

Innhold

1	Introduksjon	3
2	Kvantemekanikk	5
2.1	Bølgefunksjonen ψ	5
2.2	Schrödingerligningen	8
2.3	Spinn	9
2.4	Måleproblemet	10
2.5	Sammenfiltring	11
3	Matriser	13
3.1	Basisvektorer	13
3.2	Multiplikasjon av vektorer	14
3.3	Bra-ket notasjon	14
3.3.1	Indreprodukt i bra-ket notasjon	15
3.3.2	Matrise-vektor-produkt i bra-ket notasjon	15
4	Kvantedatamaskiner	17
4.1	Qubits	17
4.2	Dekoherens	18
5	Kvantekryptografi	19
6	Kvante-logiske porter	23
6.1	Logiske porter og boolsk algebra	23
6.1.1	Boolsk algebra	23
6.1.2	Sammensatte porter	25
6.2	Generalisering til kvante-logiske porter	27
6.2.1	Ingen kloning-teoremet	28
6.3	Matematisk beskrivelse av kvante-logiske porter	29
6.3.1	\mathbb{I} , \mathbb{Z} , \mathbb{X} og \mathbb{Y}	29
6.3.2	Hadamard-porten \mathbb{H}	31

6.3.3	CNOT	31
-------	----------------	----

Kapittel 1

Introduksjon

Mot slutten av 1800-tallet var fysikere kommet så langt at det kunne se ut til at man snart hadde oversikt over alle de fundamentale lovmessighetene som styrte naturen. Det har blitt sagt at Lord Kelvin—datidens kanskje mest toneangivende fysiker—uttalte at “There is nothing new to be discovered in physics now. All that remains is more and more precise measurement.” Sitatet passer godt inn i den vanlige historiefortellingen om hvordan fysikken utviklet seg, men antakelig sa Lord Kelvin aldri dette. Derimot holdt han en forelesning i Royal Society der han pekte på at to “skyer på horisonten” som sto i veien for forståelsen av de underliggende lovmessighetene [1]. Den ene skyen var Michelson og Morely sitt forsøk på å måle lysets hastighet gjennom eteren. Forklaringen på deres måleresultat kom gjennom Einstein sin relativitetsteori—et av de to store gjennombruddene tidlig på 1900-tallet som skulle prege fysikkens utvikling videre. Den andre skyen var den såkalte ultrafiolette katastrofen i forbindelse med svart legeme-stråling. Dette problemet fikk sin løsning gjennom kvantemekanikken—det andre av de to store gjennombruddene tidlig på 1900-tallet som skulle prege fysikkens utvikling videre. Denne teksten vil gi en kort innføring i noen aspekter ved kvantemekanikken og se på hvordan dette kan benyttes til å utvide begrepet for hva en datamaskin er og hvordan den kan gjøre beregninger.

Kapittel 2

Kvantemekanikk

Tidlig i fysikkundervisningen lærer vi at ved å se på summen av krefter på som virker på et objekt kan vi finne ut hvordan det vil bevege seg, $\sum \vec{F} = m\vec{a}$. Hvis vi prøver å bruke denne ligningen til å forutse hvordan et elektron beveger seg vil vi ofte¹ få feil resultat. Det viser seg at bevegelsen til elektroner—og andre tilstrekkelig små partikler og systemer av partikler—må beskrives på en helt annen måte. Det er det kvantemekanikken dreier seg om. Denne teksten vil ikke forsøke å gi en fullstendig innføring i kvantemekanikk, men bare diskutere litt generelle aspekter ved kvantemekanikken og gi en litt grundigere diskusjon av de elementene som er nødvendig for å forstå hvordan kvantedatamaskiner virker.

2.1 Bølgefunksjonen ψ

En kvantemekanisk beskrivelse av verden viser seg å være svært annerledes enn det vi er vant med. Det viser seg at hvis du vil forsøke å forutsi hvilket resultat en måling—for eksempel av posisjonen eller farten til et elektron—vil gi må du nøye deg med å forutsi hvordan sannsynligheten for ulike måleresultater du kan få er. Dette dreier seg ikke om den vanlige måleusikkerheten som skyldes at måleinstrumentet ikke er perfekt, men det er en underliggende fysisk realitet. La oss for konkrethet se på posisjonen til et elektron. I klassisk fysikk som vi kjenner den fra før ville vi benevnt posisjonen med en vektor

$$\vec{r} = (x, y, z)$$

som beskriver posisjonen til elektronet med tre koordinater som i prinsippet kan bestemmes eksakt. Hvis vi kjenner alle kreftene som virker kan vi beregne

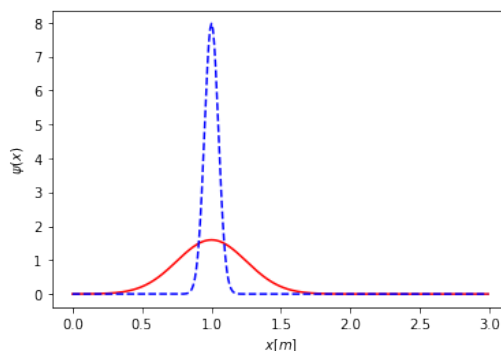
¹Det finnes tilfeller der Newtons lover gir en god beskrivelse av bevegelsen til elektroner, men i det generelle tilfellet er det ikke slik.

hvordan posisjonen varierer med tiden,

$$x = x(t), \quad y = y(t), \quad z = z(t),$$

slik at vi vet nøyaktig hvor elektronet er også på et vilkårlig tidspunkt i fremtiden.

En kvantemekanisk beskrivelse av elektronet innebærer en såkalt bølgefunksjon som forteller oss om sannsynligheten for å finne elektronet på et bestemt sted. I det videre vil jeg begrense meg til å beskrive endimensjonal bevegelse for å forenkle notasjonen, men konseptet kan enkelt utvides til tre dimensjoner. Til å beskrive elektronets posisjon bruker vi funksjonen $\psi(x)$, men denne må tolkes på en helt annen måte enn vektoren \vec{r} ovenfor. For det første vil $\psi(x)$ normalt ha en verdi som er ulik null i mer enn ett punkt, noe som betyr at elektronet ikke har en fast definert posisjon, men kan tenkes å være flere steder. Merk at dette faktisk ikke er et uttrykk for at det finnes informasjon om hvor elektronet egentlig er som vi mangler, men at posisjonen til elektronet ikke er fast definert². Figur 2.1 viser to mulige funksjoner $\psi(x)$ som beskriver posisjonen til et elektron som befinner seg ved eller nær $x = 1$ m. Den stiplede blå linjen er kun ulik null i et relativt lite område nær $x = 1$ m. Dette betyr at vi har en ganske stor visshet om hvor elektronet som beskrives av denne ψ -funksjonen er. Den heltrukne røde linjen er mer fordelt utover og innebærer derfor at det er et større område der det er sannsynlig at vi vil finne elektronet.



Figur 2.1

Hva skjer så når vi prøver å måle hvor elektronet er? Da vil vi—uansett hvor konsentrert eller utspredd bølgefunksjonen som beskriver det er—finne

²Denne bemerkningen fortjener egentlig en lang diskusjon, men dette er ikke stedet for denne diskusjonen. Det er skrevet mye om dette andre steder.

elektronet lokalisert i ett punkt³. Dette innebærer at når vi måler hvor elektronet er endrer vi samtidig bølgefunksjonen som beskriver elektronet til å bli mye mer konsentrert rundt ett punkt, men dette punktet trenger ikke nødvendigvis å være der den tidligere hadde maksimum. Det vil imidlertid alltid være et sted der $\psi(x)$ før målingen var ulik null. Hvis vi kjenner bølgefunksjonen før vi måler kan vi bruke den til å beregne sannsynligheten for å finne elektronet i ulike områder. Det gjør vi ved å integrere over kvadratet av absoluttverdien av $\psi(x)$. For eksemel er sannsynligheten for å finne elektronet et sted mellom $x = 0,75$ m og $x = 0,76$ m

$$P(0,75 \text{ m} < x < 0,76 \text{ m}) = \int_{0,75 \text{ m}}^{0,76 \text{ m}} |\psi(x)|^2 dx \quad (2.1)$$

Noen bemerkninger om funksjonen $\psi(x)$

1. For at integralet i ligning (2.1) skal gi en meningsfull sannsynlighet må funksjonen $\psi(x)$ oppfylle et normaliseringskrav, nemlig

$$1 = \int_{-\infty}^{\infty} |\psi(x)|^2 dx.$$

Dette betyr for det første at sannsynligheten for å finne elektronet et eller annet sted er 1. For det andre, siden $|\psi(x)|^2 \geq 0$ overalt vil vi da være sikret å finne sannsynlighet $P \leq 1$ dersom vi integrerer over et kortere intervall.

