KVANTEVANDRINGER

THOMAS WILSKOW THORBJØRNSEN

3. august 2021

INNHOLD

FIGURER

TABELLER

ABSTRAKT

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu

libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

1 INTRODUKSJON

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

2 KVANTEBEREGNINGER

2.1 Postulatene i kvantemekanikk

Kvantemekanikk er en beskrivelse av fysiske systemer på små størrelser. Reglene for hvordan disse systemene oppfører seg er formulert utifra 6 postulater. [1] og [2] definerer postulatene som følger

1. På hvert øyeblikk er tilstanden til det fysiske systemet beskrevet av en ket $|\psi\rangle$ i rommet av tilstander.

2. Enhver observabel fysisk egenskap av systemet er beskrevet av en operator som virker på ketten som beskriver systemet.

3. De eneste mulige resultatene av en måling av en observabel $\mathcal{A}$ er egenverdiene til den assosierte operatoren A.

4. Når en måling er gjort på en tilstand $|\psi\rangle$ er sannsynligheten for å få en egenverdi a_n gitt ved kvadratet av indreproduktet til $|\psi\rangle$ sammen med egenprojeksjonen P_{a_n}.

$$p_{a_n} = \langle\psi|P_{a_n}|\psi\rangle$$

5. Umiddelbart etter en måling av en observabel $\mathcal{A}$ har gitt egenverdien a_n, er systemet i tilstanden til den normaliserte egenprojeksjonen $P_{a_n}|\psi\rangle$.

6. Tidsutviklingen til et system bevarer normen til en ket $|\psi\rangle$.

For å forklare postulatene sammen med et eksempel antar vi at det finnes en partikkel som har to observable tilstander, vi kaller de spin opp og spin ned, som er beskrevet av vektorer i et rom av tilstander. Her tolkes rommet av tilstander som et (kompleks separabelt) Hilbertrom. En tilstand eller ket $|\psi\rangle$ er dermed en vektor i $\mathcal{H}$. Siden $\mathcal{H}$ er et Hilbertrom har den også en basis $\{|\beta_\lambda\rangle \mid \lambda : \Lambda\}$, hvor Λ er en indeksmengde. Ettersom vi har to observable tilstander holder det å anta at $\mathcal{H} = \mathbb{C}^2$ og at $|\beta_i\rangle = e_i$ for $i = 1, 2$. Man kan skrive $|\psi\rangle$ som en lineærkombinasjon av basisen,

dette er også kalt for en superposisjon av tilstandene $\{|\beta_\lambda\rangle \mid \lambda : \Lambda\}$ (eller $\{e_1, e_2\}$ for spin eksemplet).

$$|\psi\rangle = \Sigma\psi_i|\beta_i\rangle$$
$$(|\psi\rangle = \psi_1 e_1 + \psi_2 e_2)$$

Gitt at vi har en observable $\mathcal{A}$, altså en fysisk egenskap ved systemet som kan måles, så vet vi at dette er gitt ved en lineærtransformasjon A som virker på Hilbertrommet $\mathcal{H}$. De fysiske målingene til systemet skal være gitt ved egenverdiene av denne lineærtransformasjonen, noe som krever den til å være en endomorfi, aka. $A : \mathcal{H} \to \mathcal{H}$. I spin eksemplet kan man måle spin opp og spin ned med en observable hvor f.eks. spin opp har egenverdien 1 og spin ned har egenverdien -1. En vanlig antagelse er at alle de observable egenskapene skal være reelle verdier, derfor velger man i tillegg å anta at A må være en Hermitisk operator (selvadjungert).

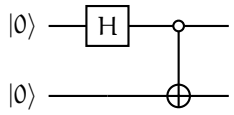
Når man gjør en måling av en observabel er det tilfeldig hva man måler. Sannsynlighetene for å måle de forskjellige egenverdiene er gitt ved formelen over. Etter måling vil systemet kollapse ned i egenrommet til vektoren $\frac{1}{\sqrt{p_{a_n}}} P_{a_n}|\psi\rangle$. Hvis den algebraiske multiplisiteten til egenverdien a_n er 1 så tilsvarer dette vektoren $\frac{|a_n\rangle}{|||a_n\rangle||}$. En konsekvens av dette er at observabelen som har tilstanden $|\psi\rangle$ som en egenvektor med egenverdi lik 1 vil ikke endre tilstanden til systemet etter måling. Hvis man derimot måler denne observabelen, vil man normalisere tilstanden. I spin eksemplet vil dette si at hvis man måler verdien 1, så vil tilstanden kollapse til den tilsvarende egenvektoren, normalisert. En konsekvens av dette er at en tilstand er bedre definert som ekvivalensklasser langs linjer i Hilbertrommet. En tilstand er dermed et element i randen av enhetskulen til Hilbertrommet.

