoriksi ja sen esittämää tilaa superpositiotilaksi.
kertoimien $\alpha_i \in \mathbb{C}$ pituus $|\alpha_i^2|$ määrittää todennäköisyyden löytää systeemi kerrointa vastaavasta tilasta x_i.

3 Kahden kvanttisysteemin muodostamaa yhdistesysteemiä kuvataan niihin liitännäisten Hilbertin avaruuksien tensoritulolla $H_m \otimes H_n$, missä H_i on systeemiin $\alpha_1\,|x_1\rangle + \alpha_2\,|x_2\rangle + \cdots + \alpha_i\,|x_i\rangle$ liitännäinen Hilbertin avaruus.

4 Kvanttisysteemien tila muuntuu vain ja ainoastaan unitaaristen operaattoreiden toimesta.

[7] Tämä ei ole aivan totta, mutta on hyvä hahmotus
[8] Myöhemmin mittauksesta

3.3 Kvanttiportit

Kvanttiportit ovat verrannollisia klassisiin logiikkaportteihin niiden toiminta on samanlaista, mutta niitä hahmotetaan unitaarisilla lineaarikuvauksilla. Esittelen hieman seuraavaksi klassisten logiikkaporttien toimintaa.

bit 1	bit 2	AND
0	0	0
1	0	0
0	1	0
1	1	1

bit 1	bit 2	OR
0	0	0
1	0	1
0	1	1
1	1	1

bit 1	bit 2	NAND
0	0	1
1	0	1
0	1	1
1	1	0

Porteista NAND portti on ns. *universaali* eli, sillä voidaan konstruktoita kaikkien muiden logiikkaporttien toiminta. Tämä tapahtuu liittämällä NAND portteja yhteen, toinen esimerkki universaalista logiikkaportista on NOR portti. Kvanttiporttien tapauksessa ei ole tämän tapaisia universaaleja kvanttiportteja, mutta on mahdollista konstruktoida joukko kvanttiportteja, joilla voidaan vähintään approksimoida hyvin kaikkien muiden porttien toimintaa.

Nyt kun tiedämme klassisten logiikkaporttien toiminnnasta, katsotaan esimerkin kautta, miten kvanttiporttien toimintaa hahmotetaan.

Esimerkki 3.1. Olkoon meillä portti X. Porttia X kutsutaan NOT-portiksi, koska se kääntää kantavektorit $|1\rangle$ ja $|0\rangle$ vektoreiksi $X|0\rangle = |1\rangle$ ja $X|1\rangle = |0\rangle$. Selvitetään portin X matriisiesitys tässä kannassa.
Standartikannassa vektorit $|0\rangle$ ja $|1\rangle$ esitttävät pystyvektoreita

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ ja } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Täten voidaan johtaa yhtälöt

$$X|0\rangle = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} x_{11} \\ x_{21} \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$X|1\rangle = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} x_{12} \\ x_{22} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

, joten tiedämmekin miten muodostaa matriisi X

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

Kvanttiportit ovat matrsiisiesityksinä abstarkteja, mutta ne avustavat hahmottamaan informaation käsittelyä kvanttipiireissä. Muita yleisiä kvanttiportteja NOT portin lisäksi ovat

- Y ja Z portit, $Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  -Nämä portit muuttavat kubitin vaihetta.
- Hadamart-walsh portti, $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
  -Tämä portti pystyy asettamaan kantavektorit superpositiotilaan.
- Vaiheensiirtoportti, $P(\omega) = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\omega} \end{bmatrix}$
  -Tämän portin toimintaa voidaan hahmottaa rotaatioiden avulla.
- kontrolloitu not portti, $CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
  -Tämä tietty CNOT portti toimii 2-kubitin systeemeissä. Se tekee NOT operaation toiselle kubitille, jos ensimmäinen kubitti on 1.
- SWAP portti, $SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
  -SWAP portti vaihtaa 2 kubitin paikat keskenään.

