

KVANTEALGORITMER OG KVANTEINTERFERENS

VERSION F

LEKTOR KIM SPLITTORFF & PH.D. STUDERENDE ANNA BJERREGAARD

Niels Bohr Institutet

Fysik KU

split@nbi.ku.dk, a.bjerregaard@nbi.ku.dk

NQCP
NIELS BOHR INSTITUTE

Indhold

I	Forord	1
1	Om noten	1
2	Tak til	1
II	Kvanteinterferens	2
3	Kvanteinterferens af en elektron	2
4	Superposition og sandsynlighed	2
5	Operationer på en enkelt qubit	3
6	Kvanteinterferens af en enkelt qubit	4
7	Mach-Zehnder interferometer	5
8	Den simpleste kvantealgoritme	5
III	Fourier multipliers	7
9	Forskydning af et signal	7
10	Fourier multipliers	8
IV	Kvantefouriertransformationen	9
11	Definition af kvantefouriertransformationen	9
12	Ekspontielt hurtigere end den klassiske	10
V	Kvantefaseestimering	11
13	Estimeringsopgaven og algoritmen	11
14	Kvante-fourier multipler	12
15	Konstruktiv kvanteinterferens udpeger fasen	13

16 Korrekt til t decimaler	13
17 Virker også hvis $ u\rangle$ ikke er en egentilstand	14
18 Fysisk intuition for kvantefaseestimerings-algoritmen	14
19 Shors algoritme for primtalsfaktorisering	14
 VI Opsummering	 16
20 Superposition af alle veje giver mulig interferens	16
21 Konstruktiv interferens ved løsningen vi søger	17
22 Afslutning	17
 VII Appendix	 18
A Implementering af kvantefouriertransformationen	18

Forord

AFSNIT 1

Om noten

Kvantealgoritmer er de instruktioner man giver en kvantecomputer for at løse specifikke problemer. Med andre ord, det er kvanteversionen af den klassiske algoritme som er kernen i et computerprogram på en klassisk computer.

Formålet med denne note er at give en introduktion til et par udvalgte, men centrale kvantealgoritmer. Ambitionen er at give en ide om hvordan disse udvalgte kvantealgoritmer udnytter kvanteinterferens og dermed bliver eksponentielt hurtigere end klassiske algoritmer der løser samme problem. Vi vil både prøve at give et intuitivt billede af hvordan algoritmerne virker men også dykke ned i den matematiske formulering.

Målgruppe: Denne note er udarbejdet med tanke på studerende, undervisere eller andre der er interesserede i at lære om kvantealgoritmer, og *godt kan lide selv at arbejde mens de lærer*.

Baggrund: For at kunne arbejde med den matematiske formulering af kvantealgoritmer, kræves et vist forkundskab til qubits og til operationer på qubits svarende til det der kan opnås ved at arbejde med noterne ‘Qubits og Kvantecomputere’, som kan findes på kan findes på <https://nqcp.ku.dk/teaching/>. Desuden antages kendskab til komplekse tal.

AFSNIT 2

Tak til

Tak, til alle der deltog i workshopen on kvantealgoritmer på LFMK årsmødet 2023 hvor en tidlig version af denne note blev brugt for første gang. Der kom meget god feedback derfra. En stor tak til Mikkel Max Jorn og Jacob Debel for en diskussion ved tavlen der førte til Kapitel III. Tak, til Jacob Hastrup, Ask Høyer Splittorff og Ove Splittorff for at kommentere β -versionen af disse noter. En særlig tak til Michael Hallundbæk for at stille sin altid skarpe pen til rådighed ved gennemlæsninger af flere versioner af denne note.

Noten er udarbejdet under Novo Nordisk Fonden, Grant number NNF22SA0081175, NNF Quantum Computing Programme.

Kvanteinterferens

Den centrale ingrediens i de kvantealgoritmer vi skal se på her er kvanteinterferens og vi lægger i dette kapitel for med at se på den simpleste version heraf.