2. Når vi integrerer over kvadratet av absoluttverdien til funksjonen ($|\psi|^2$) og ikke bare over kvadratet av funksjonen (ψ^2) er det fordi det viser seg at vi generelt må tillate $\psi(x)$ å ha komplekse verdier. I enkelte sammenhenger er dette av stor betydning, men i denne teksten får vi ikke behov for å studere dette videre.
3. Vi har så langt diskutert bølgefunksjonen som en helt vanlig funksjon som tar inn ett tall (posisjonen) og gir ut ett tall (som riktignok kan være komplekst) som kan relateres til sannsynligheten for å finne elektronet akkurat der. Generelt vil vi trenge litt mer kompliserte konstruksjoner. En første enkel utvidelse av dette er å ta med de to andre romlige koordinatene samt å ta med en tidsavhengighet som beskriver at bølgefunksjonen endrer seg når tiden går⁴:

$$\Psi(x, y, z, t).$$

³Selvfølgelig med en presisjon som er begrenset av måleinstrumentet vi bruker.

⁴En vanlig konvensjon er å bruke stor Ψ for å betegne en bølgefunksjon som avhenger av både rom- og tidskoordinater, mens man bruker liten ψ dersom bølgefunksjonen kun avhenger av de romlige koordinatene, men ikke endrer seg når tiden går.

Videre er det i en del sammenhenger—blant annet en vi skal se på snart og få mye bruk for i resten av denne teksten—ofte nyttig å la bølgefunksjonen gi ut en vektor i stedet for bare et tall:

$$\Psi(x, y, z, t) = \begin{bmatrix} \phi_1(x, y, z, t) \\ \phi_2(x, y, z, t) \end{bmatrix},$$

der $\phi_1(x, y, z, t)$ og $\phi_2(x, y, z, t)$ er vanlige funksjoner som gir ut (muligens komplekse) tall.

2.2 Schrödingerligningen

Gitt en bølgefunksjon $\Psi(x, y, z, t)$ og en funksjon $V(x, y, z)$ som beskriver den potensielle energien som funksjon av posisjonen kan vi finne tidsutviklingen til bølgefunksjonen ved å løse en partiell differensialligning som er kjent som Schrödingerligningen (her skrevet opp med bare én romlig koordinat):

$$i\hbar \frac{\partial}{\partial t} \Psi(x, t) = \left[-\frac{\hbar^2}{2m} \frac{\partial^2}{\partial x^2} + V(x) \right] \Psi(x, t)$$

Her er m massen til partikkelen som beskrives, i vårt tilfelle elektronmassen, og $\hbar = \frac{h}{2\pi} = 1,055 \times 10^{-34}$ Js er den reduserte Planck-konstanten. Schrödingerligningen spiller omtrent samme rolle i kvantemekanikken som Newtons andre lov ($\Sigma \vec{F} = m\vec{a}$) spiller i klassisk mekanikk: Den tillater oss å beregne hva som vil skje i fremtiden med kunnskap om hvordan tilstanden er nå. Det er imidlertid noen vesentlige forskjeller. For det første er det bare presisjonen i målingene som begrenser presisjonen i forutsigelsen i klassisk mekanikk. I kvantemekanikk kan vi—som allerede diskutert—kun beregne sannsynligheten for ulike måleresultater, ikke forutsi med sikkerhet hva vi vil måle. Så selv om vi skulle kjenne bølgefunksjonen slik den er nå uten usikkerhet, og dermed kunne forutsi hvordan den vil være i fremtiden uten usikkerhet vil vi fremdeles ikke vite hvilket måleresultat vi ender opp med. For det andre kan Newtons andre lov brukes “baklengs”: Hvis vi måler hva posisjon og fart er nå kan vi bruke det til å regne ut hva posisjon og fart var på et tidligere tidspunkt. Siden en måling påvirker bølgefunksjonen kan vi ikke bruke Schrödingerligningen til å finne ut hvordan bølgefunksjonen var på et tidspunkt før vi målte f.eks. posisjonen til elektronet.

I en generell innføring til kvantemekanikk legges det som regel stor vekt på å løse Schrödingerligningen for ulike potensialer $V(x)$. Dette er ikke nødvendig for diskusjonen videre i denne teksten, så det problemet vil ikke bli diskutert videre her.

2.3 Spinn

En del subatomære partikler, inkludert elektronet som vi fokuserer mest på her, har en egenskap som heter spinn. Ordet spinn antyder at det er noe som snurrer rundt, men det er ikke tilfellet. Det er snakk om en iboende egenskap i partikkelen. Likevel kan rotasjonen til en snurrebass være en brukbare analogi for *enkelte aspekter* ved spinnet. Spinn er en vektor som altså har både en størrelse og en retning. I snurrebassanalogien svarer størrelsen til hvor fort den roterer, mens retningen svarer til retningen rotasjonsaksen peker. Positiv retning defineres slik at snurrebassen roterer mot klokken når vi ser den fra den positive siden. Det viser seg at spinnet til subatomære partikler alltid er på formen $\frac{a}{2}\hbar$ der verdien av a avhenger av hvilken partikkel det dreier seg om. Partikler der a er et partall slik at spinnet er et heltall multiplisert med \hbar kalles bosoner. Partikler der a er et oddetall kalles fermioner. Elektronet har $a = 1$ slik at spinnet til elektronet har størrelse $\frac{1}{2}\hbar$. Ofte skriver vi dette bare som spinn $\frac{1}{2}$, og jeg vil bruke denne konvensjonen i det videre.

I det videre bryter analogien med en snurrebass fullstendig sammen. I stedet for å måle hvilken retning spinnet til et elektron peker er det enklere å måle projeksjonen av spinnet inn på en vilkårlig akse. Hvis vi gjør dette med en snurrebass vil vi finne en verdi av projeksjonen s slik at $-S < s < +S$, der S er størrelsen til spinnet. $s = +S$ og $s = -S$ svarer til at aksene vi måler langs er enten parallell eller antiparallell med rotasjonsaksen. $s = 0$ svarer til at aksene vi måler langs står normalt på rotasjonsaksen. Når vi gjør denne målingen på et elektron finner vi alltid $+\frac{1}{2}$ eller $-\frac{1}{2}$ uansett hvilken akse vi måler langs. Sett nå at vi preparerer et elektron med spinnet sitt rettet langs den positive x -aksen. Hvis vi nå velger å måle projeksjonen av spinnet på x -aksen vil vi med sikkerhet ende opp med resultatet $+\frac{1}{2}$. Hvis vi derimot velger å måle projeksjonen av spinnet langs positiv z -akse (som står normalt på x -aksen) vil vi ende opp med å måle enten $+\frac{1}{2}$ eller $-\frac{1}{2}$ med 50% sannsynlighet for hver av verdiene. Hvis vi etter å ha målt projeksjonen langs z -aksen igjen måler projeksjonen langs x -aksen vil vi ikke lenger med sikkerhet måle $+\frac{1}{2}$. Derimot vil vi nå bare ha 50% sannsynlighet for at målingen viser $+\frac{1}{2}$, mens det også er 50% sannsynlighet for å få verdien $-\frac{1}{2}$.

Som en avslutning av denne første diskusjonen av spinntet tar jeg med at hvis vi igjen preparerer elektronet med spinn opplinjert med x -aksen og deretter måler projeksjonen av spinnet på en akse som danner en vinkel θ med x -aksen da blir sannsynlighetene for de to mulige resultatene av målingen

$$P\left(+\frac{1}{2}\right) = \cos^2 \theta, \quad P\left(-\frac{1}{2}\right) = 1 - \cos^2 \theta = \sin^2 \theta.$$

2.4 Måleproblemet

Både i diskusjonen av posisjonen til elektronet i avsnitt 2.1 og retningen til elektronspinnets i avsnitt 2.3 var det en underliggende observasjon som ikke ble tydelig formulert:

Når vi utfører en måling på et kvantemekanisk system kan vi ikke unngå å samtidig påvirke systemet.

