En dag med kvanteinformation

Johannes Borregaard, Robert H. Jonsson
QMATH – Københavns Universitet

23 November 2018

Velkommen til QMATH!

Dette er et sæt noter, som vi vil benytte til at introducere jer til nogle af de fascinerende aspekter af kvanteinformationsteori. Vores mål er at vise jer nogle af de basale koncepter såsom qubits og kvantegates samt deres matematiske fomuleringer. Til slut i dag vil I selv lave beregninger på basale kvantekredsløb og endda vise at kvanteinformation ikke kan kopieres.

Den matematik vi vil beskæftige os med omhandler vektorrum, hvilket er et af matematikkens mest fundamentale emner. Vektorrum bliver anvendt i alt fra moderne machine learning til beskrivelsen af kvanteinformation. Dette er grunden til, at det er et af de første matematikkurser på universitet og stort set alle naturvidenskabelige retninger indeholder (i hvert fald lidt af) det. I dag vil vi kun se på de mest basale egenskaber ved vektorer, som nogle af jer måske allerede kender.

Et par kommentarer omkring disse noter:

- Alle matematiske definitioner og redskaber vil såvidt muligt blive introduceret i afsnittene "Matematisk værktøj". Disse afsnit er efterfulgt af "Hands on" afsnittene, hvor vi bruger de matematiske værktøj til at undersøge kvanteinformation. Som navnet antyder, indeholder disse afsnit en række øvelser, så I får en form for learning-by-doing oplevelse. Vi håber, at dette vil føre til en masse spændende diskussioner og spørgsmål i løbet af dagen.
- Der er selvfølgelig mange flere spændende emner inden for kvanteinformationsteori, end vi kan nå at berøre i dag. Vi har også valgt at begrænse os til de reelle tal i dag, selvom det faktisk er nødvendigt at udvide til de komplekse tal for en komplet beskrivelse af kvanteinformation. Vi har indsat fodnoter, der beskriver, hvor man skal være opmærksom på, at komplekse tal er nødvendige for en komplet beskrivelse. Dette er kun ment som en hjælp i jeres videre studier, og I behøver ikke bekymre jer videre om det i dag.

1 Matematisk værktøj: Vektorer

Den første slags vektorer man stifter bekendtskab med er typisk søjlevektorer. I dag vil vi især benytte *to-vektorer*, dvs., søjlevektorer med to tal

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}, \quad \dots$$

Generelt kan vi beskrive en to-vektor $\vec{x}$ som

$$\vec{x} = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

med to arbitrære tal $x_0, x_1 \in \mathbb{R}$[1].

[1] For en komplet beskrivelse er det nødvendigt med komplekse tal.

1.1 Addition

To vektorer kan lægges sammen til en ny vektor. Lad $\vec{x}$ og $\vec{y}$ være to-vektorer, da er

$$\vec{x}+\vec{y}=\begin{pmatrix}x_0\\x_1\end{pmatrix}+\begin{pmatrix}y_0\\y_1\end{pmatrix}=\begin{pmatrix}x_0+y_0\\x_1+y_1\end{pmatrix}.$$

For eksempel,

$$\begin{pmatrix}1\\2\end{pmatrix}+\begin{pmatrix}3\\4\end{pmatrix}=\begin{pmatrix}1+3\\2+4\end{pmatrix}=\begin{pmatrix}4\\6\end{pmatrix}.$$

1.2 Skalar multiplikation

Enhver vektor kan ganges med et tal.[2] Lad $r\in\mathbb{R}$ være et tal og $\vec{x}$ en to-vektor, da er

$$r\vec{x}=r\begin{pmatrix}x_0\\x_1\end{pmatrix}=\begin{pmatrix}rx_0\\rx_1\end{pmatrix}.$$

For eksempel,

$$\frac{1}{3}\begin{pmatrix}2\\3\end{pmatrix}=\begin{pmatrix}\frac{1}{3}\cdot 2\\\frac{1}{3}\cdot 3\end{pmatrix}=\begin{pmatrix}\frac{2}{3}\\1\end{pmatrix}.$$

Bemærk, at vi ofte udelader gange-symbolet "$\cdot$" i skalar multiplikation.