AFSNIT 3

Kvanteinterferens af en elektron

Inden vi kaster os over formalismen, så lad os starte med at se på dobbeltspalteeksperimentet, Figur 1. I forsøget sendes elektroner fra en kilde, S (source), gennem en kollimator, A, og dernæst gennem enten én eller to spalter ved B, inden de detekteres et sted på pladen C. Der er dermed hhv. én eller to veje fra A til detektion ved C. Hver enkelt elektron vil blive detekteret et sted på pladen C, og efter mange elektroner er blevet detekteret vil der dannes en fordeling P (for probability på Engelsk).

Det afgørende her er at forsøget med begge spalter åbne *ikke* giver samme resultat som summen af resultaterne vi får ved at lave forsøget med én spalte åben ad gangen. I stedet viser resultatet et mønster der minder om det klassiske interferensmønster der opstår hvis vi tilsvarende sender vandbølger imod to åbninger. Forskellen er opstået på grund af kvanteinterferens, se igen Figur 1.

Bemærk

Bemærk at interferensen også sker når intensiteten af elektronkilden er så lav at der kun er én elektron i opstillingen ad gangen. Elektronen interfererer med sig selv når der ikke er nogen måde at afgøre hvilken vej den har taget inden detektionen.

I de kvantealgoritmer vi skal se på går kvantecomputerens qubits, ligesom elektronen i dobbeltspalteforsøget, fra en given starttilstand til en sluttstand der måles. For elektronen i dobbeltspalteeksperimentet er der to veje, men for t -qubits kan vejen fra starttilstanden til sluttilstanden gå gennem 2^t kvantetilstande. Tilstanden af de t -qubits kan samle relative faser op undervejs der afhænger af vejen og det er disse faser der giver mulighed for kvanteinterferens i algoritmerne (se afsnit 6). Ligesom for elektronen i dobbeltspalteforsøget sker interferensen når der ikke er nogen måde at afgøre hvilken af vejene systemet af qubits har taget inden detektionen.

AFSNIT 4

Superposition og sandsynlighed

For at forstå hvad en relativ fase er og hvad der er for mulige veje, så lad os først slå fast hvad vi mener med superposition for en enkelt qubit.

Definition 1

Superposition: Qubit tilstanden $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ er en normaliseret superposition af de to tilstande $|0\rangle$ og $|1\rangle$ hvis de komplekse koefficienter α og β opfylder $|\alpha|^2 + |\beta|^2 = 1$.

Lad os også parametrisere de to komplekse koefficienter som vinkler.

Opgave 1 | Vis at $|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle$ er normaliseret.

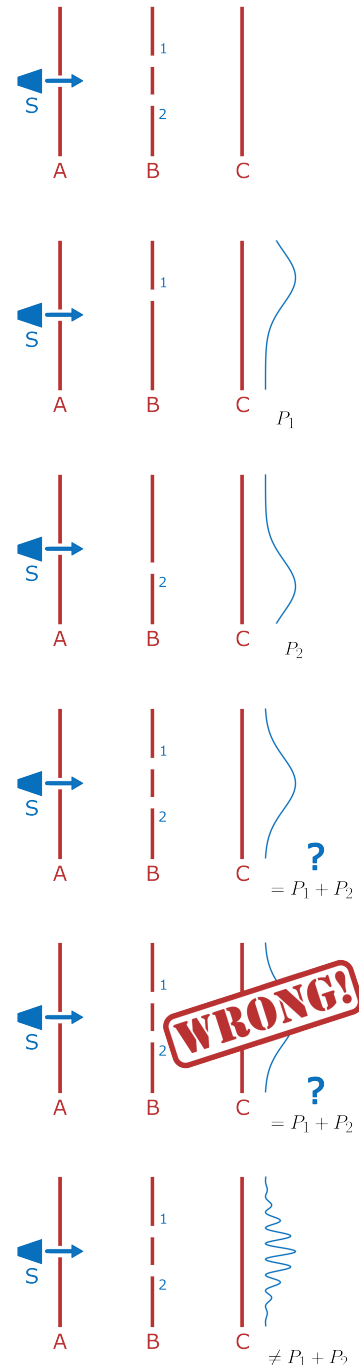
Vinklen ϕ er den relative fase mellem de to tilstande $|0\rangle$ og $|1\rangle$.

