Gymnasielærerens guide til kvanteuniverset

Albert H. Werner, QMATH og NBIA, Angelo Lucia, QMATH, Jan Philip Solovej, QMATH, Johannes Borregaard, QMATH, Laura Mančinska, QMATH, Mads Peter Steenstrup, Rysensteen Gymnasium og Robert Jonsson, QMATH

1. Indledning

Denne artikel er skrevet af en gruppe forskere fra centret QMATH (Centre of Excellence for the Mathematics of Quantum Theory, qmath.ku.dk) ved Institut for Matematiske Fag ved Københavns Universitet i samarbejde med gymnasielærer *Mads Peter Steenstrup* fra Rysensteen gymnasium. QMATH centret er oprettet med støtte fra VILLUM Fonden og beskæftiger sig med kvantefysikkens matematik med fokus på kvantestof og kvanteinformation. Det er et af centrets ambitioner at formidle disse emner til en bredere kreds og specielt at have et nært samarbejde med gymnasiet. Dette har motiveret os til at skrive denne artikel som indføring til kvanteinformation og dets potentiale for kommunikation og beregninger, som måske en dag vil finde anvendelse i en kvantecomputer. Artiklen er rettet specielt mod lærere, der underviser i matematik, men vi har forsøgt at skrive artiklen, så den kan læses af alle, der har taget et kursus i lineær algebra. Det er m.a.o. ikke nødvendigt at kunne noget fysik for at læse artiklen, men emnet er selvfølgelig interessant, fordi de tilstande og målinger vi taler om, i princippet kan implementeres i virkelige fysiske systemer. Vi håber og tror på, at aspekter af emnet er på et niveau, hvor de kan formidles til gymnasielever enten i forbindelse med særlige emner eller som SRP projekter. Afsnit 2 beskriver den grundlæggende teori, mens eksempler på udvalgte emner inden for kryptering og algoritmer er beskrevet i afsnit 3. I afsnit 4 har vi beskrevet mulige SRP retninger indenfor emnet. Vi står med glæde til rådighed for et samarbejde, hvad angår udarbejdelse af undervisningsmateriale eller hjælp omkring SRP projekter.

2. Grundlæggende kvanteteori

I dette afsnit giver vi en oversigt over, hvordan kvanteteori formuleres i termer af lineær algebra. Til dette formål studerer vi en *qubit* (kvantebit) der nok er den simpleste enhed i kvanteinformationsprocesser. En qubit er inden for kvanteinformation, hvad der svarer til en klassisk bit og er således et abstrakt teoretisk begreb, der i en computer skal implementeres, som en fysisk tilstand af computerens hardware. På tilsvarende vis realiseres værdien af en klassisk bit som magnetiseringen af et harddiskelement eller strømmen gennem et halvlederelement. Der forskes i dag i mange mulige kandidater til qubitsystemer og fremtidens kvanteteknologier kan blive baseret på qubit realiseret som polarisationstilstande af fotoner, elektroniske spintilstande i atomer eller ladningstilstande af superledende kredsløbselementer. Specielt har IBM allerede en første prototype af en kvantecomputer baseret på superledende qubit, som er åben til brug for offentligheden, quantumexperience.ng.bluemix.net/qx/experience.

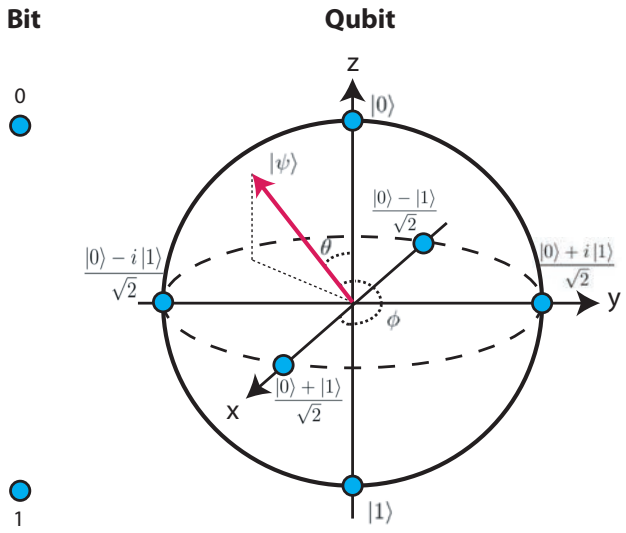


Fig. 1
Blochsfæren som visualisering af en qubit. Mens den klassiske bit kun kan findes i de to tilstande nordpolen (0) eller sydpolen (1) kan qubitten findes i superpositioner

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

overalt på sfæren.