$$|\psi\rangle : \partial D(\mathcal{H}) = \{v : \mathcal{H} \mid \|v\| = 1\}$$

Det siste postulatet forteller oss hvordan et system utvikler seg. Formelen $|\psi(t)\rangle = U(t, t_0)|\psi(t_0)\rangle$ brukes ofte for å beskrive hvordan dette ser ut. Siden vi krever at $U(t, t_0)$ skal bevare normen til $|\psi(t_0)\rangle$, dvs. at det finnes en virkning $U(t, t_0) : \partial D(\mathcal{H}) \to \partial D(\mathcal{H})$, følger det at denne operatoren er unitær. Mengden $U(\mathcal{H})$ vil betegne de unitære operatorene som operer på det Hilbertrommet. For vårt formål kan man tenke på et kvantesystem som et element i $U(\mathcal{H})$-mengden $\partial D(\mathcal{H})$.

Som beskrevet av [2] kan man lage kompositter av kvantesystemer med det algebraiske tensorproduktet. Gitt to foskjellige kvantesystemer beskrevet av to forskjellige Hilbertrom $\mathcal{H}_1$ og $\mathcal{H}_2$ så kan man lage rommet av sammensatte tilstander som $\mathcal{H}_1 \otimes \mathcal{H}_2$. Vi får da en klasse med observable og en klasse med operatorer som handler på systemene gjennom tensorproduktet. Man kan vise at tensorproduktet av to unitære og hermitiske matriser er igjen unitære og hermitiske, det er derfor veldefinert å betrakte tensoren for kompositt systemer. Sammenfiltringsfenomenet foregår når man konstruerer slike kompositt systemer. Hvis vi antar at vi har to partikler med spin egenskapen ϕ og ψ og komposittsystemet $|\phi\psi\rangle = \sigma_0 e_0 \otimes e_0 + \sigma_1 e_1 \otimes e_1$, så vil en måling av den ene partikkelen ende opp med å måle den andre partikkelen. Dersom man måler egenverdien til e_0 for ϕ så vil systemet kollapse til $\frac{1}{\sigma_0} P_1 \otimes I(|\phi\psi\rangle) = e_0 \otimes e_0$. Dette medfører at alle målinger av ψ vil gi egenverdien 1.

Figur 1: EPR-sammenfiltrings kvantekrets



H boksen viser til at man bruker Hadamard operatoren, mens sirkelen kontrollerer en X operator som er $\oplus$.

2.2 Qubits og kvantekretser

Klassiske bits har to tilstander: 0 eller 1. Kvantebits, eller qubits er et fysisk system som har en observabel som måler to diskrete tilstander. Disse tilstandene bruker vi for å representere 0 og 1. Ettersom at operatoren som måler 0 og 1 er hermitisk, så finnes det en ortonormal basis for Hilbertrommet som diagonaliserer denne operatoren. Elementene i denne basisen vil bli betegnet som $|0\rangle$ og $|1\rangle$. En qubit q er dermed et element i $\partial D(\mathbb{C}^2)$ på formen $q = q_0|0\rangle + q_1|1\rangle$.

En streng av bits er sammensettingen av flere bits. På samme måte konstruerer vi en streng av qubits til å være sammensettingen av flere qubits. Denne sammensettingen er gitt av tensorproduktet mellom de algebraiske qubitsene. F.eks. er en 2-qubit streng er et element i $\partial D(\mathbb{C}^2 \otimes \mathbb{C}^2)$ på formen under.