1.3 Skalarprodukt

Skalarproduktet er hvor to vektorer ganges sammen til et tal. Skalarproduktet for to-vektorer er defineret ved som følger[3]. Lad $\vec{x},\vec{y}$ være to-vektorer, da er skalarproduktet

$$\vec{x}\cdot\vec{y}=\begin{pmatrix}x_0\\x_1\end{pmatrix}\cdot\begin{pmatrix}y_0\\y_1\end{pmatrix}=x_0y_0+x_1y_1.$$

To vektorer siges at være ortogonale (vinkelrette på hinanden), hvis deres skalarproduktet er nul. For eksempel,

$$\begin{pmatrix}1\\1\end{pmatrix}\cdot\begin{pmatrix}1\\-1\end{pmatrix}=1\cdot 1+1\cdot(-1)=0.$$

1.4 Vektornorm

Normen af en vektor er et mål for dens længde. Kvadratet af normen er skalarproduktet af vektoren med den selv. Det betyder, at normen $\|\vec{x}\|$ af en to-vektor $\vec{x}$ er

$$\|\vec{x}\|=\sqrt{\vec{x}\cdot\vec{x}}=\sqrt{(x_0)^2+(x_1)^2}.$$

For eksempel,

$$\left\|\begin{pmatrix}3\\-4\end{pmatrix}\right\|=\sqrt{3^2+(-4)^2}=\sqrt{25}=5.$$

Hvis vi dividerer en vektor $\vec{x}$ med dens norm $\|\vec{x}\|$ får vi en ny vektor

$$\vec{y}=\frac{1}{\|\vec{x}\|}\vec{x},$$

som har norm $\|\vec{y}\|=1$. Dette kaldes at *normalisere* en vektor.

[2] Generelt kan enhver vektor ganges med en skalar. En skalar har en størrelse, men ingen retning. I vores sammenhæng svarer dette til et tal.

[3] For en komplet beskrivelse skal skalarproduktet erstattes af det indre produkt $\vec{x}\cdot\vec{y}=\overline{x_0}y_0+\overline{x_1}y_1$. Her er $\overline{x_0}$ den kompleks konjugerede af x_0.

1.5 *At konstruere ortogonale vektorer

For en arbitrær to-vektor $\vec{x} = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$ kan vi definere den ortogonale vektor $\vec{x}^{\perp} = \begin{pmatrix} x_1 \\ -x_0 \end{pmatrix}$[4] . Det ses at de to er ortogonale ved

$$\vec{x} \cdot \vec{x}^{\perp} = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ -x_0 \end{pmatrix} = x_0 x_1 - x_1 x_0 = 0.$$

Den ortogonale vektor har samme norm som den originale vektor

$$\|\vec{x}\| = \left\|\vec{x}^{\perp}\right\|.$$

2 Hands on: En qubit

I klassiske informationsteori kan en bit kun være i én ud af to mulige tilstande: Den kan enten have værdien '0', eller værdien '1'. I kvanteinformationsteori har en qubit to kvantetilstande, der svarer til disse klassiske bittilstande. Vi betegner dem med såkaldte *kets*:

$$'0' \leftrightarrow |0\rangle \text{ and } '1' \leftrightarrow |1\rangle .$$

En qubit kan dog også være i mange andre tilstande. Faktisk er der uendelig mange qubittilstande.

2.1 Kvantetilstande er normaliserede vektorer

En kvantetilstand kan repræsenteres af en vektor med norm 1, hvilket vi vil kalde for en normaliseret vektor. Dette betyder at enhver qubittilstand kan beskrives som en normaliseret to-vektor. Til dette formål definerer vi

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

To yderligere tilstande, der oftes bruges i kvanteinformation, er

$$|+\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle + |1\rangle\right), \qquad |-\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle - |1\rangle\right).$$

Øvelse: Tilstandene $|+\rangle$ og $|-\rangle$ kan også skrives som to-vektorer. Udfyld hullerne i de følgende ligninger:

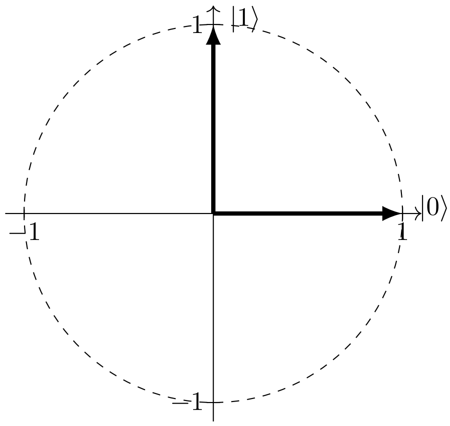
$$|+\rangle \equiv \frac{1}{\sqrt{}} \begin{pmatrix} \\ 1 \end{pmatrix}, \qquad |-\rangle \equiv \frac{1}{\sqrt{}} \begin{pmatrix} 1 \\ \end{pmatrix}$$

Øvelse*: Find det tal der skal ganges på to-vektoren $\begin{pmatrix} 3 \\ 4 \end{pmatrix}$ således at den repræsenterer en kvantetilstand. Dette kaldes at normalisere vektoren.

Øvelse: Siden qubits kan repræsenteres af vektorer med norm 1, kan vi visualisere dem på en enhedscirkel[5] . Herunder kan du se $|0\rangle$ og $|1\rangle$ indtegnet. Indtegn selv $|+\rangle$, $|-\rangle$ og den normaliserede vektor fra foregående øvelse.

[4] I tilfælde af en kompleks to-vektor definerer man $\vec{x}^{\perp} = \begin{pmatrix} \overline{x_1} \\ -\overline{x_0} \end{pmatrix}$.

[5] Normaliserede komplekse to-vektorer kan afbildes på en enhedssfære, hvilket kaldes for en *Bloch sfære*.



2.2 Målesandsynligheder er skalarprodukter

Når vi måler en qubit, tjekker vi, hvilken tilstand den er i. Antag at en qubit er i tilstanden

$$|\psi\rangle \equiv \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix}.$$

En måling tester nu om denne qubit er i en arbitrær tilstand

$$|\phi\rangle \equiv \begin{pmatrix} \phi_0 \\ \phi_1 \end{pmatrix}.$$

Resultatet af denne måling kan være JA. Sandsynligheden for dette er givet ved skalarproduktet:

$$P(\phi|\psi) = |\langle \phi \,|\psi \,\rangle|^2 = \left| \begin{pmatrix} \phi_0 \\ \phi_1 \end{pmatrix} \cdot \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix} \right|^2 = |\phi_0\psi_0 + \phi_1\psi_1|^2 .$$

Her har vi har benyttet *ket-bra* notationen for et skalarprodukt $\langle \phi \,|\psi \,\rangle$. Hvis vi får svaret NEJ betyder det at målingen viste at vores qubit var i den ortogonale tilstand [6]

$$\left|\phi^\perp\right\rangle \equiv \begin{pmatrix} \phi_0 \\ \phi_1 \end{pmatrix}^\perp = \begin{pmatrix} \phi_1 \\ -\phi_0 \end{pmatrix}.$$

(Du kan overbevise dig selv om, at der altid gælder, at $1 = P(\phi|\psi) + P(\phi^\perp|\psi)$.) Efter en måling svarer qubittilstanden altid til måleresultatet. En måling ændrer med andre ord tilstanden af en qubit.

Øvelse: Udfyld nedenstående skema ved at beregne sandsynligheden for at måle en qubit i tilstandede til venstre når den oprindeligt var i de øverste tilstande *(Du kan gøre det nemmere for dig selv ved at huske på at alle qubittilstande har norm 1 og ved at overbevise dig om at $P(\phi|\psi) = P(\psi|\phi)$.)* Hvorfor summer sandsynlighederne for at måle en qubit i enten $|0\rangle$ eller $|1\rangle$ (eller $|+\rangle$ eller $|-\rangle$) til 1?

