NASJONAL SIKKERHETSMYNDIGHET

Kvantevandringer

over endelige grafer

Thomas Wilskow Thorbjørnsen

15. august 2021

Introduksjon

Relevant kvante

- Hva er en tilstand?
- Hva er en måling?
- Hvordan virker en tidsutvikling?
- Hva er et sammensatt system?

Relevant kvante

Hva en tilstand er:

- En tilstand er en ket $|\psi\rangle$, en vektor i et Hilbertrom $\mathcal{H}$.
- Normen til ketten er enhet: $|||\psi\rangle|| = 1$

Eksempel: Spin opp, spin ned.

- Anta at det finnes en partikkel med tilstandene spin opp og spin ned.
- Dette kan modelleres som en ket $|\psi\rangle \in \mathbb{C}\{opp,\ ned\} = \mathbb{C}^2$
- Ketten er i en superposisjon $|\psi\rangle = \psi_o|opp\rangle + \psi_n|ned\rangle$

Relevant kvante

Hva en måling er:

- Gitt en observabel fysisk egenskap $\mathcal{A}$ så finnes det en operator $A : \mathcal{H} \to \mathcal{H}$.
- Alle mulige målinger av $\mathcal{A}$ er egenverdiene til A.
- Sjansen for å måle en gitt egenverdi a_n er gitt ved kvadratet av indreproduktet mellom tilstanden $|\psi\rangle$ og egenvektoren $|a_n\rangle$: $|\langle a_n|\psi\rangle|^2$.
- En måling kalles projektiv hvis operatoren A er en projeksjon.

Relevant kvante

Hvordan tidsutvikling virker:

- For at målinger skal gi reelle verdier er det tilstrekkelig at operatoren H i Schrödingers likning er hermitisk:

$$i\hbar \frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle.$$

- En løsning av denne likningen medfører at operatoren U er unitær.

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle$$

- Konsekvensen er at alle operasjoner vi skal se på er unitære.

Relevant kvante

Sammensatte systemer:

- Gitt to systemer $\mathcal{H}_1$ og $\mathcal{H}_2$, så er det sammensatte systemet beskrevet av tensorproduktet: $\mathcal{H}_1 \otimes \mathcal{H}_2$.
- Tilstandene i sammensatte systemer er gitt ved summen av elementære tensorer av basisen.
- En tilstand kalles sammenfiltret, hvis det ikke kan skrives som nøyaktig en elementær tensor.
- Bell tilstanden; $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$

$$\frac{1}{\sqrt{2}}(e_0 \otimes e_0 + e_1 \otimes e_1)$$

Kvanteberegninger; I

- Bits vs. Qubits
  $\{0,\ 1\}\ vs.\ \mathbb{C}\{0,\ 1\} = \mathbb{C}^2$
  $0 \vee 1\ vs.\ q = q_0|0\rangle + q_1|1\rangle$
- Logiske kvanteporter

Kvanteberegninger; I

- Bits vs. Qubits
  $\{0,\ 1\}^n\ vs.\ \mathbb{C}\{0,\ 1\}^n = \mathbb{C}^{2^{\otimes n}}$
  $00 \vee 01 \vee 10 \vee 11\ vs.\ q = q_{00}|00\rangle + q_{01}|01\rangle + q_{10}|10\rangle + q_{11}|11\rangle$
- Logiske kvanteporter

Kvanteberegninger; I

- Bits vs. Qubits
  $\{0,\ 1\}^n\ vs.\ \mathbb{C}\{0,\ 1\}^n = \mathbb{C}^{2^{\otimes n}}$
  $00 \vee 01 \vee 10 \vee 11\ vs.\ q = q_{00}|00\rangle + q_{01}|01\rangle + q_{10}|10\rangle + q_{11}|11\rangle$
- Logiske kvanteporter

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \begin{aligned} X(|0\rangle) &= |1\rangle \\ X(|1\rangle) &= |0\rangle \end{aligned}$$

Kvanteberegninger; I

- Bits vs. Qubits
  $\{0,\ 1\}^n\ vs.\ \mathbb{C}\{0,\ 1\}^n = \mathbb{C}^{2^{\otimes n}}$
  $00 \vee 01 \vee 10 \vee 11\ vs.\ q = q_{00}|00\rangle + q_{01}|01\rangle + q_{10}|10\rangle + q_{11}|11\rangle$
- Logiske kvanteporter

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \begin{aligned} Y(|0\rangle) &= i|1\rangle \\ Y(|1\rangle) &= -i|0\rangle \end{aligned}$$

Kvanteberegninger; I

- Bits vs. Qubits
  $\{0,\ 1\}^n\ vs.\ \mathbb{C}\{0,\ 1\}^n = \mathbb{C}^{2^{\otimes n}}$
  $00 \vee 01 \vee 10 \vee 11\ vs.\ q = q_{00}|00\rangle + q_{01}|01\rangle + q_{10}|10\rangle + q_{11}|11\rangle$
- Logiske kvanteporter