Bemærk

Bemærk at der er tre reelle frihedsgrader i den generelle superposition (to fra hvert komplekst tal α , β og et bånd pga normaliseringen) og kun to vinkler i den opgave vi lige

KAPITEL

II



Figur 1. Dobbeltspalteforsøg, med elektroner. (Illustrationer adapteret fra [1].)

har set på. Den sidste frihedsgrad er en kompleks fase der kan ganges på hele tilstanden – en såkaldt *global fase*. Det er dog kun den relative fase mellem de to tilstande $|0\rangle$ og $|1\rangle$ der er afgørende for vores kvanteinterferens og vores kvantealgoritmer, den globale fase er udeladt.

Hvis vi udfører en måling er de eneste mulige udfald af målingen 0 eller 1 og det eneste vi ved før målingen er at sandsynligheden for at detekttere 0 eller 1 er givet således:

Definition 2 Sandsynlighed: Hvis en qubit befinder sig i tilstanden $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ er sandsynligheden for at måle 0, $P_0 = |\alpha|^2$, og sandsynligheden for at måle 1, $P_1 = |\beta|^2$.

Bemærk Bemærk at den relative fase ϕ ikke umiddelbart påvirker sandsynlighederne.

Opgave 2 Vores qubit er i tilstanden $|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle$. Vis at sandsynligheden for at måle 0 eller 1 er uafhængig af vinklen ϕ .

AFSNIT 5

Operationer på en enkelt qubit

Fasen ϕ kan styres vha en operator, og vi vil først se på T -operatoren, som er defineret i Figur 2.

$$\begin{array}{ccc} |0\rangle & \xrightarrow{\boxed{T}} & |0\rangle \\ |1\rangle & \xrightarrow{\boxed{T}} & e^{i\pi/4}|1\rangle \end{array}$$

Figur 2. Definitionen af hvordan T -operatoren virker på $|0\rangle$ og $|1\rangle$.

Vi får også brug for Hadamard-operatoren, se Figur 3.

$$\begin{array}{ccc} |0\rangle & \xrightarrow{\boxed{H}} & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ |1\rangle & \xrightarrow{\boxed{H}} & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{array}$$

Figur 3. Hadamard operatoren H virker på en qubit.

Lad os prøve at få vinklen ϕ i spil. Først virker vi på $|0\rangle$ med H og derefter med T , se Figur 4. Som ønsket har vi fået introduceret vinklen $\phi = \pi/4$ i fasen $e^{i\pi/4}$.

$$|0\rangle \xrightarrow{\boxed{H}} \xrightarrow{\boxed{T}} \frac{1}{\sqrt{2}}(|0\rangle + e^{i\pi/4}|1\rangle)$$

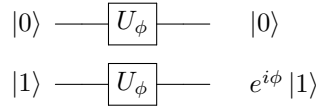
Figur 4. Simplest mulige eksempel på at introducere en fase.

Bemærk Bemærk at en operator virker på en superposition ved at virke på hvert led i superpositionen, m.a.o. den virker lienært.

Eksempel Lad os lige tage et hurtigt eksempel på denne linearitet $HH|0\rangle = H\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{\sqrt{2}}(H|0\rangle + H|1\rangle) = \frac{1}{2}(|0\rangle + |1\rangle + |0\rangle - |1\rangle) = |0\rangle$.

Opgave 3 Vis at tilstanden efter vi har virket på $|0\rangle$ med H , T dvs tilstanden $TH|0\rangle$, er som angivet på Figur 4.

T -operatoren tilføjer en fase på $\pi/4$ til tilstanden $|1\rangle$. Vi kan tilføje en generel fase ϕ med U_ϕ operatoren, se Figur 5.



Figur 5. U_ϕ -operatoren generaliserer T -operatoren til en vilkårlig vinkel.

AFSNIT 6

Kvanteinterferens af en enkelt qubit

Vi er nu klar til vores første formelle eksempel på kvanteinterferens.

- Opgave 4** Vis at tilstanden efter vi har virket på $|0\rangle$ med H , T og så H igen, dvs tilstanden $HTH|0\rangle$, er som angivet på Figur 6. Sammenlign med hvad tilstanden ville have været hvis vi havde udeladt T operatoren.

$$|0\rangle \xrightarrow{H} \xrightarrow{T} \xrightarrow{H} \frac{1}{2}((1 + e^{i\pi/4})|0\rangle + (1 - e^{i\pi/4})|1\rangle)$$

Figur 6. Simplest mulige eksempel på kvanteinterferens.