Dette er helt sentralt, og viser en tydelig forskjell på klassisk mekanikk og kvantemekanikk. I klassisk mekanikk ser vi på objekter som er store nok til at vi kan måle størrelser som for eksempel posisjon eller fart uten relevant påvirkning av størrelsen vi ønsker å måle. Vi kan for eksempel måle posisjonen til en ball ved å *se på den* mens vi har en linjal like ved for å definere måleskalaen. For at vi skal kunne se ballen må det skinne lys på den som reflekteres inn i øynene våre. Lyset består av små partikler som kalles fotoner som treffer overflaten til ballen før de sendes videre til, blant annet, øynene våre. Når fotonene treffer ballen gir de den en liten dytt, så i prinsippet kan de endre posisjonen til ballen i prosessen. I praksis er imidlertid bevegelsesmengden til fotonene så liten at de ikke gir noen relevant kraftvirkning på ballen. Derfor kan vi jobbe som om måleprosessen ikke i det hele tatt påvirker det vi ønsker å måle. Dette er ikke tilfellet når vi kommer til kvantemekanikk.

Vi fortsetter å bruke elektronet som eksempel. Massen til et elektron er $m_e = 9,1 \times 10^{-31}$ kg. Bevegelsesmengden til et foton avhenger av bølgelengden. Om vi ser på et foton omtrent midt i det synlige spekteret ($\lambda = 550$ nm) har det bevegelsesmengden $p = \frac{h}{\lambda} = 1,2 \times 10^{-27}$ kg m/s. Hvis vi bruker dette fotonet til å måle hvor elektronet er vil vi altså samtidig gi elektronet en så kraftig dytt at det etterpå vil ha stor fart bort fra det stedet det var. Slik er det med alle målinger i kvantemekanikken—måleprosessen påvirker systemet vi måler på. Og enda verre, jo mer nøyaktig vi prøver å måle, jo mer vil vi ende opp med å påvirke systemet. Generelt kan vi si at hvis vi ikke kan gjøre målingen på en slik måte at påvirkningen på systemet er neglisjerbar så må vi behandle systemet som kvantemekanisk. Hvis vi derimot kan måle på det uten at målingen gir noen relevant påvirkning på systemet kan vi behandle det med vanlig klassisk mekanikk.

Det finnes noen spesialtilfeller der vi tilsynelatende unslipper dette måleproblemet, selv når vi jobber med et system som må behandles kvantemekanisk. Et viktig eksempel, og det eneste jeg vil se på her, er gjentatte målinger av elektronspinnets. I avsnitt 2.3 diskuterte jeg hvordan projeksjonen av spinnets på en akse antar tilfeldige verdier. Men hvis vi repeterer gjentatte målinger langs den samme aksen får vi hele tiden samme resultat. Med andre

ord, hvis spinnet er opplinjert med x -aksen og vi fortsetter å måle projeksjonen av spinnet inn på x -aksen vil ikke målingen endre spinnet. Hvis vi derimot velger å måle spinnet langs en annen akse, for eksempel z -aksen, vil målingen påvirke spinnet som diskutert ovenfor.

2.5 Sammenfiltrering

Så langt har diskusjonen gitt inntrykk av at hvert enkelt elektron—og andre objekter også for den saks skyld—har hver sin bølgefunksjon. Dette er ikke realiteten. I prinsippet må hele universet beskrives av en felles bølgefunksjon som beskriver alt som er i det. Heldigvis kan vi i mange tilfeller bruke en enklere beskrivelse og likevel få en god representasjon av virkeligheten. Situasjonen er ganske lik til klassisk fysikk: Når vi beregner banen til en stein som blir kastet tar vi hensyn til tyngdekraften fra jorden, men ikke tyngdekraften fra solen, månen og de andre planetene i solsystemet. I prinsippet skulle tyngdekraften fra alt annet i universet vært med i beregningen, men tyngdekraften fra jorden er så mye større enn de andre bidragene at vi kun trenger å ta hensyn til denne. Tilsvarende argument tillater oss i mange tilfeller å regne med én bølgefunksjon per objekt i kvantemekanikken. Men det finnes også tilfeller der to eller flere objekter må beskrives av en felles bølgefunksjon for å få en riktig beskrivelse. Når dette er tilfellet sier vi at objektene er *sammenfiltret*.

Som eksempel på sammenfiltrering skal vi se på spinnet til to elektroner. Det er mulig å preparere paret av elektroner slik at summen av spinnet deres målt langs en akse er null. Siden hvert av elektronene kun har muligheten $+\frac{1}{2}$ og $-\frac{1}{2}$ må altså spinnet til de to elektronene peke hver sin vei. Det spesielle med en sammenfiltret tilstand er at det ikke er slik at det ene elektronet har spinn $+\frac{1}{2}$ og det andre $-\frac{1}{2}$. I hvert fall ikke før vi har målt. Begge elektronene er i en superposisjon mellom begge mulighetene, men straks vi måler spinnet til det ene elektronet vet vi også hva måleresultatet vil bli når vi måler spinnet til det andre. For å understreke hvor uvant dette er kan vi se på et konkret eksempel. Vi preparerer sammenfiltrede paret av elektroner og plasserer dem i hvert sitt laboratorium adskilt med 3000 km. Siden det ikke er mulig å sende noe signal raskere enn lyshastigheten vil det ta minst 10 ms å sende et signal fra det ene laboratoriet til det andre. På et avtalt tidspunkt måler man spinnet til det ene elektronet, og 1 ms senere måler man spinnet til det andre elektronet. Selv om elektronene er for langt fra hverandre til å kunne rekke å kommunisere finner man alltid perfekt korrelasjon: det ene har spinn $+\frac{1}{2}$ og det andre har spinn $-\frac{1}{2}$.

En fristende forklaring på hvordan elektronene kan ha denne perfekte

korrelasjonen uten tid til å kommunisere er at i realiteten hadde det ene elektronet hele tiden spinn $+\frac{1}{2}$ og det andre hadde hele tiden spinn $-\frac{1}{2}$. Det var bare det at vi ikke hadde nok informasjon til å vite hvilken som hadde hva frem til vi målte. I 1964 publiserte John Steward Bell en artikkel der han beskrev hvordan man kunne teste om dette faktisk var tilfellet [2]. Jeg skal ikke forsøke å gi en fullstendig beskrivelse av testen her, men bare skissere eksperimentet Bell foreslo. I likhet med eksperimentet jeg har skissert ovenfor skal man også her gjentatte ganger måle spinnet til to sammenfiltrede elektroner som er separert slik at de ikke får tid til å sende et signal fra det ene til det andre. I eksempelet ovenfor målte vi alltid spinnet langs den samme aksen. I Bell sitt eksperiment skal vi måle spinnet langs én av tre retninger som er separert med 120° . Hvilken retning som brukes i hver enkelt måling velges tilfeldig i hvert av de to laboratoriene, og beslutningen gjøres så kort tid før målingen blir gjort at det ikke er tid for et lyssignal å gå fra det ene laboratoriet til det andre. Det viser seg da at korrelasjonen mellom måleresultatene fra de to laboratoriene vil bli ulik avhengig av om

1. elektronene på forhånd har et fast definert spinn som vi ikke har nok informasjon til å vite (forutsigelsen til klassisk fysikk), eller
2. elektronene er begge i en superposisjon mellom de to mulig utfallene av målingen helt frem til vi har målt spinnet til minst ett av elektronene (forutsigelsen til kvantemekanikk).

Eksperimentet har blitt utført med mange forskjellige variasjoner⁵, de første gangene av John Clauser og Stuart Freedman[3] og Alain Aspect, Philippe Grangier og Gérard Roger [4], og det er ikke mye tvil om at det er kvantemekanikken som forutsier resultatet riktig.