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \begin{aligned} Z(|0\rangle) &= |0\rangle \\ Z(|1\rangle) &= -|1\rangle \end{aligned}$$

Kvanteberegninger; I

- Bits vs. Qubits
  $\{0,\ 1\}^n\ vs.\ \mathbb{C}\{0,\ 1\}^n = \mathbb{C}^{2^{\otimes n}}$
  $00 \vee 01 \vee 10 \vee 11\ vs.\ q = q_{00}|00\rangle + q_{01}|01\rangle + q_{10}|10\rangle + q_{11}|11\rangle$
- Logiske kvanteporter

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix} \quad \begin{aligned} H(|0\rangle) &= {}^1\!/\!\sqrt{2}(|0\rangle + |1\rangle) \\ H(|1\rangle) &= {}^1\!/\!\sqrt{2}(|0\rangle - |1\rangle) \end{aligned}$$

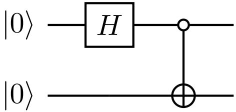
Kvanteberegninger; I

- Bits vs. Qubits
  $\{0,\ 1\}^n\ vs.\ \mathbb{C}\{0,\ 1\}^n = \mathbb{C}^{2^{\otimes n}}$
  $00 \vee 01 \vee 10 \vee 11\ vs.\ q = q_{00}|00\rangle + q_{01}|01\rangle + q_{10}|10\rangle + q_{11}|11\rangle$
- Logiske kvanteporter

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{aligned} CNOT(|00\rangle) &= |00\rangle \\ CNOT(|01\rangle) &= |01\rangle \\ CNOT(|10\rangle) &= |11\rangle \\ CNOT(|11\rangle) &= |10\rangle \end{aligned}$$

Kvanteberegninger; II

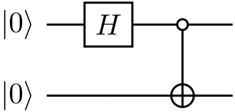
- Bell state



$$\iff CNOT \circ (H \otimes I)$$

Kvanteberegninger; II

- Bell state

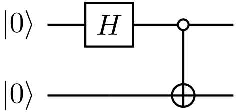


$$\iff CNOT \circ (H \otimes I)$$

- Universelle porter

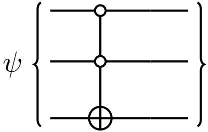
Kvanteberegninger; II

- Bell state



$$\iff CNOT \circ (H \otimes I)$$

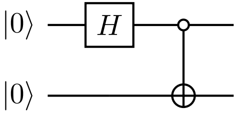
- Universelle porter
- Simulere klassiske beregninger



Toffoli

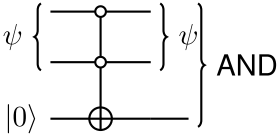
Kvanteberegninger; II

- Bell state



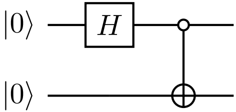
$$\iff CNOT \circ (H \otimes I)$$

- Universelle porter
- Simulere klassiske beregninger



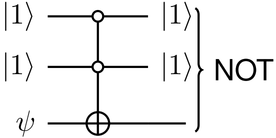
Kvanteberegninger; II

- Bell state



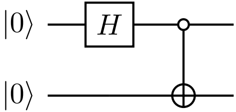
$$\iff CNOT \circ (H \otimes I)$$

- Universelle porter
- Simulere klassiske beregninger



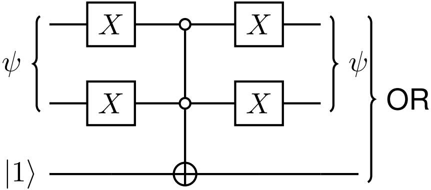
Kvanteberegninger; II

- Bell state

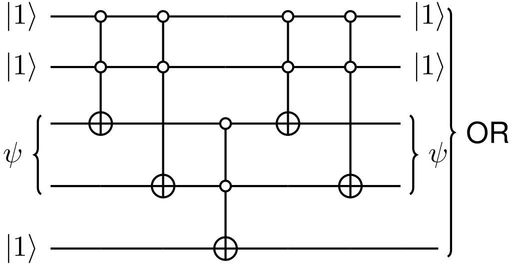


$$\iff CNOT \circ (H \otimes I)$$

- Universelle porter
- Simulere klassiske beregninger



Kvanteberegninger; III



Orakler

- Algoritmer trenger å spørre på en eller annen måte
- Kvanteparallellisme
- Merkeorakler

$$\begin{aligned} f &: \{0,\ 1\}^n \to \{0,\ 1\} \\ \mathcal{O}_f &: \mathbb{C}\{0,\ 1\}^n \otimes \mathbb{C}\{0,\ 1\} \to \mathbb{C}\{0,\ 1\}^n \otimes \mathbb{C}\{0,\ 1\} \\ &|x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle \end{aligned}$$

