Quantum Computing, getting started

Morten Hjorth-Jensen[1,2]

[1]Department of Physics, University of Oslo
[2]Department of Physics and Astronomy and National Superconducting Cyclotron Laboratory, Michigan State University

May 17, 2018

Historisk tilbakeblikk og Moores lov

I 1946 framsto ENIAC (Electronic Numerical Integrator And Computer), som kunne addere 5000 tall per sekund, som det store teknologiske gjennombruddet. Dens reknekraft svarte altså til noen tusen flytende talls operasjoner per sekund (FLOPS). Idag har vi maskiner som kan utføre trillioner av FLOPS. ENIAC besto av

- ca. 19000 vakuumrør
- veide ca. 30 tonn
- brukte ca 174 kW, eller 233 hk
- trengte ca. 150 m^2 med plass (30 ft $\times$ 50 ft)

Et ekspertpanel i 1949 uttrykte forhåpningsfullt følgende "*.... en eller annen dag kan vi utvikle en like kraftig datamaskin med bare 1500 vakuumrør, med vekt på kanskje 1500 kg og et forbruk på ca. 10 kW.....* Resten er vel historie...? Transistoren som blei introdusert på begynnelsen av 50-tallet revolusjonerte fullstendig feltet, og innen få år var vakuumrør teknologien akterutseilt.

Idag representeres bit 0 og 1 vha. spenningsforksjeller. Med dagens teknologi brukes ca. 100000 elektroner for å lagre en bit med informasjon og en chip har en utstrekning på noen få micrometer. Transistoren, som er arbeidshesten i enhver datamaskin, består i dag av noen få hundre elektroner. Skal miniatyriseringen av elektroniske kretser fortsette med uforminska styrke, vil vi, dersom vi ekstrapolerer trenden i forminskning fra 1960 til år 2010 knapt trenge et elektron for å lagre en bit med informasjon. Det sier seg sjøl at før eller siden vil kvantemekaniske effekter begynne å spille en viktig rolle, og dagens teknologi vil møte veggen dersom ikke nye måter å bygge kretser utvikles. Denne ekstrapolasjonen kalles også Moore sin lov, etter Gordon Moore ved Intel, kjent for sin observasjon i 1965, kun fire år etter at den først integrerte kretsen kom

på markedet, at antall transistorer per integrert krets ville doble hver 18 måned. Tabellen her viser antall transistorer per krets fra 1971 til Pentium 4 prosessorern fra 2000.

Prosessor	år	antall transistorer per krets
4004	1971	2250
8008	1972	2500
8080	1974	5000
8086	1978	29000
286	1982	120000
386[tm] processor	1985	275000
486[tm] DX processor	1989	1180000
Pentium 256 processor	1993	3100000
Pentium II processor	1997	7500000
Pentium III processor	1999	24000000
Pentium 4 processor	2000	42000000

Det er her kvantemekanikken kommer inn. Kvantemekanikk tilbyr en enkel og naturlig representasjon av bits: vi kan f.eks. tenke på tilstander i et atom, hvor bit 0 er gitt ved normaltilstanden (grunntilstanden) mens bit 1 er gitt ved en elller annen eksitert tilstand.

En enda enklere tilnærming er å se på enkeltelektroner. Kan vi isolere et enkelt elektron, kan vi vha. et ytre påsatt magnetfelt ha spinn egenverdier $+1/2$ eller $-1/2$. Den første kan da tilsvare bit 0 mens den andre spinnegenveriden svarer til bit 1.

En slik kvantemekanisk representasjon av en bit kalles **QUBIT** og det leder oss til neste avsnitt!

Superposisjon og qubits

Superposisjonsprinsippet

Det kvantemekaniske superposisjonsprinsippet spiller en sentral rolle i alle betraktninger om kvante informasjonsteori, de fleste såkalla 'gedanken' eksperiment og paradokser i kvantemekanikk.

Vi har i kapittel 2 allerede stifta bekjentskap med dobbelspalt eksperimentene, som i følge Feynman har i seg 'hjerte av kvantemekanikken'. De viktigste bestandelene i dette eksperimentet er en partikkel kilde, en dobbeltspalt innretning og en skjerm hvor vi kan observere eventuelle interferens mønster. Interferens mønstrene kan kun forstås dersom vi antar at materien utviser en bølgenatur. Denne type eksperiment har blitt gjort med flere partikkel typer, fra fotoner, via elektroner, til nøytroner og atomer. Kvantemekanisk er tilstanden vi observerer gitt ved en koherent superposisjon

$$\Psi(x,t) = \Psi(x,t)_a + \Psi(x,t)_b, \tag{1}$$

hvor indeks a svarer til en tilstand med bare spalt a mens indeks b er den tilsvarende tilstanden for spalt b. En slik **superposisjon** av kvantemekaniske tilstander kalles for koherente tilstander (kvante koherens) og følger fra postulatet om materiens bølge og partikkel natur. Det finnes per dags ingen eksperiment som tillater oss å si bestemt hvilken spalt f.eks. et enkelt elektron går gjennom. ønsker vi å gjøre det, vil en eventuell måling kreve at vi vekselvirker med partikkelen, noe som leder til **dekoherens**, dvs. tap av interferens. Kun når vi ikke har noen kunnskap om hvilken spalt partikkelen passerte kan vi observe interferens! Det er klart at dette strider med vår oppfatning av en partikkel som en lokalisert størrelse.