⁵De fleste eksperimentene ser på polarisasjonen til fotoner i stedet for spinnet til elektroner fordi dette er teknisk enklere å jobbe med, men prinsippet er det samme.

Kapittel 3

Matriser

Parallelt med at Erwin Schrödinger kom frem til ligningen som jeg nevnte såvidt i forrige kapittel, kom Werner Heisenberg frem til en helt annen matematisk formalisme for å utføre kvantemekaniske beregninger - basert på matriser og vektorer, altså det vi kjenner som lineær algebra. Dette var en gren av matematikken som var ukjent for de fleste fysikere på begynnelsen av 1900-tallet og derfor fikk Heisenberg sin *matrisemekanikk* i første omgang en litt kjøligere mottakelse enn Schrödinger sin *bølgemekanikk*. Det viste seg imidlertid at begge formuleringene av kvantemekanikken var like riktig, og at hvilken formulering som var få foretrekke var avhengig av hvilket problem man studerte. Når vi i det videre stort sett skal studere spinn til elektronet er det Heisenberg sin matrisemekanikk som passer best. Dette kapittelet vil gi en kort repetisjon av lineær algebra og vise hvordan dette brukes til å regne med elektron-spinn.

3.1 Basisvektorer

I et todimensjonalt koordinatsystem trenger vi nøyaktig to tall til å angi en posisjon, vanligvis omtalt som x -koordinaten og y -koordinaten. Punktet med x -koordinat X og y -koordinat Y angis da på vektorform som

$$\begin{bmatrix} X \\ Y \end{bmatrix} \text{ eller } [X \ Y].$$

Den første formen kaller vi en kolonne-vektor og den andre en rekkevektor. Det er først når vi skal se på multiplikasjon av vektorer med hverandre eller med matriser at forskjellen på disse to representasjonene blir relevant. Akkurat nå kan vi se på de som to likeverdige måte å spesifisere det samme punktet i koordinatsystemet. En litt annen måte å skrive ned den samme

informasjonen på er

$$\begin{bmatrix} X \\ Y \end{bmatrix} = X \cdot \begin{bmatrix} 1 \\ 0 \end{bmatrix} + Y \cdot \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Her er $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ en vektor med lengde 1 som peker langs x -aksen, mens $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ er en vektor med lengde 1 som peker langs y -aksen. Denne måten å skrive ned koordinatene på sier enda mer eksplisitt enn den forrige at vi skal gå X skritt langs x -aksen og så Y skritt parallelt med y -aksen. Vektorene $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ og $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ er *enhetsvektorer*, og siden alle vektorer i det todimensjonale rommet kan skrives som en lineærkombinasjon av disse to vektorene utgjør de en *basis* for det todimensjonale rommet.

Valget av basisvektorer er ikke unikt. For det første kan vi skalere vektorene som utgjør basisen med hver sin vilkårlige konstant (ulik 0), og de vil fremdeles være en basis. F.eks. er $\begin{bmatrix} -2 \\ 0 \end{bmatrix}$ og $\begin{bmatrix} 0 \\ 3 \end{bmatrix}$ også en basis. Det er heller ikke nødvendig at basisvektorene våre skal være parallelle med x - og y -aksen. For eksempel vil $\begin{bmatrix} 1 \\ 1 \end{bmatrix}$ og $\begin{bmatrix} 1 \\ -1 \end{bmatrix}$ også utgjøre en basis. Generelt vil to vilkårlige vektorer med lengde ulik 0 og som ikke er parallelle med hverandre utgjøre en basis for det todimensjonale rommet.

I denne teksten vil vi i hovedsak benytte oss av ulike ordnete, ortonormale basiser. Ordnete betyr at vi holder orden på hva som er den første og hva som er den andre basisvektoren. Hvorfor dette er viktig for oss kommer vi tilbake til senere. Ortonormale betyr for det første at basisvektorene står ortogonalt—altså vinkelrett—på hverandre, og for det andre at de er normalisert—altså har lengde 1.

3.2 Multiplikasjon av vektorer

3.3 Bra-ket notasjon

I de fleste tekster om lineæralgebra symboliseres en vektorstørrelse enten med en pil over symbolet, \vec{r} , eller med fet skrift \mathbf{r} . Om man har behov for å skille mellom kolonnevektorer og rekkevektorer er det kolonnevektoren som betegnes som nevnt, mens rekkevektoren betegnes som henholdsvis \vec{r}^T eller \mathbf{r}^T der T står for *transponert*. I denne teksten vil jeg i stedet bruke en annen notasjon som ble innført av den britiske fysikeren Paul Dirac. Dette er den

notasjonen som er mest vanlig å bruke innen kvantemekanikk, men det brukes sjelden i andre sammenhenger (selv om den gjerne kunne vært brukt ellers også). En kolonnevektor betegnes med symbolet $|r\rangle$ og omtales som en *ket*, mens en rekkevektor betegnes med symbolet $\langle r|$ og omtales som en *bra*.

3.3.1 Indreprodukt i bra-ket notasjon

For å regne ut indreproduktet mellom to vektorer må vi multiplisere en bra-vektor sammen med en ket-vektor slik at vi får en *bracket*. F.eks. gitt $\langle a|$ og $|b\rangle$ betegnes indreproduktet mellom dem med $\langle a|b\rangle$, og dette er en skalar som alltid når vi tar indreprodukt av to vektorer. Merk at det bare er notasjonen som er ny her—indreproduktet regnes ut på den vanlige måten. Hvis f.eks.

$$\langle a| = [-2 \ 4] \text{ og } |b\rangle = \begin{bmatrix} 3 \\ 1 \end{bmatrix},$$

da er

$$\langle a|b\rangle = [-2 \ 4] \begin{bmatrix} 3 \\ 1 \end{bmatrix} = (-2) \cdot 3 + 4 \cdot 1 = -2.$$

3.3.2 Matrise-vektor-produkt i bra-ket notasjon

Gitt matrisen $M = \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix}$, bra-vektoren $\langle a| = [-2 \ 4]$ og ket-vektoren $|b\rangle = \begin{bmatrix} 3 \\ 1 \end{bmatrix}$. Vi kan da regne ut

$$\begin{aligned} \langle a|M &= [-2 \ 4] \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} = [12 \ 0], \\ M|b\rangle &= \begin{bmatrix} 0 & 2 \\ 3 & 1 \end{bmatrix} \begin{bmatrix} 3 \\ 1 \end{bmatrix} = \begin{bmatrix} 2 \\ 10 \end{bmatrix}, \\ \langle a|M|b\rangle &= (\langle a|M)|b\rangle = \langle a|(M|b\rangle) = 36. \end{aligned}$$

$|b\rangle M$ og $M\langle a|$ er derimot ikke definert.

Kapittel 4

Kvantedatamaskiner

4.1 Qubits

Den grunnleggende informasjonsenheten i vanlige datamaskiner er en *bit*. En bit har enten verdien 0 eller 1 og kan representeres av et hvilket som helst fysisk objekt som har to mulige tilstander. Et enkelt eksempel er en lyspære: Vi kan tilskrive tilstanden ‘lyset på’ verdien 1 og ‘lyset av’ verdien 0. Et eksempel med litt mer teknologisk relevans er en kondensator. Vi kan måle spenningen mellom platene i en kondensator. Hvis spenningen er tilnærmet lik 0 (i praksis under en viss grenseverdi) svarer dette til at bit’en vår har verdi 0. Hvis spenningen er over grenseverdien har bit’en verdien 1. Vi kan endre verdien fra 0 til 1 ved å tilføre kondensatoren ladning, og endre verdien fra 1 til 0 ved å lade ut kondensatoren.

I kvantedatamaskiner er den grunnleggende enheten en *qubit*. En *qubit* er et kvantemekanisk system som har nøyaktig to ulike utfall av en gitt måling. Et typisk eksempel er elektron-spinnet som ble diskutert i avsnitt 2.3. Hvis vi måler spinnet langs en gitt akse, f.eks. x -aksen, vil vi alltid få enten $+\frac{1}{2}$ eller $-\frac{1}{2}$. I likhet med den klassiske datamaskinen kan vi tilskrive det ene måleresultatet verdien 1 og det andre måleresultatet 0. Hvis vi leser av verdien til en qubit har den—akkurat som en bit—altså enten verdien 1 eller verdien 0.

