Kvantecomputeren og dens beregningsmetoder

Ulrik Lund Andersen, Jonatan Bohr Brask og Jonas Schou Neergaard-Nielsen, Center for Macroscopic Quantum States (bigQ), DTU Fysik

Kvantecomputere forventes at kunne løse problemer, der ligger uden for rækkevidden af dagens mest kraftfulde supercomputere. I denne artikel introducerer vi de generelle principper bag kvantecomputeren og dykker ned i de forskellige kvanteberegningsmetoder, der i dag benyttes til implementering af forskellige kvantealgoritmer. Desuden belyses de særlige udfordringer ved kvantecomputeren, herunder deres skrøbelighed overfor dekohærens, samt de seneste fremskridt, der er foretaget indenfor kvantefejlkorrigerende koder.

Da Max Planck en sen oktoberaften i 1900 præsenterede sine teoretiske overvejelser omkring beskrivelsen af et sort legemes udstråling (black-body radiation), havde han sikkert ikke i sin vildeste fantasi forestillet sig hvad han havde igangsat. Det var nemlig startskuddet til udviklingen af en helt ny fysik – kvantefysikken – som beskriver den dynamiske opførsel af fysiske systemer helt ned til elementarpartikelniveau, og som gennem de sidste 100 år har ført til en sand teknologisk revolution. Teoriens evne til at beskrive atomare og optiske systemer førte til udvikling af mange nye vigtige apparater og teknologier, blandt andet transistoren og laseren, som har lagt grundlaget for udviklingen af computeren og mobiltelefonen, samt optisk kommunikation og internettet. Med andre ord har kvantefysikken i store træk formet den verden, vi lever i i dag. Denne transformative æra kaldes ofte den første kvanterevolution.

Lige nu står vi midt i en ny teknologisk omvæltning – den anden kvanterevolution. Takket være ekstreme teknologiske landvindinger formår vi i dag at kontrollere og måle enkelte partikler – atomer, elektroner, fotoner, m.v. – præcist nok til at bevare og manipulere deres kvantemekaniske egenskaber. Dette har åbnet en hel ny horisont af banebrydende anvendelser. Nogle af de vigtigste er sikker kommunikation med kvantekrypterede koder, måling af svage signaler med uhørt nøjagtighed ved brug af kvantesensorer og ekstrem hurtig udregning af visse matematiske problemer ved hjælp af en kvantecomputer. I denne artikel vil vi koncentere os om kvantecomputeren med fokus på dens forskellige beregningsmodeller.

Den mobiltelefon, som du sikkert snart igen sidder med i hånden, behandler information kodet i en sekvens af bits, som hver kan antage værdierne 0 eller 1. En kvantecomputer opererer derimod med kvantebits eller qubits. Qubits har også to tilstande, 0 eller 1, men kvantefysikken tillader desuden et kontinuum af andre tilstande, nemlig alle såkaldte superpositioner af de to basistilstande. En enkelt qubit har således uendelig mange tilstande, og med en lidt unøjagtig formulering kan man sige, at den kan antage værdierne 0 og 1 samtidig. Mere præcist skriver man en qubits tilstand som $c_0|0\rangle + c_1|1\rangle$, hvor $|0\rangle$ og $|1\rangle$ kaldes "ket'er" og angiver qubitens basistilstande. De to koefficienter c_0 og c_1 er komplekse tal, der er relateret til sandsynligheden for at få henholdsvis 0 eller 1 når man foretager en måling af qubiten via $P(0) = |c_0|^2$ og $P(1) = |c_1|^2$. Når der er flere qubits involveret kan en kvanteprocessor desuden behandle sammenfiltrede (*entangled*) tilstande af mange partikler på én gang, som om det var ét enkelt kvantesystem. Det vil med andre ord sige, at en streng af N qubits kan indeholde en sammenfiltret superposition af alle de 2^N mulige klassiske bittilstande: $|0\rangle, |1\rangle, |2\rangle, \ldots, |2^N - 1\rangle$. Alle disse eksponentielt mange muligheder kan i en kvantealgoritme i princippet processeres i parallel.

Det lyder jo rigtig godt, men vi kan desværre ikke altid gøre brug af denne eksponentielle fordel. Udgangen af kvanteprocessoren er også i en superpositionstilstand, og indeholder derfor en superposition af mange svarmuligheder. For at vi mennesker skal kunne forstå svaret bliver vi nødt til at omsætte denne superposition til klassiske værdier, hvilket gøres ved at foretage en måling, der kollapser den skrøbelige superpositionstilstand ned i en klassisk værdi. Kun én af svarmulighederne realiseres således og når vores hjerner. Den eksponentielle fordel ser derfor ud til at gå tabt i målingen! Det er dog heldigvis ikke det fulde billede. Det er nemlig muligt at arrangere udviklingen af tilstanden og foretage specielle, snu, målinger, således at det med meget høj sandsynlighed er det korrekte svar, der kommer ud. Det er faktisk det, der er "humlen" (og udfordringen!) ved at designe en god kvantealgoritme. Når det lykkes, kan sådanne algoritmer løse visse problemer langt mere effektivt end på en klassisk computer. I princippet kan en kvantecomputer godt simuleres nøjagtigt på en klassisk computer, og alt hvad der kan beregnes af en kvantecomputer kan derfor også beregnes af en klassisk. Men der er helt afgørende forskel på *effektiviteten*. Ved at udnytte den eksponentielle fordel kan kvantecomputere i praksis løse komplekse matematiske problemer, som på en klassisk computer, så vidt vides, ville tage længere end universets levealder at besvare.