Qubits

I informasjonsteori er den fundamentale enheten en bit. Den utgjør et system med to verdier, '0' eller '1'. I sin klassiske realisering, kan vi tenke oss en bit som en mekanisk bryter, et system med to forskjellige tilstander. Vi kunne tenke oss også at energi, eller potensialforksjellen mellom de to tilstandene er såpass stor at en ikke kan ha spontane overganger fra f.eks. bit '0' til bit '1'.

Den kvantemekaniske analog til den klassiske bit er den såkalla *qubit*, og på lik linje med sin klassiske partner, må den ha minst to tilstander, som vi heretter kaller for $|0\rangle$ og $|1\rangle$. I prinsippet kan ethvert kvantemekanisk system som har minst to tilstander tjene som en basis for en qubit, tenk bare på et elektron i et magnetfelt. Avhengig av magnetfeltets retning, kan vi ha kvantetallene $m_s = \pm 1/2$. Disse to kvantetallene kan tjene som basis for en qubit. I slutten av dette kapitlet skal vi se på et eksperimentelt oppsett som manipulerer to qubits.

Alt dette høres kanskje ikke så banebrytende. Men kopler vi superposisjons prinsippet til en slik qubit, kan vi lage oss en generell qubit tilstand

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{2}$$

med den egenskap at $|\alpha|^2 + |\beta|^2 = 1$. Det betyr ikke at qubiten har en verdi et sted mellom '0' og '1', men heller at qubiten er i en kvantemekanisk superposisjon av begge tilstander, og dersom vi foretar en måling på denne tilstanden, finner vi en sannsynlighet $|\alpha|^2$ for at den er i tilstand '0' og $|\beta|^2$ for at den er i tilstand '1'. Qubiten er i en koherent superposisjon av to kvantemekaniske basis tilstander. Et enkelt eksempel er

$$|q\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{3}$$

som betyr at vi har 50% sannsynlighet for at qubiten er i tilstand '0' og 50% sannsynlighet for at den er i tilstand '1'.

Hvorfor er anvendelsen av det kvantemekaniske superposisjonsprinsippet av interesse? Og hva er nytt i forhold til en klassisk representasjon?

La oss se på et tilfelle hvor vi har en kvantemekanisk tilstand med åtte komponenter, dvs. vi har superposisjonen

$$|\psi\rangle = a_0|\psi\rangle_0 + a_1|\psi\rangle_1 + a_2|\psi\rangle_2 + a_3|\psi\rangle_3 + a_4|\psi\rangle_4 + a_5|\psi\rangle_5 + a_6|\psi\rangle_6 + a_7|\psi\rangle_7, \quad (4)$$

hvor hver komponent $|\psi\rangle_i$ er enten i en tilstand '0' eller '1'. Vi kunne f.eks. tenke oss at hver $|\psi\rangle_i$ var et elektron med enten $m_s = -1/2$ eller $m_s = +1/2$. Koeffisientene a_i er imaginære.

Dersom vi ønsker å representere denne tilstanden i en klassisk datamaskin for en eventuell kvantemekanisk beregning, må vi lagre hver av koeffisientene a_i et sted i minnet. Vi trenger da et ord med 128 bits for å representere hver a_i som er imaginær i en konvensjonell datamaskin. Et alternativ er alltid å skrive dataene ut på disk. Men dersom vi ender opp med å lese og skrive store datamengder til og fra ei fil, senker dette hastigheten på programmet vårt, da lesing til/fra ei fil tar lengre tid enn å aksessere data i internminnet til en datamaskin. I vårt tilfelle trenger vi åtte adresser i minnet for å lagre en bestemt kombinasjon av koeffisientene a_i. Det burde ikke være vanskelig å overbevise seg sjøl at dersom antall elektroner øker (systemet vårt blir større), øker også vårt behov for minne. Med dagens teknologi, kan vi lagre informasjon som svarer til ca. $\sim 2^{30} - 2^{35}$ i minnet på de beste datamaskinene vi har tilgjengelig. Det vil da svare til et sted mellom 30 og 35 elektroner som kan ha spinn opp eller ned. Generelt har vi et totalt antall tilstander gitt ved 2^n, hvor n kan være antall elektroner i to tilstander, spinn opp eller ned.