- Opgave 5** Bestem sandsynligheden for at måle henholdsvis 0 og 1 hvis systemets tilstand er $|\psi\rangle = \frac{1}{2}((1 + e^{i\pi/4})|0\rangle + (1 - e^{i\pi/4})|1\rangle)$.

Vink: det kan være nyttigt at benytte omskrivningen $1 + e^{i\pi/4} = e^{i\pi/8}(e^{-i\pi/8} + e^{i\pi/8})$.

- Opgave 6** Udskift T -operatoren med en U_ϕ -operator, se Figur 5, og svar på samme spørgsmål. Lav også et plot af P_0 og P_1 som funktion af ϕ .

Bemærk Bemærk at sandsynligheden i opgaven ovenfor for at måle hhv. 0 og 1 afhænger af vinklen ϕ . Denne afhængighed er kommet i stand via en **kvanteinterferens**.

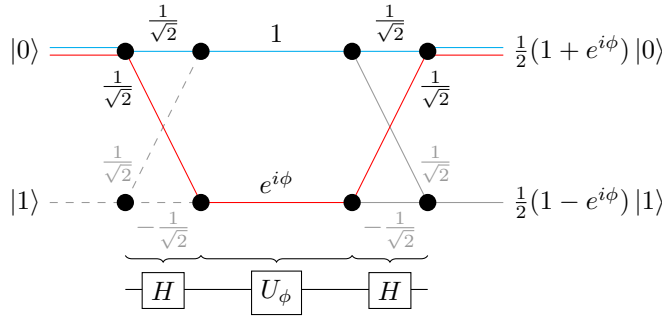
Men der er jo kun en qubit, så hvad er det der interfererer? For at forstå dette så lad os se på sandsynligheden for at få 0 i målingen. Sandsynligheden er givet ved absolutkvadratet på koefficienten $\frac{1}{2}(1 + e^{i\phi})$ foran $|0\rangle$. Værdien af denne koefficient kommer i stand ved at der er to veje fra vores begyndelsestilstand $|0\rangle$ til $|0\rangle$ -komponenten af sluttilstanden. Den ene vej er

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|0\rangle \xrightarrow{U_\phi} \frac{1}{\sqrt{2}}|0\rangle \xrightarrow{H} \frac{1}{2}|0\rangle$$

mens den anden vej er

$$|0\rangle \xrightarrow{H} \frac{1}{\sqrt{2}}|1\rangle \xrightarrow{U_\phi} \frac{1}{\sqrt{2}}e^{i\phi}|1\rangle \xrightarrow{H} e^{i\phi}\frac{1}{2}|0\rangle$$

hvor fasen $+e^{i\phi}$ bliver samlet op ved U_ϕ -operationen. Vejen er altså en vej gennem tilstandene i superpositionen og interferensen opstår fordi 1) tilstandens fase afhænger af vejen og 2) vi adderer bidragene fra de to veje inden vi bestemmer sandsynligheden ved at absolut-kvadrere. En illustration af dette kan ses i Figur 7.



Figur 7. Kvanteinterferens for en enkelt qubit. En qubit starter i tilstanden $|0\rangle$. Vi udfører nu operationerne H , så U_ϕ og endeligt igen H . Den tyrkise og den røde linje på figuren illustrerer de mulige veje fra begyndelsestilstand $|0\rangle$ til $|0\rangle$ -komponenten af sluttilstanden. Bemærk at der ligeledes er to veje fra begyndelsestilstanden $|0\rangle$ til $|1\rangle$ -komponenten af sluttilstanden. (De stiplede linjer er veje som kun kan udnyttes hvis begyndelsestilstanden ikke er $|0\rangle$.) Illustrationen er inspireret af [3].