Ikke alle problemer kan løses eksponentielt hurtigere. Indtil videre kender vi en begrænset række af eksempler, hvoraf primtalsfaktorisering (dvs. opdeling af et naturligt tal i dets primtalsfaktorer) af store tal er det meste berømte, med vigtige anvendelser indenfor kryptering. Klassen af problemer med eksponentiel fordel er potentielt stor, men dens grænser er ikke præcist kendte i dag. Man har faktisk identificeret en række problemer, som vil kunne løses med en kvantefordel, omend ikke altid eksponentielt hurtigere. Dette inkluderer blandt andet simulering af komplekse systemer (brændstoffer,

lægemidler, biosystemer, materialer osv.), optimering, databehandling og maskinlæring.

At bygge en fuldblods kvantecomputer, som er i stand til at implementere ovenstående anvendelser, er dog en kæmpestor udfordring. Hvis det lykkes, vil det være blandt de største teknologiske bedrifter udført af mennesket. Udfordringen skyldes, at qubits, og især deres sammenfiltrede tilstande, er uhyre skrøbelige, og at enhver lille interaktion med omgivelserne derfor vil lede til støj (eller dekohærens), som er fatalt for kvanteinformationen og den efterfølgende databehandling. Denne støj er hovedårsagen til, at vi endnu ikke endegyldigt har demonstreret kvantecomputerens fordel ved løsning af praktisk relevante problemer. Der arbejdes derfor hårdt i diverse laboratorier rundt om i verden på at komme dekohærens til livs ved på den ene side at forbedre eksisterende teknologi og opfinde nye teknologiske platforme, som bedre isolerer qubits fra omgivelserne, og på den anden side at udvikle såkaldte kvantefejlkorrigerende koder, som algoritmisk beskytter qubits fra omgivelserne. Der er indenfor de seneste år blevet forsket en del i udviklingen af sådanne koder, og et par eksperimenter har netop i år påvist korrektion af fejl hurtigere end de opstår. Der er dog stadig rigtig lang vej til det endelige mål: Den universelle, fejlkorrigerende kvantecomputer.

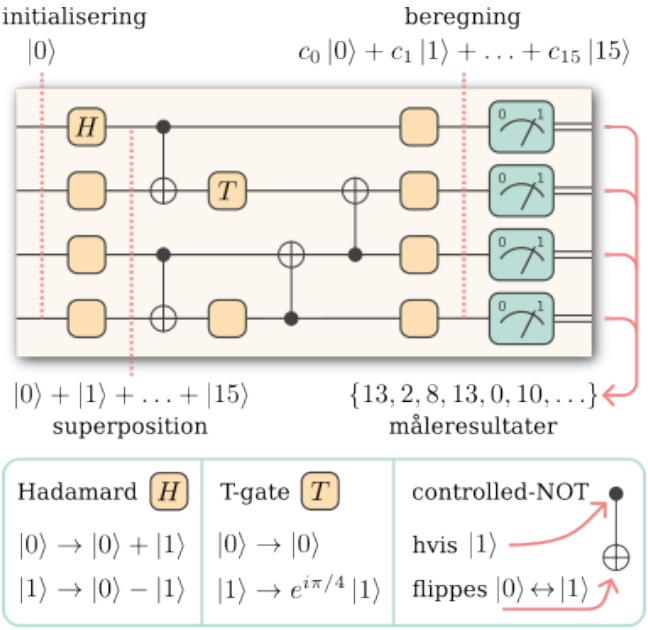
Kvanteberegningsmetoder

I løbet af de sidste fire årtier har forskere udviklet en mangfoldighed af kvanteberegningsmetoder til at udføre kvantealgoritmer. Vi fokuserer her på såkaldte universelle modeller, som er i stand til at foretage enhver transformation af kvantetilstande, hvilket betyder, at de kan implementere alle tænkelige kvantealgoritmer. Selvom disse modeller således i princippet alle kan det samme, har de varierende fordele og ulemper i forhold til at realisere dem på forskellige fysiske platforme. I det følgende vil vi gennemgå fire forskellige modeller.