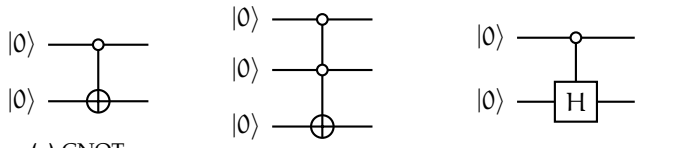
$$q = q_{00}|0\rangle \otimes |0\rangle + q_{01}|0\rangle \otimes |1\rangle + q_{10}|1\rangle \otimes |0\rangle + q_{11}|1\rangle \otimes |1\rangle$$

For kortfatthetens skyld skriver vi $|ab\rangle = |a\rangle \otimes |b\rangle$. Notasjonen $|\_\rangle$ vil få en ekstra presisjon i denne rapporten. La $nBit$ være mengden av strenger med n-bits, vi definerer $|\_\rangle : \bigcup_{n=0}^{\infty} nBits \to \mathbb{T}(\mathbb{C}^2)$ til å være en funksjon fra alle strenger og inn i tensoralgebraen til $\mathbb{C}^2$. Den er definert på $|0\rangle$ og $|1\rangle$ som over, også utvides den lineært og fritt over tensoralgebraen. En av de viktigste egenskapene qubits har som bits ikke har er nemlig at to eller flere qubits kan bli sammenfiltret.

EPR paret (Einstein, Rosen og Podolsky) er et klassisk eksempel på sammenfiltring. Man kan se at et system av qubits er sammenfiltret hvis det ikke kan skrives som en elementær tensor, $a \otimes b$. Et EPR par er et 2-qubit system på formen $\psi = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. Man kan se at dette systemet er sammenfiltret, ettersom de to elementære tensorene ikke har noen felles faktorer. Hvis vi derimot måler den første qubiten i systemet vil vi ende opp med at det er en $(\frac{1}{\sqrt{2}})^2 = 50\%$ sjanse for å måle 0 og 50% sjanse for å måle 1. Hvis vi derimot har målt 0 på den første qubiten, så vil systemet kollapse til $\psi = |00\rangle$, og vi vet dermed at den andre qubiten må være i tilstand $|0\rangle$.

På samme måte som at klassiske bits kan manipuleres med kretser, kan man manipulere qubits med kvantekretser. En kvantekrets er et flytdiagram med et register, en arbeidsplass, logiske kvanteporter og målinger. Registeret er inputtet av qubits, arbeidsplassen er tilleggs qubits som man kan bruke til å utføre/definere operasjoner. Se figur 1 for et eksempel av en krets. I motsetning til klassiske kretser kan ikke kvantekretser ødelegge qubits, og alle prosessene må være unitære og reversible. Alle logiske kvanteporter er derfor unitære transformasjoner. Målinger følger ikke disse reglene, og disse er gitt ved hermitiske operatorer. Bemerk at en måling gjør om en qubit om til en klassisk bit.

Figur 2: Kontrollerte kvanteporter



(a) CNOT **(b)** Toffoli **(c)** Kontrollert Hadamard

De elementære logiske kvanteportene er unære, binære og trinære unitære operatorer over $\mathbb{C}^2$. De unære operatorene er kjent som Pauli matrisene I, X, Y, Z, sammen med Hadamard operatoren H og fase skift operatoren R_θ. Man kan observere at X operatoren flipper qubiten, Z operatoren snur fasen hvis argumentet var $|1\rangle$ og Y operatoren er en kombinasjon av X og Z ganget med skalaren i.

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \text{ og } R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$$

Den elementære binære operatoren kalles controlled not og skrives CNOT. CNOT fliper qubiten til det andre argumentet hvis den første qubiten er $|1\rangle$. SWAP porten er en binær port som bytter om rekkefølgen på argumentene.

$$\text{CNOT} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Den trinære porten som er av stor interesse er Toffoli porten. Toffoli porten kalles også CCNOT, ettersom det er en dobbel kontrollert not. Hvis de to første argumentene har verdien $|1\rangle$ så flippes qubiten i det tredje argumentet.

$$\text{Toffoli} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Disse portene er universelle i den forstand av at alle andre logiske kvanteporter kan uttrykkes som en komposisjon av disse portene. Vi har i tillegg at Hadamard porten og Toffoli porten kan konstruere alle porter med reelle innlegg, som beskrevet av [3].

Som sagt tidligere er CNOT og Toffoli portene kontrollerte porter. En kontrollert port er en port som kun blir aktivert, gitt at tilstanden til en annen qubit tilfredstiller en betingelse. CNOT er kontrollert i den forstanden at man kun anvender X

operatoren hvis den første qubiten er i tilstanden $|1\rangle$. Toffoli porten er et eksempel på en port som er multikontrollert. Alle logiske kvanteporter kan kontrolleres av andre qubits. Se figur 2 for eksempler.

