Kvanttimekaaninen Groverin etsintäalgoritmi

Petri Liimatta

LuK-tutkielma
Fysiikan koulutusohjelma
Teoreettinen fysiikka
Oulun yliopisto
2018

Sisältö

1 Johdanto **2**

2 Bra-ket-notaatio ja lineaarialgebraa **3**
2.1 Vektorit ja bra-ket-notaatio 3
2.2 Matriisit 4

3 Groverin algoritmi: johto **6**
3.1 Oraakkeli 6
3.2 Ehdollinen vaihesiirto 7
3.3 Geometrinen tulkinta 8
3.4 Esimerkki: 2 kubittia 10
3.5 Groverin algoritmin funktiot f_n ja g_n 10

4 Groverin algoritmi käytännössä **12**

5 Teoreettisia tutkimustuloksia **13**

6 Loppupäätelmät **15**

Tiivistelmä

Käsittelemme kvanttitietokoneeseen kehitettävää Groverin algoritmia teoreettisesta näkökulmasta. Esittelemme Diracin bra-ket-notaation ja kertaamme lineaarialgebraa, jonka jälkeen johdamme Groverin algoritmin. Groverin algoritmia tulkitaan geometrisesta näkökulmasta, jonka avulla osoitamme algoritmin iteraatioiden lukumäärän skaalautuvan $\sqrt{N}$ verrannollisesti, missä N onetsittävien alkioiden lukumäärä. Lisäksi johdamme funktiot todennäköisyydelle saada haluttu tulos Groverin algoritmista. Lopuksi katsomme Groverin algoritmiin liittyviä tutkimustuloksia, sekä teoreettisia että kokeellisia.

1 Johdanto

Kvanttimekaniikan tutkimus on avannut mahdollisuuden hyödyntää kvanttitason ilmiöitä kiinteän aineen tutkimuksessa. Yksi näistä hyötykohteista on tietokoneet, joiden toimintaa voitaisiin nopeuttaa kvanttimekaanisten ilmiöiden avulla. Näiden niin sanottujen kvanttitietokoneiden avulla voidaan parantaa tietokoneen laskentatehoa huomattavasti verrattuna "klassisiin" tietokoneisiin.

Tässä tutkielmassa käsittelemme yhtä kvanttitietokoneella toteutettavaa algoritmia, Groverin algoritmia, parantaaksemme tiedonhakua järjestämättömästä tietokannasta. Yleisesti tietokanta on kokoelma dataa, esimerkiksi ihmisten nimiä ja heidän puhelinnumeroitaan. Haettaessamme tietoa tietokannasta etsimme tiettyä tunnistetta (esimerkiksi nimeä) vastaavaa dataa (puhelinnumeroa). Puhelinluetteloa selatessa tällainen tiedonhaku on helppoa, koska nimet on järjestetty aakkosjärjestykseen.

Kuitenkaan kaikki tietokannat eivät ole järjestettyjä. Tällaisia tietokantoja sanotaan järjestämättömiksi tietokannoiksi ja niistä tiedonhaku on hankalaa. Klassisten tietokoneiden algoritmi hakuun tällaisesta tietokannasta on verrata jokaista tietokannan alkion tunnistetta etsittävään tunnisteeseen niin kauan, että haluttu tunniste löytyy. Kuten saattaa arvata, tällainen prosessi kestää kauan varsinkin, jos tietokanta on suuri.

Kvanttitietokone pystyisi kuitenkin nopeuttamaan huomattavasti tällaista hakua Groverin algoritmin avulla. Esimerkiksi haku puhelinluettelosta, jonka koko on noin 10^8 alkiota, vaatii klassisesti noin 10^8 alkion käsittelyn. Kvanttimekaaninen haku vaatisi puolestaan vain noin 10^4 alkion käsittelyn, mikä nopeuttaisi hakua huomattavasti.

2 Bra-ket-notaatio ja lineaarialgebraa

Groverin algoritmi esitetään käyttäen Diracin bra-ket-notaatiota. Käyttääksemme kyseistä notaatiota on meidän ensin pureuduttava sen pohjalla olevaan matematiikkaan, erityisesti lineaarialgebraan. Tässä osassa esitellään kompleksiset vektorit juuri Diracin notaation avulla. Lisäksi katsomme matriiseja, joiden komponentit voivat olla myös kompleksilukuja.

2.1 Vektorit ja bra-ket-notaatio

Vektoreille käytetään yleensä merkintää $\vec{r} = x\vec{i} + y\vec{j} + z\vec{k}$, missä ylänuoli on vektorin merkki. Vektorin edessä oleva luku kertoo vektorin pituuden. Kvanttimekaniikassa vektoreiden merkkinä käytetään Diracin bra-ket-notaatiota $|\psi\rangle$.

Bra-ket-notaatiossa vektori ilmaistaan ylänuolen sijaan sulkeilla $|r\rangle = x\,|i\rangle + y\,|j\rangle + z\,|k\rangle$. Näin saadaan merkintätapa ket-vektorille, joka on tavallinen vektori. Koska kvanttimekaniikassa käytetään kompleksilukuja, ket-vektorin kerroin voi olla kompleksinen.

Fysikaalisesti ket-vektori esittää lineaarikombinaatiota (superpositiota) systeemin mahdollisista tiloista ja vastaa Shcrödingerin yhtälön aaltofunktiota $\psi(x,t)$. Tilat ovat keskenään ortonormaaleja, eli niiden pituus on 1 ja ne ovat toisiaan kohtisuorassa. Kohtisuoruus vaaditaan, koska mitattaessa kvanttimekaanista systeemiä vain yksi tiloista on mahdollista mitata kerralla.