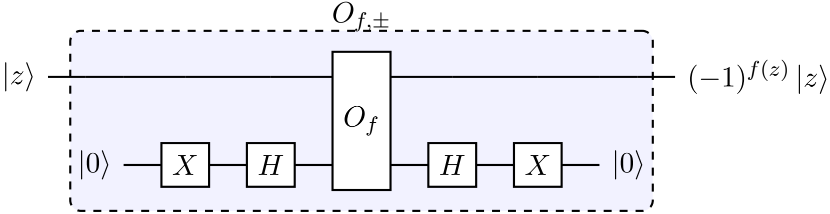
Orakler

- Algoritmer trenger å spørre på en eller annen måte
- Kvanteparallellisme
- Faseorakler

$$f : \{0,\ 1\}^n \to \{0,\ 1\}$$
$$\mathcal{O}_{f,\pm} : \mathbb{C}\{0,\ 1\}^n \to \mathbb{C}\{0,\ 1\}^n$$
$$|x\rangle \mapsto (-1)^{f(x)}|x\rangle$$

Orakler

- Algoritmer trenger å spørre på en eller annen måte
- Transformere merkeorakel til faseorakel



Deutsch-Jozsa

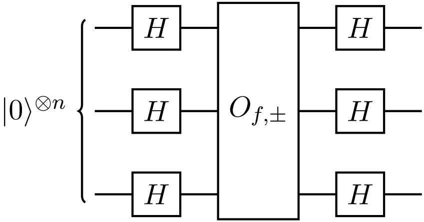
- Problemet:
  - La $f : \{0,\ 1\}^n \to \{0,\ 1\}$ være en funksjon som enten er konstant eller balansert (50% er 0 og 50% er 1).
- Mål: Finne ut om f er konstant eller balansert.

Deutsch-Jozsa

- Problemet:
  - La $f : \{0,\ 1\}^n \to \{0,\ 1\}$ være en funksjon som enten er konstant eller balansert (50% er 0 og 50% er 1).
- Mål: Finne ut om f er konstant eller balansert.
- Klassisk løsning:
  1. Evaluere f i $\frac{2^n}{2} + 1$ elementer.
  2. Hvis alle er 0 eller 1 fastslå konstant, hvis ikke fastslå balansert.

Deutsch-Jozsa

- Problemet:
  - La $f : \{0,\ 1\}^n \to \{0,\ 1\}$ være en funksjon som enten er konstant eller balansert (50% er 0 og 50% er 1).
- Mål: Finne ut om f er konstant eller balansert.
- Kvante løsning:



Grover's algoritme; I

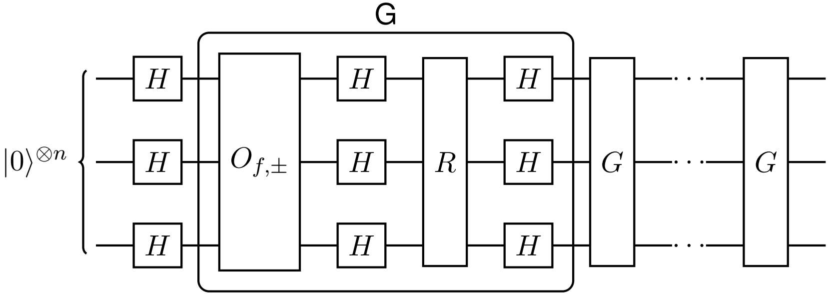
- Problemet:
  - La $f : \{0,\ 1\}^n \to \{0,\ 1\}$ være en funksjon
- Mål: Finne et element som evalueres til 1.

Grover's algoritme; I

- Problemet:
  - La $f : \{0,\ 1\}^n \to \{0,\ 1\}$ være en funksjon
- Mål: Finne et element som evalueres til 1.
- Klassisk løsning:
  1. Evaluer hvert element fra 0 til $2^n - 1$.
  2. Stopp når man finner et element z slik at $f(z) = 1$.

Grover's algoritme; I

- Problemet:
  - La $f : \{0,\ 1\}^n \to \{0,\ 1\}$ være en funksjon
- Mål: Finne et element som evalueres til 1.
- Kvante løsning:



Grover's algoritme; II

- Hva er R?

$$R = \begin{pmatrix} 1 & 0 & 0 & ... \\ 0 & -1 & 0 & ... \\ 0 & 0 & -1 & ... \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix} = 2|0\rangle^{\otimes n}\langle 0|^{\otimes n} - I$$

- Hva er H$^{\otimes n}$RH$^{\otimes n}$?

$$H^{\otimes n}RH^{\otimes n} = 2(H|0\rangle\langle 0|H)^{\otimes n} - I = 2dd^* - I$$

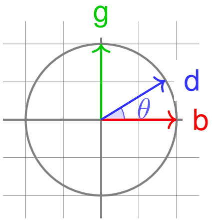
$$d = \frac{1}{\sqrt{2}^n}\Sigma_{z=0}^{2^n}|z\rangle$$