2.3 Kvantealgoritmer og orakler

Klassiske algoritmer er metoder som løser problemer basert på input av bits, kvantealgoritmer kan dermed ses på som metoder som løser problemer basert på qubits. Bits brukes for å representere datastrukturer som tall, lister og grafer. Qubits kan brukes for å representere de samme strukturene. Kvantekretser blir dermed den naturlige måten for å representere algoritmene, en kvantealgoritme er dermed en komposisjon av unitære operatorer og målinger på en tilstand ψ i $\partial D(\mathcal{H})$.

Kvanteparallellisme er en egenskap kvantealgoritmer får fra kvantemekanikken. Dette fenomenet er beskrevet som at en beregning kan inneholde informasjonen fra flere. For å se dette ser vi på en funksjon $f : n\mathrm{Bits} \to 1\mathrm{Bits}$ og vi antar at det finnes en unitær operator $\mathcal{O}_f$ slik at $\mathcal{O}_f(|z\rangle\,|0\rangle) = |z\rangle\,|0\rangle$. Ved å anvende $\mathcal{O}_f$ på en tilstand som er i en superposisjon av alle baisiselementene får man følgende:

$$\mathcal{O}_f(\Sigma_{z=0}^{n}\,|z\rangle\,|0\rangle) = \Sigma_{z=0}^{n}\,|z\rangle\,|f(z)\rangle\,.$$

Man kan se at $\mathcal{O}_f$ har kun blitt anvendt en gang, men informasjon om alle evalueringene er i den nye tilstanden. Når man måler tilstanden i standard basisen vil den kollapse til en av evalueringene, så klassisk er ikke Kvanteparallellisme noe bedre, men interferens og sammenfiltring kan gi effekter som gir bedre utslag enn med klassiske algoritmer.

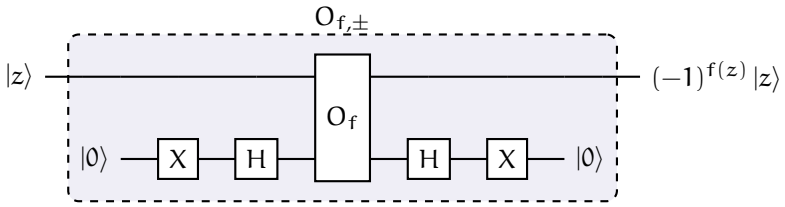
Nesten alle kvantealgoritmer bruker en slags *query*. Disse kommer som oftest i form som en evaluering av en klassisk funksjon. Den unitære operatoren ovenfor er et eksempel på en slik *query*. De operatorene som utfører *queries* kalles for orakler eller black-boxes. En unitær operator $\mathcal{O} : \mathcal{H} \otimes \mathcal{H}' \to \mathcal{H} \otimes \mathcal{H}'$ som gjør en *query* på rommet $\mathcal{H}$ og merker tilstandene i $\mathcal{H}'$ basert på utfallet kalles for et merkeorakel. Operatoren $\mathcal{O}_f$ som definert over er et eksempel på et merkeorakel. En annen klasse med orakler er faseorakler, disse er operatorer på formen $\mathcal{O}_\pm : \mathcal{H} \to \mathcal{H}$, disse gjør en *query* på rommet $\mathcal{H}$ og endrer fasen basert på utfallet.

I tilfellet med merkeorakelet $\mathcal{O}_f$, så finnes det en metode for å gjøre det om til et faseorakel $\mathcal{O}_{f,\pm}$. Bemerk først at merkeorakelet er definert som $\mathcal{O}_f(|z\rangle\,|w\rangle) = |z\rangle\,|w \oplus f(z)\rangle$ på basisen. Vi kan definere $\mathcal{O}_{f,\pm}$ som følgende:

$$\begin{aligned} \mathcal{O}_f(|z\rangle \otimes H\,|1\rangle) &= (-1)^{f(z)}\,|z\rangle \otimes H\,|1\rangle \\ \implies \mathcal{O}_{f,\pm}(|z\rangle) &= (-1)^{f(z)}\,|z\rangle \end{aligned}$$

Figur 4 beskriver hvordan denne konstruksjonen ser ut som med kvantekretser.