Bemærk Læg mærke til at det ligesom med elektronen i dobbeltspalteforsøget ikke er muligt at afgøre hvilken vej qubit'en har taget. Vi skal derfor lægge amplituderne $1/2$ og $1/2 e^{i\phi}$ sammen inden vi absolutkvadrerer for at bestemme sandsynligheden P_0 og dermed opstår der kvanteinterferens. Hvis vi på en eller anden vis kunne opnå kendskab til hvilken vej qubit'en havde taget, så skulle vi i stedet have lagt sandsynlighederne for de to veje sammen. Med andre ord skulle vi først have taget absolutkvadraterne og derefter have lagt resultaterne sammen. Resultatet ville derfor være uafhængig af ϕ og interferensen ville forsvinde.

Opgave 7 Forklar hvilke veje der giver den samlede koefficient $\frac{1}{2}(1 - e^{i\phi})$ af tilstanden $|1\rangle$ og hvor faserne samt fortegnet bliver samlet op.

AFSNIT 7

Mach-Zehnder interferometer

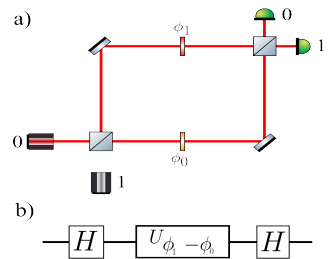
For at få en mere fysisk forståelse af den kvanteinterferens vi netop har arbejdet med tager vi nu et eksempel på hvordan den kan realiseres.

Eksempel Qubit-operationerne vi har set på svarer til hvad der sker i et Mach-Zehnder interferometer, se Figur 8. En foton sendes ind mod interferometeret langs vej 0 svarende til at starttilstanden er $|0\rangle$. I interferometeret er der to veje, den laveste som vi betegner $|0\rangle$ og den øverste der betegnes $|1\rangle$. Efter beamsplitteren er tilstanden $1/\sqrt{2}(|0\rangle + |1\rangle)$ præcist som hvis vi havde virket med H på $|0\rangle$. I hver vej er der indsat en faseskifter, og de har den relative fase $\phi = \phi_1 - \phi_0$. Samlet set svarer de til U_ϕ -operationen. Endelig samles vejene i den anden beamsplitter som igen svarer til H . Hvis fotonen efter interferometeret detekteres i den øverste detektor har vi målt nul, mens et klik i detektoren længst til højre viser at vi har målt 1.

AFSNIT 8

Den simpleste kvantealgoritme

Det enkle qubit-kredsløb vi har studeret i dette kapitel udfører faktisk en kvantealgoritme der kan løse et problem effektivt. Problemet er følgende: En af vores venner vælger to tal, og hvert tal er enten 0 eller 1. Vores opgave er at finde ud af om de to tal er ens eller



Figur 8. a) Mach-Zehnder interferometer med to faseskiftere. b) Tilsvarende qubit operationer. (Illustrationen er adapteret fra [3].)

forskellige. Vi vil selvfølgelig gerne være effektive, hvilket her betyder at vi vil spørge vores ven færrest muligt gange.

Arbejder vi klassisk er vi nødt til først at spørge vores ven hvad det ene tal er og derefter at spørge hvad det andet er, for at vi kan sammenligne de to og se om de er ens eller forskellige.

Vi vil nu se hvordan Mach-Zehnder opstillingen implementerer den simpleste kvantealgoritme og løser problemet: Inden vi går igang har vi instrueret vores ven til at gøre følgende (uden at vi kigger selvfølgelig). Hvis det første tal vores ven valgte var 0 indstiller hun faseskifteren i den nederste vej til fasen 0 men hvis det første tal er 1 indstiller hun fasen til π . Vores ven gør det tilsvarende med det andet tal i den øverste vej. Vi sender nu en enkelt foton, startende langs vej 0, ind gennem Mach-Zehnder interferometeret. Vi foretager altså en enkelt forespørgsel. Hvis de to faseskiftere er indstillet ens ankommer fotonen med 100 % sandsynlighed i detektor 0 mens der er total destruktiv interferens ved detektor 1. Men hvis den ene faseskifter er indstillet til 0 og den anden til π vil fotonen med sikkerhed blive detekteret i detektor 1 (total destruktiv interferens ved detektor 0). Med interferometeret kan vi derfor med en enkelt forespørgsel til vores ven med sikkerhed afgøre om de to valgte tal er ens eller ej og dermed løse den stillede opgave.

