Kvantedatamaskiner

to ortogonale tilst., f.eks : $|0\rangle = |\downarrow\rangle, |1\rangle = |\uparrow\rangle$

Qubit : $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

Hva kan vi gjøre med qubit'er ? 1) Unitær evolusjon $i\hbar \frac{d|\psi(t)\rangle}{dt} = H|\psi(t)\rangle$

$\Rightarrow$ $|\psi(t)\rangle = e^{\frac{-iHt}{\hbar}}|\psi(0)\rangle$

Husk h.av t

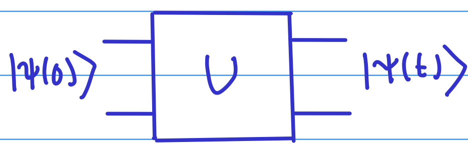
F.eks. kan $|\psi(0)\rangle$ bestå av to qubit'er:

$|\psi(0)\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$

En "boks"/port opererer med H tiden T:

$|\psi(t)\rangle = U|\psi(0)\rangle$, $U = e^{\frac{-iHt}{\hbar}}$

U er unitær : $U^\dagger U = e^{iHt/\hbar} e^{-iHt/\hbar} = 1$



2) Måling. Måling av $\alpha|0\rangle + \beta|1\rangle$ i basis $\{|0\rangle, |1\rangle\}$ gir "0" med $P = |\alpha|^2$ og "1" med $P = |\beta|^2$.

Deutsch-algoritmen:

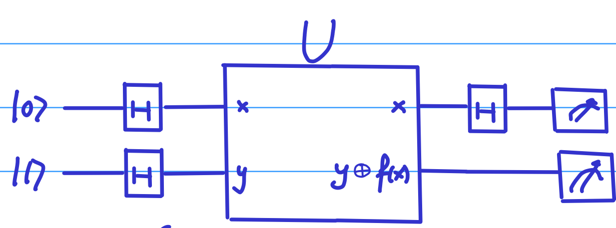
Anta $f(x)$ er en ukjent funksjon av en bit. Ønsker å finne $f(0) \oplus f(1)$.

4 muligheter:

x	$f_1(x)$	$f_2(x)$	$f_3(x)$	$f_4(x)$
0	0	1	0	1
1	0	1	1	0

Klassisk må vi da evaluere funksjonen to ganger, trenger $f(0)$ og $f(1)$.

Med kvantedatamaskin:



($\oplus$ betyr addisjon mod. 2)

$|0\rangle|0\rangle \xrightarrow{U} |0\rangle|0 \oplus f(0)\rangle$

$|0\rangle|1\rangle \xrightarrow{U} |0\rangle|1 \oplus f(0)\rangle$

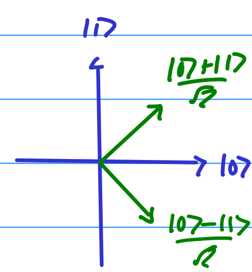
$|1\rangle|0\rangle \xrightarrow{U} |1\rangle|0 \oplus f(1)\rangle$

$|1\rangle|1\rangle \xrightarrow{U} |1\rangle|1 \oplus f(1)\rangle$

Hadamard H :

$|0\rangle \xrightarrow{H} \frac{|0\rangle + |1\rangle}{\sqrt{2}}$

$|1\rangle \xrightarrow{H} \frac{|0\rangle - |1\rangle}{\sqrt{2}}$



$\frac{|0\rangle + |1\rangle}{\sqrt{2}} \xrightarrow{H} |0\rangle$

$\frac{|0\rangle - |1\rangle}{\sqrt{2}} \xrightarrow{H} |1\rangle$

$$|0\rangle|1\rangle \xrightarrow{H\otimes H} \frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle-|1\rangle}{\sqrt{2}} = \frac{1}{2}\Big[|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|0\rangle - |1\rangle|1\rangle\Big]$$