Figur 4: Standardkonstruksjon av faseorakel



3 KVANTEVANDRINGER

3.1 Grover's algoritme og metoden av amplitude amplifikasjon

Grover's algoritme løser problemet med ustrukturert søk, og teknikken amplitude amplifikasjon som den bruker er av stor interesse. Problemet går som følger: Tenk at man er gitt en bistring med $N = 2^n$ bits, hvor t bits er satt til 1. Finn minst 1 bit som har verdi 1. Dette problemet kan åpenbart løses i "worstcase" lineær tid med konstant minne ved å randomisert iterere gjennom alle bitene og sjekke om de er 1 eller 0. Om den er 1 kan man terminere programmet, og returnere den posisjon som ga 1. Grover's algoritme har en kvadratisk hastighetsøkning på dette problemet, og man kan dermed løse det i worst case kvadratisk tid.

For å beskrive problemet med et fysisk kvantesystem trenger vi å oversette problemet først. La $(b_k)_N$ være bitstringen med lengde N, definer så orakelet $\mathcal{O}_{(b_k)_N} : \mathbb{C}^{2^n} \otimes \mathbb{C}^2 \to \mathbb{C}^{2^n} \otimes \mathbb{C}^2$ til å merke målbiten hvis registerbiten var en løsning. Dette vil si at hvis $\mathcal{O}_{(b_k)_N}(|r\rangle \otimes |0\rangle) = |r\rangle \otimes |1\rangle$ så følger det at $b_r = 1$. For å fullføre Grover's algoritme trenger man matrisen R som flipper fortegnet til registeret hvis den ikke er tilstanden $|0\rangle^{\otimes n}$.

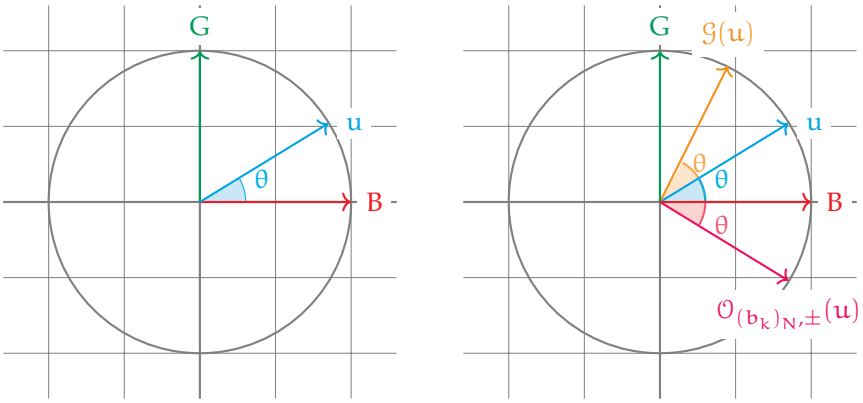
$$R = \begin{pmatrix} 1 & 0 & \dots \\ 0 & -1 & \dots \\ \vdots & \vdots & \ddots \end{pmatrix}$$

En Grover iterate $\mathcal{G}$ er definert som

$$\mathcal{G} = H^{\otimes n} R H^{\otimes n} \mathcal{O}_{(b_k)_N,\pm}.$$

Gorver's algoritme er komposisjonen av operatorene $G = M\mathcal{G}^k \circ H^{\otimes n}$, hvor M er en projektiv måling, og k er en konstant. Man skal da kunne fastslå med en høy sannsynlighet at målingen gir deg posisjonen til en bit i $(b_k)_N$ som er 1. For å finne denne k-en som man bruker for å kjøre algoritmen trenger vi å se på metoden av amplitude amplifikasjon.

Figur 5: Grover's algoritme



(a) Initiell tilstand **(b)** En Grover iteration

Definer tre tilstander hvor t er antall 1-ere i $(b_r)_N$

$$u = H^{\otimes n}|0\rangle^{\otimes n}$$
$$G = \frac{1}{\sqrt{t}}\Sigma_{|r\rangle|b_r=1}|r\rangle$$
$$B = \frac{1}{\sqrt{N-t}}\Sigma_{|r\rangle|b_r=0}|r\rangle$$

.

