

Matematikken bag Kvantemekanik

Hvad kan en kvantecomputer?

Du skal nok ikke regne med se en kvante-gamer pc lige foreløbig, men den spiller en stor rolle inde for internetsikkerhed. Når du på Messenger sender en besked om en fest lokation så krypteres din besked, så kun dem du sender den til kan læse den.

Kort sagt er kryptering to meget store primtal ganget sammen, hvor at kun afsenderens og modtagerens computer kender primtallene, som gør det muligt at læse beskeden. Hvis andre vil læse dine beskeder, skal de altså kunne afkode primtallet. Den klassiske computer er rigtig dårlige til dette. Kvantecomputere er ikke så hurtige, men i stedet for blindt at gætte, så bruger den ***Shor’s algorime***. Kvantecomputere kan altså gætte på tallet, er det ikke det rigtige, kan man med algoritmen regne gæt, som er ’bedre’ end det første. Går man det flere gange, ender man med de rigtige primtal. Laves en kvantecomputer med nok qubits, så vil ejeren derfor kunne ***dekryptere*** alt på internettet og ødelægge alt sikkerhed og privatliv. Det hele kommer an på hvem der først får lavet en stor kvantecomputer.

Nu ser du måske kvantecomputere, som noget slemt, men heldigvis for os, så er der en masse godsindede forskere, som arbejder på at få lavet en kvantecomputer først. Der findes også ***kvantekryptering***, som er en krypteringsform kvantecomputere vil kunne bruge og som heller ikke en kvantecomputer ville have nemt ved at knække. Så hvis vi får udbredt denne kryptering først, så ville denne kryptering kunne integreres i vores alles internet og vi vil igen kunne føles os bare lidt mere trygge.

Men du skal ikke gå og være bange. Kvantecomputere er langt fra at kunne destruere eller sikre noget endnu, så du kan trygt skrive din adresse til dine venner og vide at kun dig, din ven og Facebook kan læse din besked.

Komplekse tal

Komplekse tal er i bund og grund bare tal, hvor variabelen ”i” indgår, og kan altså generaliseres til formen: $z = x + y \cdot i$ hvor x og y begge er reelle tal og x er den reelle del og $y \cdot i$ den imaginære del.

Eksempler på komplekse tal kan altså være: $5 + 3 \cdot i$, $7 \cdot i$ hvor x er 0, 2 hvor y er 0.

”i” i komplekse tal opfylder, at $i^2 = -1$. Det betyder, at vi kan reducere enhver kompleks ligning ned til grundformlen $z = x + y \cdot i$, f.eks. med ligningen: $3i + 6 + 2i = 6 + 5i$ eller $2i \cdot 4i + 7 = 7 + 8 \cdot i^2 = 7 + 8 \cdot (-1) = -1$

Kompleks konjugering

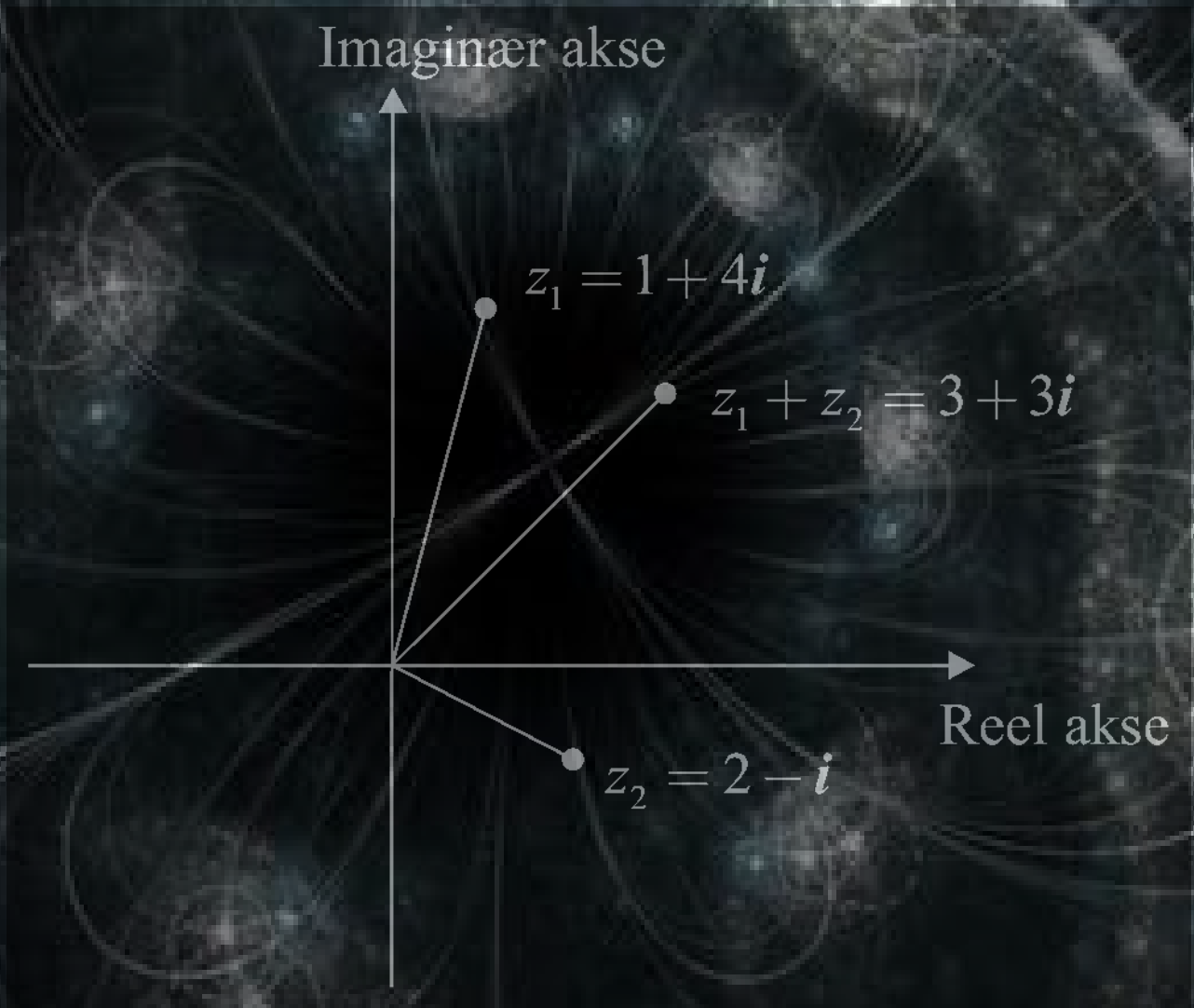
Komplekse tal kan konjugeres ved at sætte en streg over, der betyder, at fortegnet i det komplekse tal bliver ændret således, at det ser sådan ud: $\bar{z} = x - y \cdot i$.