Gatebaseret kvantecomputing

En gatebaseret kvantecomputer er den direkte kvante-analoge til den almindelige digitale computer. I denne computer starter man med at initialisere en sekvens af bit-værdier, der efterfølgende undergår en række enkelt-bit- og to-bit-operationer og slutteligt giver en ny sekvens af bit-værdier, der er svaret på udregningen. I kvantecomputeren starter man med at initialisere qubits i en starttilstand, som efterfølgende bliver manipuleret i en serie af kvantegates, som er særlige operationer, der ændrer på qubit'enes tilstande. Til sidst måler man tilstandene, hvilket giver os et resultat i form af en række almindelige bits. Som nævnt tidligere, så skal målingen foretages med en vis portion kreativitet for at trække det relevante resultat ud af kvantetilstanden.

Ligesom i traditionelle computere, der bygger på simple logiske operationer som OG og ELLER, har kvantecomputeren kvantegates, der udfører grundlæggende operationer på qubits. Det er interessant at bemærke at enhver operation på et vilkårligt antal qubits (dvs. universel kvantecomputing) kan brydes ned til en kombination af simple operationer på blot én eller to qubits. Det betyder at enhver kvantealgoritme kan dekomponeres til en lang, og til tider kompleks, række af enkelt- og to-qubit-operationer, som illustreret i figur 1.



Figur 1. Kredsløbs- eller gatemodellen for kvantecomputere er den mest kendte og anvendte model. Et antal qubits (her 4) initialiseres i en bestemt tilstand, typisk $|0\rangle$. Derefter udføres en serie af operationer, eller gates, enkeltvis eller parvis på de forskellige qubits. I mange tilfælde starter man med at udføre en Hadamardgate på hver qubit, hvilket ændrer dens tilstand fra $|0\rangle$ til $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, hvormed den samlede tilstand af de N qubits bliver en superposition af 2^N forskellige basistilstande, som kan repræsentere tallene i fra 0 til $2^N - 1$. De følgende gates i kredsløbet udfører nu operationer parallelt på alle komponenter i denne superposition, hvilket ændrer deres relative vægt, angivet ved deres komplekse amplituder c_i. Til sidst udføres en måling af hver enkelt qubit i $|0\rangle/|1\rangle$ basen. Tilsammen giver disse målinger nu et tilfældigt svar i med sandsynligheden $|c_i|^2$. Ved at køre det fulde kredsløb et antal gange opbygger man en fordeling af måleresultater som – hvis kredsløbet er snedigt konstrueret – giver svaret på ens problem.
Nederst ses et eksempel på to enkelt-qubit-gates, H og T, og en to-qubit-gate, CNOT, og deres funktion. Disse tre gates er universelle, dvs. at ethvert kredsløb i princippet kan konstrueres ved kombinationer af dem. I praksis vil en kvantecomputer have adgang til flere eller andre typer af gates.

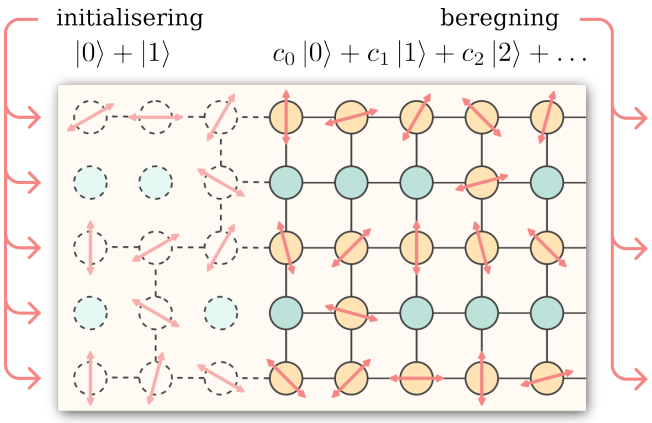
Et eksempel på et sæt af operationer, som giver anledning til universel kvantecomputing, er de to enkelt-qubit-gates; Hadamardgate og T-gate, samt en enkel to-qubitgate; CNOT-gate. Hadamard- og CNOT-gaten (se figuren) muliggør etableringen af sammenfiltring (som er det "brændstof", som driver computeren), men er dog ikke nok til at give en kvantefordel ifølge det såkaldte Gottesman-Knill-teorem. For at kunne demonstrere en kvantefordel, dvs. foretage bestemte udregninger eksponentielt hurtigere end på en klassisk computer, skal en T-gate (eller lignende) tilføjes. Der findes andre sæt af gates, som kan føre til universel kvantecomputing, og det valgte sæt afhænger tit af, hvilken hardware der bruges til realisering af gatene, da nogle gates er nemmere at implementere på en given maskine end de er på andre.