Målesandsynlighed $P(\phi\|\psi) = \|\langle \phi \,\|\psi \,\rangle\|^2$					
	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$	$\|\beta\rangle \equiv \frac{1}{5}\begin{pmatrix} 3 \\ 4 \end{pmatrix}$
$\langle 0\|$					
$\langle 1\|$					
$\langle +\|$					
$\langle -\|$					
$\langle \beta\|$					

[6] Du kan verificere, at vi altid har at $1 = P(\phi|\psi) + P(\phi^\perp|\psi)$.

Øvelse: Antag at vi ved en måling finder en qubit i tilstand $|1\rangle$. Hvilke tilstande i ovenstående skema kunne have beskrevet denne qubits originale tilstand før målingen? Hvad er den eneste tilstand, vi med sikkerhed kan sige, ikke beskrev den originale tilstand?

Øvelse*: Alice måler på en qubit der oprindelig er i tilstand $|1\rangle$ og får resultatet $|+\rangle$. Efter hendes måling sender hun sin qubit videre til Bob, som måler, om den er i tilstand $|1\rangle$. Hvilket resultat kan Bob få? Hvad er målesandsynlighederne?

3 Matematisk værktøj: Matricer

En kvantecomputer foretager beregninger ved at manipulere den information, der er gemt i dens qubits. Dette er matematisk beskrevet ved matricer der virker på to-vektorene. En 2×2-matrix A består af 4 tal $a_{00}, a_{01}, a_{10}, a_{11}$ arrangeret i en tabel

$$A = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix}$$

Vi kan lade en 2×2-matrix virke på en to-vektor $\vec{v} = \begin{pmatrix} v_0 \\ v_1 \end{pmatrix}$ og få en ny to-vektor defineret ved

$$A\vec{v} = \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} v_0 \\ v_1 \end{pmatrix} = \begin{pmatrix} a_{00}v_0 + a_{01}v_1 \\ a_{10}v_0 + a_{11}v_1 \end{pmatrix}.$$

Bemærk, at den første søjle af matricen giver den to-vektor, som vi får ved at lade den virke på to-vektoren $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$. Tilsvarende giver den anden søjle den vektor, vi får ved at virke på $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$:

$$\begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_{00} \\ a_{10} \end{pmatrix}, \quad \begin{pmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a_{01} \\ a_{11} \end{pmatrix}$$

4 Hands on: At rotere qubittilstande

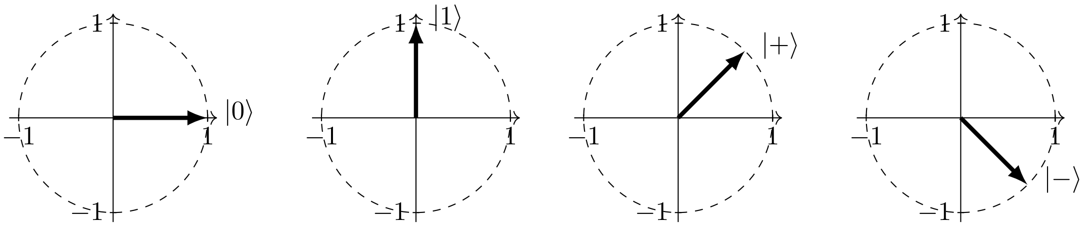
De elementære operationer, en kvantecomputer kan udføre på en qubit, kaldes for kvantegates. Den første enkelt-qubit kvantegate ci definerer kaldes for en *Hadamard gate*.

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

Øvelse: Hvilke tilstande får vi ved at virke med en Hadamard gate i nedenstående tilfælde?

$$H|0\rangle = \quad , \quad H|1\rangle = \quad , \quad H|+\rangle = \quad , \quad H|-\rangle =$$

Visualiser hvad en Hadamard gate gør i nedenstående cirkel diagrammer.