Man kan se at G (Good) og B (Bad) vektorene er ortogonale, ettersom de er en sum av ortogonale vektorerer. I det 2 dimensjonale underrommet av $\mathbb{C}^{2^n}$ utspent av G og B, finner man vektoren u.

$$\begin{aligned} u &= \frac{1}{\sqrt{N}}\Sigma_{|r\rangle}|r\rangle = \frac{\sqrt{t}}{\sqrt{N}}G + \frac{\sqrt{N-t}}{\sqrt{N}}B \\ &= \sin\circ\arcsin(\frac{\sqrt{t}}{\sqrt{N}})G + \cos\circ\arcsin(\frac{\sqrt{t}}{\sqrt{N}})B \\ &= \sin(\theta)G + \cos(\theta)B \end{aligned}$$

Her er $\theta = \arcsin(\frac{\sqrt{t}}{\sqrt{N}})$. Vi ønsker nå å manipulere tilstanden til u i underrommet utspent av G og B for å maksimere $\sin(\theta)$. Dette vil maksimere sannsynligheten for at algoritmen avslutter i en tilstand hvor man har maksimal sjanse for å måle en qubit som er merket. La $\alpha : \mathbb{R}$ være en vinkel og $T = \sin(\alpha)G + \cos(\alpha)B$ være en tilstand. For å se hva orakelet gjør med T kan vi se på hva den gjør med G og B.

$$\begin{aligned} &\mathcal{O}_{(b_k)_N,\pm}(B) = B \\ &\mathcal{O}_{(b_k)_N,\pm}(G) = -G \\ \implies &\mathcal{O}_{(b_k)_N,\pm}(T) = -\sin(\alpha)G + \cos(\alpha)B = \sin(-\alpha)G + \cos(-\alpha)B \end{aligned}$$

Operatoren R har en annen beskrivelse som en refleksjon om en enhetsvektor.

$$R = 2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - I$$

Det følger at den andre komponenten i en Grover's iterate er en refleksjon om tilstanden u.

$$\begin{aligned} &H^{\otimes n} R H^{\otimes n} \\ &= H^{\otimes n}(2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - I)H^{\otimes n} \\ &= 2H^{\otimes n}|0\rangle^{\otimes n}\langle 0|^{\otimes n}H^{\otimes n} - H^{\otimes n}H^{\otimes n} \\ &= 2uu^* - I \end{aligned}$$

En Grover's iterate kan derfor også bli betegnet som $\mathcal{G} = (2uu^* - I)\mathcal{O}_{(b_k)_N,\pm}$. Dette gjør at vi kan observere hva tilstanden til T er etter å anvende $H^{\otimes n} R H^{\otimes n}$ operatoren, og vi kan se hva Grover's iterate k ganger gjør.

$$\begin{aligned} H^{\otimes n} R H^{\otimes n}(T) &= \sin(-\alpha + 2\theta)G + \cos(-\alpha + 2\theta)B \\ \implies \mathcal{G}^k(T) &= \sin(\alpha + 2k\theta)G + \cos(\alpha + 2k\theta)B \end{aligned}$$

Hvis man initialiserer $\alpha = \theta$ vil k Grover's iterate gi

$$\mathcal{G}^k(T) = \sin((1 + 2k)\theta)G + \cos((1 + 2k)\theta)B.$$

En naiv k for når man skal stoppe Grover's algoritme er den tilstanden som er nærmest G først.

$$\begin{aligned} &\sin((2k' + 1)\theta) = 1 \\ \implies &(2k' + 1)\theta = \frac{\pi}{2} \\ \implies &k \approx \frac{\pi}{4\theta} - \frac{1}{2} = \lfloor \pi/4 \arcsin(\sqrt{\frac{t}{N}}) \rfloor. \end{aligned}$$

Denne verdien av k vil gi sannsynligheten for å treffe et merket element

$$p = \sin((1 + 2k)\theta) = \sin((1 + \lfloor \pi/2 \arcsin(\sqrt{\frac{t}{N}}) \rfloor) \arcsin(\sqrt{\frac{t}{N}}))$$

Legg til eksempler og figurer

Sannsynlighet amplifikasjon og Amplitude amplifikasjon

3.2 Kvantevandringer basert på kvantemyntkast

Kvantevandringer prøver å ta ideen til Grover's algoritme for søk og å generalisere den til andre datatyper, som grafer. For å gjøre denne generaliseringen deler vi opp problemet inn i traversering og oppdagelse. Det er mange metoder for å traversere over grafer, og her er det noen viktige klasser med grafer som vi vil studere.