Bemærk Vi udnytter her at en enkelt foton kan give information om begge faseskiftere, selvom den når der måles, selvfølgelig kun vil detekteres et sted.

Opgave 8 | Opskriv tilstanden af en foton for hvert step i Mach-Zehnder interferometeret, hvor begge faseskiftere er indstillet til 0. Hvilke operatorer skal bruges til dette? Hvordan ser Mach-Zehnder interferometeret ud som kvantecomputerkredsløb?

Opgave 9 | Gentag opgave 8, men hvor den relative fase mellem de to faseskiftere er π .

Fourier multipliers

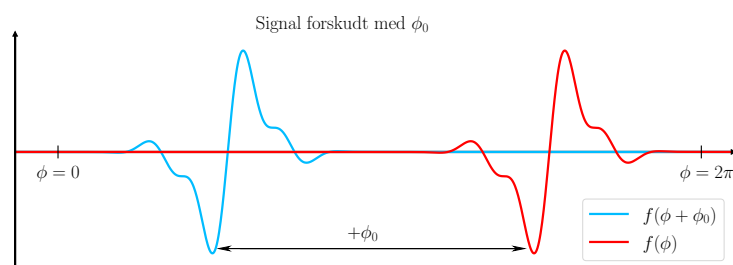
Inden vi kaster os over mere komplicerede kvantealgoritmer, så lad os tage et hurtigt kig på den klassiske Fouriertransformation og specielt hvordan vi med hjælp af Fourier multipliers kan forskyde et signal uden at ændre dets form. Dette er ikke blot en interessant matematisk øvelse, som vi vil se nedenfor er den helt central for de kvantealgoritmer vi vil studere.

AFSNIT 9

Forskydning af et signal

Lad os forestille os at vi har et signal hvis amplitude er beskrevet af en periodisk funktion, $f(\phi)$, med perioden 2π ; $f(\phi) = f(\phi + 2\pi)$.

Her vil vi undersøge hvad der sker med den Fouriertransformerede af signalet hvis vi forskyder ϕ med en konstat ϕ_0 men ellers ikke ændrer formen af signalet, se Figur 9.



Figur 9. Signal $f(\phi)$ forskudt med en konstant værdi ϕ_0 .

Lad os starte med at opskrive Fouriertransformationen af $f(\phi)$

$$\tilde{f}(m) = \frac{1}{2\pi} \int_0^{2\pi} f(\phi) e^{-im\phi} d\phi, \quad (9.1)$$

og den inverse transformation

$$f(\phi) = \sum_{m=-\infty}^{\infty} \tilde{f}(m) e^{im\phi}. \quad (9.2)$$

Bemærk at vi her har et integrale over ϕ og en sum over m , da $f(\phi)$ er en periodisk funktion.

Opgave 10 | Check at $f(\phi)$ som udtrykt i (9.2) er en funktion med periode 2π .

For at undersøge hvordan en forskydning påvirker Fourierkoefficienterne, erstatter vi nu

$f(\phi)$: oprindeligt signal

m : frekvenserne

$\tilde{f}(m)$: amplituden af m

ϕ med $\phi + \phi_0$ i ligning (9.2) og finder

$$f(\phi + \phi_0) = \sum_{m=-\infty}^{\infty} \tilde{f}(m) e^{im(\phi + \phi_0)}, \quad (9.3)$$

$$= \sum_{m=-\infty}^{\infty} \tilde{f}(m) e^{im\phi_0} e^{im\phi}. \quad (9.4)$$

Som forventet er det præcis de samme frekvenser m der indgår i det oprindelige og det forskudte signal. Men i det forskudte signal er Fourierkoefficienterne $\tilde{f}(m)$ blevet ganget med en m -afhængig fase $e^{im\phi_0}$.

Opgave 11 Udtryk $\tilde{f}(m)$ i ligning (9.4) ved hjælp af ligning (9.1) og verificer ved eksplicit beregning af summen at resultatet er $\tilde{f}(\phi + \phi_0)$.
Vink: Benyt at $\sum_{m=-\infty}^{\infty} e^{im(x-y)} = \delta(x-y)$.