Øvelse: Vi definerer en enkelt-qubit rotationsgate som

$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix},$$

hvor $\theta = 0...2\pi$. Hvad sker der med en qubit i tilstand $|0\rangle$ når R_θ virker på den?

$$R_\theta |0\rangle \equiv \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} =$$

Hvordan ser denne tilstand ud i ket-notation?

$$R_\theta |0\rangle = \qquad\qquad |0\rangle + \qquad\qquad |1\rangle$$

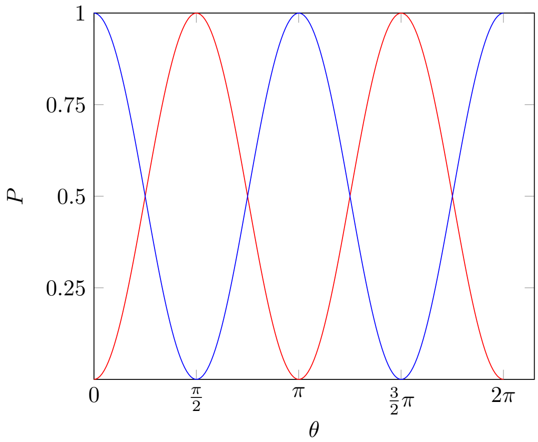
Øvelse: Målinger med hensyn til tilstandende $|0\rangle$ og $|1\rangle$ forekommer meget ofte i kvanteinformationsteori. Fra formlen omkring målesandsynligheder følger, at sandsynligheden for at finde en tilstand

$$|\psi\rangle = \psi_0 |0\rangle + \psi_1 |1\rangle \equiv \begin{pmatrix} \psi_0 \\ \psi_1 \end{pmatrix}$$

i en af tilstandende $|0\rangle$ og $|1\rangle$ er bestemt ved kvadraterne af absolutværdierne af koefficienterne ψ_0, ψ_1:

$$P(0|\psi) = |\psi_0|^2, \qquad P(1|\psi) = |\psi_1|^2$$

Lad os nu foretage en måling af qubittilstanden $R_\theta |0\rangle$. Hvilken af nedenstående grafer viser sandsynligheden for at målingen viser tilstanden $|1\rangle$? Hvilken viser sandsynligheden for at målingen viser tilstanden $|0\rangle$? Kan du beskrive funktionerne bag den røde og blå graf?



Det eneste krav, for at en matrix repræsenterer en kvantegate er, at den transformerer qubittilstande til qubittilstande. Det betyder, at hvis matricen virker på en vektor med norm 1 skal den resulterende vektor også have norm 1. Sådanne matricer kaldes for *unitære*.
Der er mange andre enkelt-qubit gates udover ovenstående Hadamard gate H og rotations-gate R_θ. Det er dog muligt at vise, at alle disse kan skrives som en kombination af H og R_θ[7].

5 Matematisk værktøj: Tensorprodukt

En kvantecomputer vil bestå af mange qubits. For at beskrive tilstanden af flere qubtis har man brug for vektorer med mere end to tal. Til dette formål benytter man et tensorprodukt.

Givet to to-vektorer $\vec{x} = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$ and $\vec{y} = \begin{pmatrix} y_0 \\ y_1 \end{pmatrix}$ definerer vi tensorproduktet som fire-vektoren

$$\vec{x} \otimes \vec{y} = \begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{pmatrix}.$$

Fire-vektorer kan lægges sammen, ganges med en skalar og har skalarprodukt og norm fuldsændig ligesom vi har diskuteret det for to-vektorer. Definitionerne udvides på en ligefrem måde, akkurat som man ville forvente.

[7] For komplekse vektorrum er der dog flere rotationsmatricer end R_θ.

6 Hands on: To-qubittilstande og sammenfiltring

Forestil dig at Alice har en qubit i sit laboratorium som er i en eller anden arbitrær tilstand. Bob kommer nu og giver Alice en anden qubit i en anden tilstand. Hvilken tilstand og tilsvarende fire-vektor beskriver nu begge qubits?

Hvis de to qubits ikke er korrelerede kan deres fælles tilstand beskrives ved tensorproduktet af deres repræsentative to-vektorer. For eksempel, de fire tilstande vi kan have for to qubits der hver især er i tilstand $|0\rangle$ eller $|1\rangle$, er:

$$|0\rangle_A \otimes |0\rangle_B \equiv \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \quad |0\rangle_A \otimes |1\rangle_B \equiv \begin{pmatrix}1\\0\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\1\\0\\0\end{pmatrix},$$

$$|1\rangle_A \otimes |0\rangle_B \equiv \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \quad |1\rangle_A \otimes |1\rangle_B \equiv \begin{pmatrix}0\\1\end{pmatrix} \otimes \begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

Disse fire tilstande svarer til de fire forskellige tilstande som to klassiske bits kan være i: '00','01','10' og '11'.