For å illustrere hvordan kvantevandring kan virke, starter vi med å se på en klassisk tilfeldig vandring. Se for deg at det er en vandrer som vandrer gjennom en skog med forgreninger. Når vandreren møter på en forgrening kaster de en mynt for å velge hvilken retning de går. En slik vandring vil være et eksempel på en rettet tilfeldig vandring over et binærtre. Denne ideen kan man gjøre om til en kvante vandringsalgoritme ved at man gjør om vandreren til en kvantepartikkel, med en kvantemynt som kan være i superposisjon av 2 forskjellige tilstander. Partikkelen vandrer gjennom skogen avhengig av tilstanden til mynten, akkurat som den klassiske vandreren. Dette tillater partikkelen til å flytte seg gjennom skogen som en superposisjon av forskjellige muligheter. Det vil først være når vi måler partikkelen sin posisjon at vi vil få vite hvor den er, og hvilke utfall mynten har gitt.

For å være mer presis kan man tilegne to Hilbertrom til en slik kvantevandringsalgoritme. $\mathcal{H}_V$ representerer posisjonene til vandreren, og $\mathcal{H}_C$ representerer utfallene av kvantemyntkastet. Et kvantesteg defineres som komposisjonen av to operatorer $U = S(I \otimes C)$, en myntkast operator $C : \mathcal{H}_C \to \mathcal{H}_C$ som kaster mynten og en forflyttings operator (skift operater) $S : \mathcal{H}_V \otimes \mathcal{H}_C \to \mathcal{H}_V \otimes \mathcal{H}_C$ som leser av myntkastet og forflytter seg henholdsvis. En kvantevandring vil være en algoritme som MU^kT, hvor M er en måling, U er et kvantesteg og T er en operator som setter systemet i starttilstanden. Dette er det som vi kaller for en myntbasert kvantevandringsalgoritme og er den formen for vandring som er standarisert i litteraturen.

d-*regulære grafer*

Den første kvantevandringsmetoden som vi skal se på er vandring over d-regulære grafer, den kalles for *position-coin notation*. For at denne metoden skal virke krever vi tillegg at det maksimale kantkromatiske tallet er det samme som d. Hvis man i tillegg ikke tillater at grafen har noen løkker vil spektraldekomposisjonen til algoritmen bli simplere.

La $G = (V, E)$ være en d-regulær graf slik at det maksimale kantkromatiske tallet også er d. Siden kantene i grafen kan fargelegges med d forskjellige farger, så kan vi separere grafen i d forskjellige undergrafer. I hver undergraf er en node koblet til nøyaktig en annen node. La $\mathcal{H}_V = \mathbb{C}V$ være det frie Hilbertrommet over nodene og $\mathcal{H}_C = \mathbb{C}^d$ være myntrommet. Vi definerer forflyttingsoperatoren S på følgende måte: La f være en farge og $v : V$ en node. Assosiert med denne noden og fargen finnes det en unik node $v' : V$, slik at det er en kant $(v, v') : E$ som har fargen f.

$$S(v \otimes f) = v' \otimes f$$

Denne operatoren kalles for *flip-flop operatoren*. En enkel egenskap ved denne operatoren som er enkel å bemerke er at $S^2 = I$, hvilket som gjør at den er hermitisk.

Myntoperatoren C kan velges litt mer vilkårlig, men det er noen mynter som er bedre enn andre. En ønskelig egenskap fra mynten er at den er uniformt fordelt. Det kan finnes tilfeller hvor det er interessant å se på mynter som er vektet slik at en farge er vektet mer enn andre. Tre veldig vanlige mynter er Hadamard mynten, Fourier mynten og Grovers mynt .

Forklar hva disse myntene er

Et kvantesteg langs denne grafen kan man nå definere som $U = S(I \otimes C)$. Vi bemerker oss at egenskapen som lar oss bruke $I \otimes C$ er at grafen er d-regulær. Hvis grafen ikke hadde hatt denne egenskapen, men heller at den maksimale graden var lik det maksimale kantkromatiske tallet kan man fremdeles bruke det samme prinsippet. Siden vi ikke lengre kan være sikre på at alle noder har d tilstøtende farger, så må man ha en mynt for hver node som tilordner ny farge langs den noden.