Määritellään seuraavaksi tällaiselle kompleksiselle vektorille sen pistetulo (sisätulo). Tavalliselle vektorille pistetulo määritetään

$$\vec{a} \cdot \vec{b} = a_x b_x + a_y b_y + a_z b_z, \tag{1}$$

missä sekä $\vec{a}$:n että $\vec{b}$:n komponentit kerrotaan keskenään ja summataan yhteen. Kompleksilukujen tapauksessa kuitenkin tavallinen kertominen ei käy, sillä

$$z_1 z_2 = (x_1 + y_1 i)(x_2 + y_2 i) = x_1 x_2 - y_1 y_2 + (x_1 y_2 + x_2 y_1) i$$

ei yleisessä tapauksessa ole reaaliluku. Sen sijaan on luku kerrottava kompleksikonjugantillaan $z^* = x - yi$. Tällöin saadaan

$$z^* z = (x - yi)(x + yi) = x^2 + y^2. \tag{2}$$

Koska z:n reaali- ja imaginääriosa x ja y ovat reaalilukuja, saadaan tällaisesta pistetulosta myös reaaliluku.

On myös syytä huomioida vektorin tulkinta pystymatriisina ($n \times 1$ matriisi). Jotta vektori saataisiin luvuksi, tulee tämä kertoa vaakamatriisilla ($1 \times n$ matriisi), jotta saadaa luku (1×1 matriisi). Jotta saisimme normaalia kaavan (1) pistetuloa vastaavan pistetulon kompleksiluvuille, määrittelemme bra-vektorin

$$\langle\phi| = |\phi\rangle^{*T} = |\phi\rangle^{\dagger}, \tag{3}$$

joka osoittautuu olevan ket-vektorin Hermiten transpoosi. Tämän nojalla saadaan määritettyä ket-vektorien sisätulo

$$\langle\phi| \cdot |\psi\rangle = |\phi\rangle^{\dagger} \cdot |\psi\rangle = \phi_x^* \psi_x + \phi_y^* \psi_y + \phi_z^* \psi_z, \tag{4}$$

joka tuottaa toivotun reaaliluvun.

Kvanttitietokoneessa käsittelemme kubitteja, jotka vastaavat klassisen tietokoneen bittejä (0 tai 1). Yleisessä tapauksessa kuibitit ovat superpositiossa näistä kahdesta tilasta. Merkitään $|0\rangle$ vastaamaan bittiä 0 ja $|1\rangle$ vastaa bittiä 1. Tällöin ket-vektorimme on muotoa $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ [1, 2].

Koska samaistamme ket-vektorin aaltofunktion kanssa, tulee sillä olla samat ominaisuudet kuin aaltofunktiolla. Erityisesti ket-vektorimme tulee olla normalisoitu, josta seuraa, että

$$\langle\psi|\psi\rangle = \alpha^2 + \beta^2 = 1. \tag{5}$$

Tästä voimme todeta α^2:n ja β^2:n olevat tilojen $|0\rangle$ ja $|1\rangle$ todennäköisyys mitattaessa [1, 2]. Useamman tilan tapauksessa kaavan (4) pistetulo antaa summan, joka vastaa aaltofunktion neliöintegraalia (tilannetta voidaan verrata ylinumeroituvaan kantaan, josta $\psi(x) = \langle x|\psi\rangle$).

Monen kubitin systeemiä merkitään $|\psi\rangle = |\psi_1\psi_2...\rangle$, missä ψ_1, ψ_2... ovat kubitit järjestyksessä. Kahden kubitin tapausessa vektori on $|\psi_1\psi_2\rangle$. Tällöin mahdolliset tilat ovat 00, 01, 10 ja 11. Näille tiloille käytetään merkintätapaa $|00\rangle$, $|01\rangle$, $|10\rangle$ ja $|11\rangle$ [2] ja vahden kubitin tilavektori voidaan kirjoittaa $|\psi\rangle = \alpha_{00}\,|00\rangle + \alpha_{01}\,|01\rangle + \alpha_{10}\,|10\rangle + \alpha_{11}\,|11\rangle$, missä etukertoimien neliöt kertovat todennäköisyyden mitata kyseisen tilan.

2.2 Matriisit

Diracin bra-ket-notaatiossa tilan $|\psi\rangle$ muutosta kuvataan matriiseilla. Kvanttilaskennassa muutosta kuvaavan matriisin riittää toteuttaa yksi ehto: matriisin U on oltava unitaarinen [1, 2]. Unitaarinen matriisi U on neliömatriisi, jonka Hermiten transpoosi on itse matriisin käänteismatriisi. Matemaattisesti ehto on

$$U^{\dagger}U = UU^{\dagger} = I, \tag{6}$$

jossa I on yksikkömatriisi.

Unitaarisella matriisilla on tärkeä ominaisuus: se säilyttää normalisaation (ts. vektorin pituus säilyy).
Todistus: Oletetaan, että vektori $|\psi\rangle$ muuttuu unitaarisella matriisilla U vektoriksi $|\psi'\rangle$, eli $|\psi'\rangle = U|\psi\rangle$. Tällöin

$$\begin{aligned}\langle\psi|\psi\rangle = \langle\psi| I |\psi\rangle = \langle\psi| U^\dagger U |\psi\rangle = (\langle\psi| U^\dagger) U |\psi\rangle = (U|\psi\rangle)^\dagger U |\psi\rangle \\ = (|\psi'\rangle)^\dagger |\psi'\rangle = \langle\psi'|\psi'\rangle .\end{aligned}$$

Tärkeimpiä matriiseja kvanttilaskennassa ovat Hadamardin matriisi H sekä Paulin matriisit σ_x, σ_y ja σ_z [1, 2]:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{7a}$$

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{7b}$$

$$\sigma_y = \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \tag{7c}$$

$$\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{7d}$$

Todistetaan seuraavaksi, että nämä matriisit ovat myös unitaarisia. Selvästi nähdään, että näille matriiseille pätee $U = U^\dagger$. Nyt on vain osoitettava, että $UU^\dagger = U^2 = I$. Saadaan

$$\begin{aligned}H^2 &= \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \\ \sigma_x^2 &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \\ \sigma_y^2 &= \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \\ \sigma_z^2 &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I.\end{aligned}$$