2.1 Kvantetilstande som vektorer

Tilstandsrummet for en enkelt klassisk bit er mængden indeholdende præcis to elementer svarende til tilstandene 0 eller 1. En qubit har tilsvarende to tilstande, der betegnes $|0\rangle$ og $|1\rangle$, men disse er elementer i et langt større tilstandsrum: Tilstandene $|0\rangle$ og $|1\rangle$ er vektorer i det todimensionelle komplekse Hilbertrum $\mathcal{H} = \mathbb{C}^2$ (Hilbertrum: Fuldstændigt vektorrum med positiv definit indre produkt). Desuden udgør de en ortonormalbasis i tilstandsrummet, dvs. vi kan identificere dem med søjlevektorerne

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad , \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

En vilkårlig vektor $|\psi\rangle \in \mathcal{H}$ i tilstandsrummet kan derfor skrives som en linearkombination

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \equiv \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

med komplekse koefficienter $\alpha, \beta \in \mathbb{C}^2$. Blandt alle vektorerne i $\mathcal{H}$ vil de, der har norm 1, dvs. $|\alpha|^2 + |\beta|^2 = 1$, svare til forskellige fysiske tilstande for qubitten (dette betyder, at tilstandsrummet for en qubit er et komplekst projektivt rum). En

qubittilstand som linearkombination kaldes for en superposition. Normaliseringsbetingelsen er der, fordi qubittilstanden beskriver udfaldssandsynlighederne for målinger på det fysiske system, som udgør qubitten. Normaliseringen sikrer, at sandsynlighederne for de forskellige måleresultater summer til 1. Sandsynligheden for at en qubit i tilstand $|\psi\rangle$ ved en måling observeres i tilstand $|0\rangle$, er bestemt ved det indre produkt mellem de to tilstande ud fra

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

Denne sandsynlighedsregel generaliserer til alle typer af målinger (se afsnit 2.2).

Ovenfor har vi implicit introduceret Dirac notationen for vektorer og deres duale. En vektor betegnes her ved et såkaldt *ket*–symbol $|\psi\rangle \in \mathcal{H}$, mens en dual vektor betegnes ved et *bra*–symbol

$$\langle\psi| = \alpha^*\langle 0| + \beta^*\langle 1| \equiv (\alpha^*, \beta^*) \in \mathcal{H}^*$$

hvor en asterisk betegner kompleks konjugering. Det indre produkt mellem to vektorer $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ og $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ fås ved at anvende den duale vektor $\langle\psi_1|$ på vektoren $|\psi_2\rangle$, og er givet ved *braket*–symbolet

$$\langle\psi_1|\psi_2\rangle = \alpha_1^*\langle 0| + (\beta_1^*\langle 1|)(\alpha_2|0\rangle + \beta_2|1\rangle) = \alpha_1^*\alpha_2 + \beta_1^*\beta_2$$

som nemt evalueres ved at hæve parenteserne og benytte, at $\langle 0|0\rangle = \langle 1|1\rangle = 1$, og $\langle 0|1\rangle = \langle 1|0\rangle = 0$. Det er selvfølgelig lig med det sædvanlige udtryk for det indre produkt.

$$\langle\psi_1|\psi_2\rangle = (\alpha_1^*, \beta_1^*)\cdot\begin{pmatrix}\alpha_2\\ \beta_2\end{pmatrix} = \alpha_1^*\alpha_2 + \beta_1^*\beta_2$$

For fuldstændighedens skyld har vi anvendt komplekse tal til at beskrive en general qubittilstand, men vi bemærker, at det er muligt at restringere til reelle koefficienter. Det indre produkt vil da reducere til det velkendte skalarprodukt. Specielt vil indholdet af de følgende afsnit ikke kræve kendskab til komplekse tal. På den anden side kan studiet af en qubit være en god anledning til at introducere komplekse tal til eleverne.

En interessant visualisering af en generel qubittilstand er ved brug af Blochsfæren (se Fig. 1). De tilladte værdier af koefficienterne α og β kan naturligt repræsenteres som punkter på enhedskuglen i 3 dimensioner, hvor hvert punkt på kuglen svarer til en fysiske tilstand af qubitsystemet. Specielt kan vi parametrisere koefficienterne ved $\alpha = \cos\left(\frac{\theta}{2}\right)$ og $\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$, hvor $\theta \in [0;\pi]$ og $\phi \in [0, 2\pi]$. Som det fremgår af Fig. 1 er θ vinklen roteret fra z–aksen og ϕ er rotationen i xy–planen. Vi har benyttet, at en global fase ikke er af betydning for qubittilstanden dvs. $|\psi\rangle$ er samme qubittilstand som $e^{i\phi}|\psi\rangle$, idet kun relative faser har betydning. Det er derfor muligt at lade α være reel. Ortogonale qubittilstande afbildes i modsatte punkter på kuglen fx er $|0\rangle$ på nordpolen ortogonal på $|1\rangle$ på sydpolen.