Det som virkelig skiller en *qubit* fra en *bit* er hva som skjer med den når vi ikke sjekker hvilke verdi den har. En bit er et klassisk system, og den har den verdien den har inntil vi gjør noe for å endre verdien (eller noe går galt). En qubit derimot er et kvantemekanisk system og må altså beskrives av en bølgefunksjon som diskutert i avsnitt 2.1. Dette innebærer at vi *kan* sette qubiten til å ha en bestemt verdi som vi kan lese ut igjen senere. For eksempel hvis vi preparerer elektronet vårt slik at det har spinnet rettet i

x -retning, vil vi finne nettopp at spinnet er rettet i x -retning når vi senere måler det. Men vi kan også sette qubiten til å være i en *superposisjon* av de to tilstandene. Som diskutert i avsnitt 2.3 kan vi preparere elektronet til å ha spinnet sitt i positiv z -retning. Hvis da senere måler verdien av spinnet i x -retning har vi 50% sannsynlighet for å få verdien $+\frac{1}{2}$ og 50% sannsynlighet for å få verdien $-\frac{1}{2}$. Det er akkurat som om qubiten har både verdien 0 og 1 helt frem til den blir målt, og først da ender opp med den ene eller den andre muligheten. Det er heller ikke nødvendig å la superposisjonen være slik at det er nøyaktig 50% sannsynlighet for hvert av utfallene. Generelt kan vi ende opp med en vilkårlig fordeling av sannsynligheten på de to ulike utfallene. Det er muligheten for superposisjon mellom de to ulike utfallene som utnyttes i kvantedatamaskiner og som gjør at de kan utføre enkelte beregninger langt raskere enn klassiske datamaskiner.

4.2 Dekoherens

Så langt har vi diskutert kvantemekaniske systemer som om de er helt stabile. Ta eksempelet med elektronet som vi preparerer med spinnet i positiv x -retning. Vi har da sagt at hvis vi måler verdien av spinnet i x -retning på et senere tidspunkt (uten å ha gjort noen andre målinger på det i mellomtiden) vil vi nødvendigvis finne at elektronet fremdeles er spinnet i positiv x -retning. Dette er en grov forenkling. Dersom elektronet hadde vært fullstendig isolert fra omgivelsene til enhver tid bortsett fra når vi utfører målingen hadde det vært sant, men dette er selvfølgelig umulig å oppnå. Vi må med andre ord innse at vi har muligheten for at en annen vekselvirkning med omgivelsene enn målingen også påvirker tilstanden til elektronet. Dette fenomenet kalles *dekoherens* og utgjør den sannsynligvis største teknologiske utfordringen når man skal konstruere en kvantedatamaskin. Ofte når kvantedatamaskiner omtales brukes antall qubits—per i dag er det som regel opp til noen få titalls—som et mål på hvor kraftig maskinene er, men uten informasjon om forventet tid før dekoherens ødelegger informasjonen i en qubit er dette ikke tilstrekkelig til å vurdere hvor god kvantedatamaskinen er.

Siden fokus for denne teksten er mer på prinsippene bak kvantedatamaskiner enn praktisk realisering vil jeg ikke diskutere problemet med koherens videre. Når jeg beskriver algoritmer for kvantedatamaskiner vil jeg derfor beskrive dem som om vi har en maskin der dekoherens ikke er noe problem tilgjengelig.

Kapittel 5

Kvantekryptografi

Klassisk kryptografi har en fundamental utfordring: hvordan distribuere krypteringsnøkkelen. Hvis man har en krypteringsnøkkel som er like lang som meldingen er det prinsipielt umulig å bryte koden, men sikkerheten avhenger fremdeles av at man vet at ingen har klart å få tak i nøkkelen. Vet hjelp av kvantemekanisk sammenfiltrering kan vi distribuere en nøkkel over et åpent nettverk og forsikre oss om at kun den rette mottakeren har fått nøkkelen. For å se hvordan dette kan gjøres tar vi utgangspunkt i BB84-protokollen som ble funnet opp av Charles Bennett og Gilles Brassard [5].

Alice ønsker å sende en kodet melding til Bob, men frykter at Eva kan forsøke å fange opp meldingen og dekryptere den. For å hindre Eva i å kunne dekryptere meldingen bruker Alice og Bob qubits til å overføre kodenøkkelen, mens selve den kodete meldingen vil bli sendt over en vanlig datakanal. Alice velger nå krypteringsnøkkelen sin som er en streng av klassiske bit, for eksempel 0110011110001... Nøkkelen består av $4n$ bit, der n er lengden på den egentlige nøkkelen. Hvorfor Alice trenger å sende en fire ganger så lang nøkkel blir klart etter hvert. For hver bit i nøkkelen sender Alice ett elektron til Bob. Før hun sender elektronet måler hun spinnets i enten vertikal eller horisontal retning. Hvilken retning hun bruker for hvert elektron velges tilfeldig med lik sannsynlighet for de to retningene. Siden målingen påvirker elektronet vil altså Alice vite kvantetilstanden til hvert enkelt elektron relativt til en av de to ordnete, ortonormale basisene

$$V = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\} \quad \text{og} \quad H = \left\{ \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix}, \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \right\}.$$

I begge tilfellene lar vi den første basisvektoren i paret svare til den klassiske biten 0, mens den andre basisvektoren svarer til 1. Hvis Alice for eksempel velger basisen V , som svarer til å måle i vertikal retning, og hun måler at

spinnet peker nedover gir dette bit-verdien 1 siden spinn nedover svarer til $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Hvis Bob senere måler det samme elektronet i vertikal retning vil han også finne $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ og vite at den biten hadde verdien 1. Hvis han i stedet måler elektronet med basisen H vil det være tilfeldig hvilken vei spinnets peker og dermed om han mottar overført bit-verdien 0 eller 1. Dette betyr at det er kun når Alice og Bob bruker samme basis at det er noen reell informasjonsoverføring.

Hvordan kan så dette brukes til å overføre en krypteringsnøkkel på en pålitelig måte? Alice starter med å sende Bob en serie qubits (elektroner) som beskrevet ovenfor. Hun holder rede på hvilken basis hun har brukt for hvert elektron, men denne informasjonen sendes *ikke* sammen med elektronene. Nedenfor vises på første linje begynnelsen av krypteringsnøkkelen Alice vil sende, på andre linje hvilken basis hun velger for hvert elektron og på tredje linje hvilke kvantetilstand elektronet hun sender er i.

$$\begin{array}{cccccccccc}
 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \\
 H & V & V & H & V & H & H & H & H \\
 \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix}
 \end{array}$$

Når Bob mottar elektronene måler han også spinnets. På samme måte som Alice velger han tilfeldig, med lik sannsynlighet for begge, mellom basisene V og H og holder rede på hvilken han bruker for hvert elektron. Siden han ikke vet noe om hvilken basis Alice har brukt på hvert elektron må han forvente at det er kun halvparten av gangene de velger den samme basisen. Nedenfor vises på første linje kvantetilstanden til elektronet Bob mottar (men som han ikke kjenner), på andre linje hvilken basis han velger for å måle, på tredje linje hvilken kvantetilstand han måler og på fjerde linje hvilken bit-verdi han tolker ut av målingen.

$$\begin{array}{cccccccccc}
 \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{-1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \\
 V & H & V & V & V & H & V & V & H \\
 \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} & \begin{bmatrix} 1 \\ 0 \end{bmatrix} & \begin{bmatrix} 0 \\ 1 \end{bmatrix} & \begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{bmatrix} \\
 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1
 \end{array}$$

Merk at i de tilfellene der Alice og Bob valgte samme basis er bit-verdien riktig overført, mens når de valgte motsatt basis er det tilfeldig om bit-verdien blir riktig overført eller ikke. Etter at alle elektronene er overført og

Bob har gjort sine målinger sammenligner Alice og Bob sine sekvenser av basis-valg. Dette kan de gjøre på en ukryptert linje. Alle tilfeller der de har valgt motsatt basis forkaster de siden de ikke kan vite om de har målt samme bit-verdi der. Siden det for hvert enkelt elektron er 50% sannsynlighet for at de velger samme basis, og siden vi har forutsatt at det er et stort antall bit i krypteringsnøkkelen kan vi gå ut fra at de i halvparten av tilfellene har valgt samme basis. Etter at Alice sendte $4n$ qubit sitter nå Alice og Bob igjen med $2n$ bit som skal være like.