Määritellään seuraavaksi ulkotulo: matriisi Π on ulkotulo, jos se voidaan esittää vektorin $|\psi\rangle$ avulla, $\Pi = |\psi\rangle\langle\psi|$. Π ei kuitenkaan ole unitaarinen, sillä

$$\Pi \cdot \Pi^\dagger = |\psi\rangle\langle\psi| \cdot (|\psi\rangle\langle\psi|)^\dagger = |\psi\rangle\langle\psi|\psi\rangle\langle\psi| = |\psi\rangle\langle\psi| = \Pi.$$

Tästä nähdään, että $\Pi^\dagger = \Pi$ (Π on hermiittinen) ja $\Pi^n = \Pi, n \in \mathbb{N}$. Ulkotuloa sanotaan usein projektioksi, koska sillä operoitu vektori $|\phi\rangle$ antaa projektion ulkotulon vektorin $|\psi\rangle$ suuntaan

$$\Pi|\phi\rangle = |\psi\rangle\langle\psi|\phi\rangle = a|\psi\rangle .$$

3 Groverin algoritmi: johto

Alustetaan Groverin algoritmia varten n kubittia tilaan $|0\rangle$. Kubitit saatetaan superpositioon kaikista mahdollisista tiloista operoimalla jokaista kubittia erikseen Hadamardin matriisilla H. Merkitään tällaista operaatiota operoimalla H_n suoraan tilaan $|0...0\rangle$, jolloin saadaan

$$|\psi\rangle = H\,|0...0\rangle = \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |x_i\rangle\,, \tag{8}$$

missä x_i:t ovat erilaisten bittiyhdistelmien tilavektorit ja $N = 2^n$ on mahdollisten tilojen määrä. Tällöin mahdollisuus mitata mikä tahansa tila on $1/N$. Lisäksi merkitään oikeaa vastausta tilavektorilla $|a\rangle$, joka on jokin N:stä mahdollisesta tilasta [1, 2].

Groverin algoritmi koostuu kahdesta kvanttiportista, joita esitetään matriiseilla. Näitä portteja operoimalla tilavektoriin $|\psi\rangle$ vuorotellen päästään hyvin lähelle tilaa $|a\rangle$, joka saadaan mitattua suurella todennäköisyydellä. Lisäksi algoritmiin kuluvien iteraatioiden määrä kasvaa verrannollisesti $\sqrt{N}$ (merkitään $\mathcal{O}(\sqrt{N})$, Big-O-notaatio), mikä on parannus klassiseen verrannollisuuteen $\mathcal{O}(N)$.

3.1 Oraakkeli

Oletetaan, että meillä on "oraakkeli", joka kertoo, olemmeko löytäneet oikean vastauksen [1, 2]. Oraakkeli voi olla esimerkiksi funktio, joka vertaa tulosta haluttuun tulokseen. Kvanttitietokoneessa oraakkeli on kvanttiportti, joka merkkaa oikean vastauksen.

Määrittelemme oraakkelimatriisin O, joka palauttaa väärän tilavektorin sellaisenaan, mutta palauttaa oikean tilavektorin tapauksessa tilavektorin kerrottuna luvulla -1. Matriisi on siten määritelty

$$O = I - 2\,|a\rangle\,\langle a|\,, \tag{9}$$

missä $\langle a|$ ja $|a\rangle$ ovat oikean vastauksen bra- ja ket-vektorit ja I on yksikkömatriisi. Oraakkelin on kvanttiporttina oltava unitaarinen ja hermiittinen:

$$O^\dagger = (I - 2\,|a\rangle\,\langle a|)^\dagger = I^\dagger - (2\,|a\rangle\,\langle a|)^\dagger = I - 2\,|a\rangle\,\langle a| = O$$

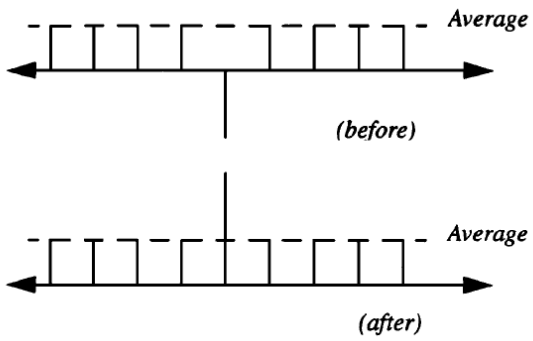
$$\begin{aligned} O^\dagger O = O^2 &= (I - 2\,|a\rangle\,\langle a|)(I - 2\,|a\rangle\,\langle a|) = I^2 - 4I\,|a\rangle\,\langle a| + 4\,|a\rangle\,\langle a|a\rangle\,\langle a| \\ &= I - 4\,|a\rangle\,\langle a| + 4\,|a\rangle\,\langle a| = I + 0 = I. \end{aligned}$$

Jos oraakkelilla operoidaan sattumanvaraiseen kantavektoriin $|x\rangle$, saadaan selville, onko kantavektori haluttu vastaus (ts. onko bittiyhdistelmä ratkaisu ongelmaamme)

$$O|x\rangle = \begin{cases} |x\rangle & \text{jos } x \neq a \\ -|a\rangle & \text{jos } x = a. \end{cases}$$

3.2 Ehdollinen vaihesiirto

Oraakkelin operoinnin jälkeen meillä on tila, jossa $|a\rangle$:n vaihe on vaihtunut. Muuttaaksemme todennäköisyyksiä hyödyllisempään suuntaan käännämme tilavektoria sen keskiarvon suhteen. Tämä tarkoittaa, että jokainen tilan vaihetermi (etutekijä α) muuttuu. Muutoksen suuruus on kaikkien tilojen vaihetermien keskiarvon erotus kuhunkin vaihetermiin. Käytännössä tämä tarkoittaa, että jokaisen väärän tilan vaihetermi pienenee ja $|a\rangle$:n vaihetermi kasvaa, tarkemmin sanottuna kaksinkertaistuu.