De grundlæggende principper bag gatebaseret kvantecomputing er blevet demonstreret i en lang række meget forskellige fysiske systemer de sidste 20–30 år: optiske fotoner, atom- og ion-fælder, magnetisk resonans i molekyler, superledende kredsløb, halvledere, diamant-farvecentre, m.m. Mens de første mange demonstrationer blev foretaget af forskergrupper ved universiteter, så er udviklingen de senere år i højere og højere grad blevet drevet af private virksomheder; både giganter som Google, IBM, Microsoft, Amazon m.fl., og mindre startups i mange forskellige afskygninger. Blandt disse kan især nævnes de to børsnoterede startups Rigetti, der p.t. har 80 superledende qubits, og IonQ, med 32 ion-qubits. IBM er længst fremme med at tilbyde adgang til deres kvantecomputere. I skrivende stund har de 17 maskiner online med enten 27 eller 127 qubits. Disse kan i begrænset omfang tilgås gratis via skyen. Flere andre virksomheder tilbyder også adgang til deres kvantecomputere for betalende kunder, typisk via kendte cloud platforme som AWS og Microsoft Azure. Selvom man således allerede nu kan køre kredsløb på kvantecomputere med flere end 100 qubits, så er der stadig lang vej til, at vi kan opnå ægte kvantefordele med de traditionelle kredsløbs-algoritmer. Det skyldes støj og fejl i qubits, gates og målinger. Uden kvantefejlkorrektion vil disse i høj grad begrænse antallet af operationer, man kan udføre i træk, og dermed længden af kredsløb og kompleksiteten af algoritmer.

Målebaseret kvantecomputing

En gatebaseret kvantealgoritme vil typisk involvere mange to-qubit-gates, som generelt er de mest krævende at implementere. Dette omgås elegant i den målebaserede kvanteberegningsmodel, hvor hele beregningen kan realiseres gennem målinger på enkelte qubits, ved til gengæld at udnytte en sammenfiltret starttilstand. Processen, der vises i figur 2, indledes med at generere en omfattende sammenfiltret tilstand blandt et netværk af qubits, kendt som en klyngetilstand. Det er først efter at denne sammenfiltrede tilstand er etableret, at beregninger kan påbegyndes, hvilket gøres ved trinvist at måle qubit'ene. Disse målinger forårsager ændringer i de resterende, umålte qubits inden for klyngetilstanden, hvilket effektivt simulerer udførelsen af en gateoperation. Den specifikke gateoperation, der udføres, afhænger helt af de udførte målinger. Ved at udføre disse målinger sekventielt på klyngetilstanden, kan man realisere en sekvens af gateoperationer, både enkelt- og to-qubit-gates, hvilket muliggør konstruktionen af en kvantealgoritme.

Målebaseret kvantecomputing er specielt relevant i systemer, hvor det er svært at gemme qubits i en kvantehukommelse. Det er for eksempel tilfældet med optiske systemer, hvor fotoner farer afsted med lysets hastighed og kun kan stoppes, dvs. lagres, gennem en stærk vekselvirkning med et materialesystem, hvilket i dag ikke er særligt effektivt. Benyttes derimod en målebaseret model, er det ikke nødvendigt at lagre fotonerne, men blot at detektere dem umiddelbart efter, at de er skabt i en klyngetilstand. Disse fotonmålinger udfører således gateoperationer på de efterfølgende fotoner, der et splitsekund senere detekteres og udfører gateoperationer på de efterfølgende fotoner osv. Sådanne klyngetilstande er genereret af en række forskningsgrupper rundt om i verden, heriblandt på DTU, hvor vi har formået at skabe en sammenfiltret klyngetilstand af cirka 30.000 optiske modes og eftervist en række gates gennem optiske målinger.