Grover's algoritme, III

- Definer to tilstander

$$g = \frac{1}{\sqrt{t}} \sum_{f(z)=1} |z\rangle$$

$$b = \frac{1}{\sqrt{2^n - t}} \sum_{f(z)=0} |z\rangle$$



- Velg θ

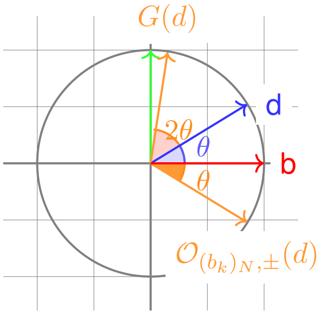
$$\theta = \arcsin\left(\frac{\sqrt{t}}{\sqrt{2^n}}\right)$$

$$d = \sin(\theta) g + \cos(\theta) b$$

Grover's algoritme; IV

- $\mathcal{O}_{f,\pm}$ er en refleksjon i planet $\mathbb{C}\{g,\ b\}$.

$$\mathcal{O}_{f,\pm}(g) = -g$$
$$\mathcal{O}_{f,\pm}(b) = b$$



Grover's algoritme; V

- Kjøretidsanalyse

$$G(d) = \sin(3\theta)g + \cos(3\theta)b$$
$$\implies G^k(d) = \sin((2k+1)\theta)g + \cos((2k+1)\theta)b$$

- Maksima når $\sin((2k+1)\theta) = 1$

$$k = \frac{\pi}{4\theta} - \frac{1}{2} \approx \lfloor \frac{\pi}{4\arcsin(\sqrt{t}/\sqrt{N})} \rfloor$$
$$p = \sin((1 + 2\lfloor \frac{\pi}{4\arcsin(\sqrt{t}/\sqrt{N})} \rfloor) \arcsin(\sqrt{t}/\sqrt{N}))$$

Grover's algoritme; V

- Kjøretidsanalyse

$$
\begin{aligned}
G(d) &= \sin(3\theta)g + \cos(3\theta)b \\
\implies G^k(d) &= \sin((2k+1)\theta)g + \cos((2k+1)\theta)b
\end{aligned}
$$

- $\sin(\sqrt{t}/\sqrt{N}) \approx \sqrt{t}/\sqrt{N}$ når $N \gg 1$.

$$
\begin{aligned}
k &= \lfloor \frac{\pi\sqrt{N}}{4\sqrt{t}} \rfloor \\
p &= \sin((1 + 2\lfloor \frac{\pi\sqrt{N}}{4\sqrt{t}} \rfloor)\frac{\sqrt{t}}{\sqrt{N}})
\end{aligned}
$$

Amplitudeforsterkningsteknikken

- Sannsynlighetforsterkning
  - Anta at A er en klassisk Monte Carlo algoritme
  - Anta at vi kan sjekke om en løsning er korrekt i polynom tid
  - La ψ_0 være inputet og $\psi = A(\psi_0)$ være et output
  - Anta at p er sannsynligheten for at ψ er et korrekt svar
  - Hvordan kan vi forbedre algoritmen og øke sjansen for at A gir oss riktig svar?

Amplitudeforsterkningsteknikken

- Sannsynlighetforsterkning
  - Anta at A er en klassisk Monte Carlo algoritme
  - Anta at vi kan sjekke om en løsning er korrekt i polynom tid
  - La ψ_0 være inputet og $\psi = A(\psi_0)$ være et output
  - Anta at p er sannsynligheten for at ψ er et korrekt svar
  - Hvordan kan vi forbedre algoritmen og øke sjansen for at A gir oss riktig svar?
  - Vi kjører A flere ganger, si n ganger.
  - Hvis $p \ll 1$ så gir $n = {}^1\!/_p$ et godt estimat for maksima.

Amplitudeforsterkningsteknikken

- Anta at A er en kvantealgoritme
- La ψ_0 være inputet og $\psi = A(\psi_0)$ være et output
- Anta at det finnes et faseorakel $\mathcal{O}_\pm$ som sjekker om outputet er korrekt
- Anta at p er sannsynligheten for at ψ er et korrekt svar
- Hvordan kan vi forbedre algoritmen og øke sjansen for at A gir oss riktig svar?

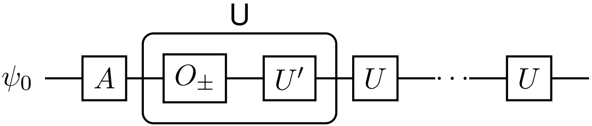
Amplitudeforsterkningsteknikken

- Algoritme A, input ψ_0, output ψ, faseorakel $\mathcal{O}_\pm$ og p
- Hvordan kan vi forbedre algoritmen og øke sjansen for at A gir oss riktig svar?