Hvordan omgå dette problemet? Det kvantemekaniske superposisjonsprinsippet kommer oss her til unnsetting. En tilstand som den beskrevet i likning (4), gitt ved en bestemt kombinasjon av koeffisientene a_i, kan da tenkes lagret som et enkelt ord i et enkelt kvanteregister, dvs. kun en adresse, i motsetning til de åtte vi trenger for en klassisk datamaskin. Dersom vi f.eks. kan manipulere $n = 500$ qubits, har vi 2^{500} mulige tilstander, som er mye større enn det estimerte antallet atomer i verdensrommet. Kvantemekanikk gir oss dermed et potensiale for informasjonsbehandling langt utover det en klassiske datamaskin kan gjøre.

Hvordan en skal lage slike kvanteregistre er dog ikke klart. Det en har klart eksperimentelt hittil er å lage enkle kvantemekaniske kretser hvor en manipulerer noen få qubits.

Operasjoner på en qubit

Innsikt i noen av de mer grunnleggende operasjonene som danner grunnlaget for en kvantedatamaskin og kvanteinformasjons teori, finnes ved å studere et tenkt oppsett for en enkel strålesplitter, f.eks. gitt ved endringen av polarisasjonsretningen til en innkommende lysstråle.

Vi kan tenke oss at vi har en innkommende stråle som kan være i to tilstander, med lik sannsynlighet. I vårt tilfelle ser vi for oss en partikkel som enten kommer inn ovenifra (tilstand $|0\rangle$) eller nedenfra (tilstand $|1\rangle$) mot strålesplitteren. Strålen påvirkes deretter av en stråle splitter. Strålen splittes i to, med lik sannsynlighet for at partikkelen kommer ut ovenfor eller nedenfor. En enkel

matematisk beskrivelse av denne strålesplitteren er gitt ved den såkalte Hadamard transformasjonen $\hat{H}$, hvis virkning på en tilstand $|0\rangle$ eller $|1\rangle$ er

$$\hat{H}|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{5}$$

og

$$\hat{H}|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{6}$$

Vi merker oss også at

$$\hat{H}\hat{H}|0\rangle = \hat{H}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |0\rangle, \tag{7}$$

og

$$\hat{H}\hat{H}|1\rangle = \hat{H}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = |1\rangle. \tag{8}$$

Virkningen av denne kvantemekaniske transformasjonen er altså å lage en midlertidig tilstand som består av en superposisjon av bit '0' og bit '1'. Klassisk er ikke det mulig. En alternativ beskrivelse er gitt ved en matriserepresentasjon av tilstandene $|0\rangle$ og $|1\rangle$ og transformasjonen $\hat{H}$, gitt ved

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \tag{9}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{10}$$

og

$$\hat{H} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}. \tag{11}$$

Overbevis deg selv om at dette stemmer!

Det finnes flere slike operasjoner på qubits. Den såkalte NOT-kretsen, hvor bit '0' skifter til bit '1', eller omvendt, kan skrives som

$$\hat{H}_{\mathrm{NOT}} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{12}$$

Vi ser da at

$$\hat{H}_{\mathrm{NOT}}|0\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle, \tag{13}$$

og

$$\hat{H}_{\mathrm{NOT}}|1\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle. \tag{14}$$

Det siste er ikke noe annet enn en alternativ måte å uttrykke virkningen av en standard NOT-krets i elektronikk.

En annen viktig operasjon er den såkalte faseskiftsoperasjonen, hvor vi kan skifte fasen til en av amplitudene ved hjelp av f.eks. laserlys med en bestemt frekvens. Matematisk kan vi uttrykke denne operasjonen som

$$\hat{H}_\Phi|0\rangle = e^{i\phi}|0\rangle, \tag{15}$$

og

$$\hat{H}_\Phi|1\rangle = |1\rangle, \tag{16}$$

eller med operatoren på følgende form

$$\hat{H}_\Phi = \begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{pmatrix}. \tag{17}$$

Når vi skal lage kvantemekaniske kretser, kan vi tenke oss at flere slike operasjoner på en qubit tilstander utgjør en bestemt endelig krets.

Hittil har vi sett på en begynnelsestilstand som bare består av en tilstand. Vi kan også lage en begynnelsetilstand gitt ved en superposisjon, f.eks.

$$|q\rangle_{in} = \alpha|0\rangle_{in} + \beta|1\rangle_{in}, \tag{18}$$

hvor α og β er to imaginære konstanter. Virkningen av vår strålesplitter er gitt ved

$$|q\rangle_{ut} = \hat{H}|q\rangle_{in} = \frac{1}{\sqrt{2}}((\alpha+\beta)|0\rangle_{ut} + (\alpha-\beta)|1\rangle_{ut}), \tag{19}$$

hvor $\alpha+\beta$ er sannsynlighetsamplituden for å finne partikkelen i den øvre utgående strålen mens $\alpha-\beta$ er den tilsvarende amplituden for å finne den i nedre utgående strålen. Velger vi enten $\alpha = 0$ eller $\beta = 0$, ser vi at partikkelen har like stor sannsynlighet for å være i den nedre utgående strålen som den øvre. Velger vi $\alpha = \beta$ vil partikkelen definitivt komme ut i den øvre strålen. Virker vi en gang til på den resulterende tilstanden får vi tilbake begynnelsestilstanden,

$$|q\rangle_{ut} = \hat{H}\hat{H}|q\rangle_{in} = |q\rangle_{in}. \tag{20}$$

Som et siste eksempel kan vi tenke oss en krets representert vha. følgende operasjoner

$$\hat{H}\hat{\Phi}\hat{H}|0\rangle, \tag{21}$$

hvis resultat er

$$\frac{1}{\sqrt{2}}((e^{i\phi}+1)|0\rangle + (e^{i\phi}-1)|1\rangle). \tag{22}$$