AFSNIT 10

Fourier multipliers

Fasen $e^{im\phi_0}$ kaldes en *Fourier multiplier*. Denne Fourier multiplier er konsekvensen af det skift vi har givet funktionen

$$f(\phi + \phi_0) \xrightarrow{\text{FT}} \tilde{f}(m) \cdot e^{i\phi_0 m} \xrightarrow{\text{FT}^{-1}} f(\phi + \phi_0). \quad (10.1)$$

Omvendt hvis vi har muligheden for at tilføje en sådan Fourier multiplier (FM) kan vi forskyde funktionen

$$f(\phi) \xrightarrow{\text{FT}} \tilde{f}(m) \xrightarrow{\text{FM}} \tilde{f}(m) \cdot e^{i\phi_0 m} \xrightarrow{\text{FT}^{-1}} f(\phi + \phi_0). \quad (10.2)$$

Det er præcis en Fourier multiplier som i (10.2) der indgår i den kvantealgoritme vi vil beskrive nedenfor. Men istedet for Fouriertransformationen indgår kvantefouriertransformationen.

Kvante -fouriertransformationen

En central del af de kvantealgoritmer vi kigger på her er kvantefouriertansformationen. Den er analog til den diskrete Fouriertransformation men adskiller sig ved at være en transformation af en kvantetilstand. Og så kan vi implementere den eksponentielt mere effektivt på en kvantecomputer end den diskrete Fouriertransformation kan implementeres på en klassisk computer!

AFSNIT 11

Definition af kvantefouriertransformationen

For at skrive kvantefouriertransformationen op på en måde der minder om den klassiske diskrete Fouriertransformation er det nyttigt at skrive tilstandene via almindeligt (10-tals) system.

Eksempel | Hvis vi har 4 qubits skriver vi eksempelvis tilstanden $|0101\rangle$ som $|5\rangle$. Det er dog helt samme tilstand blot skrevet op i lidt mere kompakt notation.

Nu til definitionen:

Definition 3 | Givet et sæt af 2^t tilstande, $|l\rangle$ med $l = 0, \dots, 2^t - 1$ hvor $\langle l|l'\rangle = \delta_{ll'}$, så er kvantefouriertransformationen (over denne ortonormale basis) af $|l\rangle$ givet ved

$$|l\rangle \rightarrow \frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{2\pi i l j / 2^t} |j\rangle \quad (11.1)$$

Og lad os med det samme også opskrive den inverse transformation:

Definition 4 | Givet et sæt af 2^t tilstande, $|j\rangle$ with $j = 0, \dots, 2^t - 1$ så er den inverse kvantefouriertransformationen af tilstanden $|j\rangle$ er givet ved

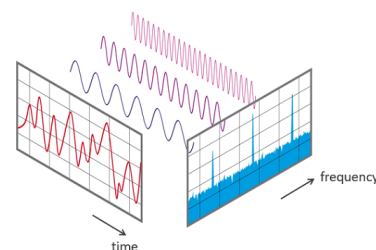
$$|j\rangle \rightarrow \frac{1}{\sqrt{2^t}} \sum_{k=0}^{2^t-1} e^{-2\pi i j k / 2^t} |k\rangle \quad (11.2)$$

Bemærk | De 2^t tilstande svarer til at vi har t qubits.

Lad os tage et eksempel og et par opgaver for at vænne os til definitionerne.

Eksempel | For en enkelt qubit har vi $t = 1$ og sættet der består af tilstandene $|0\rangle$ og $|1\rangle$. Kvantefouriertransformationen af tilstanden $|0\rangle$ er ifølge definitionen $|0\rangle \rightarrow 1/\sqrt{2}(|0\rangle + |1\rangle)$ da $e^{2\pi i l j / 2^t} = 1$ for $l = 0$ uafhængigt af j . Tilsvarende får vi at $|1\rangle \rightarrow 1/\sqrt{2}(|0\rangle - |1\rangle)$ da $e^{2\pi i l j / 2^t} = 1$ når $j = 0$ og da $e^{2\pi i l j / 2^t} = -1$ for $j = l = 1$ og $t = 1$.