Inkompatible målinger

Lad os betragte to målebaser: $\{|0\rangle, |1\rangle\}$ og $\{|+\rangle, |-\rangle\}$. Det faktum, at en måling ændrer et systems tilstand, leder til fænomenet inkompatible målinger, hvilket betyder, at målingsstatistikken kan afhænge af hvilken rækkefølge, målingerne foretages i. Betragt for eksempel tilstanden $|0\rangle$. Hvis vi først udfører en måling i 0/1–basen vil Prob(0) = 1 og Prob(1) = 0, og tilstanden vil være uændret efter målingen. En efterfølgende måling i ±–basen vil give begge udfald med 50 % sandsynlighed. Det vil vi også få, hvis vi først udfører en måling i ±–basen. Men hvis vi nu på den resulterende tilstand (enten $|+\rangle$ eller $|-\rangle$) udfører en 0/1–måling vil vi ikke få $|0\rangle$ med sikkerhed, men kun med sandsynlighed 50 %. Det er derfor tydeligt, at målestatistikken afhænger af rækkefølgen af målingerne, hvilket er blevet eksperimentelt eftervist i fx Stern–Gerlach–eksperimentet.

2.2 Målinger

I det foregående afsnit diskuterede vi, hvordan man beskriver tilstanden af et fysisk system i termer af en tilstandsvektor i et Hilbert rum. Det er dog vigtigt at bemærke, at denne tilstandsvektor er et abstrakt objekt, som ikke lader sig direkte observere i et eksperiment. Vi kan kun opnå viden om tilstanden af et ukendt system ved at måle på den. For en qubit svarer en måling til et simpelt Ja/Nej spørgsmål, fx om systemet er i tilstand $|0\rangle$ eller i $|1\rangle$. Som vi så i sidste afsnit er svaret på dette specifikke spørgsmål ikke deterministisk, men sandsynligheden for at opnå et af de to mulige måleresultater afhænger af det indre produkt mellem tilstanden og basisvektorerne $\{|0\rangle, |1\rangle\}$ dvs. $\text{Prob}(0) = |\langle 0|\psi\rangle|^2$ og $\text{Prob}(1) = |\langle 1|\psi\rangle|^2$. Denne procedure kan nu generaliseres til enhver anden ortonormalbasis i $\mathbb{C}^2$. Dvs. ethvert par af ortonormale vektorer $|a\rangle$ og $|b\rangle$ udgør en mulig målebasis med udfaldssandsynligheder $\text{Prob}(a) = |\langle a|\psi\rangle|^2$ and $\text{Prob}(b) = |\langle b|\psi\rangle|^2$. En anden vigtig målebasis udover $\{|0\rangle, |1\rangle\}$ er $\{|+\rangle, |-\rangle\}$–basen, der består af tilstandene $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Da ortonormale vektorer afbildes i modsatte punkter på Blochsfæren kan valget af målebasis visualiseres som en måling langs aksen, der forbinder de to punkter.

Måling i $\{|0\rangle, |1\rangle\}$–basen (0/1–basen) svarer således til en måling langs z-aksen, mens måling i $\{|+\rangle, |-\rangle\}$–basen (±–basen) svarer til x–aksen. Projektionen af en tilstand på måleaksen bestemmer sandsynligheden, fx bliver tilstanden $|1\rangle$ projiceret på midten af x–aksen svarende til, at sandsynlighederne for udfald $|+\rangle$ og $|-\rangle$ begge er 50 % i en måling langs x–aksen (se Fig. 1). En anden vigtig pointe er, at systemets tilstand efter målingen afhænger af udfaldet af målingen. Hvis vi vælger en målebasis $\{|a\rangle, |b\rangle\}$ for et system i tilstand $|\psi\rangle$, og vi observerer måleresultatet $|a\rangle$, så vil tilstanden af systemet efter målingen have ændret sig fra $|\psi\rangle$ til $|a\rangle$ og tilsvarende for resultat $|b\rangle$. Denne opførsel er baggrunden for mange tilsyneladende paradokser ved kvantemekanikken, hvis vi forsøger at forstå den ud fra rent klassiske termer (se også Boks: Inkompatible målinger).

2.3 Flere qubits og sammenfiltring

Interessante problemstillinger i kvanteinformation involverer ofte mere end en enkelt qubit. For at modelere tilstanden af et sammensat kvantesystem, har vi brug for et Hilbertrum som er større end blot summen af dets dele. Hvis Hilbertrummet for en enkelt qubit er $\mathcal{H}_1 = \mathbb{C}^2$, da vil Hilbertrummet for n qubit være $\mathcal{H}_n = \mathbb{C}^{2^n}$. Som i tilfældet med en enkelt qubit vil flerqubit tilstande generelt kunne udtrykkes som linearkombinationer af 2^n enhedsvektorer. Den naturlige generalisering af en–qubit basisvektorerne ($|0\rangle$, $|1\rangle$) til to–qubit basisvektorer er:

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

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

Generalisering af superposition til fler–qubit tilstande leder til fænomenet sammenfiltring (*entanglement* på engelsk), en af kvanteteoriens mest slående konsekvenser. Et eksempel på en to–qubit sammenfiltret tilstand er

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

Denne tilstand er en superposition af tilstandene, hvor begge qubit er i tilstand $|0\rangle$ og begge qubit er i $|1\rangle$. Det betyder, at hvis de to qubit måles i 0/1–basen, vil udfaldene være enten 00 eller 11 med 50 % sandsynlighed hver. Hvis de to qubit måles i ±–basen, vil udfaldet være enten ++ eller −− også med 50 % sandsynlighed hver. Udfaldene er derfor fuldstændigt korreleret uafhængigt af hvilken målebasis, der anvendes, så længe begge qubit måles i den same basis. Det ville også være rigtigt, hvis den ene qubit var på Månen og den anden var nede på Jorden, dvs. hvis de to qubit var fuldstændig adskilt fra hinanden.

Selvom måleresultaterne er tilfældige så vil sammenfiltrede qubit altid give fuldstændig korrelerede resultater, hvis de måles i den samme basis. Det er som om de øjeblikkeligt kender til hinandens målinger (bemærk dog, at sammenfiltring ikke kan bruges direkte til at sende information mellem de to qubit). Dette tilsyneladende paradoks førte Einstein til at tro, at kvantemekanikken var ufuldstændig. Bohr delte ikke denne opfattelse, og det førte til langvarige diskussioner mellem de to. Ikke desto mindre er Bohrs fortolkning blevet underbygget af nylige eksperimentelle verifikationer af de såkaldte Bell–uligheder. På trods af den fundamentale karakter af emnet er Bell–ulighederne velegnede som en SRP problemstilling, der vil tillade eleverne at udforske grundlaget for kvantemekanikken (se afsnit 4).

De korrelationer, som en sammenfiltret tilstand har, overgår, hvad der er muligt for klassiske systemer. Som vi vil illustrere nedenfor, kan dette også udnyttes til at udføre opgaver, som ville være umulige for ethvert klassisk system. Vi understreger, at langt fra alle fler–qubit tilstande er sammenfiltrede. Et eksempel på en ikke–sammenfiltret to–qubit tilstand er $|0\rangle|0\rangle$, som kaldes en separabel tilstand.

2.4 Unitære operatorer og kvantekredsløb

Det centrale mål for en kvanteberegning er at manipulere tilstanden af en eller flere qubit svarende til den informationproces, der ønskes foretaget. Fysisk opnås sådanne operationer ved at manipulere omgivelserne som vores qubit befinder sig i, fx ved at påvirke en elektrons spin med et magnetfelt. I den abstrakte formulering af kvanteinformationsteori kaldes sådanne operationer for kvantegates svarende til logiske gates i en klassisk computer. Matematisk er kvantegates repræsenteret ved unitære operatorer i form af matricer, der virker på systemets Hilbertrum. Specielt opfylder unitære operatorer, at målesandsynlighederne for et kvantesystem stadigt summer til 1 efter en operation (unitære operatorer har den egenskab, at de bevarer det indre produkt. En matrix U er unitær, hvis $U^\dagger U = UU^\dagger = \mathbb{I}$, hvor $U^\dagger$ er den kompleks konjugerede matrix, og $\mathbb{I}$ er identitetsmatricen). Et eksempel på en sådan kvantegate, der virker på en enkelt qubit, er Hadamardgaten

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

Dens effekt er at transformere tilstanden $|0\rangle$ til tilstanden $|+\rangle$ og tilstanden $|1\rangle$ til tilstanden $|-\rangle$ og vice versa, dvs. $H|0\rangle = |+\rangle$ og $H|1\rangle = |-\rangle$. På Blochsfæren (se Fig. 1) vil virkningen af Hadamardgaten svare til en rotation med vinkel π af tilstanden omkring x–aksen efterfulgt af en $\pi/2$–rotation omkring y–aksen. Hadamardgaten kan derfor også benyttes til at skifte mellem 0/1 og ± målebaserne.

I teorien for kvanteberegninger er det bekvemt at repræsentere unitære kvantegates som elementer i såkaldte kvantekredsløbsdiagrammer. For eksempel er kredsløbselementet, der repræsenterer Hadamardgaten:

hvor den højre figur viser dens virkning på input $|0\rangle$, som resulterer i output tilstanden $|+\rangle$. Denne repræsentation er nyttig, når man skal lave kvantekredsløb, der virker på mange qubit.

Et vigtigt eksempel på en gate virkende på to qubit er CNOT (controlled–not) gaten.
Dens virkning er ikke at gøre noget, hvis den første qubit er i tilstand $|0\rangle$, men at ombytte den anden qubit fra $|0\rangle$ til $|1\rangle$ eller fra $|1\rangle$ til $|0\rangle$, hvis den første qubit er i tilstand $|1\rangle$, dvs.