Hva så med Eva som ønsker å fange opp krypteringsnøkkelen som utveksles? Anta at hun klarer å fange opp elektronene på vei fra Alice til Bob. Hun kan da måle spinnnet og sende elektronet videre til Bob. Anta også at hun vet hvilke retninger, altså hvilke basiser, Alice og Bob har blitt enig om å velge mellom. Men når hun skal gjøre målingen sin kan hun ikke vite hvilken av de to basisene hverken Alice eller Bob bruker for det samme elektronet, for den informasjonen utveksles ikke før både Alice og Bob har gjort sine målinger. Det beste hun kan gjøre da er å velge tilfeldig med lik sannsynlighet for begge de to basisene og holde rede på hvilken basis hun brukte for hvilket elektron. I likhet med Bob har Eva 50% sannsynlighet for å velge samme basis som Alice. Men der halvparten av tilfellene der Alice og Bob velger ulik basis er unyttig siden disse blir forkastet. Så selv om Eva lytter til Alice og Bob sin sammenligning av basisene de brukte kan hun ikke utnytte dette fullt ut, for det vil bare være halvparten av tilfellene der Alice og Bob har brukt samme basis at også Eva har brukt denne basisen. Men situasjonen for Eva er faktisk ennå verre enn som så. Ikke bare mangler hun informasjon om halvparten av bitene Alice og Bob har utvekslet, ved å gjøre målinger på elektronene har hun lagt igjen informasjon som gjør at Alice og Bob kan forstå at overføringen har blitt avlyttet.

La oss nå se på de bitene Alice og Bob der de har brukt samme basis og dermed velger å beholde. Vi må da studere to tilfeller: enten har også Eva brukt samme basis, eller har Eva brukt motsatt basis. Valget til Eva vet selvfølgelig ikke Alice og Bob noe om, men det trenger de heller ikke å vite.

1. Eva velger samme basis som Alice og Bob:
Siden gjentatte målinger av spinnnet med samme basis ikke påvirker kvantetilstanden til elektronet vil alle tre sitte igjen men samme måleresultat på disse qubitene.
2. Eva velger motsatt basis som Alice og Bob:
Anta for konkrethets skyld at Alice og Bob brukte basis V , mens Eva brukte H . Elektronet Eva fanger opp er altså i en kvantetilstand med et veldefinert spinn i basis V . Men som diskutert i avsnitt 2.3 vil det da målingen med basis H ha 50% sannsynlighet for å gi resultatet 0

og 50% sannsynlighet for å gi resultatet 1 uansett hvilken bit-verdi den hadde målt i basis V . Når Eva sender elektronet videre etter å ha målt det med basis H har elektronet et veldefinert spinn i basisen H , men ikke i basisen V . Når Bob til slutt måler elektronet med basis V har han altså 50% sannsynlighet for å ende opp med resultat 0 og 50% sannsynlighet for å ende opp med resultat 1, uansett hvilken verdi de to andre sitter med. Siden Alice og Bob fremdeles har beholdt $2n$ bit og de kun trenger n bit til selve kodingen av meldingen kan de bruke halvparten til å verifisere at ingen tyvlyttet til overføringen. De kan for eksempel bruke annenhver bit til verifikasjon og annenhver til koding. Bitene de bruker til verifikasjon kan de trygt sammenligne over en ukryptert linje. Dersom ingen har tyvlyttet hadde alle elektronene samme kvantetilstand da Bob mottok dem som da Alice sendte dem. I så fall har Alice og Bob to identiske rekker av 0 og 1. Hvis Eva har forsøkt å snappe opp nøkkelen derimot, vil halvparten av elektronene ha endret kvantetilstand før Bob mottok dem. Siden det da kun er 50% sannsynlighet for å måle samme bit-verdi som den som ble sendt vil dette si at en fjerdedel av bitene Alice og Bob sammenligner ikke stemmer overens. Alice og Bob kan altså på denne måten utveksle en krypteringsnøkkel og få en sikker verifikasjon av at nøkkelen ikke ble fanget opp underveis.

Kapittel 6

Kvante-logiske porter

Beregninger i en klassisk datamaskin blir gjort av logiske porter som tar inn en eller flere bit og gir ut en eller flere bit som svar. For eksempel tar en AND-port inn to bit og gir ut svaret 1 dersom begge inn-bitene er 1, ellers gir den ut svaret 0. Tilsvarende blir beregninger i en kvantedatamaskin gjort av kvante-logiske porter som tar inn en eller flere qubit og gir ut en eller flere qubit som svar. Likhetene mellom de to typer datamaskiner er altså store, men vi skal etter hvert se at kombinasjonen av at en qubit kan være i en superposisjon mellom 0 og 1 og at to eller flere qubit kan være sammenfiltret gir kvantedatamaskinen muligheter som går langt utover det klassiske datamaskiner har.

6.1 Logiske porter og boolsk algebra

På grunn av den klare analogien med vanlige logiske porter er det nyttig å ha dette friskt i minne når vi skal studere kvante-logiske porter. Derfor gir jeg et kort overblikk av klassiske logiske porter og hvordan de kan kombineres før jeg introduserer den kvantemekaniske versjonen.

6.1.1 Boolsk algebra

Matematikken som brukes for å analysere logiske porter¹ og nettverk av slike er boolsk algebra. Boolsk algebra er en enkel algebra som opererer på variabler som kun kan ha to mulig verdier: SANT eller USANT. I en datamaskin

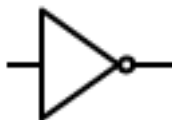
¹Ofte brukes begrepet operasjoner i stedet for porter, spesielt når man snakker om boolsk algebra på et mer abstrakt nivå. Det er et en-til-en forhold mellom operasjonene i boolsk algebra og logiske porter anvendt i logiske kretser så distinksjonen mellom operasjoner og porter er ikke viktig.

assosieres SANT med bit-verdien 1 og USANT med bit-verdien 0, og i det videre vil jeg bruke 1 og 0 som de mulige verdiene til de boolske variablene. De grunnleggende regneoperasjonene i den boolske algebraen er:

NOT (symbol \neg)

NOT er en port/operasjon som tar inn en bit og gir ut en bit. En NOT-port vil alltid endre bit-verdien til det motsatte som vist i sannhetstabellen nedenfor.

P	$\neg P$
0	1
1	0

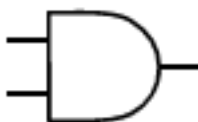


Figur 6.1: Venstre: Sannhetstabell for NOT-operatoren. Høyre: Kretssymbol for NOT-port.

AND (symbol \wedge)

AND er en port/operasjon som tar inn to bit og gir ut en bit. AND gir ut 1 dersom begge inn-bitene er 1, ellers gir den ut 0 som vist i sannhetstabellen nedenfor.

P	Q	$P \wedge Q$
0	0	0
0	1	0
1	0	0
1	1	1



Figur 6.2: Venstre: Sannhetstabell for AND-operatoren. Høyre: Kretssymbol for AND-port.

OR (symbol \vee)

OR er en port/operasjon som tar inn to bit og gir ut en bit. OR gir ut 1 dersom minst én av inn-bitene er 1, ellers gir den ut 0 som vist i sannhetstabellen nedenfor.

P	Q	$P \vee Q$
0	0	0
0	1	1
1	0	1
1	1	1



Figur 6.3: Venstre: Sannhetstabell for OR-operatoren. Høyre: Kretssymbol for OR-port.