Det kan man f.eks. bruge, når man dividerer komplekse tal.

Det komplekse plan

Komplekse tal kan visualiseres på et komplekst plan i et koordinatsystem, hvor 1. akse er x, den reelle del og 2. akse er $y \cdot i$, den imaginære del. De komplekse tal hvor y er 0 vil ligge på den reelle akse og være rent reelle, de komplekse tal hvor x er 0 vil ligge på den imaginære akse og være rent imaginære, og komplekse tal hvor hverken x eller y er 0 vil kunne bevæge sig rundt i hele koordinatsystemet.

Det komplekse plan:



Hvis du vil vide mere om kryptering og Shor:



Qubits

Som nævnt bruger man i en kvantecomputer noget, der hedder qubits. Qubits er en partikel med det, man kalder et spin. Det kunne f.eks. være en elektron, men man kan også anvende andre partikler med andre former for spin f.eks. fotoner. Elektronen kan så optræde i to tilstande.

De to tilstande hedder spin op +½ og spin ned -½. I en kvantecomputer regner man med sandsynligheden for at elektronen er spin op eller spin ned. Før man har målt den, befinder den sig i begge tilstande.

Efter man har målt dens tilstand til at være spin op eller ned, vil man fremover altid måle den samme tilstand.

Blochsfæren:



Entanglement

Et særligt specielt fænomen opstår, når to qubits sættes sammen. De to qubits vil lave det man kalder en entanglement, der betyder sammenfiltrering. Under denne sammenfiltrering sker der noget med de to qubits, der får dem til at opføre sig som værende både i spin op og i spin ned tilstanden på samme tid. Hvis man efter sammenfiltreringen separerer de to qubits, vil de altså igen være enten spin op eller ned med en vis sandsynlighed. Det mystiske består i, at hvis vi nu antager, at de to qubits befinder sig virkelig langt fra hinanden, flere hundrede kilometer, så kan man måle den ene qubits tilstand, og så vil den anden på mystisk vis have den samme tilstand. Så hvis man måler den ene qubit til at være spin op, ved man, at den anden også er spin op. Selvom de ikke længere er forbundet, er det altså som om, der er en slags mystisk kraft, der gør at man kun kan måle den samme tilstand for de to partikler. Det er svært at tro, at sådan noget skulle have gang på jord, men ikke desto mindre har forskere eksperimenteret og igen og igen fået bekræftet teorien.

Generaliseringen af basisvektorerne ($|0\rangle$, $|1\rangle$) til to-qubits basisvektorer er:

$$\begin{aligned} |0\rangle|0\rangle &= \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, & |0\rangle|1\rangle &= \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \\ |1\rangle|0\rangle &= \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, & |1\rangle|1\rangle &= \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \end{aligned}$$
$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Ikke alle to-qubit tilstande er sammenfiltret, men et eksempel på en to-qubit sammenfiltret tilstand, hvor $|0\rangle|0\rangle$ og $|1\rangle|1\rangle$ er to-qubits, er:

Kvante Målinger

Som beskrevet under “Qubits” er det muligt at måle tilstanden af en qubit. Klassiske bits i computeren du bruger har to tilstande: 1 eller 0 (Se venstre side af fig. Blochsfæren).

En Qubits mulige tilstande er illustreret af en Blochsfæren (Se højre side af fig. Blochsfæren), og er lidt mere besværlig at måle. Et eksempel på en mulig Qubit er en elektron, som er noget forsker undersøger.

Svaret på målingen af en qubit er sandsynligheden for at vi finder en qubit i et tilstand vi måler for. Det er lidt ligesom farven grøn. Grøn er både blå og gul tilsammen. Hvis vi “måler grøns tilstand” i basis eller for “gul” får vi en procent af gul. I basis “blå” får vi et procent af blå. Men det vil sige at det godt kan være det samme samtidig: grøn (hvilket er blå og gul).

Formlen vi bruger for at måle er som følger, forklaret med et eksempel:

$$\text{Prob}(0) = |\langle 0 | \psi \rangle|^2 \equiv \left| (1, 0) \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \right|^2 = |\alpha|^2$$

Måling i basis: bra 0. Ligesom at måle for grøn i basis "blå" eller "gul"

Bra 0 som rækkevektor

Absolut værdien i anden af indreproduktet

Sandsynligheden for at vektoren vi måler for findes i tilstand nul. Ligesom sandsynligheden for at finde "blå" i "grøn"

Vektoren/Qubiten vi måler tilstanden af. Det er vores "grøn".

Vektoren vi måler tilstanden af. Det er "farven grøn"