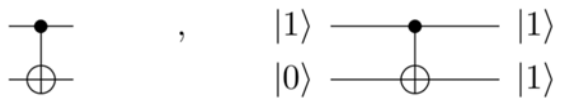
$$U_{\text{CNOT}}|0\rangle|0\rangle = |0\rangle|0\rangle, \quad U_{\text{CNOT}}|0\rangle|1\rangle = |0\rangle|1\rangle,$$

$$U_{\text{CNOT}}|1\rangle|0\rangle = |1\rangle|1\rangle \text{ og } U_{\text{CNOT}}|1\rangle|1\rangle = |1\rangle|0\rangle$$

Den svarer til den unitære operator

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

Kredsløbselementet for CNOT–gaten er



hvor den højre figur viser, hvordan den øverste linie svarer til den første qubit (kontrollen) og den anden linie svarer til den anden (den kontrollerede) qubit.

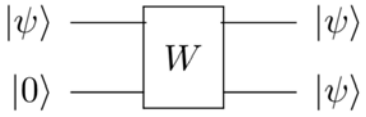
Endelig beskrives en måling ved kredsløbselementet

uden nogen udgående qubit linie.

2.5 No-cloning teoremet

Med den formalisme vi har introduceret indtil videre, er det muligt at vise, at kvanteinformation ikke kan kopieres. Dette er det såkaldte No–Cloning teorem, hvilket er et fundamentalt resultat i kvanteinformationsteori.

En kvantekopieringsmaskine ville være et kredsløbselement, der virker på to qubit. Det ville modtage en generel og ukendt qubittilstand $|\psi\rangle$ som den første qubit og ville så skulle returnere den anden qubit (som startede i tilstanden $|0\rangle$) i samme tilstand samtidig med, at den første qubit forbliver uændret. Med andre ord ville en sådan kopieringsgate W have kredsløbsrepræsentationen:



Kopieringsgaten skal kunne kopiere basistilstandene $|0\rangle$ og $|1\rangle$ korrekt. Dette betyder, at $W|0\rangle|0\rangle = |0\rangle|0\rangle$, og $W|1\rangle|0\rangle = |1\rangle|1\rangle$. Da W er en unitær operator bestemmer disse to egenskaber allerede, hvordan gaten virker på tilstanden $|+\rangle$

$$W|+\rangle|0\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle|0\rangle + |1\rangle|1\rangle\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

Dette er dog ikke tilstanden

$$|+\rangle|+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

hvilket en korrekt kopieringsgate ville skulle returnere. Vi ser, at i modsætning til klassisk information, er det umuligt at kopiere kvanteinformation perfekt. Dette er også grunden til, at teleportation af en kvantetilstand (på sin vis) involverer, at tilstanden først ødelægges for senere at blive genskabt ved destinationen.

3. Kvanteinformation i brug

3.1 Kvantekrypteringsnøgler

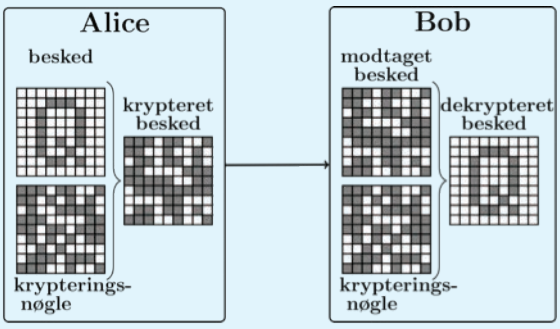
Muligheden for at kommunikere privat i offentlige netværk er en grundsten i moderne kommunikation. Det er forudsætningen for mange online–servicer såsom netbank, autentifikation og hemmelig kommunikation. Standardscenariet for disse kryptografiske opgaver er, at Alice gerne vil sende en besked til Bob på en sådan måde, at Eva, som potentielt aflytter deres kommunikation, ikke kan få nogen information om beskedens indhold.

De fleste kryptografiske protokoller i dag, især asymmetriske protokoller såsom RSA, beror på ikke–beviste antagelser omkring vanskeligheden af at beregne forskellige matematiske funktioner. I RSA er det antagelsen om, at det er vanskeligt at beregne primtalsfaktorerne af et givent tal. En antagelse som bliver udfordret af en potentiel kvantecomputer. På den anden side kan en såkaldt one time pad (se boks) benyttes til en bevisbar sikker krypteringsprotokol. Denne protokol er dog ikke særlig praktisk, fordi Alice og Bob skal dele en hemmelig krypteringsnøgle, der er lige så lang som den besked, de vil sende til hinanden. De må heller ikke genanvende krypteringsnøglen, hvilket ville kompromittere sikkerheden. For at kunne udveksle krypteringsnøglen ville det derfor være nødvendigt for dem at mødes forud for deres kommunikation og blive enige om en tilfældig bit–streng, som de kan bruge som krypteringsnøgle.