Amplitudeforsterkningsteknikken

- Algoritme A, input ψ_0, output ψ, faseorakel $\mathcal{O}_\pm$ og p
- Hvordan kan vi forbedre algoritmen og øke sjansen for at A gir oss riktig svar?

$$U' = 2|\psi\rangle\langle\psi| - I$$



Amplitudeforsterkningsteknikken

- Algoritme A, input ψ_0, output ψ, faseorakel $\mathcal{O}_\pm$ og p
- Hvordan kan vi forbedre algoritmen og øke sjansen for at A gir oss riktig svar?

$$\psi = \sum_{z:\{0,\ 1\}^n} \zeta_z |z\rangle$$

$$g = \frac{1}{\sqrt{p}} \sum_{f(z)=1} \zeta_z |z\rangle$$

$$b = \frac{1}{\sqrt{1-p}} \sum_{f(z)=0} \zeta_z |z\rangle$$

$$\theta = \arcsin(\sqrt{p})$$

$$k = \lfloor \frac{\pi}{4 \arcsin(\sqrt{p})} \rfloor \approx \lfloor \frac{\pi}{4\sqrt{p}} \rfloor$$

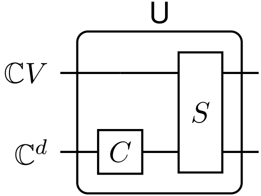
$$p' \approx \sin^2(\frac{\pi}{2} + \sqrt{p})$$

Kvantevandringer

- Generalisering av Grover's algoritme
- Hva er en graf? $G = (V, E)$; $\mathcal{H} = \mathbb{C}V$
- Lokale operatorer
- Komponenter til andre algoritmer
- Myntede vandringer
  - Position-coin notation
  - Arc notation
- Umyntede vandringer
- QSS

Position-coin notation

- d-regulær, d-kantkromatisk graf
- Fra enhver node, velger vi en farge og følger den
- $\mathcal{H} = \mathbb{C}V \otimes \mathbb{C}^d$



S er flip-flop operatoren

$$S^2 = I$$

C er coin operatoren

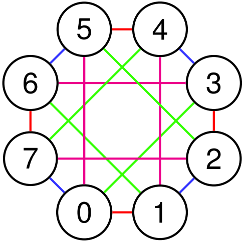
Position-coin notation

- d-regulær, d-kantkromatisk graf
- Fra enhver node, velger vi en farge og følger den
- $\mathcal{H} = \mathbb{C}V \otimes \mathbb{C}^d$

S er definert av fargeleggingen

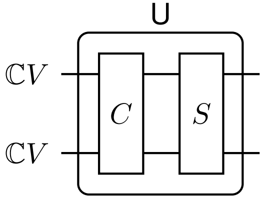
Vi kan velge C

$$C = H \otimes H$$



Arc notation

- Virker på generelle grafer
- Kan tolkes som en vandring på kantene istedenfor nodene
- $\mathcal{H} = \bigoplus_{v:V} \mathbb{C}\{u : V \mid (v, u) : E\} \simeq \bigoplus_{v:V} \mathbb{C}^{deg(v)}$
- $\mathcal{H} \subseteq \mathbb{C}V \otimes \mathbb{C}V$

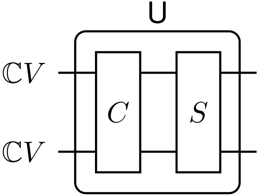


S er flip-flop operatoren

$$S^2 = I$$
$$S(v, u) = u \otimes v$$

Arc notation

- Virker på generelle grafer
- Kan tolkes som en vandring på kantene istedenfor nodene
- $\mathcal{H} = \bigoplus_{v:V} \mathbb{C}\{u : V \mid (v, u) : E\} \simeq \bigoplus_{v:V} \mathbb{C}^{deg(v)}$
- $\mathcal{H} \subseteq \mathbb{C}V \otimes \mathbb{C}V$



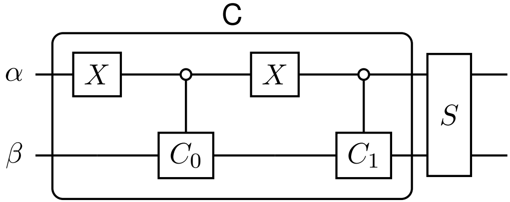
C er coin operatoren

For enhver $v : V$ har vi en lokal mynt C_v s.a.

$$C = \bigoplus_{v:V} C_v$$

Arc notation

- Virker på generelle grafer
- Kan tolkes som en vandring på kantene istedenfor nodene
- $\mathcal{H} = \bigoplus_{v:V} \mathbb{C}\{u : V \mid (v, u) : E\} \simeq \bigoplus_{v:V} \mathbb{C}^{deg(v)}$
- $\mathcal{H} \subseteq \mathbb{C}V \otimes \mathbb{C}V$
- Anta at $V = \{0,\ 1\}$, og at G er den komplette grafen