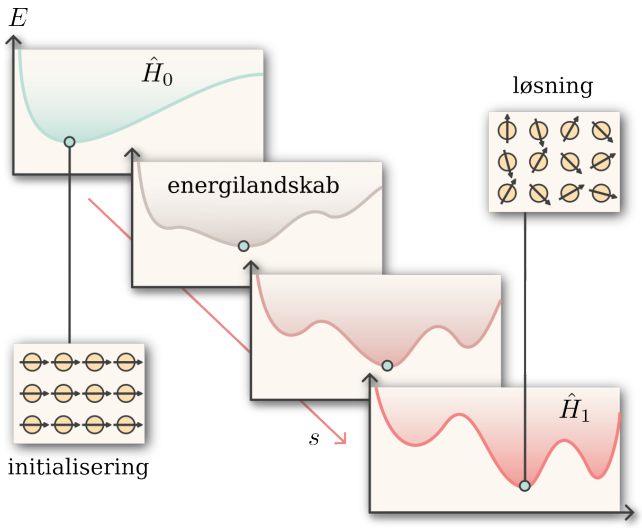


Figur 2. Målebaseret kvantecomputing er væsensforskellig fra kredsløbsmodellen, men de to modeller er teoretisk set fuldt ækvivalente i forhold til hvilke kvanteberegninger, de kan foretage. I stedet for et vist antal qubits hvorpå man opererer mange gange med en række gates, starter man i målebaseret kvantecomputing med et langt større antal qubits som præpareres i en stor sammenfiltret tilstand – en klynge- eller graf-tilstand. Det er her illustreret med qubits forbundet i en gittergraf via sammenfiltring med deres nærmeste naboer. Herefter måles hver qubit én gang i et variabelt målebasis. Måles den i $|0\rangle/|1\rangle$ basen (de blå cirkler) fjernes den og dens forbindelser til naboerne fra grafen. Måles den derimod i et komplementært basis (repræsenteret ved røde pile), så forplanter informationen i qubit'en sig til naboen under påvirkning af en transformation, der afhænger af den specifikke base. Sættes flere af disse transformationer sammen, kan man effektivt udføre én- og to-qubit-gates på kvanteinformation der propagerer ned gennem gitteret. Figuren viser et snapshot af en beregning, hvor qubits til venstre i grafen allerede er blevet målt (og grafen dermed også blevet brudt op), mens qubits til højre endnu ikke er målt – deres målebaser er dog forudbestemt baseret på det ønskede program. En vigtig detalje, der ikke er illustreret her, er, at de ønskede målebaser i nogle tilfælde skal ændres på baggrund af udfaldet af tidligere målinger.

Målebaseret kvantecomputing er også det grundlæggende princip bag de kvantecomputere som to store kvante-startups i Nordamerika, Xanadu og PsiQuantum, forsøger at bygge. PsiQuantums model er baseret på enkelt-foton- og tre-foton-tilstande mens Xanadus model, ligesom DTUs, er baseret på såkaldte "klemte" (*squeezed*) og Gottesman-Kitaev-Preskill-(GKP)-tilstande. Designs for den komplette arkitektur for målebaserede kvantecomputere er udarbejdet af både PsiQuantum reference [1], Xanadu [2] og DTU[3]. Der er dog stadig store udfordringer at overkomme: For den foton-baserede arkitektur er det vanskeligt at skabe de store sammenfiltrede tilstande på deterministisk vis. For den squeezing-baserede arkitektur mangler vi endnu at kunne skabe GKP-tilstande, som skal bruges til at kode kvanteinformationen som qubits og gøre beregningerne fejlresistente. Meget forskning er derfor rettet mod disse udfordringer.

Adiabatisk kvantecomputing

Den adiabatiske kvantecomputermodel udfører beregninger på en radikalt anderledes måde end den gatebaserede eller målebaserede model. Mens den stadig benytter sig af et mange-qubit sammenfiltret system, som de to tidligere modeller, er den ikke baseret på kontrollerede enkelt-qubit eller to-qubit gateoperationer men derimod en adiabatisk ændring af energilandskabet, hvis minimum repræsenterer løsningen på det givne problem. Tanken bag adiabatisk kvantecomputing er således effektivt at finde denne minimumsenergi, dvs. grundtilstanden for systemet. Det svarer til at befinde sig i et landskab af bakker og dale, hvor den laveste dal repræsenterer løsningen.



Figur 3. Adiabatisk kvantecomputing er et helt andet koncept end de tidligere omtalte modeller. Selvom en adiabatisk kvantecomputer er universel og derfor i princippet kan udføre de samme beregninger, som en gate eller målebaseret kvantecomputer, så vil de forskellige modeller i praksis have forskellige anvendelsesområder. For den adiabatiske model vil målet typisk være at finde grundtilstanden for et komplekst system, repræsenteret ved dets Hamiltonian, $\hat{H}_1$. For en given tilstand af systemet, $|\psi\rangle$, er energien $E = \langle\psi|\hat{H}_1|\psi\rangle$, og det gælder altså om at finde den $|\psi\rangle$, der minimerer denne energi. På figuren er energien for forskellige tilstande illustreret som et simplificeret én-dimensionelt energilandskab – i virkeligheden vil det være et meget komplekst, multi-dimensionelt landskab, der kan være næsten umuligt at optimere over. I den adiabatiske kvantecomputer løser man dette optimeringsproblem ved at initialisere sine qubits i grundtilstanden for et enklere, kendt system, givet ved $\hat{H}_0$. Derefter ændrer man gradvist systemets Hamiltonian til $(1-s)\hat{H}_0 + s\hat{H}_1$, hvor den skalerede tidsparameter s går fra 0 til 1. Gøres dette tilstrækkelig langsomt, vil systemet hele tiden forblive i grundtilstanden, som så til slut, $s = 1$, kan udlæses.

Men hvordan findes denne laveste energi i et komplekst energilandskab? Som vist i figur 3 starter man med at initialisere et simpelt kvantesystem, der er let at styre, og som er indstillet på en sådan måde, at det allerede befinder sig i sin laveste dal – ligesom et fladt, jævnt landskab. Forestil dig nu, at dette landskab langsomt begynder at ændres til et mere komplekst et, med mange flere bakker og dale – det, som repræsenterer det svære problem, du vil løse. Kunsten er at ændre landskabet så langsomt, at systemet ikke engang indser, at det bevæger sig, og dermed forbliver i den laveste dal. Dette er muligt ifølge det såkaldte adiabatiske teorem, der garanterer, at hvis vi gør tingene langsomt nok, vil vores kvantesystem forblive i grundtilstanden, og vi ender med det rigtige svar. Den hastighed, hvormed vi sikkert kan ændre vores kvantelandskab, afhænger af energiforskellen mellem den laveste dal og den næstlaveste. Hvis denne forskel er stor, kan vi foretage ændringen hurtigere. Hvis den er lille, skal vi være ekstra langsomme.