One time pad

Antag, at Alice gerne vil sende en hemmelig bit $b \in \{0,1\}$ til Bob, og at de tidligere er blevet enige om en tilfældig bit $k \in \{0,1\}$ ved at slå plat og krone med en perfekt mønt. For en spion, Eva, der ikke var tilstede, da de slog plat og krone, ville sandsynligheden for, at k var enten 0 eller 1 være 1/2. Alice beregner nu $m = b \oplus k$ og afhængigt af værdien af b, vil m enten være lig med k ($b = 0$) eller $1 - k$ ($b = 1$). Symbolet $\oplus$ betyder her addition modulo 2, hvilket svarer til at tjekke om summen er lige eller ulige. For Eva derimod vil m være fuldstændig lige så tilfældig som k, fordi at lægge 0 eller 1 til k modulo 2 ændrer ikke på, at $p(k = 1) = p(k = 0) = 1/2$.

Siden Bob kender værdien af k, kan han dog let beregne $m \oplus k = k \oplus k \oplus b = b$ siden ($0 \oplus 0 = 1 \oplus 1 = 0$). Bob kan derfor let dekryptere beskeden b, selvom den for Eva virker fuldstændig tilfældig. For at kryptere en længere besked, kan man benytte ovenstående metode bit for bit. På den måde kan man vise, at beskeden, der sendes fra Alice til Bob, virker fuldstændig tilfældig for alle, der ikke kender til den tilfældige bit–streng, der er benyttet som krypteringsnøgle. For garanteret sikkerhed er det dog nødvendigt at krypteringsnøglen er lige så lang som beskeden, og at den aldrig genanvendes.



BB84 protokollen

For at køre denne protokol skal Alice være i stand til at generere kvantetilstande i 0/1–basen ($s_{00} = |0\rangle$, $s_{01} = |1\rangle$) samt i ±–basen ($s_{10} = |+\rangle$, $s_{11} = |-\rangle$). Derudover skal Bob være i stand til at måle i begge baser. I den første del af protokollen gentager Alice og Bob følgende punkter L gange:

1. Alice vælger to tilfældige bit p og a.
2. Alice genererer kvantetilstanden s_{ap} og sender den til Bob.
3. Bob vælger en tilfældig bit b og måler tilstanden i tilsvarende 0/1 eller ±–basis. Han noterer både basisvalget (b) og måleresultatet x.

I anden del af protokollen annoncerer Alice offentligt hendes basisvalg p_1. Bob fortæller Alice i hvilke tilfælde, de valgte den samme basis – dette vil i gennemsnit være sket for halvdelen af de L runder. I disse tilfælde skulle Bobs måleresultat gerne stemme overens med Alices tilfældige bit dvs. $p_1 = x_1$. For at teste dette vælger de et tilfældigt udsnit og accepterer de resterende bits som krypteringsnøgle, hvis de ikke finder nogen uoverensstemmelser i udsnittet.

Alice	basis-valg	±	0/1	0/1	0/1	±	±	0/1	±	0/1	0/1
	tilfældig bit	0	1	1	1	0	1	1	0	0	1
Bob	måle-basis	±	±	0/1	0/1	±	±	±	0/1	0/1	0/1
	måle-resultat	0	0	1	1	0	1	1	1	0	1

Hvis Alice er i stand til at sende qubits til Bob, og han er i stand til at foretage kvantemålinger på dem, kan de dog generere en krypteringsnøgle, som kun de kender uden at mødes. Denne kan efterfølgende benyttes som en one time pad. Alle kendte kvantekommunikationsprotokoller til at opnå dette tilhører overordnet en af to kategorier. For at garantere sikker kommunikation beror de enten på sammenfiltring mellem Alice og Bob eller på no–cloning teoremet sammen med inkompatible målinger. Standardeksemplet på den sidstnævnte gruppe er den såkaldte BB84–protokol (se boks). Her sender Alice en række qubit til Bob i enten 0/1 eller ±–basen, og Bob vælger at måle de modtagne qubit tilfældigt i en af de to baser. Efterfølgende vælger de et tilfældigt udsnit af måleresultaterne og tjekker, om Bobs resultater stemmer overens med Alices i de tilfælde, hvor han målte i den samme base som Alice. På denne måde kan de opdage, hvis nogen lyttede med, da dette ville resultere i uperfekte korrelationer. Hvis de ikke har nogle uoverensstemmelser, kan de med høj sikkerhed bruge de resterende måleresultater som krypteringsnøgle. Protokoller baseret på sammenfiltring fungerer ved, at Alice og Bob først verificerer, at de deler en samling af maksimalt sammenfiltrede tilstande, hvilket sikrer, at ingen anden har information om deres kvantetilstande.