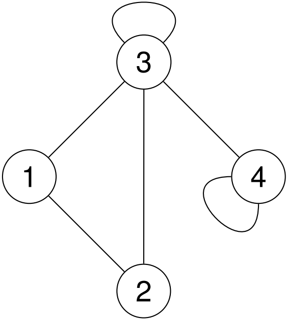


Arc notation

- Virker på generelle grafer
- Kan tolkes som en vandring på kantene istedenfor nodene
- $\mathcal{H} = \bigoplus_{v:V} \mathbb{C}\{u : V \mid (v,u) : E\} \simeq \bigoplus_{v:V} \mathbb{C}^{deg(v)}$
- $\mathcal{H} \subseteq \mathbb{C}V \otimes \mathbb{C}V$

Velg C som følger:

$$C_1 \simeq H$$
$$C_2 \simeq H$$
$$C_3 \simeq H \otimes H$$
$$C_4 \simeq H$$



Kvantemynter

- Hadamardmynten
  - $dim(\mathcal{H}_C) = 2^n$

$$H_M = H^{\otimes n}$$

  - $n = 2$

$$H_M = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

- Grovermynten
- Fouriermynten

Kvantemynter

- Hadamardmynten
- Grovermynten
  - $dim(\mathcal{H}_C) = n$

$$d = \frac{1}{\sqrt{n}} \sum_{i=0}^{n-1} |i\rangle$$

$$G_M = 2dd^* - I$$

  - Anta $n = 4$

$$G_M = \frac{1}{2} \begin{pmatrix} -1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 \\ 1 & 1 & 1 & -1 \end{pmatrix}$$

- Fouriermynten

Kvantemynter

- Hadamardmynten
- Grovermynten
- Fouriermynten
  - $dim(\mathcal{H}_C) = n$

$$F_M = F_n$$

  - La $\omega_{k,l} = e^{\frac{2\pi ikl}{n}}$

$$F_n = \frac{1}{\sqrt{n}} \left(\omega_{k,l}\right)_{(k,l):\{0,\dots,n-1\}\times\{0,\dots,n-1\}}$$

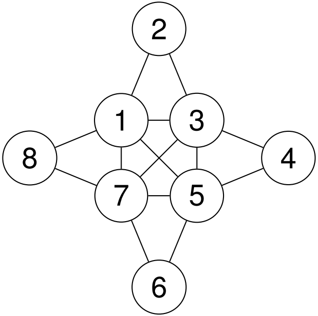
Staggered model

- Umyntet kvantevandring
- Bruker graftessellering for å definere U
- $\mathcal{H} = \mathbb{C}V$

$$\mathbb{C}V \;—\boxed{U}—$$

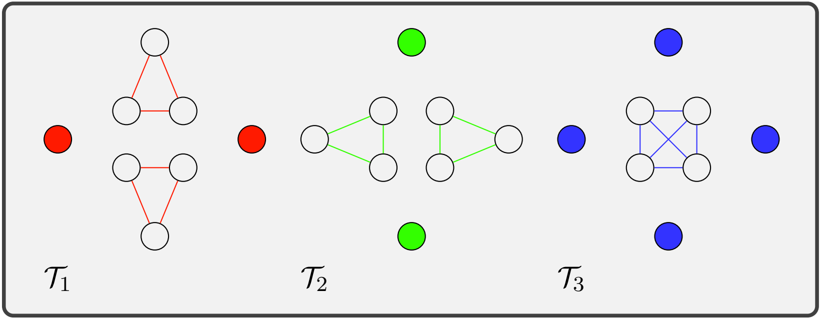
Staggered model

- Umyntet kvantevandring
- Bruker graftessellering for å definere U
- $\mathcal{H} = \mathbb{C}V$



Staggered model

- Umyntet kvantevandring
- Bruker graftessellering for å definere U
- $\mathcal{H} = \mathbb{C}V$



Staggered model

- Umyntet kvantevandring
- Bruker graftessellering for å definere U
- $\mathcal{H} = \mathbb{C}V$

$$\mathbb{C}V \;—\boxed{U}—$$

- $U = \circ_i H_{\mathcal{T}_i}$

$$H_{\mathcal{T}_i} = 2 \sum_{\alpha : \mathcal{T}_i} \alpha\alpha^* - I$$

Grensepunktet og quasi-periodisitet

- Hva skjer med kvantevandringen når $\lim_{k\to\infty} U^k(\psi_0)$?

Grensepunktet og quasi-periodisitet

- Hva skjer med kvantevandringen når $\lim_{k\to\infty} U^k(\psi_0)$?
- $||U^{k+1}(\psi_0) - U^k(\psi_0)||$ er konstant for alle k
- Grensen konverger kun om ψ_0 er et fikspunkt for U

Grensepunktet og quasi-periodisitet

- Hva skjer med kvantevandringen når $\lim_{k\to\infty} U^k(\psi_0)$?
- $||U^{k+1}(\psi_0) - U^k(\psi_0)||$ er konstant for alle k
- Grensen konverger kun om ψ_0 er et fikspunkt for U
- Finnes det en k slik at $U^k\psi_0 = \psi_0$?