Den adiabatiske kvantemodel repræsenterer således en helt anderledes måde at bygge en kvantecomputer på; de traditionelle kvantecomputere beror på qubits der indgår i en kontrolleret sekvens af gates, som at følge en given opskrift, hvorimod adiabatisk kvantecomputing lidt svarer til at putte alle ingredienser i en gryde, opvarme det forsigtigt og lade dem transformere over tid.

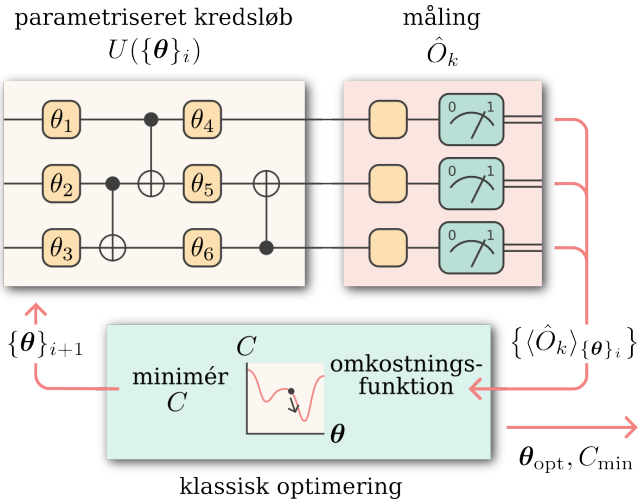
Det er også vigtigt at bemærke, at eftersom ethvert energilandskab (dvs. Hamiltonian) for systemet i princippet kan skabes, er den adiabatiske model, ligesom de gate- og målebaserede modeller, universel. En sådan universel adiabatisk processor er dog endnu ikke blevet realiseret i laboratoriet. Det nærmeste, man er kommet dette mål, er implementering af en kvante-annealer, der kan ses som det første skridt mod den universelle maskine. Det canadiske firma D-Wave har arbejdet på dette gennem de sidste 20 år, og er det første firma i verden, som har kommercialiseret og solgt en computer baseret på kvanteprincipper. Selvom firmaet er kommet langt med udviklingen af en kvante-annealer, bliver det stadig diskuteret hvorvidt deres maskine opfylder det adiabatiske teorem, hvilket er vigtigt for at kunne demonstrere en kvantefordel.

Variationel kvantecomputing

Den variationelle kvanteberegningsmetode, som blev udviklet for få år siden, har vakt stor interesse, idet det menes, at man vil kunne opnå en kvantefordel med denne metode uden fejlkorrigering, dvs. ved brug af et relativt støjende system. Den kan betragtes som en hybrid mellem den gatebaserede og den adiabatiske beregningsmetode: Ligesom for den adiabatiske metode, er målet at finde den laveste energitilstand, grundtilstanden, for et system, men dette gøres ved hjælp af et gatebaseret kvantekredsløb, der løbende bliver justeret på en sådan måde, at systemet bringes ned i den ønskede grundtilstand, der rummer svaret på udregningen. Denne justering af kvantegatene, der får systemet til at konvergere mod grundtilstanden, opnås ved iterativt at måle systemet, bruge måleresultaterne til at udregne systemets energi på en almindelig computer og slutteligt benytte denne værdi til at ændre en smule på gateindstillingerne, sådan at gate transformationerne bringer systemet mod en lavere energi. Denne proces gentages igen og igen, og får til sidst systemet til at havne i den ønskede energitilstand, grundtilstanden. Metoden, som er illustreret i figur 4, involverer altså en klassisk optimering af et kvantekredsløb, og er derfor et eksempel på en hybrid kvante-klassisk beregningsmetode.

Selvom den variationelle metode også er universel,

dvs. at enhver kvanteberegning kan udføres, er det alligevel nogle helt specifikke kvantealgoritmer, som har givet anledning til den største interesse. Det drejer sig for eksempel om den såkaldte "variational quantum eigensolver", der blandt andet kan bruges til at findes grundtilstanden af elektronerne i et komplekst molekyle, samt algoritmer, der hurtigere kan finde en løsning på komplekse kombinatoriske optimeringsproblemer som det klassiske Traveling Salesman-problem. Dette problem går ud på at finde den kortest mulige rute mellem en række byer, der skal besøges præcis én gang af en sælger, og kompleksiteten af løsningen øges hurtigt med antallet af byer.