Dersom $\phi = 0$ får vi bit '0' som resultat mens for $\phi = \pi$ finner bit '1' som sluttresultat. Det betyr at faseskiftet ϕ gjør en i stand til å veksle mellom bit '0' eller bit '1'.

Entanglement og to-qubit tilstander

Forestill deg nå en partikkelkilde som sender ut et par med partikler, slik at en partikkel dukker opp til venstre mens den andre kommer ut til høyre for kilden. Vi kan tenke oss at kilden er slik innretta at partiklene som sendes ut kommer med motsatt retta bevegelsesmengder, eller spinn, eller polarisasjonsretning for å nevne noen muligheter. Vi gir partikkelen til venstre merkelappen partikkel '1' mens partikkelen til høyre merkes som partikkel '2'. Dersom vi beholder eksemplet med strålesplitteren, er det slik at dersom partikkel '1' kommer ut i den øvre strålen, vil alltid partikkel '2' komme ut i den nedre strålen til høyre. I vår bit-sjargong, betyr det at dersom partikkel '1' kommer ut med bit '0', må partikkel '2' komme ut med bit '1', eller motsatt. Kvantemekanisk kan vi tenke oss denne tilstanden av to partikler, eller to qubits om vi vil, gitt ved to qubits kombinasjonen

$$\frac{|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2}{\sqrt{2}}, \tag{23}$$

hvor indeksene '1' og '2' henspeiler på henholdsvis partikkel 1 og 2. Denne likningen beskriver det som kalles for en entangled tilstand (kryssa tilstand) med den interessante egenskap at ingen av de to qubiten har en bestemt verdi. Men det vi finner ut om denne kvantetilstanden ved måling på en av qubitene (partiklene), en måling hvis resultat ikke er kjent a priori, er at den andre qubiten har motsatt verdi av f.eks. spinn eller bevegelsesmengde. Det ser ut som om det kan være kvantekorrelasjoner, sjøl om målingen på partiklene foretas når partiklene er langt borte. Denne kvantemekaniske ikke-lokaliteten ga opphav til den store disputten mellom Einstein og Bohr om paradokser i kvantemekanikken. Tiltsanden i siste likning kalles også for en Bell tilstanden (etter den irske fysikeren John Bell), eller EPR par (etter Einstein, Podolsky og Rosen) og er en viktig byggestein i kvanteinformasjonsteori, teleportasjon og kryptering. Korrelasjonene som framkommer i slike tilstander har vært heftig debattert siden artikkelen til Einstein, Podolsky og Rosen i 1935. John Bell viste at målingskorrelasjonene mellom slike kvantemekaniske tilstander er mye sterkere enn de som finnes blant klassiske systemer.

I vår diskusjon skal vi nøye oss med å slå fast, på lik linje med dobbelspalt eksperiment hvor vi ikke kan fastslå hvorvidt partikkelen går gjennom spalt 1 eller to, at den kvantemekaniske superposisjonen slik vi ser den i likning (23) ikke tillater oss å si hvilke av de to en-qubit mulighetene går inn i tilstanden. Vi kan ikke si om qubit '1', partikkel '1', er i bit '0' eller '1', likeså om qubit '2', partikkel '2', er i bit '0' eller '1'. Men, dersom vi måler på qubit '1' kan vi umiddelbart si noe om hva slags tilstand qubit '2' er i. Disse betraktningene leder oss til spørsmålet om hvordan vi kan lage og observere såkalte 'entangled' tilstander.

En mulighet er ved henfall av partikler med spinn 0 til to partikler med halvtallig spinn. Det totale spinnet må være bevart, noe som betyr at de to utgående partiklene må ha motsatt retta spinn. Et slikt eksempel er et nøytralt pion, et boson (meson) med masse 134 MeV/c^2, som kan henfalle til et elektron

og et positron, en partikkel med elektronets masse men motsatt ladning, et såkalt antielektron. Dersom det kun er spinnets verdi som tillater oss å skille mellom mulige utkommer ved kilden, vil den resulterende to qubit kvantetilstanden se ut som følger

$$\frac{|+\rangle_1|-\rangle_2 - |-\rangle_1|+\rangle_2}{\sqrt{2}}, \tag{24}$$

hvor + og − henspeiler til henholdsvis spinn opp og spinn ned, mens indeksene 1 og 2 refererer til partikkel '1' og '2'. En måling på partikkel '1' vil umiddelbart også fastlegge spinnet til partikkel '2'. Det er slik virkning 'uten vekselvirkning' samt det kvantemekaniske superposisjonsprinsippet som danner grunnlaget for det nye forskningsfeltet om kvantedatamaskiner og kvante informasjonsteori.