Kuva 1: Groverin esitys ehdollisesta vaihesiirrosta, lähde: viite [3]

Kuvassa 1 on esitetty vaihesiirron vaikutus tilojen vaiheisiin. Huomattavaa on, että oikean tilan ($|a\rangle$) vaihe on alussa ainoana negatiivinen. Vaihesiirron jälkeen nähdään, että väärien tilojen vaiheet pienenevät vähän ja $|a\rangle$:n vaihe kasvaa, kuten oli tarkoitus.

Tällaista kvanttiporttia nimitetään ehdolliseksi vaihesiirroksi ja sitä merkitään matriisilla W [1, 2]. W:lle saadaan kaava

$$W = 2|\psi\rangle\langle\psi| - I, \tag{10}$$

jossa $\langle\psi|$ ja $|\psi\rangle$ ovat alkuperäisen kaavan (8) tilavektorin bra- ja ket-vektorit ja I on yksikkömatriisi. Myös W:n tulee olla unitaarinen (lisäksi W on hermiittinen).

$$W^\dagger = (2\,|\psi\rangle\,\langle\psi| - I)^\dagger = (2\,|\psi\rangle\,\langle\psi|)^\dagger - I^\dagger = 2\,|\psi\rangle\,\langle\psi| - I = W$$

$$W^\dagger W = W^2 = (2\,|\psi\rangle\,\langle\psi| - I)(2\,|\psi\rangle\,\langle\psi| - I) = 4\,|\psi\rangle\,\langle\psi|\psi\rangle\,\langle\psi| - 4\,|\psi\rangle\,\langle\psi|\,I + I^2$$
$$= 4\,|\psi\rangle\,\langle\psi| - 4\,|\psi\rangle\,\langle\psi| + I = 0 + I = I.$$

Näin määritettyjen matriisien avulla saadaan Groverin iteraattori G

$$G = WO, \tag{11}$$

jota käyttämällä voidaan kompaktisti esittää Groverin algoritmi:

$$G^k\,|\psi\rangle = \frac{1}{\sqrt{N}} G^k \sum_{i=1}^{N} |x_i\rangle \approx |a\rangle\,, \tag{12}$$

missä k on verrannollinen $\sqrt{N}$:ään.

3.3 Geometrinen tulkinta

Koska käsittelemme vektoreita, voimme katsoa, miten Groverin algoritmi käyttäytyy geometrisesti. Tulkitaan $\langle a|\psi\rangle\ |a\rangle$:n ja $|\psi\rangle$:n väliseksi pistetuloksi, jolloin $\langle a|\psi\rangle = |a||\psi|\cos\theta = \cos\theta$, missä θ on kulma $|a\rangle$:n ja $|\psi\rangle$:n välillä. Toisaalta $\langle a|\psi\rangle = 1/\sqrt{N}$, josta saadaan $\cos\theta = 1/\sqrt{N}$ [1].

Koska $|\psi\rangle$ lähestyy $|a\rangle$:a, θ pienenee. Vastaavasti θ:n komplementtikulma $\gamma = \pi/2 - \theta$ kasvaa. Tällöin $\cos\theta = \sin\gamma$. Kuvassa 2 on esitetty kulma γ tasossa, jonka akseleina ovat $|a\rangle$ ja $|a\rangle$:n vastainen vektori $|a\rangle_\perp$. Lisäksi kuvassa on tilavektori $|\psi\rangle$.

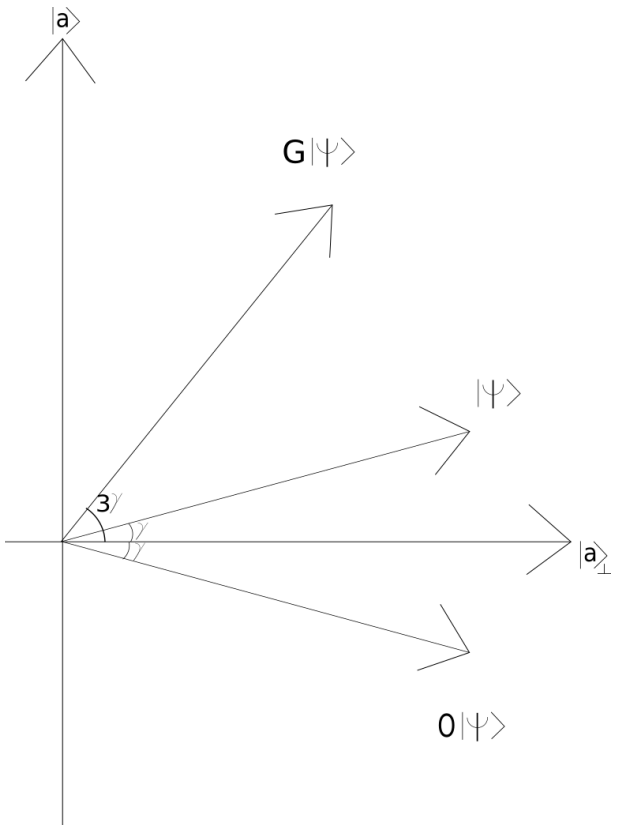
Groverin iteraattori voidaan nyt osoittaa olevan kääntömatriisi 2γ:n suhteen, jos valitaan kannaksi $|\psi\rangle = \alpha\,|a\rangle + \beta\,|b\rangle$, missä $|b\rangle$ on väärä vastaus (kaikkien väärien vastausten superpositio). Kuvassa 2 $|b\rangle$ on $|a\rangle_\perp$. Lasketaan ensiksi Groverin iteraattori matriisimuotoon tässä kannassa

$$G = WO = (2\,|\psi\rangle\,\langle\psi| - I)(I - 2\,|a\rangle\,\langle a|) = 2\,|\psi\rangle\,\langle\psi| - I - 4\alpha\,|a\rangle\,\langle\psi| + 2\,|a\rangle\,\langle a|$$
$$= 2\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} - \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} - 4\alpha\begin{pmatrix}\alpha & 0\\ 0 & \beta\end{pmatrix} + 2\begin{pmatrix}\alpha & \beta\\ 0 & 0\end{pmatrix} = \begin{pmatrix}1 - 2\alpha^2 & -2\alpha\beta\\ 2\alpha\beta & 2\beta^2 - 1\end{pmatrix}.$$