Øvelse: To qubits kan selvfølgelig være i mange flere tilstande end de ovenstående fire. For eksempel kan Alica have sin qubit i tilstand $|+\rangle$ mens Bob har sin i tilstand $|0\rangle$. Eller begge kan have deres qubits i tilstand $|+\rangle$. Hvad er de tilsvarende fire-vektorer?

$$|+\rangle_A \otimes |0\rangle_B \equiv \qquad\qquad\qquad , \quad |+\rangle_A \otimes |+\rangle_B \equiv$$

De to-qubit tilstande vi har set på indtil videre kaldes for separable tilstande. Der findes dog to-qubittilstande som ikke kan skrives som et simpelt tensorprodukt. Disse kaldes for *sammenfiltrede* tilstande og et et godt eksempel på det, der gør kvantefysik så forskellig fra klassisk fysik.

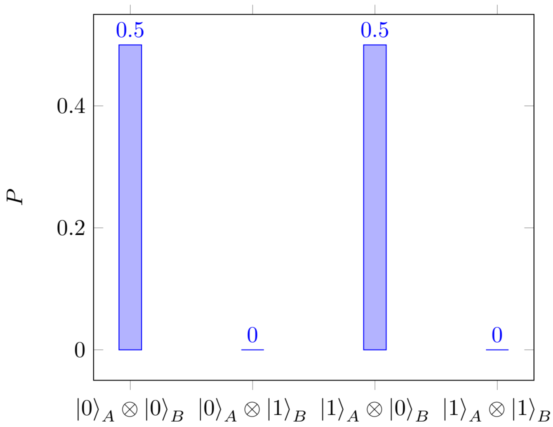
Øvelse: Betragt tilstanden

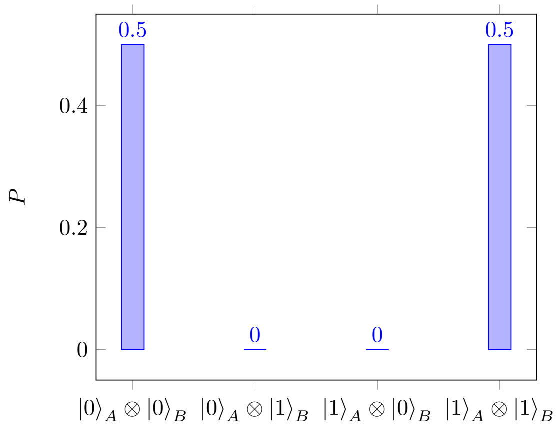
$$\left|\Psi^+\right\rangle = \frac{1}{\sqrt{2}} |0\rangle_A \otimes |0\rangle_B + \frac{1}{\sqrt{2}} |1\rangle_A \otimes |1\rangle_B \equiv \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\0\end{pmatrix} + \begin{pmatrix}0\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix}.$$

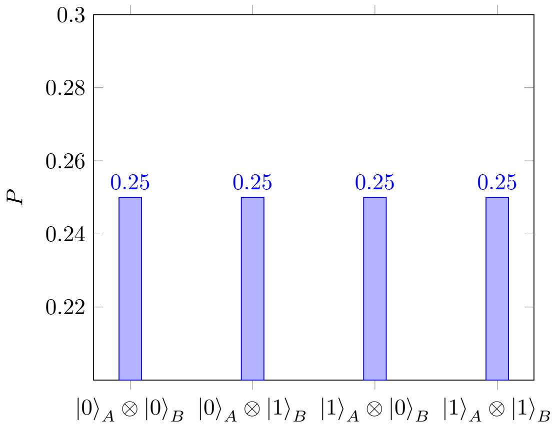
Tjek at denne fire-vektor repræsenterer en kvantetilstand, dvs. at den har norm 1. Hvis vi måler de to qubits, hvad er så sandsynlighederene for at finde dem i hver af de fire tilstande $|0\rangle_A \otimes |0\rangle_B$, $|0\rangle_A \otimes |1\rangle_B$, $|1\rangle_A \otimes |0\rangle_B$, and $|1\rangle_A \otimes |1\rangle_B$?