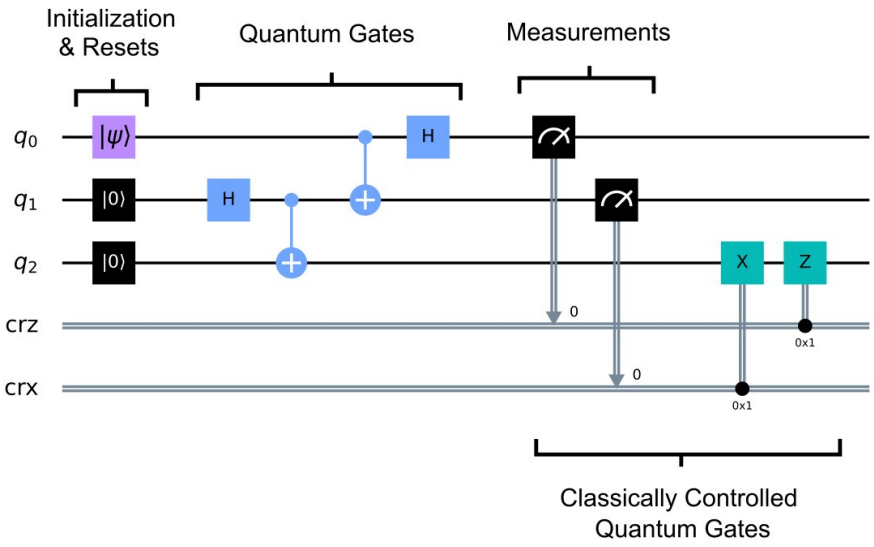
Huomautus 3.2. Mainitsin esimerkissä (3.1), että selvitämme matriisiesitystä tietyssä kannassa. Operaattoreiden esitys onkin liitännäinen kantaan, missä ne esitetään, kuitenkin operaattoreiden olemassaolo ei ole riippuvainen kannasta, vaan ne voidaan siirtää aina hilbertin avaruudelta toiselle. Hilbertin avaruuksista mainitsin myös aiemmin niiden isomorfisuuden, kun löydämme isomofismin hilbertin avaruuksien välillä voimme hyväksikäyttää tätä operaattoreiden muodostamiseen.

3.4 kvanttipiirit

Kvanttilaskenta on periaatteessa matemaattinen pohja kvanttitietokoneille. kvanttitietokoneet ovat tietokoneita, jotka operoivat klassisten bittien sijasta kubiteilla. Kvanttipiirit kuuluvat osaksi yhtä kvanttitietokone mallia. Piiriesitys on näistä malleista yleisesti helpoin ymmärtää, mutta muita mallejakin on. (esim topologiset kvanttietokoneet)

Esimerkki 3.3. Kvanttipiiri esitys voidaan pelkistää kolmeen osaan syötteeseen(engl. input) piiriin(engl. circuit) ja ulostuloon (engl. output).

Kuva 1: Esimerkki piiristä, joka implementoi kvanttiteleportaatio algoritmin



4 Systeemeistä ja niiden ominaisuuksista

Tässä osiossa käyn hieman läpi fyysisiä asioita kvanttisysteemeistä. Kvanttilaskenta perustuu hyvin vahvasti kvanttimekaniikan postulaatteihin ja tuloksiin. Koska kvanttilaskenta on abstrakti malli, se voidaan ajatella toimivaksi ilman fyysistä realisaatiota. Kvanttilaskenta on kuitenkin jatketta tälle fysiikan osa-aluelle, joten on tärkeää ymmärtää hieman siitäkin.

4.1 Lomittuminen

Kvanttisysteemit joista puhun, ovat fysiikassa paljon esiintyvän aaltofunktion tiloja[9]. Tämä aaltofunktio pystyy kertomaan meille, kuinka hiukkaset käyttäytyvät avaruudessa suhteessa aikaan ja paikkaan. Kuitenkin sen tarkastelu matemaattisesti johtaa hyvin kiinnostaviin tuloksiin. Näistä tuloksista *lomittuminen* on hyvin tärkeä kvanttilaskennan kannalta. Lomittuminen tarkoittaa matemaattisesti, sitä että kubittien tapauksessa emme voi purkaa systeemiä tensorituloksi kahdesta eri systeemistä. Fyysisesti se johtaa esimerkiksi tuloksiin, että systeemit esimerkiksi kaksi hiukkasta voivat vuorovaikuttaa toistensa kanssa pitkienkin etäisyyksien päästä ilman minkäänlaista klassista selitystä[10].