Koska $\langle\psi|\psi\rangle = \alpha^2 + \beta^2$, saadaan $\langle a|\psi\rangle = \alpha = \sin\gamma$ ja $\beta = \cos\gamma$. Tällöin

$$G = \begin{pmatrix} 1 - 2\sin^2\gamma & -2\sin\gamma\cos\gamma \\ 2\sin\gamma\cos\gamma & 2\cos^2\gamma - 1 \end{pmatrix} = \begin{pmatrix} \cos 2\gamma & -\sin 2\gamma \\ \sin 2\gamma & \cos 2\gamma \end{pmatrix}$$

on erikoistapaus kääntömatriisista, kun kulmana on 2γ. Kuvasta 2 nähdään Groverin iteraattorin nähdään kääntävän $|\psi\rangle$ vastapäivään 2γ:n verran. Kuvasta nähdään myös, että oraakkeli peilaa tilavektoria $|a\rangle_\perp$:n suhteen ja ehdollinen vaihesiirto peilaa näin saatua vektoria alkuperäisen tilaverktorin $|\psi\rangle$ suhteen.



Kuva 2: Groverin algoritmin geometrinen tulkinta

Suurilla N:n arvoilla voidaan hyvin approksomoida $1/\sqrt{N} = \cos\theta = \sin\gamma \approx \gamma$ eli $\gamma \approx 1/\sqrt{N}$. Kun käytetään Groverin algoritmia k:n kertaa, saadaan kulmaksi $k \cdot 2\gamma$, joka on lähellä arvoa $\pi/2$. Tällöin $G^k|\psi\rangle$ on lähinnä vektoria $|a\rangle$. Tästä voidaan approksimoida k:lle arvo $k \approx \frac{\pi}{2\cdot 2\gamma} = \frac{\pi}{4}\sqrt{N}$, josta nähdään, että Groverin algoritmi on $\mathcal{O}(\sqrt{N})$ [1, 2].

3.4 Esimerkki: 2 kubittia

Lasketaan Groverin algoritmi kahdelle kubitille, jolloin $n = 2$. Tällöin $N = 2^2 = 4$ ja Groverin algoritmia tarvitsee käyttää kerran. Nyt tilavektoriksi saadaan

$$|\psi\rangle = \frac{1}{\sqrt{4}} \sum_{i=1}^{4} |x_i\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle).$$

Valitaan $|a\rangle = |00\rangle$, jolloin $\langle\psi|a\rangle = 1/2$. Operoidaan $|\psi\rangle$:tä Groverin iteraattorilla, jolloin

$$\begin{aligned} G|\psi\rangle &= WO|\psi\rangle = W(I - 2|00\rangle\langle 00|)|\psi\rangle = W(|\psi\rangle - 2|00\rangle\langle 00|\psi\rangle) \\ &= W(|\psi\rangle - |00\rangle) = (2|\psi\rangle\langle\psi| - I)(|\psi\rangle - |00\rangle) \\ &= 2|\psi\rangle\langle\psi|\psi\rangle - 2|\psi\rangle\langle\psi|00\rangle - |\psi\rangle + |00\rangle = 2|\psi\rangle - |\psi\rangle - |\psi\rangle + |00\rangle \\ &= |00\rangle . \end{aligned}$$

Saadaan, että kahden kubitin tapauksessa löydämme vastauksen jo ensimmäisellä iteraatiokerralla. Tämä on parannus klassiseen etsintäalgoritmiin, jossa iteraatioita tarvitaan keskimäärin 2, pahimmassa tapauksessa jopa 3.

3.5 Groverin algoritmin funktiot f_n ja g_n

Yleisessä tapauksessa keskellä Groverin algoritmin suorittamista olemme tilanteessa, jossa on suoritettu $n < k$ iteraatiota. Tällöin olemme operoineet alkuperäistä tilaa $|\psi\rangle$ n kertaa ja saaneet kaavan (12) mukaan $G^n|\psi\rangle = f_n(A)|\psi\rangle + g_n(A)|a\rangle$, jossa $A = 1/\sqrt{N}$.

Tästä voidaan lukea funktion $f_n(A)$ neliön antavan todennäköisyyden mitata mikä tahansa tila (erityisesti mikä tahansa väärä tila). Vastaavasti g_n vastaa todennäköisyyttä mitata haluttu tila, kun on Groverin algoritmia on iteroitu n kertaa. On kuitenkin huomattava, että f_n sisältää osan $|a\rangle$:n mittaustodennäköisyydestä.

Selvästi $f_0(A) = 1$ ja $g_0(A) = 0$. Muiden iteraatioiden funktiot saadaan

$$\begin{aligned} G^{n+1} &= GG^n|\psi\rangle = G(f_n(A)|\psi\rangle + g_n(A)|a\rangle) = WO(f_n(A)|\psi\rangle + g_n(A)|a\rangle) \\ &= W(I - 2|a\rangle\langle a|)(f_n(A)|\psi\rangle + g_n(A)|a\rangle) \\ &= W((f_n(A)|\psi\rangle + g_n(A)|a\rangle - 2Af_n(A)|a\rangle - 2g_n(A)|a\rangle) \\ &= (2|\psi\rangle\langle\psi| - I)(f_n(A)|\psi\rangle - |a\rangle(2Af_n(A) + g_n(A))) \\ &= 2f_n(A)|\psi\rangle - 2A(2Af_n(A) + g_n(A))|\psi\rangle - f_n(A)|\psi\rangle + (2Af_n(A) + g_n(A))|a\rangle \\ &= [f_n(A) - 4A^2 f_n(A) - 2Ag_n(A)]|\psi\rangle + [2Af_n(A) + g_n(A)]|a\rangle \\ &= f_{n+1}(A)|\psi\rangle + g_{n+1}(A)|a\rangle , \end{aligned}$$

	$f_n(A)$	$g_n(A)$
0	1	0
1	$1-4A^2$	$2A$
2	$1-12A^2+16A^4$	$4A-8A^3$
3	$1-24A^2+80A^4-64A^6$	$6A-32A^3+32A^5$

Taulukko 1: Groverin algoritmin funktiot

josta voidaan lukea

$$f_{n+1}(A) = f_n(A) - 4A^2 f_n(A) - 2A g_n(A) \tag{13a}$$
$$g_{n+1}(A) = 2A f_n(A) + g_n(A). \tag{13b}$$

Taulukossa 1 on esitetty muutamia ensimmäisiä $f_n(A)$:n ja $g_n(A)$:n funktioita.