Grensepunktet og quasi-periodisitet

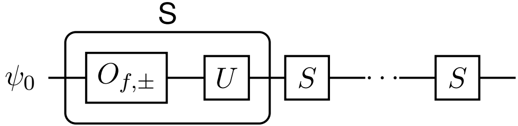
- Hva skjer med kvantevandringen når $\lim_{k\to\infty} U^k(\psi_0)$?
- $||U^{k+1}(\psi_0) - U^k(\psi_0)||$ er konstant for alle k
- Grensen konverger kun om ψ_0 er et fikspunkt for U
- Finnes det en k slik at $U^k\psi_0 = \psi_0$?
- Nei, dette gjelder ikke generelt
- Vi kan derimot finne en k slik at $||U^k\psi_0 - \psi_0|| < \epsilon$ for en gitt $\epsilon > 0$

$$U = \begin{pmatrix} e^{2\pi i\lambda_1} & 0 \\ 0 & e^{2\pi i\lambda_2} \end{pmatrix}.$$

- Tilnærm $\lambda_i \approx {}^{a_i}/_{b_i}$, deretter sett $k = b_1 b_2$

Quantum Spatial Search

- La $G = (V, E)$ og $f : V \to \{0,\ 1\}$ slik at nøyaktig 1 $v : V$ tilfredstiller $f(v) = 1$
- Hvordan kan vi finne v?



- Kjøretiden k er gitt ved å maksimere følgende funksjon

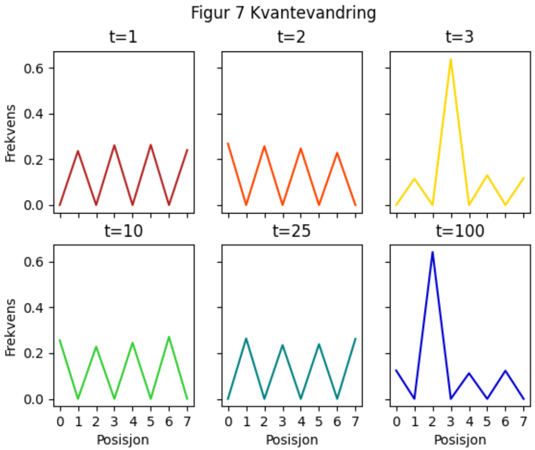
$$p(k) = |\langle v|S^k\psi_0\rangle|^2$$