Figur 4. En variationel kvantecomputer er en slags kvante-klassisk hybrid, da den benytter sig af en løkke, hvori der skiftevis 1) udføres et kvantekredsløb U, hvis gates har variable parametre $\{\boldsymbol{\theta}\}$, 2) foretages en måling af en given observabel $\hat{O}_k$, og 3) køres en klassisk algoritme, der bruger måleresultat til at opdatere kredsløbets parametre i næste skridt, baseret på beregning af en omkostningsfunktion C der skal minimeres. Ligesom en adiabatisk kvantecomputer er den variationelle særligt egnet til at løse optimeringsproblemer, men den er baseret på et standard kvante-kredsløb af gates. Dette kredsløb er typisk meget kortere end for konventionelle algoritmer, hvilket gør det mere realistisk at køre en variationel algoritme på de nuværende støjende kvantecomputere.

Selvom en kvantefordel endnu ikke er påvist, har man afprøvet den variationelle beregningsmetode i en række anvendelser på kvantecomputere baseret på ioner og superledende elektronik.

Kvantefejlkorrektionskoder

Den største udfordring, vi står overfor i forhold til konstruktionen af en skalerbar kvantecomputer, er måske håndteringen af beregningsfejl. På grund af den utrolig skrøbelige natur af kvantetilstande vil enhver påvirkning fra omgivelserne give anledning til støj og dermed beregningsfejl. I modsætning til almindelig informationsteknologi, som bruger bit-redundans til fejldetektion og -korrektion fx på harddiske og i internetkommunikation, står kvantecomputere over for nogle helt specielle begrænsninger. Tilstanden af en qubit kan hverken kopieres eller måles uden at forstyrre den, i modsætning til den klassiske bit som nemt kan kopieres for at skabe redundans og nemt kan måles for at finde og korrigere en eventuel opstået fejl. Men den går altså ikke i den kvantemekaniske verden, hvorfor traditionelle fejlkorrektionsmetoder er uegnede til kvantecomputeren.

Løsningen ligger i de sofistikerede kvantefejlkorrektionskoder, som benytter sig af et større antal fysiske qubits (for eksempel atomer eller fotoner) til at repræsentere en enkelt logisk qubit. Man "smører" sin logiske qubit ud over et større antal fysiske qubits på en sådan måde, at fejl vil kunne observeres ved at måle et begrænset sæt af de fysiske qubits, og det uden at den logiske qubit kollapser. I mere korrekte termer kodes den logiske qubit i et underrum af et stort Hilbertrum, som udspændes af egenvektorerne for de fysiske qubits. En fejl vil skubbe den logiske qubit ind i et andet underrum i det samme Hilbertrum, og dette nye underrum kan skelnes fra det oprindelige underrum, hvorfor en fejl kan detekteres. Dette bruges efterfølgende til at korrigere den logiske qubit. En af de tidligste fejlkorrigerende koder, som var med til at kickstarte hele kvantecomputereventyret, er den meget kendte Shors fejlkorrigerende kode, opkaldt efter dens opfinder, Peter Shor. Koden benytter sig af ni fysiske qubits til at kode én logisk qubit, og er kun i stand til at korrigere fejl, der optræder med meget lille sandsynlighed. Er fejlraten for stor, kan fejlene ikke detekteres og korrigeres. Men hvor store fejlrater kan man mon tolerere? Svaret på dette spørgsmål findes i det såkaldte kvantetærskelteorem ("Quantum threshold theorem"), der giver den maksimalt tilladte værdi for den fysiske fejlrate for at koden vil kunne undertrykke en logisk fejl. Denne værdi afhænger af den benyttede kode, og der er således en verdensomspændende jagt på at finde nye koder, som tillader højere værdier for den fysiske fejlrate, og som samtidig kan implementeres på de kvanteprocessor-arkitekturer, der er mulige at konstruere.

Som nævnt dannes fejlkorrektionskoderne ved at kombinere en række fysiske qubits, hvilket realiseres via qubit-qubit-vekselvirkninger. Det er dog ikke altid nemt at udføre sådanne vekselvirkninger, idet de forskellige qubits kan ligge langt fra hinanden. Det er derfor vigtigt at bygge computerens arkitektur på en sådan måde, at det er praktisk muligt at skabe de ønskede koder. Shors kode kræver for eksempel et komplekst netværk af forbindelser mellem qubits, som ikke nemt lader sig implementere i mange computerarkitekturer. Man har dog indenfor de seneste år udviklet en ny kodetype, som kun kræver forbindelser på en overflade mellem en qubit og dens nærmeste naboer – de såkaldte overfladekoder. Udover at være meget nemmere at implementere end de traditionelle koder, har disse koder også en meget højere fejltærskelværdi. Overfladekoden er derfor i øjeblikket den mest lovende kode til fejltolerant kvantecomputing. Dette kan dog hurtigt ændre sig. Udvikling af nye koder med endnu bedre fejltærskel er et brandvarmt forskningsfelt, og hvem ved, måske man en skønne dag opdager en kode, som kan håndtere rigtig meget støj – det ville være et ægte gennembrud.