Funktion $f_n(A)$ positiivisten nollakohtien avulla saadaan selville, minkä suuruisten kubittien joukoille saadaan tulos, jossa mahdollisuus mitata $|a\rangle$ olisi 100%. Esimerkiksi

$$f_1(A) = 0 \iff 1 - 4A^2 = 0 \iff A^2 = 1/4$$
$$N = 2^n \iff n = \log_2 N = \log_2 1/A^2 = \log_2 4 = 2$$

saadaan, että 2 kubitin systeemi saa 1 iteraation jälkeen varmasti tuloksen $|a\rangle$. Tätä tulosta ei voida johtaa koskemaan tapausta $g_n(A) = 1$, koska $|\psi\rangle$ sisältää osan $|a\rangle$:n mittaustodennäköisyydestä (kuitenkin $g_n(A) = 1$ toteutuu, jos $f_n(A) = 0$). Jos halutaan saada $|a\rangle$:n mittaustodennäköisyys, on laskettava $|a\rangle$:n etutekijä kokonaisuudessaan.

Lasketaan seuraavaksi etutekijät kaikille tilavektorin termeille

$$|\psi\rangle = A\sum_{i=1}^{N} |x_i\rangle = A\,|a\rangle + A\sum_{\substack{i \\ x_i \neq a}}^{N} |x_i\rangle$$

Groverin algoritmin n:n iteraation jälkeen saadaan

$$\begin{aligned} f_n(A)\,|\psi\rangle + g_n(A)\,|a\rangle &= f_n(A)(A\,|a\rangle + A\sum_{\substack{i \\ x_i \neq a}}^{N} |x_i\rangle) + g_n(A)\,|a\rangle \\ &= (Af_n(A) + g_n(A))\,|a\rangle + Af_n(A)\sum_{\substack{i \\ x_i \neq a}}^{N} |x_i\rangle\,, \end{aligned}$$

mistä nähdään, että

$$p_n(A) = (Af_n(A) + g_n(A))^2 \tag{14}$$

antaa todennäköisyyden mitata $|a\rangle$. Esimerkiksi $n = 4$ kubittia saadaan 2 iteraatiolla $p_2(1/4) = 0.908447$, eli todennäköisyys mitata tila $|a\rangle$ on 90,8%. Toisaalta 3 iteraatiolla $p_3(1/4) = 0.961319$ saadaan 96,1% todennäköisyys mitata oikea tila. Tämä tulos vastaa approksimaatiota $k \approx \frac{\pi}{4}\sqrt{N} = \pi \approx 3$. Näin ollen näiden todennäköisyyksien avulla voimme päätellä, kuinka monta iteraatiota Groverin algoritmi tarvitsee onnistuakseen suurimalla todennäköisyydellä.

4 Groverin algoritmi käytännössä

Kvanttitietokone rakennettaisiin käytännössä kokoelmaksi hiukkasia, joilla on kaksi mitattavaa tilaa, esimerkiksi elektroneja [4]. Muita mahdollisia rakenneosia olisivat fotonit ja muut spinin omaavat hiukkaset, kuten atomiytimet ja kvanttipisteet. Nykyiset kvanttitietokoneet on rakennettu fotoneista eli valohiukkasista. Tällaisia hiukkasia ohjaillaan magneettikentillä ja mikroaalloilla. Kvanttitietokoneisiin liittyviä tutkimuksia on onnistuttu toteuttamaan käytännössä, vaikka suurin osa tutkimuksista on silti vasta teoreettista. Kuitenkin Groverin algoritmia on jo onnistuttu käyttämään kahden [5] ja kolmen [6] kubitin systeemeissä.

L. DiCarlo tutkimusryhmineen julkaisivat artikkelin [5], jossa he esittävät kahden kubitin kvanttitietokoneen suprajohtavan piirin avulla. Vaikka koe kärsikin suuresta systemaattisesta virheestä, tutkimusryhmän tulosksista selviää, että heidän mittauksessa Groverin algoritmista vaikuttaa onnistuneelta. Tulosten perusteella Groverin algoritmi pääsi oikeaan tulokseen yli 80% todennäköisyydellä. Lisäksi väärien tulosten mittaustodennäköisyydet olivat lähes yhtä suuria. Näiden tulosten perusteella Groverin algoritmin toteutus onnistui tutkimusryhmän mielestä.

Toisen tutkimuksen Groverin algomitmista toteutti C. Figgatt tutkimusryhmineen, josta hän kertoo artikkelissa [6]. Tutkimuksessa kvanttitietokone kehitettiin viidestä vangitusta ytterium-ionista, jotka laserjäähdytettiin lähelle perustilaansa. Kvanttitietokonetta hyödynnettiin käyttämään Groverin algoritmia kolmelle kubitille. Groverin algoritmi toteutettiin yhdellä iteraatiolla kaikille mahdollisille tilakombinaatioille, joissa oli yksi tai kaksi oikeaa vastausta. Ideaalisesti Groverin algomitmi ratkaisisi tällaiset tapaukset $78,125\%$ todennäköisyydellä 1 vastaukselle ja 100% todennäköisyydellä 2 vastaukselle.