- Grover er en optimal QSS algoritme

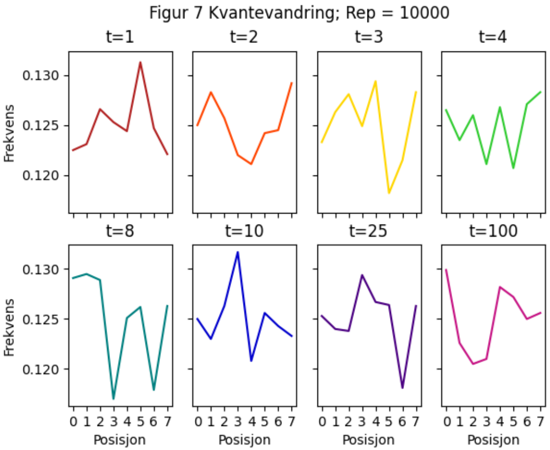
Kvantespråk

- Qiskit
- Q#
- Cirq
- Openql/Quantpy
- Quipper
- Quantum IO Monad

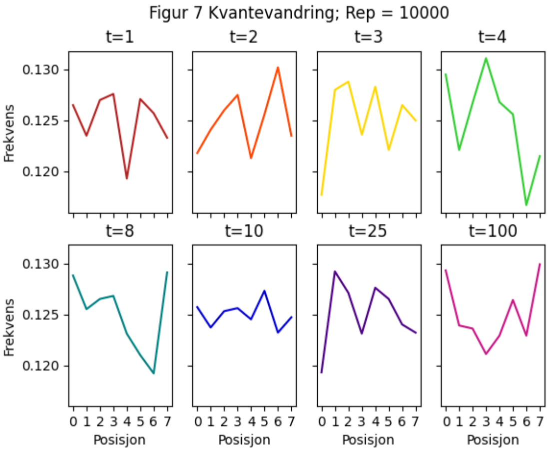
Position-coin simulering



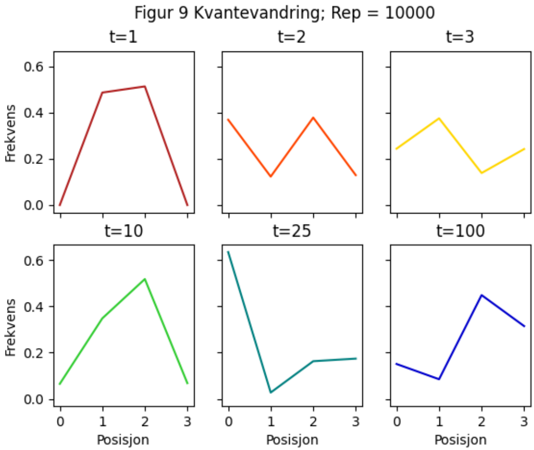
Position-coin simulering



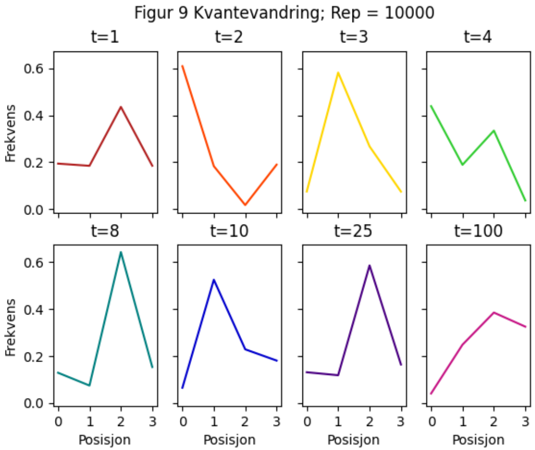
Position-coin simulering



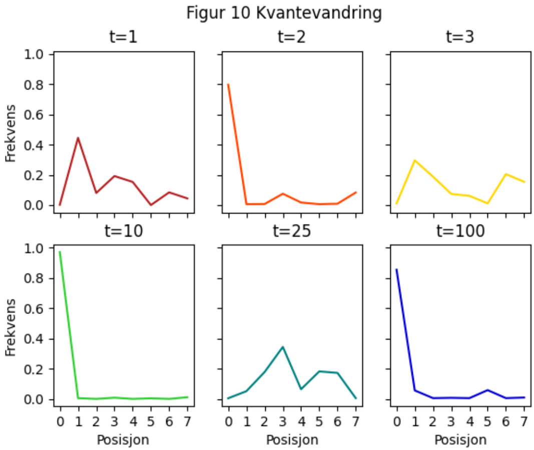
Arc simulering



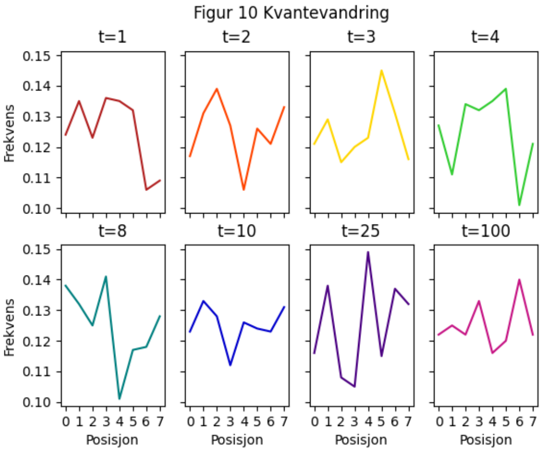
Arc simulering



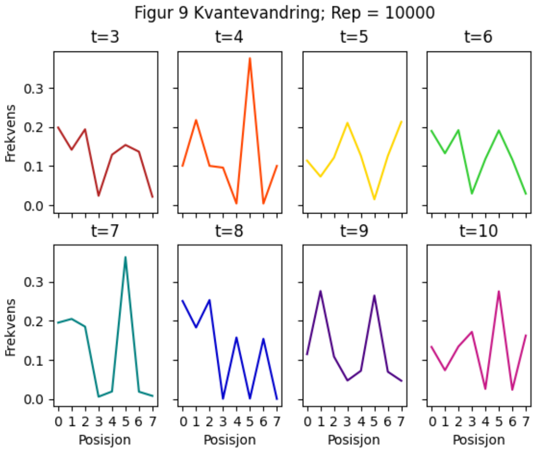
Staggered simulering



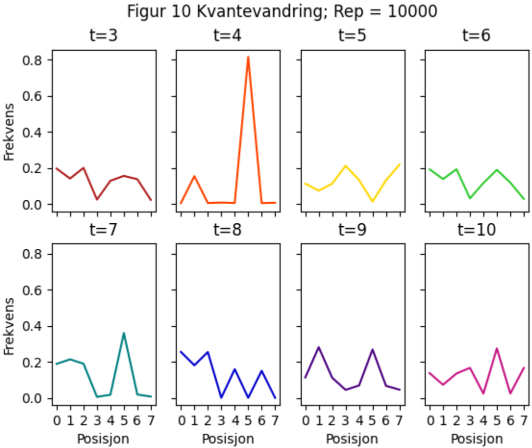
Staggered simulering



QSS simulering



QSS simulering



Hvor kan man gå videre?

- Szegedy vandring
- Kontinuerlige Kvantevandringer
- Flyt og elektriske nettverk
- Kriterier for optimalitet av kvantevandringer
- Kvantevandringer over grafer med mer struktur
- Hvordan bruke kvantevandringer til å løse problemer

NASJONAL SIKKERHETSMYNDIGHET

Thomas Wilskow Thorbjørnsen

Kvantevandringer

over endelige grafer