At opdage aflytning

Eva ønsker at kende den hemmelige bit a_l, som Alice har indkodet i en kvantetilstand og sendt til Bob. Ifølge No–cloning teoremet kan hun ikke bare gemme en kopi af kvantetilstanden og vente til at Alice annoncerer den korrekte målebasis. Hun bliver i stedet nødt til at vælge en målebasis uden at kende til Alices valg af basis. Lad os for nemheds skyld antage, at Eva også kan vælge mellem målinger i 0/1– eller ±–basen selvom konklusionen i sidste ende gælder for generelle målinger. Vi ser på tilfældet, hvor Alice og Bob altid vælger samme basis. Eva kunne fx have valgt altid at måle i ±–basen. I det tilfælde at Alice også valgte ±–basen, hvilket sker med sandsynlighed 1/2, ville Alice, Bob og Eva alle få den samme bit. Evas måleresultat ville derimod være fuldstændig tilfældigt, hvis Alice og Bob opererede med 0/1–basen, og det samme ville Bobs måleresultat være pga. de inkompatible målinger foretaget af ham og Eva. Bobs måling ville derfor kun stemme overens med Alice halvdelen af tiden, og sandsynligheden for, at alle hans målinger stemte overens, ville aftage eksponentielt med antallet af runder som Alice og Bob vælger at tjekke. Et tilsvarende argument gælder, hvis Eva vælger hendes basis tilfældigt.

3.2 Kvantealgoritmer

Ideen, om at kvanteeffekter kan benyttes til at give en beregningsmæssig fordel over for klassiske computere, stammer fra Feynmans observation om, at simuleringen af et kvantemekanisk system kræver eksponentielt store klassiske ressourcer. Vi kender i dag til mange beregningsmæssige opgaver, hvor kvantealgoritmer overgår deres bedste kendte klassiske modparter, og listen over sådanne opgaver vokser i takt med forskningen på området.

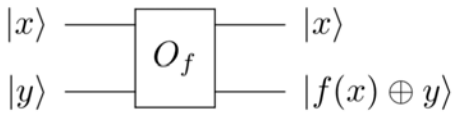
For at give et eksempel på, hvordan kvantealgoritmer virker, kan vi se på følgende problem (Constant–vs–Balanced refererer til, hvorvidt funktionen har den samme eller forskellige værdier for de to input 0,1)

Constant–vs–Balanced Problemet

Antag, at vi er givet black–box adgang til en ukendt funktion $f:\{0,1\}\to\{0,1\}$, og vi vil gerne beregne værdien $f(0)\oplus f(1)$ med så få forespørgsler til vores black–box som muligt.

Black–box adgang betyder, at funktionen er gemt i en sort boks, og vi kan kun tjekke funktionen i nogle specifikke værdier, hvilket vi kalder for forespørgsler. Det ville fx være en forespørgsel at tjekke værdien $f(0)$.

Lad os først overveje, hvad vi kan gøre klassisk. Det er klart, at vi kan beregne $f(0)\oplus f(1)$ med to forespørgsler: første forespørgsel er værdien $f(0)$, og anden forespørgsel er værdien $f(1)$. Det er ikke svært at overbevise sig om, at en enkelt forespørgsel, om det er værdien $f(0)$ eller $f(1)$, ikke er nok til at beregne $f(0)\oplus f(1)$ med sikkerhed. Overraskende nok viser det sig, at en kvantealgoritme af David Deutsch kan løse opgaven med en enkelt forespørgsel. For at kunne gennemgå denne algoritme er det nødvendigt at formalisere, hvordan en kvantecomputer kan foretage forespørgsler i superposition. Det er problematisk at antage, at vores black–box bare giver $|f(x)\rangle$ ved en forespørgsel i $|x\rangle$ for $x\in\{0,1\}$, idet den tilsvarende lineære transformation ikke er unitær i tilfælde, hvor $f(0)=f(1)$. Vi antager derfor en adgang til black–box funktionen via et 2–qubit orakel O_f, som altid er unitær og defineret ved $O_f|x\rangle|y\rangle = |x\rangle|f(x)\oplus y\rangle$ for $x, y\in\{0,1\}$, hvilket udvides til generelle superpositioner (enhedsvektorer i $\mathbb{C}^4$) ved linearitet. Vi kan repræsentere O_f grafisk med det følgende kredsløb



Oraklet har et såkaldt fase kick–back, når $x\in\{0,1\}$ og den anden qubit er i tilstanden $|-\rangle$. Vi ser at

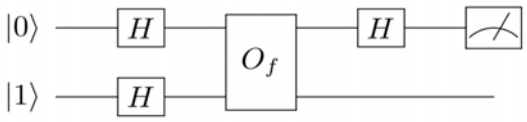
$$O_f(|x\rangle|-\rangle) = |x\rangle \frac{|f(x)\oplus 0\rangle - |f(x)\oplus 1\rangle}{\sqrt{2}}$$
$$= (-1)^{f(x)}|x\rangle|-\rangle$$

Med disse redskaber er vi klar til at beskrive og analysere Deutschs algoritme.