Vi avslutter dette avsnittet med en kort beskrivelse av to-qubit tilstander. I neste avsnitt skal vi se hvordan vi kan bruke slike to-qubit tilstander til å simulere kvantemekaniske kretser.

En en-qubit tilstand er gitt ved

$$|q\rangle_1 = \alpha_1|0\rangle_1 + \beta_1|1\rangle_1, \tag{25}$$

hvor indeksen '1' henviser til qubit '1'. Setter vi sammen en slik en-qubit tilstand sammen med en annen en-qubit tilstand har vi

$$|q\rangle_{12} = |q\rangle_1|q\rangle_2 \tag{26}$$

eller

$$|q\rangle_{12} = \alpha_1\alpha_2|0\rangle_1|0\rangle_2 + \alpha_1\beta_2|0\rangle_1|1\rangle_2 + \beta_1\alpha_2|1\rangle_1|0\rangle_2 + \beta_1\beta_2|1\rangle_1|1\rangle_2, \tag{27}$$

slik at våre nye basistilstander blir $|0\rangle_1|0\rangle_2$, $|0\rangle_1|1\rangle_2$, $|1\rangle_1|0\rangle_2$ og $|1\rangle_1|1\rangle_2$.

Dersom alle koeffisientene er forskjellige fra null, kan vi lage en tilstand som nå er en superposisjon av fire ulike tilstander.

Slik kan vi fortsette med flere qubits og lage superposisjoner av flere og mer kompliserte basistilstander.

Kvantemekaniske kretser

I elektronikk er det slik at vi kan bygge alle mulige type kretser vha. kun to basiskretser, en såkalt NOT krets og en AND krets. Disse kan slås sammen til en NAND krets, slik at i grunnen trenger vi kun en basis krets.

Enhver kvantekrets må kunne formuleres som virkningen av en eller annen kvantemekanisk operator $\hat{H}$. Generelt har vi da at

$$|q\rangle_{ut} = \hat{H}|q\rangle_{in}, \tag{28}$$

men siden $\hat{H}$ må være hermitesk, dvs. $\hat{H}^\dagger = \hat{H}$ og $\hat{H}^\dagger\hat{H} = 1$, har vi

$$\hat{H}^\dagger|q\rangle_{ut} = \hat{H}^\dagger\hat{H}|q\rangle_{in} = |q\rangle_{in}. \tag{29}$$

Vi ser av siste likning at vi kan få ut begynnelsestilstanden utifra den inverse transformasjonen $\hat{H}^\dagger|q\rangle_{ut}$ på sluttilstanden. Det betyr igjen at vi må kunne dedusere fra utgangs-biten(e) hvilken verdi inngangs-biten(e) hadde. En slik krets kalles reversibel og skiller seg fra en klassisk irreversibel AND krets.

Det er mulig å vise innenfor informasjonsteori at en kan lage en reversibel Turingmaskin vha. kun to basis kretser, på lik linje med en klassisk irreversibel Turingmaskin basert på kun en NAND krets. Dvs. at vi kan lage oss alle mulige typer reversible kretser vha. kun to basis kretser. Disse er en NOT krets og en CNOT krets.

En CNOT krets, eller kontrollert NOT som den kalles, har blitt demonstrert vha. både ionefelle teknikker, hvor enkeltioners kvantemekaniske tilstander representerer bit '0' og '1', og kjernemagnetisk resonans teknikker.

Vi skal diskutere disse to kretsene i neste underavsnitt og avslutte med en faktisk realisering av en CNOT krets.

CNOT kretser

En CNOT krets beskriver vekselvirkningen mellom to qubits. Den ene qubiten kalles for kontroll-biten mens den andre kalles target-biten. Vi bruker indeks c for den første og indeks t for den siste. Dens virkning er slik at når kontrollbiten har verdi bit '0', forblir targetbiten også uforandra. Dersom kontroll-biten har verdien bit '1', forandres target-biten fra f.eks. bit '0' til bit '1', eller motsatt, dvs. virkningen på target-biten er som en NOT krets dersom kontroll-biten har verdi bit '1'. Vi kan derfor tenke oss en kvantemekanisk begynnelsestilstand gitt ved en qubit for kontroll-biten og en qubit for target-biten. Virkningen kan da oppsummeres som følgende

$$|0\rangle_c|0\rangle_t \rightarrow |0\rangle_c|0\rangle_t, \tag{30}$$

$$|0\rangle_c|1\rangle_t \rightarrow |0\rangle_c|1\rangle_t, \tag{31}$$

$$|1\rangle_c|0\rangle_t \rightarrow |1\rangle_c|1\rangle_t, \tag{32}$$

og

$$|1\rangle_c|1\rangle_t \rightarrow |1\rangle_c|0\rangle_t. \tag{33}$$

Matematisk kan vi uttrykke en CNOT krets som en 4×4 matrise

$$\hat{H}_{\text{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \tag{34}$$

som virker på basistilstandene $|0\rangle_c|0\rangle_t$, $|0\rangle_c|1\rangle_t$, $|1\rangle_c|0\rangle_t$ og $|1\rangle_c|1\rangle_t$. Som vektorer kan vi skrive disse tilstandene på følgende vis

$$|0\rangle_c|0\rangle_t = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \tag{35}$$

$$|0\rangle_c|1\rangle_t = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \tag{36}$$

$$|1\rangle_c|0\rangle_t = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \tag{37}$$

og

$$|1\rangle_c|1\rangle_t = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}. \tag{38}$$