6.1.2 Sammensatte porter

De ulike portene som er presentert ovenfor kan kombineres til å representere en vilkårlig bineær funksjon², altså en funksjon som tar et antall bit inn og gir ut et antall bit ut med en spesifisert regel for hva som ut verdien(e) blir gitt innverdien(e). Noen slike kombinasjoner er spesielt hyppig brukt og har derfor fått egne navn og symboler. Dette inkluderer:

XOR (symbol \oplus)

XOR, eller exclusive or, er en operasjon/port som tar inn to bit og gir ut en bit. Denne representerer en enten/eller, altså en port som gir ut verdien 1 hvis én, men ikke begge inn-bitene har verdien 1. Ellers gir den ut verdien 0. XOR kan konstrueres som $P \oplus Q = (P \wedge \neg Q) \vee (\neg P \wedge Q)$.

²Det kan vises at det er tilstrekkelig med operasjonene \neg og \wedge for å oppnå dette, men det er likvel en vanlig konvensjon å beholde \vee på listen over de grunnleggende logiske operasjonene.

P	Q	$P \oplus Q$
0	0	0
0	1	1
1	0	1
1	1	0



Figur 6.4: Venstre: Sannhetstabell for XOR-operatoren. Høyre: Kretssymbol for XOR-port.

NAND (symbol \uparrow)

NAND er en kombinasjon av NOT og AND. Den tar inn to bit og gir ut en bit. Siden NOT er kombinert med AND gir den alltid ut den motsatte verdien av hva AND ville gjort. NAND kan konstrueres som $P \uparrow Q = \neg(P \wedge Q)$.

P	Q	$P \uparrow Q$
0	0	1
0	1	1
1	0	1
1	1	0



Figur 6.5: Venstre: Sannhetstabell for NAND-operatoren. Høyre: Kretssymbol for NAND-port.

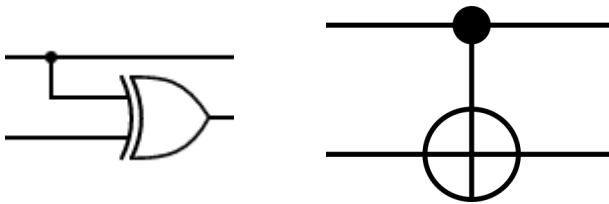
CNOT - Controlled NOT

CNOT er en port som er veldig viktig for oss når vi kommer til kvantedata-maskiner, så derfor tar jeg med beskrivelsen av den klassiske versjonen her. Dette er det første eksempelet vi treffer på av en port med mer enn én ut-bit: CNOT tar inn to bit og gir ut to bit. Den første inn-biten (x) er kontroll-biten. Verdien av denne biten påvirker hva porten kommer til å gjøre med den andre biten (y). I tillegg blir kontroll-biten sendt uforandret ut av porten. Dersom kontroll-biten er 0 vil porten sende den andre biten uforandret ut, mens dersom kontroll-biten er 1 vil porten virke som en NOT-port og

altså endre verdien av den andre biten før den sendes ut. Om vi sammenligner med portene som er diskutert ovenfor finner vi at den andre ut-biten bestemmes av en XOR mellom de to innbitene, altså beskrives CNOT av funksjonen $f(x,y) = (x, x \oplus y)$. Effekten av CNOT-porten er oppsummert i sannhetstabellen nedenfor.

CNOT kan konstrueres av en oppsplitting og en XOR-port som vist i figuren nedenfor. Figuren viser også kretssymbolet som vanligvis brukes for CNOT-porter.

Inn		Ut	
x	y	x	$x \oplus y$
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0



The diagram consists of two parts. The left part shows a circuit where an input line splits into two, which then enter an XOR gate. The right part shows the standard CNOT gate symbol, which consists of a control line (top) with a dot and a target line (bottom) with a circle, connected by a vertical line.

Figur 6.6: Venstre: Sannhetstabell for CNOT-operatoren. Midten: CNOT konstruert med en oppsplitting og en XOR. Øverste inn-bit er x og nederste er y . Tilsvarende er øverste ut-bti x og nederste $x \oplus y$. Høyre: Kretssymbol for CNOT-port.

CNOT har den interessante egenskapen at den er reversibel. Dette er den fordi det er et en-til-en-forhold mellom hva som blir sendt ut og hva som blir sendt inn. Med andre ord: Hvis vi ser hva som kommer ut er det bare én mulighet for hva som ble sendt inn for å produsere dette resultatet. CNOT er dessuten sin egen invers—altså hvis vi lar det som kommer ut av en CNOT-port være innverdiene for den neste kommer vi tilbake til de bit-verdiene vi startet med.

6.2 Generalisering til kvante-logiske porter

For å lage en kvantedatamaskin trenger vi å lage en qubit-versjon av portene som er diskutert ovenfor. Vi støter da straks på en interessant utfordring: mens en klassisk bit alltid er enten 0 eller 1 vil en qubit generelt være i en superposisjon av 0 og 1. Hvordan skal vi lage sannhetstabellene når qubitene har et kontinuerlig sett av mulige verdier? La oss først få på plass litt notasjon som er nyttig i den videre diskusjonen. Nå er det tilstrekkelig for oss å jobbe

med én basis, og der velger vi $\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 0 \end{bmatrix} \right\}$. For å forenkle notasjonen litt kommer jeg for det meste til å skrive vektorene i bra-ket notasjon, med der basisvektorene er identifisert som

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ og } |1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

En generell qubit kan da skrives som $|a\rangle = a_0|0\rangle + a_1|1\rangle$ der $a_0^2 + a_1^2 = 1$. Når vi måler verdien av denne qubiten vil vi finne enten $|0\rangle$ eller $|1\rangle$ med sannynligheter henholdsvis a_0^2 og a_1^2 . Hvis vi har mer enn en qubit å ta hensyn til, må vi ta tensorproduktet av basisvektorene for å finne den nye basisen. For eksempel er basisen for to qubit

$$\{|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle\}.$$

For å forenkle notasjonen ytterligere innfører vi konvensjonen at $|00\rangle = |0\rangle \otimes |0\rangle$ og så videre, slik at basisen kan skrives som

$$\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}.$$

En generell kombinasjon av to qubit kan da skrives som $|b\rangle = b_{00}|00\rangle + b_{01}|01\rangle + b_{10}|10\rangle + b_{11}|11\rangle$ der $b_{00}^2 + b_{01}^2 + b_{10}^2 + b_{11}^2 = 1$.

6.2.1 Ingen kloning-teoremet

Vi treffer på en annen viktig forskjell mellom klassisk logikk og kvantelogikk dersom vi ønsker å klonen en qubit—det vil si å lage en ekstra kopi av en qubit som er identisk med den vi har. Med klassiske bit er dette ikke noe problem. Hvis vi har en bit med en vilkårlig verdi kan vi uten problemer lage vilkårlig mange kopier av denne. Slik er det ikke i kvanteverden. Det kan vises at i det generelle tilfellet kan man ikke lage en kopi av en qubit slik at man sitter igjen med to qubit som er identiske og lik den vi startet med. Så lenge vi jobber med qubit som har en bestemt verdi er det riktignok ingen forskjell, men for å utnytte oss av fordelene som kan oppnås ved å bruke qubit i superposisjon mellom ulike verdier må algoritmene i en kvantedatamaskin lages på en slik måte at kloning av qubit er unødvendig.

Jeg vil ikke forsøke å bevise ingen kloning-teoremet her, men kun gi kvalitative argumenter som sannsynliggjør at det er riktig. En vilkårlig qubit kan som tidligere beskrevet skrives som $|a\rangle = a_0|0\rangle + a_1|1\rangle$. Dersom vi ønsker å måle verdien av qubiten vil vi aldri få noe annet enn $|0\rangle$ eller $|1\rangle$. Hvis vi kjenner a_0 og a_1 kan vi riktignok beregne sannsynligheten for hvert av de to

ulike måleresultatene, men hva hvis vi har en qubit i en ukjent tilstand? Der-som vi for eksempel får resultatet $|0\rangle$ er det eneste vi kan si om koeffisientene at $a_0 > 0$. Vi kan altså ikke måle oss frem til hva koeffisientene a_0 og a_1 er. Men hvis vi ikke kan hente ut denne informasjonen, hvordan kan vi da lage en identisk kopi?