Figgatt tutki lisäksi kahta vaihtoehtoista oraakkelia, joista ensimmäinen oli vaihesiirtoon perustuva oraakkeli (kaava 9). Toinen oraakkeli oli "boolean'-'oraakkeli, jolle rakennetaan rinnalle ylimääräinen kubitti alustettuna tilaan $|1\rangle$. Tämän oraakkelikubitin vaihetta tarkkaillaan ja käännetään, jos ja vain jos tarkasteltava

datakubitti on oikea vastaus. Tällöin oraakkelikubitti tuottaa vaihe-kickbackin, jolloin itse datakubitin vaihe muuttuu. Figgatt väittää näin rakennetun oraakkelin olevan enemmän klassista etsintäalgoritmia vastaava. Lisäksi kummankin oraakkelin tulisi olla klassista vastinettaan parempi.

Mittaustuloksia Figgatt raportoi onnistumistodennäköisyyksinä ja mittaustulosten hyvyyttä suhteessa teoreettiseen ideaaliin mittaamaan hän valitsi squared statistical overlap -metodin (sso). Yhden oikean vastauksen tapausessa "boolean"-oraakkeli sai oikean tuloksen $38,9(4)\%$ mittauksista (sso $83,2(7)\%$) ja vaiheoraakkeli $43,7(2)\%$ mittauksista (sso $84,9(4)\%$). Mittaustulosten ero johtuu Figgatt:n mielestä vaiheoraakkelin pienemmästä resurssimäärästä, joka nostaa onnistumistodennäköisyyttä. Lisäksi tuloksia voi verrata klassiseen onnistumistodennäköisyyteen 25%.

Kahden oikean vastauksen tapauksessa "boolean" oraakkeli sai oikean tuloksen $67,9(2)\%$ mittauksista (sso $67,6(2)\%$) ja vaiheoraakkeli $75,3(2)\%$ mittauksista (sso $74,4(2)\%$). Tulosten eroa Figgatt kommentoi vastaavasti vaiheoraakkelin pienemmän resurssimäärän ansioksi. Lopuksi Figgatt pohtii Groverin algoritmin käyttökohdetta aliohjelmana (subroutine) muille etsintäalgoritmeille.

5 Teoreettisia tutkimustuloksia

Kokeellisten tutkimustulosten rinnalla Grovein algoritmia käsitellään myös teoreettiselta pohjalta. Yhtenä suurimmista aiheista näissä tutkimuksissa on lomittumisen (entanglement) merkitys kvanttialgoritmeissa. Groverin algoritmi hyödyntää lomittumista onnistuakseen, paitsi jos tiloja käsitellään yhden atomin avulla [7]. Lomittuneessa tilassa tarkastellaan useaa kubittia, jotka ovat keskenään superpositiossa. Esimerkiksi tila $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ on lomittunut. Lomittunut tila voidaan mitata mittaamatta kaikkia kubitteja. Esimerkiksi yllä mainittu tila saadaan selville mittaamalla vain ensimmäinen kubitti. Kuitenkaan lomittuminen ei ole oleellinen osa Groverin algoritmia, vaan vain sivuseuraus siitä [8].

E. Fahri ja S. Gutmann kirjoitta artikkelissaan [4] Groverin algoritmin kaltaisesta menetelmästä, jossa kvanttimekaanisen systeemin tilat vastaisivat Groverin algoritmin kubitteja. Tällaisessa tilanteessa Schrödingerin yhtälö tuottaisi oikeaa kubittikombinaatiota vastaavan tilan. Fahrin menetelmä käyttäytyy $\mathcal{O}(\sqrt{N})$ ja lisäksi on optimaalinen, jos kanta on tiedetty ja ortonormaalinen.

Jatkoa Fahrin esitykselle [4] tarjoaa J. Roland ja N. J. Cerf artikkelissaan [9] adiabaattisuuden näkökulmasta. Fahrin mukaan tila muuttuu oikeaan vastaukseen

itsestään, jonkin potentiaalin (Hamintonin) ajamana. Rolandin esittää tällaisen tilanteen tapahtuvan, jos systeemissä vallitsee lokaali adiabaattisuus. Näin ollen voidaan systeemin Hamiltoniin vaikuttaa siten, että lokaali adiabaattisuus säilyy. Tällaisen tapauksen Roland kuvaa seuraavasti: rakennetaan ensin jokin helppo Hamilton ja muutetaan sitä hitaasti sellaiseen Hamiltoniin, jonka tiedetään ratkaisevan ongelma. Kuitenkin muutosnopeus tulee riippumaan systeemin kulusta. Roland toteaa vielä lopuksi, että jos on olemassa M oikeaa ratkaisua ongelmalle, Groverin algoritmissa esiintyvät N:t korvataan N/M:llä.

Fahrin tulokseen [4] viitaten S. Lloyd kirjoittaa artikkelissaan [8], kuinka Groverin algoritmi ei tarvitsisikaan lomittumista onnistuakseen vastoin aiempaa tietämystä. Lloydin mukaan superpositio on syynä Groverin algoritmin onnistuneisuudelle. Ilman lomitusta toteutettava Groverin algoritmi kasvattaisi kuitenkin tarvitsemaansa muistitilaa. Tämän seurauksena algoritmi ei ole kuitentaan yhtä tehokas kuin lomitusta hyödyntävä Groverin algoritmi, mutta se olisi silti parannus klassiselle vastineelleen. Lisäksi Groverin algoritmi on optimaalinen kubiteille. Lloydin mukaan superposition perimmäinen ajatus juontaa juurensa aaltoluonteeseen ja huomauttaa, että jopa klassiset aallot pystyisivät ratkaisemaan käsittelemämme etsintäongelman $\mathcal{O}(\sqrt{N})$-verrannollisesti.

Lomituksesta käytävää keskustelua jatkaa D. A. Meyer artikkelissaan [7]. Meyerin mukaan superpositiota käytettäessä ei tarvittaisi lomitusta. Lloydiin [8] viitaten hän toteaa superposition klassisista tiloista muodostavan kannan Hilbertin avaruudelle, jonka elementit ovat kvanttitietokoneen tiloja. Yksinkertaisin esitys tästä olisi kubitti, jonka Hilbertin avaruus on yksiulotteinen. Lisäksi Meyer toteaa Lloydin artikkelista, että lomitus katoaa, jos kaikki N tilaa ovat yhden hiukkasen tiloja eivätkä n:n hiukkasen tiloja (siis n:n hiukkasen tilat $|0\rangle$ tai $|1\rangle$). Näin ollen n:n kubitin tilaa voidaan katsoa isomorfisesti N:nä yhden hiukkasen tilana. Tällöin lomituksen määritelmän mukaan se katoaa.