Vi illustrer denne metoden med et eksempel:

Lag eksempel her

Rettede grafer

En myntet metode for kvantevandring som virker på en generell klasse av grafer er den som kalles for *arc notation*. Vi beskriver hvordan man bruker arc notation på en retted graf. Vi vil kreve av grafen at alle pilene har en pil som går i motsatt retning.

Ofte så blir denne metoden beskrevet som at man vandrer over kantene, istedenfor at man vandrer over nodene.

La $G = (V, E)$ være en rettet graf som beskrevet over. Hvert element $e : E$ kan representeres på formen $(u, v) : VxV$, her er u start noden og v er slutt noden. Med denne metoden kan vi ikke nødvendigivis ha en mynt, så vi må definere det totale rommet til å være $\mathcal{H} = \mathbb{C}E \subseteq \mathbb{C}V \otimes \mathbb{C}V$. $\mathcal{H}$ er det frie Hilbertrommet over kantene. For en kant $e : E$ er det assosiert 2 noder $u, v : V$ slik at $e = u \otimes v$. Vi velger da å definere $S(e) = S(u \otimes v) = v \otimes u = S(e^{-1})$, altså *flip-flop operatoren*.

For å definere myntene må vi først dele opp rommet $\mathcal{H}$. Observer at

$$\mathcal{H} = \bigoplus_{v:V} \mathbb{C}\{v \otimes u \mid \forall u : V, (v, u) : E\}.$$

Vi trenger nå å definere en mynt på hvert av disse underrommene, og dermed direktesumme de sammen. Vi definerer mynten $C = \bigoplus_{v:V} C_v : \mathcal{H} \to \mathcal{H}$, hvor C_v er definert på hvert underrom. Med andre ord er C en blokkdiagonal matrise, hvor hver blokk tilsvarer en mynt.

Et kvantesteg med *arc notation* algoritmen ser ut som $U = SC = S \bigoplus_{v:V} C_v$. Vi illustrer dette med et eksempel.

Kvantemynter

3.3 Umyntede kvantevandringer

Staggered model

Den første umyntede metoden som vi skal se på er den forskyvede metoden. Denne metoden baserer seg på å finne graf tesselleringer og en graf tesselleringsdekke. En graftessellering er en oppdeling av en graf inn i dens cliquer. En clique kalles også for et polygon, en kant er med i graftesselleringen hvis det er en kant i polygonet. En graf tesselleringsdekke er en samling av graf tesselleringer slik at alle kantene i grafen er dekket. Dette vil si at unionen av alle tesseleringene er den originale grafen.

Kom med et eksempel på en graf tesselleringer her

Valget av en graf tesselleringsdekke vil bestemme hvordan kvantestegsoperatoren vil se ut. For enhver graf tessellering $\mathcal{T}$ assosierer vi en operator $H_{\mathcal{T}}$. For hvert polygon $\alpha : \mathcal{T}$ assosierer vi en vektor $\vec{\alpha} = 1/\sqrt{|\alpha|}\Sigma_{v:\alpha}|v\rangle$. Vi definerer operatoren $H_{\mathcal{T}}$ og U som under. Her skal tensorproduktet tolkes som funksjonskomposisjon.

$$H_{\mathcal{T}} = 2\Sigma_{\alpha:\mathcal{T}}\langle \_ , \alpha\rangle\alpha - I$$
$$U = \bigotimes_{\mathcal{T}:\mathrm{Cover}} H_{\mathcal{T}}$$

Vi illustrer hvordan vandringen virker med den samme grafen.

Szegedy vandring

3.4 Kvantesøk

4 Q# OG IMPLEMENTASJON AV KVANTEVANDRINGER

4.1 Q# intro

4.2 Praktisk kvantevandringer og utfordringer

REFERANSER

[1] R. L. Jaffe. Supplementary notes on dirac notation, quantum states and etc. http://web.mit.edu/8.05/handouts/jaffe1.pdf, 2007.

[2] Renato Portugal. *Quantum Walks and Search Algorithms*. Springer, 2 edition, 2019.

[3] Ronald de Wolf. Quantum computing: Lecture notes, 2021.

[4] Bradben, dime10, geduardo, cjgronlund, rmshaffer, and gillenhaalb. Q# user guide. https://docs.microsoft.com/en-us/azure/quantum/user-guide/0, 2021.

[5] Salvador Elías Venegas-Andraca. Quantum walks: a comprehensive review. *Quantum Information Processing*, 11(5):1015–1106, Jul 2012.