En anden stor udfordring er det meget store antal fysiske qubits der skal til for at skabe bare en enkel

logisk qubit. Det vurderes at man med de mest lovende koder skal bruge cirka 1.000–10.000 fysiske qubits for a beskytte en enkel logisk qubit, og for at lave virkelig spændende beregninger skal vi altså bruge 100–1.000 logiske qubits, dvs. ca. 1 million qubits i alt. De fylder rigtig meget, og det forventes derfor at de første fejltolerante kvantecomputere vil komme til at optage det meste af pladsen i et datacenter. Det vil derfor være godt at udvikle nye koder, som ikke kræver så mange fysiske qubits. Vi forsøger at gå i den retning på DTU. Her studerer vi de såkaldte Gottesman-Kitaev-Preskill-(GKP)-koder, som er en helt speciel kode, der kan korrigere fejl med bare en enkelt fysisk qubit! Det lyder jo næsten for godt til at være sandt. Og ja, intet kommer gratis. GKP-koden er nemlig ikke så nem at skabe. Selvom koden er blevet realiseret i to fysiske opstillinger – den ene baseret på ion-fælder og den anden på superledende elektronik – bliver det først for alvor spændende, når det kan lade sig gøre i skalerbare optiske systemer. Vi har på DTU fremsat en ny metode til skabelsen af GKP-koder i optiske systemer [4], og har derudover realiseret egnede klyngetilstande [5], som tidligere beskrevet i Kvant [6], samt demonstreret implementering af de relevante gates [7].

Afrunding

Kvantecomputing er kommet en meget lang vej fra de første teoretiske idéer og algoritmer i 1980'erne og 1990'erne og de første spæde eksperimenter. Vi har nu et højt udviklet sæt af matematiske metoder til at beskrive og analysere kvantecomputere fra flere forskellige perspektiver, som vi har beskrevet her. Alle de nødvendige grundlæggende elementer er blevet demonstreret med høj effektivitet i talrige eksperimenter på forskellige fysiske platforme, og bliver nu sat sammen i mere og mere avancerede kombinationer. Store og små firmaer verden over tager del i udviklingen, og de første kvantecomputersystemer er allerede tilgængelige online, både for offentligheden og kommercielt. Der er stadigvæk meget store teknologiske udfordringer, som skal overvindes, før vi får en universel fejlkorrigeret kvantecomputer, som kan realisere en eksponentiel fordel i praksis. Men udviklingen af kvanteteknologi går i disse år rivende hurtigt. Danmark er med i allerforreste række. Det bliver spændende at se, hvad de kommende år bringer!

Litteratur

[1] S. Bartolucci, P. Birchall, H. Bombin, H. Cable, C. Dawson, M. Gimeno-Segovia, E. Johnston, K. Kieling, N. Nickerson, M. Pant, F. Pastawski, T. Rudolph og C. Sparrow (2023) "Fusion-based quantum computation", *Nature Communications*, bind **14**, side 912.

[2] I. Tzitrin, T. Matsuura, R.N. Alexander, G. Dauphinais, J.E. Bourassa, K.K. Sabapathy, N.C. Menicucci og I. Dhand (2021) "Fault-tolerant quantum computation with static linear optics", *PRX Quantum*, bind **2**, side 040353.

[3] M. V. Larsen, C. Chamberland, K. Noh, J. S. Neergaard-Nielsen og U. L. Andersen (2021) "Fault-tolerant continuous-variable measurement-based quantum computation architecture", *PRX Quantum*, bind **2**, side 030325.

[4] J. Hastrup, U. L. Andersen (2022) "Protocol for generating optical Gottesman-Kitaev-Preskill states with cavity QED", *Physical Review Letters*, bind **128**, side 170503.

[5] M. V. Larsen, X. Guo, C.R. Breum, J. S. Neergaard-Nielsen og U.L. Andersen (2019) "Deterministic generation of a two-dimensional cluster state", *Science*, bind **366**, side 369.

[6] U. Hoff, J. S. Neergaard-Nielsen, M. V. Larsen og U. L. Andersen (2020) "Kvantecomputere og grafteori", *KVANT*, bind **31**, nr. 4, side 21.

[7] M. V. Larsen, X. Guo, C. R. Breum, J. S. Neergaard-Nielsen og U. L. Andersen (2021) "Deterministic multi-mode gates on a scalable photonic quantum computing platform", *Nature Physics*, bind **17**, side 1018.

Ulrik L. Andersen er kvantefysiker og leder af Danmarks Grundforskningsfonds center for makroskopiske kvantetilstande (bigQ) på DTU Fysik. Hans forskning er centreret om kvanteinformationssystemer.

Jonatan Bohr Brask er lektor ved DTU Fysik og arbejder med teoretisk kvanteinformation, ikke-lokalitet, og kvantetermodynamik.

Jonas S. Neergaard-Nielsen er lektor ved DTU Fysik med speciale i ikke-klassisk lys og dets anvendelse indenfor kvanteinformation.