Som et eksempel kan vi rekne

$$\hat{H}_{\mathrm{CNOT}}|1\rangle_c|1\rangle_t = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \tag{39}$$

som er $|1\rangle_c|0\rangle_t$, dvs. target-biten forandrer verdi fra bit '1' til bit '0' når kontroll-biten har verdi bit '1'.

Introduction

A theoretical understanding of the behavior of many-body systems is a great challenge and provides fundamental insights into quantum mechanical studies, as well as offering potential areas of applications. However, apart from some few analytically solvable problems, the typical absence of an exactly solvable contribution to the many-particle Hamiltonian means that we need reliable numerical many-body methods. These methods should allow for controlled approximations and provide a computational scheme which accounts for successive many-body corrections in a systematic way. Typical examples of popular many-body methods are coupled cluster methods, various types of Monte Carlo methods, perturbative expansions, Green's function methods, the density-matrix renormalization group, ab initio density functional theory and large-scale diagonalization methods.

All these methods have to face in some form or the other the problem of an exponential growth in dimensionality. For a system of P fermions which can be placed into N levels, the total number of basis states are given by $\begin{pmatrix} N \\ P \end{pmatrix}$. The dimensional curse means that most quantum mechanical calculations on classical computers have exponential complexity and therefore are very hard to solve for larger systems. On the other hand, a so-called quantum computer, a particularly dedicated computer, can improve greatly on the size of systems that can be simulated, as foreseen by Feynman. A quantum computer does not need an exponential amount of memory to represent a quantum state. The basic unit of information for a quantum computer is the so-called qubit or quantum bit. Any suitable two-level quantum system can be a qubit, but the standard model of quantum computation is a model where two-level quantum systems are located at different points in space, and are manipulated by a small universal set of operations. These operations are called gates in the same fashion as operations on bits in classical computers are called gates.

For the example of P spin 1/2 particles, a classical computer needs 2^P bits to represent all possible states, while a quantum computer needs only P qubits. The complexity in number of qubits is thus linear. Based on these ideas, several groups have proposed various algorithms for simulating quantal many-body systems on quantum computers. Abrams and Lloyd introduced a quantum algorithm that uses the quantum fast Fourier transform to find eigenvalues and eigenvectors of a given Hamiltonian, illustrating how one could solve classically intractable problems with less than 100 qubits. Achieving a polynomial complexity in the number of operations needed to simulate a quantum system is not that straightforward however. To get efficient simulations in time one needs to transform the many-body Hamiltonian into a sum of operations on qubits, the building blocks of the quantum simulator and computer, so that the time evolution operator can be implemented in polynomial time.

The aim of this work is to develop an algorithm than allows one to perform a quantum computer simulation (or simply quantum simulation hereafter) of any many-body fermionic Hamiltonian. We show how to generate, via various Jordan-Wigner transformations, all qubit operations needed to simulate the time evolution operator of a given Hamiltonian. We also show that for a given term in an m-body fermionic Hamiltonian, the number of operations needed to simulate it is linear in the number of qubits or energy-levels of the system. The number of terms in the Hamiltonian is of the order of m^2 for a general m-body interaction, making the simulation increasingly harder with higher order interactions. We specialize our examples to a two-body Hamiltonian, since this is also the most general type of Hamiltonian encountered in many-body physics. Besides fields like nuclear physics, where three-body forces play a non-neglible role, a two-body Hamiltonian captures most of the relevant physics.

Hamiltonians

A general two-body Hamiltonian for fermionic system can be written as

$$H = E_0 + \sum_{ij=1} E_{ij} a_i^\dagger a_j + \sum_{ijkl=1} V_{ijkl} a_i^\dagger a_j^\dagger a_l a_k, \tag{40}$$

where E_0 is a constant energy term, E_{ij} represent all the one-particle terms, allowing for non-diagonal terms as well. The one-body term can represent a chosen single-particle potential, the kinetic energy or other more specialized terms such as those discussed in connection with the Hubbard model or the pairing Hamiltonian discussed below. The two-body interaction part is given by V_{ijkl} and can be any two-body interaction, from Coulomb interaction to the interaction between nucleons. The sums run over all possible single-particle levels N. Note that this model includes particle numbers from zero to the number of available quantum levels, n. To simulate states with fixed numbers of fermions one would have to either rewrite the Hamiltonian or generate specialized input states in the simulation.

