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

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

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

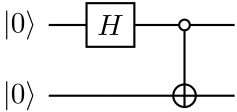
- Bits vs. Qubits
  $\{0,\ 1\}^n\ vs.\ \mathbb{C}\{0,\ 1\}^n = \mathbb{C}^{2^{\otimes n}}$
  $00 \vee 01 \vee 10 \vee 11\ vs.\ q = q_{00}|00\rangle + q_{01}|01\rangle + q_{10}|10\rangle + q_{11}|11\rangle$
- Logiske kvanteporter

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

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

Kvanteberegninger; II

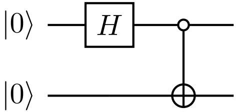
- Bell state



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

Kvanteberegninger; II

- Bell state

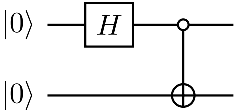


$$\iff CNOT \circ (H \otimes I)$$

- Universelle porter

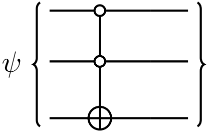
Kvanteberegninger; II

- Bell state



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

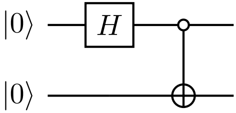
- Universelle porter
- Simulere klassiske beregninger



Toffoli

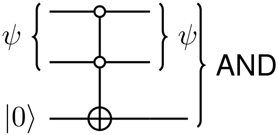
Kvanteberegninger; II

- Bell state



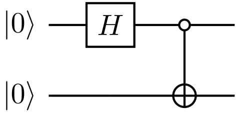
$$\iff CNOT \circ (H \otimes I)$$

- Universelle porter
- Simulere klassiske beregninger



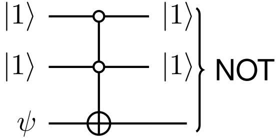
Kvanteberegninger; II

- Bell state



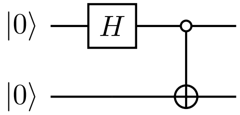
$$\iff CNOT \circ (H \otimes I)$$

- Universelle porter
- Simulere klassiske beregninger



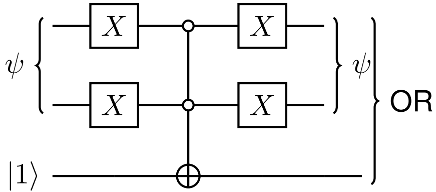
Kvanteberegninger; II

- Bell state

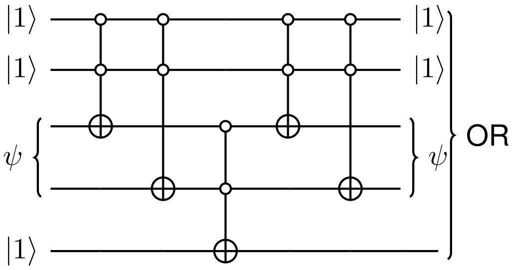


$$\iff CNOT \circ (H \otimes I)$$

- Universelle porter
- Simulere klassiske beregninger



Kvanteberegninger; III



Orakler

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

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

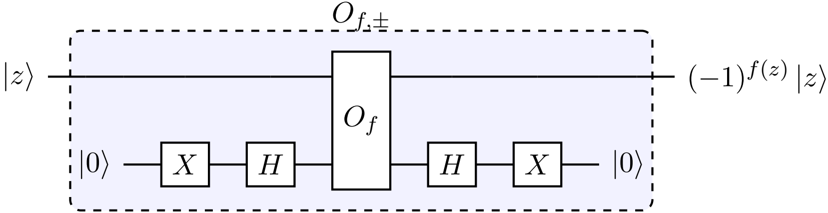
Orakler

- 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

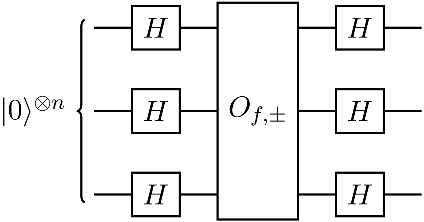
- Problemet:
  - La $f : \{0,\ 1\}^n \to \{0,\ 1\}$ være en funksjon som enten er konstant eller balansert (50% er 0 og 50% er 1).
- Mål: Finne ut om f er konstant eller balansert.

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

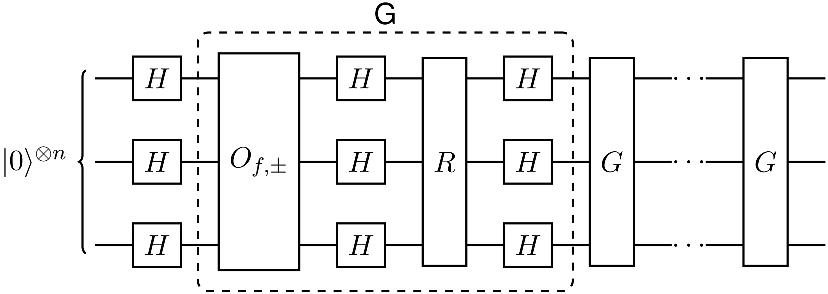
- Problemet:
  - La $f : \{0,\ 1\}^n \to \{0,\ 1\}$ være en funksjon
- Mål: Finne et element som evalueres til 1.

Grover's algoritme; I

- Problemet:
  - La $f : \{0,\ 1\}^n \rightarrow \{0,\ 1\}$ 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?

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

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

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

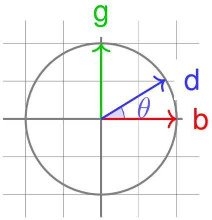
$$d = \frac{1}{\sqrt{2}^n}\Sigma_{z=0}^{2^n}|z\rangle$$

Grover's algoritme, III

- Definer to tilstander

$$g = \frac{1}{\sqrt{t}} \Sigma_{z \in \{0,\ 1\}^n | f(z)=1} |z\rangle$$

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



- Velg θ for effekt

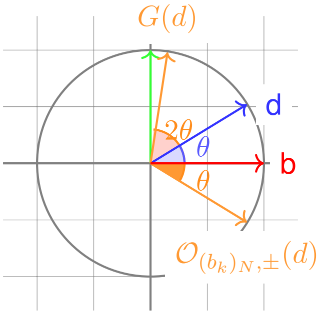
$$\theta = \arcsin\left(\frac{\sqrt{t}}{\sqrt{2^n}}\right)$$

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

Grover's algoritme; IV

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

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



Kvantevandringer

Litt om DSLer

Elektriske nettverk

NASJONAL
SIKKERHETSMYNDIGHET

Thomas Wilskow Thorbjørnsen

Kvantevandringer
over endelige grafer