$$\xrightarrow{U} \frac{1}{2}\Big[|0\rangle|0\oplus f(0)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|0\oplus f(1)\rangle - |1\rangle|1\oplus f(1)\rangle\Big]$$

$$= \begin{cases} \frac{1}{2}[|0\rangle+|1\rangle]\,|0\oplus f(0)\rangle - \frac{1}{2}[|0\rangle+|1\rangle]\,|1\oplus f(0)\rangle, & f(0)=f(1) \\ \frac{1}{2}[|0\rangle-|1\rangle]\,|0\oplus f(0)\rangle - \frac{1}{2}[|0\rangle-|1\rangle]\,|1\oplus f(0)\rangle, & f(0)\neq f(1) \end{cases}$$

$$= \begin{cases} \frac{|0\rangle+|1\rangle}{\sqrt{2}}\;\frac{|0\oplus f(0)\rangle - |1\oplus f(0)\rangle}{\sqrt{2}}, & f(0)=f(1) \\[2ex] \frac{|0\rangle-|1\rangle}{\sqrt{2}}\;\frac{|0\oplus f(0)\rangle - |1\oplus f(0)\rangle}{\sqrt{2}}, & f(0)\neq f(1) \end{cases}$$

$$\xrightarrow{H\otimes I} \begin{cases} |0\rangle \otimes \frac{|0\oplus f(0)\rangle - |1\oplus f(0)\rangle}{\sqrt{2}}, & f(0)=f(1) \\[2ex] |1\rangle \otimes \frac{|0\oplus f(0)\rangle - |1\oplus f(0)\rangle}{\sqrt{2}}, & f(0)\neq f(1) \end{cases}$$

Mål øverste qubit. Gir "0" hvis $f(0)=f(1)$ og "1" hvis $f(0)\neq f(1)$. Dvs. finner en <u>global</u> egenskap til f vha. <u>en</u> evaluering!

Kvantedatamaskiner er effektive til

- unyttige algortimer — 2019
- simulering av kvantesystemer — 2025 ?
- faktorisere store tall — 2035 ???
- søking i ustrukturerte datamengder

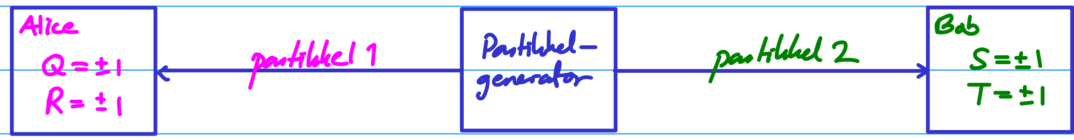
↓ år

CNOT: $|00\rangle \to |00\rangle$
$|01\rangle \to |01\rangle$
$|10\rangle \to |11\rangle$
$|11\rangle \to |10\rangle$

Realisere kvantedatamaskiner

Trengs:
- robust repr. av qubits
- universell familie av unitære transf., f.eks CNOT + enkelt-qubit-rotasjoner
- mulighet til å preparere en starttilstand, f.eks. $|0\rangle\otimes|0\rangle\otimes|0\rangle\otimes\ldots$
- målinger

Bells ulikhet – sammenfiltring



Alice og Bob måler to ulike partikkelegenskaper hver, Q, R, S, T.
Vi antar at partikkel 1 har objektive egenskaper Q og R.
partikkel 2 —— " —— S og T.

Se på $QS + RS + RT - QT = (Q+R)S + (R-Q)T$.
Siden $R, Q = \pm 1$, er enten $Q+R = 0$ eller $R-Q = 0$.
Gir $QS + RS + RT - QT = \pm 2$.

$$\underbrace{E}_{\text{forventningsverdi}}[QS + RS + RT - QT] = \sum_{q,r,s,t} p(q,r,s,t)(qs + rs + rt - qt) \leq \sum_{q,r,s,t} p(q,r,s,t) 2 = 2$$

Bells ulikhet: $\boxed{E[QS] + E[RS] + E[RT] - E[QT] \leq 2}$

Ikke tilfredsstilt av kvantemek.:

La partiklene være qubit'er, tilstand $|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$ (singlet)

La $Q = \sigma_z$ $\qquad S = \frac{-\sigma_z - \sigma_x}{\sqrt{2}}$

$R = \sigma_x$ $\qquad T = \frac{\sigma_z - \sigma_x}{\sqrt{2}}$

$$\langle QS \rangle = -\langle \psi | \sigma_z \otimes \frac{\sigma_z + \sigma_x}{\sqrt{2}} | \psi \rangle = -\frac{1}{2\sqrt{2}} \left[\langle 01| - \langle 10| \right] I \otimes (\sigma_z + \sigma_x) \left[|01\rangle + |10\rangle \right]$$

$$= -\frac{1}{2\sqrt{2}} \left[\langle 01| - \langle 10| \right] \left[-|01\rangle + |10\rangle + |00\rangle + |11\rangle \right] = \frac{1}{\sqrt{2}}$$

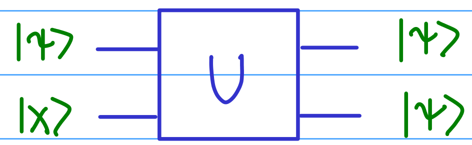
Tilsvarende: $\langle RS \rangle = \langle RT \rangle = -\langle QT \rangle = \frac{1}{\sqrt{2}}$.

Gir $\langle QS \rangle + \langle RS \rangle + \langle RT \rangle - \langle QT \rangle = 2\sqrt{2} > 2$!!!

Eksperimenter gir $\approx 2\sqrt{2}$. Så kvantemek. virker å være rett, mens minst en av antagelsene bak Bells ulikhet er feil.

- Realisme: Partiklene har objektive egenskaper uavh. av observasjon
- Lokalitet: Alice' måling påvirker ikke Bobs måleresultat.

Kvanteinformasjon kan ikke klones / kopieres perfekt



Klonemaskinen virker for $|\psi_1\rangle$ og for $|\psi_2\rangle$:

$$|\psi_1\rangle \otimes |\chi\rangle \xrightarrow{U} |\psi_1\rangle \otimes |\psi_1\rangle$$
$$|\psi_2\rangle \otimes |\chi\rangle \xrightarrow{U} |\psi_2\rangle \otimes |\psi_2\rangle$$

Ta innerproduktet:

$$\overbrace{\langle\psi_1| \otimes \langle\psi_1| \quad |\psi_2\rangle \otimes |\psi_2\rangle}^{\langle\psi_1|\psi_2\rangle\langle\psi_1|\psi_2\rangle} = \langle\psi_1|\otimes\langle\chi| \overbrace{U^\dagger U}^{I} |\psi_2\rangle\otimes|\chi\rangle$$
$$= \langle\psi_1|\psi_2\rangle\langle\chi|\chi\rangle = \langle\psi_1|\psi_2\rangle$$

Så $\langle\psi_1|\psi_2\rangle = \langle\psi_1|\psi_2\rangle^2 \Rightarrow \langle\psi_1|\psi_2\rangle = 0$ eller 1.
Altså kopimaskinen virker bare for like eller ortogonale tilstander, ikke vilkårlige.

Kvantekryptering / kvante-nøkkeldistribusjon

Alice $\boxed{\text{Eve}}$ Bob

Genererer sammenfiltrede partikler

1) Det genereres sammenfiltrede partikkelpar $\frac{|01\rangle - |10\rangle}{\sqrt{2}}$ (kan pessimistisk anta at dette kontrolleres av en avlytter Eve)
2) Alice og Bob ofrer noen tilfeldige par, og finner ut om Bells ulikhet er brudt.
3) Måler resten, Alice' resultater utgjør nøkkelen. Bob inverterer sine bits.

I praksis må de ofre noen flere bits til feilkorrigering og "privacy amplification", avhengig av resultatet i 2).