Esimerkki 4.1. Olkoon meillä kvanttisysteemi tilassa

$$|\psi\rangle = \alpha\,|11\rangle + \beta\,|01\rangle\,.$$

Tämä systeemi on ei ole lomittunut koska se voidaan purkaa tensorituloksi.

$$\alpha\,|11\rangle + \beta\,|01\rangle = (\alpha\,|1\rangle + \beta\,|0\rangle)\,|1\rangle\,.$$

Toinen systeemi, joka määritellään

$$|\psi\rangle = \alpha\,|01\rangle + \beta\,|10\rangle$$

taas on lomittunut, koska sitä ei voida purkaa tensorituloksi. Tämän voi varmistaa esimerkiksi luomalla yhtälöryhmän ja yrittämällä löytää sen ratkaisua.

[9] Tilavektoreita

[10] Tämä on totta, mutta miksi vaatii matemaattista selittämistä

4.2 Mittauksesta

Mittaus on hieman kiistanalainen aihe ja sen tulkinnalla ei itse-asiassa ole mitään väliä. Tärkeintä on tietää, että kun mittaamme kubitin esimerkiksi superpositiotilassa

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,,$$

missä kubitin todennäköisyys olla tilassa $|0\rangle$ on määrätty kertoimen $|\alpha^2|$ mukaan ja tilan $|1\rangle$ todennäköisyys kertoimen $|\beta^2|$ mukaan. Mitattaessa saamme tulokseksi jomman kumman näistä tiloista. On mittaus siis yksikäsitteinen, Vaikka kubitti onkin superpositiossa.

4.3 Yhdistesysteemit

Yhdistesysteeminä pidetään systeemiä, joka koostuu kahden tai useamman kvanttisysteemistin tensoritulosta.

Esimerkki 4.2. Olkoot meillä kaksi kubittia superpositio tiloissa

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \quad |\phi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle\,.$$

Näiden kubittien muodostama yhdisttesysteemi saadaan selville laskemalla

$$\begin{aligned}
|\psi\rangle \otimes |\phi\rangle &= (\alpha\,|0\rangle + \beta\,|1\rangle) \otimes (\gamma\,|0\rangle + \delta\,|1\rangle) \\
&= (\alpha\,|0\rangle + \beta\,|1\rangle)\gamma\,|0\rangle + (\alpha\,|0\rangle + \beta\,|1\rangle)\delta\,|1\rangle \\
&= \alpha\gamma\,|00\rangle + \beta\gamma\,|10\rangle + \alpha\delta\,|01\rangle + \beta\delta\,|11\rangle \\
&= c_1\,|00\rangle + c_2\,|01\rangle + c_3\,|10\rangle + c_4\,|11\rangle\,.
\end{aligned}$$

Tällaiset systeemit voidaan esittää pystyvektoreilla

$$c_1\,|00\rangle + c_2\,|01\rangle + c_3\,|10\rangle + c_4\,|11\rangle = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix}.$$

Yhdistesysteemeille kvanttiportit laajenevat hyvin luonnollisesti

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} c_1 \\ c_2 \\ c_3 \\ c_4 \end{bmatrix} = \begin{bmatrix} c_1 \\ c_3 \\ c_2 \\ c_4 \end{bmatrix} = c_1\,|00\rangle + c_3\,|01\rangle + c_2\,|10\rangle + c_4\,|11\rangle\,.$$

5 Sovelluksia ja tuloksia

5.1 Kvanttitietokoneet

Kvanttitietokoneet ovat koneita, joilla on tehdään kvanttilaskentaa hyväksikäyttäen kvanttisysteemeille ominaisia tuloksia. Aiemmin mainitsin, että kvanttitietokonemalleja on olemassa enemmänkin, kuin yksi ja että tutkielmassa keskitytään erityisesti kvanttipiiri malliin. Edellä esittelen hieman muita malleja ja kerron miissä niistä on kyse.