Kuitenkin Meyer huomauttaa, että (koska kaikki fyysiset resurssin hyödynnetään jollain tavoin) muut systeemin käyttämät resurssit kasvavat eksponenttiaalisesti. Mutta on myös väärin olettaa, että kvanttialgoritmi (ja siten myös kvanttitietokone) vaatisi lomituksen tai eksponentiaaliset resurssit. Meyer pohtii lopuksi erilaisen tietokannan hyödyntämistä: oraakkelin oikea/väärä -vastauksen sijaan saadaan tieto, kuinka lähellä oikeaa vastausta ollaan. Tästä Meyer esittää Bernsteinin ja Vaziranin algoritmin, joka on $\mathcal{O}(1)$. Groverin algoritmiin rinnastaen tämäkin voitaisiin tehdä ilman lomitusta, mutta se olisi tarpeetonta, sillä tämä algoritmi ei hyödynnä lomitusta ollenkaan.

Bernsteinin ja Vaziranin algoritmin toteutus ilman lomitusta on Meyerin aikaisemman huomautuksen mukainen: tässä tilanteessa muut resurssit kasvavat. Tämä puolestaan näkyisi esimerkiksi energiassa tai mittaustarkkuudessa. Kaiken kaikkiaan Meyer päättelee, että lomitusta ei tarvita saamaan kvnattitietokonetta

klassista tietokonetta nopeammaksi. Kvanttimekaanisesta aaltoluonteesta johtuva interferenssi yksinään riittäisi tällaiseen. Erityisesti Bernsteinin ja Vaziranin algoritmi demostroi aaltoluonteen ja ortogonalisuuden merkitytä kvanttialgoritmeissa lomittumisen sijaan.

Kokeellista Groverin algorimin toteutusta hahmottavat M. N. Leuenberger ja D. Loss molekyylien magneeteilla artikkelissaan [10]. Leuenberger toteaa myös Groverin algoritmin tarvitsevan pelkästään superposition ja vertaa tätä Shorin algoritmiin, joka puolestaan tarvitsee lomituksen. Kvanttitietokoneen muistia Leuenberger hahmottelee kiderakenteeksi, joka toimisi keskusmuistina. Täältä luku tapahtuisi resonanttipulsseilla elektronien spineistä ajassa 10^{-10} s. Leuenbergerin ehdottaa, että tällainen kvanttitietokone voitaisiin rakentaa rauta- tai mangaaniatomeista. Kuitenkin ongelmaksi koituisivat tilat, joiden spin $> 1/2$. Lopuksi Leuenberger toteaa, että tällainen systeemi voitaisiin rakentaa lähes kaikkiin spinin omaaviin systeemeihin, joissa energiatilojen erot eroavat toisistaan (eli $|E_j - E_i|$ on uniikki kaikille uniikeille pareille i, j).

6 Loppupäätelmät

Groverin algoritmia käsiteltiin teoreettisesti ja huomattiin sen olevan klassista etsintäalgoritmia nopeampi. Lisäksi johdettiin kaava todennäköisyydelle saada oikea tulos Groverin algoritmista. Lopuksi käsiteltiin kvanttitietokoneisiin ja Groverin algoritmiin liittyviä tutkimustuloksia.

Groverin algoritmi nopeuttaisi klassisesti hidasta hakua järjestämättömästä tietokannasta. Lisäksi algoritmi ei käytä paljon resursseja tai lomittumista, joten se olisi hyvä toteuttaa kvanttitietokoneen pohjalle etsintäalgoritmiksi. Kuitenkin suurin osa tietokannoista on järjestettyjä ja tällöin klassiset etsintäalgoritmit $\mathcal{O}(\log N)$ voittavat Groverin algoritmin $\mathcal{O}(\sqrt{N})$. Kuitenkin Groverin algoritmin avulla voitaisiin rakentaa muita etsintäalgoritmeja, jotka olisivat klassisia vastineitaan parempia. Esimerkkinä muista algoritmeista mainittakoon Bernsteinin ja Vaziranin algoritmi [7], joka olisi kaikista nopein $\mathcal{O}(1)$.

Viitteet

[1] N. David Mermin. *Quantum computer science: An introduction*. Cambridge University Press, 2007.

[2] M. A. Nielsen and I. L. Chuang. *Quantum computation and quantum information*. Cambridge University Press, 2000.

[3] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, 1997.

[4] E. Farhi and S. Gutmann. Analog analogue of a digital quantum computation. *Physical Review A - Atomic, Molecular, and Optical Physics*, 57(4):2403–2406, 1998.

[5] L. DiCarlo, J. M. Chow, J. M. Gambetta, Lev S. Bishop, B. R. Johnson, D. I. Schuster, J. Majer, A. Blais, L. Frunzio, S. M. Girvin, and R. J. Schoelkopf. Demonstration of two-qubit algorithms with a superconducting quantum processor. *Nature*, 460(7252):240–244, 2009.

[6] C. Figgatt, D. Maslov, K. A. Landsman, N. M. Linke, S. Debnath and C. Monroe. Complete 3-qubit grover search on a programmable quantum computer. *Nature Communications*, 8, 2017.

[7] D. A. Meyer. Sophisticated quantum search without entanglement. *Physical Review Letters*, 85(9):2014–2017, 2000.

[8] S. Lloyd. Quantum search without entanglement. *Physical Review A - Atomic, Molecular, and Optical Physics*, 61(1):103011–103014, 2000.

[9] J. Roland and N.J. Cerf. Quantum search by local adiabatic evolution. *Physical Review A. Atomic, Molecular, and Optical Physics*, 65(4 A):423081–423086, 2002.

[10] M. N. Leuenberger and D. Loss. Quantum computing in molecular magnets. *Nature*, 410(6830):789–793, 2001.