The algorithm which we will develop in this section and in However, in our demonstrations of the quantum computing algorithm, we will limit ourselves to two simple models, which however capture much of the important physics in quantum mechanical many-body systems. We will also limit ourselves to spin $j = 1/2$ systems, although our algorithm can also simulate higher j-values, such as those which occur in nuclear, atomic and molecular physics, it simply uses one qubit for every available quantum state. These simple models are the Hubbard model and a pairing Hamiltonian. We start with the spin 1/2 Hubbard model, described by the following Hamiltonian

$$\begin{aligned} H_H &= \epsilon \sum_{i,\sigma} a_{i\sigma}^\dagger a_{i\sigma} - t \sum_{i,\sigma} \left(a_{i+1,\sigma}^\dagger a_{i,\sigma} + a_{i,\sigma}^\dagger a_{i+1,\sigma} \right) \\ &\quad + U \sum_{i=1} a_{i+}^\dagger a_{i-}^\dagger a_{i-} a_{i+}, \end{aligned} \tag{41}$$

where $a^\dagger$ and a are fermion creation and annihilation operators, respectively. This is a chain of sites where each site has room for one spin up fermion and one spin down fermion. The number of sites is N, and the sums over σ are sums over spin up and down only. Each site has a single-particle energy ϵ. There is a repulsive term U if there is a pair of particles at the same site. It is energetically favourable to tunnel to neighbouring sites, described by the hopping terms with coupling constant $-t$.

The second model-Hamiltonian is the simple pairing Hamiltonian

$$H_P = \sum_i \varepsilon_i a_i^\dagger a_i - \frac{1}{2} g \sum_{ij>0} a_i^\dagger a_{\bar{i}}^\dagger a_{\bar{j}} a_j, \tag{42}$$

The indices i and j run over the number of levels N, and the label $\bar{i}$ stands for a time-reversed state. The parameter g is the strength of the pairing force while ε_i is the single-particle energy of level i. In our case we assume that the single-particle levels are equidistant (or degenerate) with a fixed spacing

d. Moreover, in our simple model, the degeneracy of the single-particle levels is set to $2j+1=2$, with $j=1/2$ being the spin of the particle. This gives a set of single-particle states with the same spin projections as for the Hubbard model. Whereas in the Hubbard model we operate with different sites with spin up or spin down particles, our pairing models deals thus with levels with double degeneracy. Introducing the pair-creation operator $S_i^+ = a_{im}^\dagger a_{i-m}^\dagger$, one can rewrite the Hamiltonian in Eq. (42) as

$$H_P = d\sum_i iN_i + \frac{1}{2}G\sum_{ij>0} S_i^+ S_j^-,$$

where $N_i = a_i^\dagger a_i$ is the number operator, and $\varepsilon_i = id$ so that the single-particle orbitals are equally spaced at intervals d. The latter commutes with the Hamiltonian H. In this model, quantum numbers like seniority $\mathcal{S}$ are good quantum numbers, and the eigenvalue problem can be rewritten in terms of blocks with good seniority. Loosely speaking, the seniority quantum number $\mathcal{S}$ is equal to the number of unpaired particles. Furthermore, in a series of papers, Richardson obtained the exact solution of the pairing Hamiltonian, with semi-analytic (since there is still the need for a numerical solution) expressions for the eigenvalues and eigenvectors. The exact solutions have had important consequences for several fields, from Bose condensates to nuclear superconductivity and is currently a very active field of studies, see for example Finally, for particle numbers up to $P \sim 20$, the above model can be solved exactly through numerical diagonalization and one can obtain all eigenvalues. It serves therefore also as an excellent ground for comparison with our algorithm based on models from quantum computing.

Basic quantum gates

Benioff showed that one could make a quantum mechanical Turing machine by using various unitary operations on a quantum system. Benioff demonstrated that a quantum computer can calculate anything a classical computer can. To do this one needs a quantum system and basic operations that can approximate all unitary operations on the chosen many-body system. We describe in this subsection the basic ingredients entering our algorithms.

Qubits, gates and circuits. In this article we will use the standard model of quantum information, where the basic unit of information is the qubit, the quantum bit. As mentioned in the introduction, any suitable two-level quantum system can be a qubit, it is the smallest system there is with the least complex dynamics. Qubits are both abstract measures of information and physical objects. Actual physical qubits can be ions trapped in magnetic fields where lasers can access only two energy levels or the nuclear spins of some of the atoms in molecules accessed and manipulated by an NMR machine. Several other ideas have been proposed and some tested.