- **Kvanttipiiri malli**
  Tämä malli on siis tutkielmassa käytetty, se pitää kvanttitietokoneita piireinä[11], jotka koostuvat syötteestä operaatioista sekä mittauksesta. Malli on varmaankin yleistynyt koska se on lähimpänä nykyistä klassista tietokonemallia, joka koostuu myös syötteestä ja logiikkaporteista.

- **Mittausperusteinen malli**
  Tämän mallin perusidea on, että tietokoneeseen valmistella suuri systeemi lomittuneita kubitteja ja sen jälkeen systeemiin tehdään mittaus, joka kohdistuu yhteen kubittiin.

- **Topologinen malli**
  Tämä malli käyttää hyväkseen niin kutsuttuja anyoneja, jotka ovat quasipartikkeleita. Anyonit ovat vähemmän herkkiä interferenssille, kuin mitä muut kubitti vaihtoehdot, mutta niitä on vaikea valmistaa. Microsoftilla on kehitteillä tällainen tietokone.

- **Adiabaattinen malli**
  Adiabaattinen malli luottaa *adiabaattiseen teoriaaan*. Adiabaattinen teoria sanoo, että kvanttisysteemit, jotka ovat vähitellen muuttuvassa ympäristössä muuttavat funktionaalista muotoaan[12], mutta systeemit jotka ovat nopeasti muuttuvassa ympäristössä eivät pysty tähän, joten ne säilyttävät funktionaalisen muotonsa.

[11] vähän kuin sähköpiirit, joita esiteltiin lukio fysiikassa, mutta ne eivät vain kierrä itsensä ympäri

[12] Aaltofunktio

5.2 Kvanttialgoritmit

Kvanttitietokoneiden käytännöllisyys liittyy niiden kykyyn ratkaista laskennallisia ongelmia nopeammin verrattuna klassisiin tietokoneisiin. Tähän kvanttitietokone käyttää hyväkseen kubittien superpositiota ja lomittumista. Luetellaan seuraavaksi hieman kvanttialgoritmeja, mutta jätetään niiden esittäminen välistä.

- **Shorin algoritmi**
  Shorin algoritmi pystyy ratkaisemaan diskreetin logaritmin ja kokonaislukujen alkulukuhajotelmat polynomisessa ajassa. Tämä tarkoittaa sitä, että jos ongelman arvon koko on N niin algoritmilla menee N^2 aikayksikköä sen ratkaisemiseen keskimäärin.

- **Groverin algoritmi**
  Groverin algoritmilla on mahdollista etsiä järjestämättömästä listasta alkoita nopeampaa, kuin klassisilla algoritmeilla.

- **Kvanttisimulaatiot**
  On ajateltu, että kvanttitietokoneella olisi mahdollista simuloida kvanttimekaanisia systeemejä polynomisessa ajassa, kun klassisilla tietokoneilla menee siihen eksponentiaalisesti aikaa.

- **Deutsch-jozsa algoritmi**
  Deutsch-jozsa algoritmi pystyy määrittämään yhdellä kyselyllä onko annetun funktion f arvojoukko kokonaan 0 tai 1 vaiko puoleksi 0 ja puoleksi 1, kun tiedetään sen olevan jompaa kumpaa. Klassinen algoritmi joutuu tekemään 2^{n-1} kyselyä. Deutsch-jozsa algoritmi on hyvin olennainen algortimi, koska se esittää hyvin kvanttitietokoneiden tehokkuuden ja on mahdollisimman yksinkertainen.

Viitteet

[1] M. Hirvensalo, *Quantum computing*. Springer Science & Business Media, 2003.

[2] D. McMahon, *Quantum computing explained*. John Wiley & Sons, 2007.