$$P_{00} = \qquad , P_{01} = \qquad , P_{10} = \qquad , P_{11} =$$

Øvelse: Hvilke af nedenstående histogrammer viser målesandsynlighederne, der svarer til tilstandede $|+\rangle_A \otimes |+\rangle_B$, $|+\rangle_A \otimes |0\rangle_B$ og $|\Psi^+\rangle$?



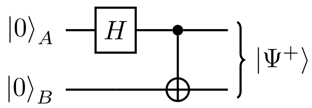




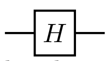
7 Hands on: Et kvantekredsløb

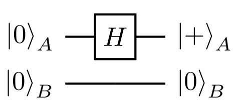
I dette afsnit samler vi op på alt det vi har beskæftiget os med indtil videre ved at designe et kvantekredsløb, der producerer tilstanden $|\Psi^+\rangle$. Et kvantekredsløb er en teoretikers byggeklods for en kvantecomputer.

Det kredsløb vi ser på er:

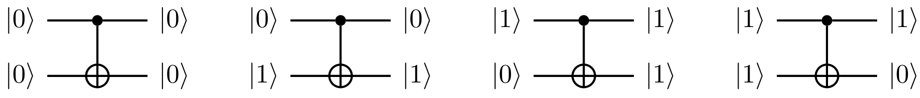


Man læser et kvantekredsløb fra venstre mod højre: Til venstre kommer to qubits repræsenteret ved linier ind. Begge qubits er i tilstand $|0\rangle$. Dette betyder, at to-qubittilstanden er $|0\rangle_A \otimes |0\rangle_B$. Til højre kan vi se, at de to qubits kommer ud i den sammenfiltrede tilstand $|\Psi^+\rangle$. For at forstå hvad der sker inde i kredsløbet, skal vi se nærmere på kredsløbselementerne.

Det første, der sker i kredsløbet, er, at gaten  virker på den øverste qubit. Dette symbol repræsenterer en Hadamard gate, og vi har allerede udregnet, at $H|0\rangle = |+\rangle$. Dette betyder at efter den første gate er de to qubits i tilstanden $|+\rangle_A \otimes |0\rangle_B$.



Det næste, der sker, er en to-qubit gate. Denne gate virker simultant på begge qubits. Dette gør, at den kan ændre deres to-qubittilstand på mange flere måder end individuelle enkelt-qubit gates kan. Den gate, der bliver brugt her, er en *controlled NOT*-gate eller *CNOT*-gate.

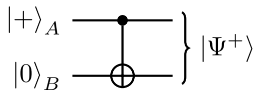


Dens virkning kan ses ved at kigge på de fire to-qubittilstande $|0\rangle_A \otimes |0\rangle_B$, $|0\rangle_A \otimes |1\rangle_B$, $|1\rangle_A \otimes |0\rangle_B$ og $|1\rangle_A \otimes |1\rangle_B$. Hvis den første qubit er i tilstand $|0\rangle_A$ gør den ingenting, men hvis den første qubit er i tilstand $|1\rangle_A$ bytter den om på værdien af den anden bit $|0\rangle_B \leftrightarrow |1\rangle_B$.

Øvelse: Hvilken af nedenstående 4×4-matricer repræsenterer en CNOT gate?

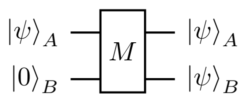
$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Øvelse: Vis at den anden del af kvantekredsløbet producerer den sammenfiltrede tilstand $|\Psi^+\rangle$ ved at lade CNOT-matricen virke på fire-vektoren for $|+\rangle_A \otimes |0\rangle_B$.