The computational basis for one qubit is $|0\rangle$ (representing for example bit 0) for the first state and $|1\rangle$ (representing bit 1) for the second, and for a set of

qubits the tensor products of these basis states for each qubit form a product basis. Below we write out the different basis states for a system of n qubits.

$$\begin{aligned}
&|0\rangle \equiv |00\cdots 0\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |0\rangle \\
&|1\rangle \equiv |00\cdots 1\rangle = |0\rangle \otimes |0\rangle \otimes \cdots \otimes |1\rangle \\
&\vdots \\
&|2^n - 1\rangle \equiv |11\cdots 1\rangle = |1\rangle \otimes |1\rangle \otimes \cdots \otimes |1\rangle.
\end{aligned} \tag{43}$$

This is a 2^n-dimensional system and we number the different basis states using binary numbers corresponding to the order in which they appear in the tensor product.

Quantum computing means to manipulate and measure qubits in such a way that the results from a measurement yield the solutions to a given problem. The quantum operations we need to be able to perform our simulations are a small set of elementary single-qubit operations, or single-qubit gates, and one universal two-qubit gate, in our case the so-called CNOT gate defined below.

To represent quantum computer algorithms graphically we use circuit diagrams. In a circuit diagram each qubit is represented by a line, and operations on the different qubits are represented by boxes.

Number of work qubits versus number of simulation qubits

The largest possible amount of different eigenvalues is 2^s, where s is the number of simulation qubits. The resolution in the energy spectrum we get from measuring upon the work qubits is 2^w, with w the number of work qubits. Therefore the resolution per eigenvalue in a non-degenerate system is 2^{w-s}. The higher the degeneracy the less work qubits are needed.

Number of operations

Counting the number of single-qubit and $\sigma_z\sigma_z$ operations for different sizes of systems simulated gives us an indication of the decoherence time needed for different physical realizations of a quantum simulator or computer. The decoherence time is an average time in which the state of the qubits will be destroyed by noise, also called decoherence, while the operation time is the average time an operation takes to perform on the given system. Their fraction is the number of operations possible to perform before decoherence destroys the computation. In table we have listed the number of gates used for the pairing model, H_P, and the Hubbard model, H_H, for different number of simulation qubits.

	$s=2$	$s=4$	$s=6$	$s=8$	$s=10$	$s=12$
H_P	9	119	333	651	1073	1598
H_H	9	51	93	135	177	219

Number of two-qubit gates used in simulating the time evolution operator of the pairing model, H_P, and the Hubbard model, H_H, for different number of simulation qubits s.

We list here some useful relations involving different σ matrices,

$$\sigma_x\sigma_z = -i\sigma_y, \quad \sigma_z\sigma_x = i\sigma_y, \quad [\sigma_x, \sigma_z] = -2i\sigma_y, \tag{44}$$

$$\sigma_x\sigma_y = i\sigma_z, \quad \sigma_y\sigma_x = -i\sigma_z, \quad [\sigma_x, \sigma_y] = 2i\sigma_z, \tag{45}$$

and

$$\sigma_y\sigma_z = i\sigma_x, \quad \sigma_z\sigma_y = -i\sigma_x, \quad [\sigma_y, \sigma_z] = 2i\sigma_x. \tag{46}$$

For any two non-equal σ-matrices a and b we have

$$aba = -b. \tag{47}$$

The Hermitian σ-matrices σ_x, σ_y and σ_z result in the identity matrix when squared

$$\sigma_x^2 =_1 , \quad \sigma_y^2 =_1 , \quad \sigma_z^2 =_1 , \tag{48}$$

which can be used to obtain simplified expressions for exponential functions involving σ-matrices

$$e^{\pm i\alpha\sigma} = \cos(\alpha)_1 \pm i\sin(\alpha)\sigma. \tag{49}$$

The equations we list below are necessary for the relation between a general unitary transformation on a set of qubits with a product of two-qubit unitary transformations. We have the general equation for $a, b \in \{\sigma_x, \sigma_y, \sigma_z\}$, where $a \neq b$.

$$\begin{aligned} e^{-i\pi/4a}be^{i\pi/4a} &= \frac{1}{2}({}_1 - ia)b({}_1 + ia) \\ &= \frac{1}{2}(b + aba + i[b, a]) \\ &= \frac{i}{2}[b, a]. \end{aligned} \tag{50}$$

The more specialized equations read

$$e^{-i\pi/4\sigma_x}\sigma_z e^{i\pi/4\sigma_x} = -\sigma_y, \tag{51}$$

$$e^{-i\pi/4\sigma_y}\sigma_z e^{i\pi/4\sigma_y} = \sigma_x, \tag{52}$$

$$e^{-i\pi/4\sigma_z}\sigma_x e^{i\pi/4\sigma_z} = \sigma_y, \tag{53}$$

$$e^{-i\pi/4\sigma_z}\sigma_y e^{i\pi/4\sigma_z} = -\sigma_x. \tag{54}$$

We need also different products of the operatorσ_z with the raising and lowering operators

$$\sigma_+\sigma_z = -\sigma_+ \tag{55}$$
$$\sigma_z\sigma_+ = \sigma_+, \tag{56}$$
$$\sigma_-\sigma_z = \sigma_-, \tag{57}$$
$$\sigma_z\sigma_- = -\sigma_-. \tag{58}$$
$$\tag{59}$$