Deutschs kvantealgoritme

1. Initialiser de to qubits i tilstanden $|0\rangle|1\rangle$.
2. Anvend Hadamardgates på begge qubits.
3. Brug O_f til at lave en forespørgsel til black–box funktionen.
4. Anvend en Hadamardgate på den første qubit og mål den i 0/1–basen.

Det kompakte kredsløb for Deutschs algoritme er



Lad os nu vise, at måleresultatet i punkt 4 altid giver værdien $f(0) \oplus f(1)$. For nemheds skyld lader vi $|\psi_i\rangle$ betegne tilstanden efter punkt i af Deutschs algoritme. Det er klart, at $|\psi_1\rangle = |0\rangle|1\rangle$ og $|\psi_2\rangle = |+\rangle|-\rangle$. Vi kan beregne den næste tilstand som

$$|\psi_3\rangle = O_f(|+\rangle|-\rangle)$$
$$= \frac{1}{\sqrt{2}} O_f(|0\rangle|-\rangle) + \frac{1}{\sqrt{2}} O_f(|1\rangle|-\rangle)$$
$$= \frac{(-1)^{f(0)}}{\sqrt{2}}|0\rangle|-\rangle + \frac{(-1)^{f(1)}}{\sqrt{2}}|1\rangle|-\rangle$$
$$= (-1)^{f(0)} \frac{|0\rangle + (-1)^{f(0)\oplus f(1)}|1\rangle}{\sqrt{2}}|-\rangle$$

hvor vi har benyttet det såkaldte fase kick–back i tredje linje. Vi kan nu se, at den første qubit er i tilstanden $|+\rangle$, hvis $f(0) \oplus f(1) = 0$, mens den er i tilstanden $|-\rangle$, hvis $f(0) \oplus f(1) = 1$. Siden $H|+\rangle = |0\rangle$ and $H|-\rangle = |1\rangle$, har vi at

$$|\psi_4\rangle = (-1)^{f(0)}|f(0) \oplus f(1)\rangle|-\rangle$$

og ved at måle den første qubit i 0/1–basen fås værdien $f(0) \oplus f(1)$. Man tænker måske, at det at spare en enkelt forespørgsel ikke betyder så meget. Ikke desto mindre var en generalisering af Constant–vs–Balanced problemet til Boolske funktioner med længere inputs det første problem, hvor det blev vist, at en kvantealgoritme (mere præcist Deutsch–Joza algoritmen) gav en eksponentiel fordel over deterministiske klassiske algoritmer. Andre eksempler på problemer, hvor kvantealgoritmer overgår deres bedste kendte klassiske modparter, er bl.a. søgning i en ustruktureret database (Grovers algoritme) og beregning af primtalsfaktorer (Shors algoritme). Den sidstnævnte er berømt for potentielt at kunne bryde RSA public–key kryptering, hvilket benyttes i stort omfang til sikker overførsel af data.

4. SRP opgaver

Vi mener, at Kvanteinformation kan være et godt emne for en matematik–fysik, –informatik eller –historie SRP. Eleverne kan dykke ned i matematiske emner som matricer, komplekse tal, heltalsmatematik og algoritmer og bruge teorien til at vise overraskende resultater.

Den klassiske krypteringsopgave kan fx få en drejning ved at se på kvantekryptering og informationsoverførsel. Her kan den redegørende del være en beskrivelse at elektroner eller fotoner og deres kvantemekaniske egenskaber og analysen være af systemet Alice–Bob–Eva samt den matematiske formalisme for rotation. No–cloning teoremet beskrevet i afsnit 2.5 spiller en central rolle, da det sikrer, at information ikke kopieres. Det er også muligt at tage fat i den snart gamle diskussion mellem Bohr og Einstein og bruge den matematiske beskrivelse af sammenfiltrede tilstande til at vise, at korrelationen er stærkere kvantemekanisk end klassisk. Her er det oplagt at tage fat på Bells ulighed og udledningen af denne. Det er også muligt at lave forsøg med en rigtig kvantecomputer. IBM har en og har lavet et online interface, hvor man relativt nemt kan eksperimentere med forskellige kvantetilstande og målinger, IBM quantum experience (quantumexperience.ng.bluemix.net/qx/experience). Der er selvfølgeligt mange flere muligheder, og vi vil gerne være behjælpelige med ideer og litteratur, hvis det bliver aktuelt.

Kontakt

Prof. *Jan Phillip Solovej*
Email: solovej@math.ku.dk