8 Et par sidste kommentarer: Kvanteinformation kan ikke kopieres!

Beregningerne som I lige har lavet kan faktisk bruges til at bevise, at kvanteinformation ikke kan kopieres. Dette vil sige, at det er umuligt at kontruere en kvantekopieringsmaskine, der kan kopiere arbitrære qubits. Hvis vi ser påto qubits betyder dette, at der ikke findes et kvantekredsløb der tager en qubit i en ukendt tilstand $|\psi\rangle_A$, den "originale" qubit, og en anden qubit i tilstanden $|0\rangle_B$, en "kopi" qubit og udsender de to qubits i tilstanden $|\psi\rangle_A \otimes |\psi\rangle_B$:



Grunden til dette er, at et sådant kvantekredsløb ville skulle kunne repræsenteres ved en matrix M, som alle andre kvantekredsløb kan. En sådan matrix skal have en egenskab som vi har benyttet indtil videre, men ikke har diskuteret explicit endnu. Denne egenskab er, at matricens virkning på en vektor skal være *linær*. Dette betyder:

- Når en matrix M virker på en vektor $\vec{z}$ som er en sum af to vektorer $\vec{z} = \vec{x} + \vec{y}$ skal den resulterende vektor være lig summmen af de to vektorer vi får ved at lade M virke på $\vec{x}$ og $\vec{y}$ separat:

$$M\vec{z} = M(\vec{x} + \vec{y}) = M\vec{x} + M\vec{y}$$

- Når en matrix virker på en vektor $\vec{w} = r\vec{v}$ som er fået ved at gange et tal r på en anden vektor $\vec{v}$ skal den resulterende vektor være den samme, som hvis vi lader M virker på $\vec{v}$ og derefter ganger med r.

$$M\vec{w} = M(r\vec{v}) = r\,(M\vec{v})$$

Hvad betyder dette for en kvantekopieringsmaskine? Hvis maskinen skal virke korrekt, skal den være i stand til at kopiere tilstandene $|0\rangle_A$ og $|1\rangle_A$. Dette betyder, at den skal opfylde

$$M\,|0\rangle_A \otimes |0\rangle_B = |0\rangle_A \otimes |0\rangle_B\,, \quad M\,|1\rangle_A \otimes |0\rangle_B = |1\rangle_A \otimes |1\rangle_B\,,$$

hvilket med vektor-notation er

$$M\begin{pmatrix}1\\0\\0\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix},\quad M\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\0\\1\end{pmatrix}.$$

Allerede fra dette følger, at maskinen ikke vil være i stand til at kopiere tilstanden $|+\rangle_A$ korrekt. Vi ser at

$$|+\rangle_A\otimes|0\rangle_B\equiv\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}$$

Vi benytter at M er lineær til at se at

$$\begin{aligned}M|+\rangle_A\otimes|0\rangle_B &\equiv M\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}=M\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}\right)=M\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\0\end{pmatrix}+M\begin{pmatrix}0\\0\\\frac{1}{\sqrt{2}}\\0\end{pmatrix}\\
&=M\left(\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\end{pmatrix}\right)+M\left(\frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\1\\0\end{pmatrix}\right)=\frac{1}{\sqrt{2}}M\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+\frac{1}{\sqrt{2}}M\begin{pmatrix}0\\0\\1\\0\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\0\\0\end{pmatrix}+\frac{1}{\sqrt{2}}\begin{pmatrix}0\\0\\0\\1\end{pmatrix}\\
&=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\0\end{pmatrix}+\begin{pmatrix}0\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix}=\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\\frac{1}{\sqrt{2}}\end{pmatrix}\equiv\left|\Psi^+\right\rangle\end{aligned}$$

Maskinen vil atså give den sammenfiltrede tilstand $|\Psi^+\rangle$ i stedet for den korrekte tilstand $|+\rangle_A\otimes|+\rangle_B$. Dette viser, at det er umuligt at kopiere en ukendt qubit med et kvantekredsløb.

Man kan nu forestille sig, at en kvantekopieringsmaskine måske ville fungere, hvis man målte sin qubit først. Så ville man jo kende qubittilstanden, og vi ville så kunne kopiere den. Problemet med dette er, at en måling ændrer qubittilstanden, som vi har set tidligere. Vi ville derfor ikke kopiere den originale qubit.