6.3 Matematisk beskrivelse av kvante-logiske porter

Siden vi beskriver tilstanden til en qubit i form av en vektor er det naturlig å beskrive portene i form av matriser. Gitt en vilkårlig qubit

$$|a\rangle = a_0|0\rangle + a_1|1\rangle = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix}$$

Oppgaven til en port er å gjøre en operasjon på denne vektoren slik at resultatet også blir en vektor som representerer en gyldig qubit-verdi. En enkel slik operasjon er å multiplisere vektoren med en 2×2 matrise, siden resultatet av denne multiplikasjonen er en vektor med samme dimensjon som vi startet med. Enhver 2×2 matrise vil representere en mulig port som tar en qubit som inn-verdi og gir ut en qubit som ut-verdi, men vi skal bare se på fem matriser som representerer alle en-til-en porter vi har behov for.

6.3.1 \mathbb{I} , \mathbb{Z} , \mathbb{X} og \mathbb{Y}

Den enkleste porten representeres av identitetsmatrisen

$$\mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

som ganske enkelt gir tilbake den samme qubiten vi startet med som vi kan se ved å anvende den på en vilkårlig qubit

$$\mathbb{I}|a\rangle = \mathbb{I}(a_0|0\rangle + a_1|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = a_0|0\rangle + a_1|1\rangle = |a\rangle.$$

En port som tilsynelatende gir ganske lik virkning representeres av matrisen

$$\mathbb{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Anvendt på basisvektorene gir denne

$$\begin{aligned} |0\rangle &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle, \\ |1\rangle &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ -1 \end{bmatrix} = -|1\rangle. \end{aligned}$$

Siden en qubit $-|1\rangle$ er ekvivalent med en qubit $|1\rangle$ gir altså \mathbb{Z} i likhet med \mathbb{I} ingen endring så lenge vi anvender den på basisvektorer—altså på qubiter som er i en veldefinert tilstand (i motsetning til å være i en superposisjon). For \mathbb{I} var den samme konklusjonen gyldig for en vilkårlig qubit, men det er ikke tilfellet for \mathbb{Z} . Hvis vi nå anvender denne operatoren på en vilkårlig qubit finner vi:

$$\mathbb{Z}|a\rangle = \mathbb{Z}(a_0|0\rangle + a_1|1\rangle) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_0 \\ -a_1 \end{bmatrix} = a_0|0\rangle - a_1|1\rangle.$$

Dette er en qubit med lik sannsynlighet for at målingen av verdien vil gi hver av de to mulighetene som qubiten vi startet med, altså

$$\begin{aligned} P(|0\rangle) &= a_0^2, \\ P(|1\rangle) &= (-a_1)^2 = a_1^2, \end{aligned}$$

men det er fremdeles ikke den samme qubiten. Endringen som \mathbb{Z} gjør på qubiten omtaler vi som at den *endrer det relative fortegnet*, og dette relative fortegnet er av stor betydning når vi ser på sammenfiltrede qubiter.

\mathbb{X} og \mathbb{Y} er i likhet med \mathbb{I} og \mathbb{Z} et par av porter som har lignende, men ikke identisk virkning på qubiter. Vi ser effekten av portene ved å anvende de på en vilkårlig qubit

$$\begin{aligned} \mathbb{X}|a\rangle &= \mathbb{X}(a_0|0\rangle + a_1|1\rangle) = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_1 \\ a_0 \end{bmatrix} = a_1|0\rangle + a_0|1\rangle, \\ \mathbb{Y}|a\rangle &= \mathbb{Y}(a_0|0\rangle + a_1|1\rangle) = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_1 \\ -a_0 \end{bmatrix} = a_1|0\rangle - a_0|1\rangle. \end{aligned}$$

Hvis vi først setter $a_0 = 1, a_1 = 0$ eller $a_0 = 0, a_1 = 1$ for å studere virkningen på basisvektorer ser vi at både \mathbb{X} og \mathbb{Y} er en slags NOT-port—de endrer $|0\rangle$ til $|1\rangle$ og motsatt. Forskjellen på de to portene er at dersom vi har en qubit som er i en superposisjon vil \mathbb{Y} endre det relative fortegnet, mens \mathbb{X} ikke gjør det.

6.3.2 Hadamard-porten \mathbb{H}

Den viktigste porten som virker på én qubit er Hadamard-porten

$$\mathbb{H} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

Faktoren $\frac{1}{\sqrt{2}}$ er tatt med for å beholde normaliseringen av qubitene—altså slik at kvadratsummen av koeffisientene ikke endres. For å se hvorfor Hadamard-porten er viktig studerer vi hvilken effekt den har på basisvektorene:

$$\begin{aligned} \mathbb{H}|0\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ \mathbb{H}|1\rangle &= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \end{aligned}$$

Vi ser altså at når Hadamard-porten virker på en qubit som er i en veldefinert tilstand blir resultatet en qubit som er i en superposisjon med lik sannsynlighet for å bli målt til hver av de to ulike verdiene.

6.3.3 CNOT

Vi har sett at den klassiske CNOT-porten tar inn to bit og gir ut to bit. Dersom kontroll-biten har verdien 1 virker CNOT som en NOT-port på den andre biten. I den kvantemekaniske versjonen av CNOT ønsker vi at porten skal ha den samme effekten så lenge den anvendes på basisvektorer. Det vil si at vi vil at sannhetstabellen skal se slik ut

Inn		Ut	
x	y	x	$x \oplus y$
$ 0\rangle$	$ 0\rangle$	$ 0\rangle$	$ 0\rangle$
$ 0\rangle$	$ 1\rangle$	$ 0\rangle$	$ 1\rangle$
$ 1\rangle$	$ 0\rangle$	$ 1\rangle$	$ 1\rangle$
$ 1\rangle$	$ 1\rangle$	$ 1\rangle$	$ 0\rangle$

Inn	Ut
$ 00\rangle$	$ 00\rangle$
$ 01\rangle$	$ 01\rangle$
$ 10\rangle$	$ 11\rangle$
$ 11\rangle$	$ 10\rangle$

Figur 6.7: Sannhetstabell for kvantemekanisk CNOT-port. Venstre: tabellen skrevet fullt ut. Høyre: kompakt notasjon.

Foreløpig ser dette veldig likt ut til den klassiske versjonen, men som vi så med \mathbb{Z} og \mathbb{Y} kan det likevel skje ting når vi bruker porten på vektorer som ikke er basisvektorer. En generell kobinasjon av to qubit kan skrives som

$$r|00\rangle + s|01\rangle + t|10\rangle + u|11\rangle$$

Siden matrisemultiplikasjon er en lineær operasjon gir CNOT anvendt på denne tilstanden av to qubit

$$\begin{aligned} \text{CNOT}(r|00\rangle + s|01\rangle + t|10\rangle + u|11\rangle) \\ = r \text{CNOT}(|00\rangle) + s \text{CNOT}(|01\rangle) + t \text{CNOT}(|10\rangle) + u \text{CNOT}(|11\rangle) \\ = r|00\rangle + s|01\rangle + u|10\rangle + t|11\rangle. \end{aligned}$$

Effekten er altså å bytte om amplitudene til $|10\rangle$ og $|11\rangle$, mens amplitudene til de andre komponentene forblir uforandret. Et konkret eksempel viser hvorfor denne porten er svært interessant. La

$$\begin{aligned} x &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \\ y &= |0\rangle. \end{aligned}$$

Inn-tilstanden skrevet i den kompakte notasjonen er da

$$\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle).$$

Når vi så anvender CNOT får vi

$$\text{CNOT}\left(\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle).$$

De to qubitene vi startet med var uavhengig av hverandre, men resultatet etter CNOT-porten er to sammenfiltrete qubit!

Bibliografi

- [1] Right. Hon. Lord Kelvin G.C.V.O. D.C.L. LL.D. F.R.S. M.R.I. I. nineteenth century clouds over the dynamical theory of heat and light. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, 2(7):1–40, 1901.
- [2] J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1:195–200, Nov 1964.
- [3] Stuart J. Freedman and John F. Clauser. Experimental test of local hidden-variable theories. *Phys. Rev. Lett.*, 28:938–941, Apr 1972.
- [4] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental tests of realistic local theories via bell’s theorem. *Phys. Rev. Lett.*, 47:460–463, Aug 1981.
- [5] C.H. Bennett and G Brassard. Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, 175, 1984.