Bemærk | Vi har i eksemplet ovenfor at $H|0\rangle$ giver kvantefouriertransformationen af tilstanden $|0\rangle$ og tilsvarende for $|1\rangle$.



Figur 10. Klassisk Fouriertransformation. (Illustration fra Wikipedia)

Opgave 12 Betragt igen en enkelt qubit og sættet der består af de to tilstande $|0\rangle$ and $|1\rangle$. Vis at $H|\psi\rangle$ giver kvantefouriertransformationen af en vilkårlig tilstand $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.
Vink: Benyt at operationerne er lineære.

Opgave 13 Betragt igen en enkelt qubit og de to tilstande $|0\rangle$ and $|1\rangle$. Vis at $H|\psi\rangle$ giver den inverse kvantefouriertransformation af tilstanden $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

Bemærk Som vi lige har set i opgaverne giver H både kvantefouriertransformationen og den inverse når vi kun betragter en enkelt qubit. I eksemplet med kvanteinterferens på en enkelt qubit (afsnit 6) lavede vi derfor en kvantefouriertransformation før vi virkede med T og derefter lavede vi en invers kvantefouriertransformation. Vi kommer til at se denne struktur igen i kapitlet om kvantefaseestimering nedenfor.

AFSNIT 12

Ekspontielt hurtigere end den klassiske

Inden vi kommer så langt, så lad os vise at en kvantecomputer kan lave en kvantefouriertransformation med *langt* færre operationer end en klassisk computer kan lave den tilsvarende diskret Fouriertransformation.

Den diskrete Fouriertransformation af en vektor med 2^t elementer vil på en klassisk computer tage $O(2^{2t})$ operationer at udføre, fordi transformationen svarer til, at gange en $2^t \times 2^t$ -matrice på en søjle med 2^t -elementer. Den hurtigst kendte algoritme (fast Fourier transform) kan få dette ned på $O(t \cdot 2^t)$. Til sammenligning kan vi på en kvantecomputer lave den tilsvarende kvantefouriertransformation med $O(t^2)$ operationer.

Bemærk Udledningen heraf er ganske teknisk, da den nødvendigvis involverer en generel algoritme til at implementere kvantefouriertransformationen på en kvantecomputer. Hvis du er interesseret så tag et kig i appendix A. Hvis detaljerne ikke har din interesse kan du roligt springe dem over, det efterfølgende afhænger ikke heraf.

Kvantefaseestimering

Nu kan man måske tro at kvantefouriertransformationen giver os en eksponentielt hurtigere måde at udføre en klassisk diskret Fouriertransformation. Men dette vil kræve at vi kan aflæse koefficienterne af den tilstand som kvantefouriertransformationen giver, hvilket desværre ikke er ligetil (målinger kollapse tilstanden). Til gengæld gør kvantefouriertransformationen det muligt at estimere eigenverdierne af en unitær operator med eksponentiel høj præcision meget effektivt [4] ! Indrømmet, dette lyder måske ikke super anvendeligt første gang man hører om det, men denne kvantefaseestimering er et centralt element i flere andre kvantealgoritmer bl.a. i Shors algoritme [5] der kan primtalsfaktorisere i polynomiel tid.

AFSNIT 13

Estimeringsopgaven og algoritmen

Vi er givet en unitær operator U og en egentilstand $|u\rangle$ af U . Eigenverdierne af en unitær operator, U , er alle komplekse faser $e^{i\phi}$ så egenverdiligningen tager formen

$$U|u\rangle = e^{i\phi}|u\rangle. \quad (13.1)$$

Målet med kvantefaseestimeringsalgoritmen er at give et estimat af fasen ϕ der er korrekt til t -decimaler.

Bemærk

Unitære operatore er centrale i kvantemekanik, f.eks. er tidsudviklings- og rotationsoperatoren unitær. Det er ikke tilfældigt at disse operatore er unitære, for det at de er unitære betyder at den samlede sandsynlighed er bevaret under operationen. Som vi skal se nedenfor i afsnit 19 om Shors algoritme findes der en unitær operator der er relevant for primtalsfaktorisering.

Opgave 14

Vis at tidsudviklingsoperatoren $U = e^{-iH\tau/\hbar}$ er unitær. Her er $H = H^\dagger$ Hamiltonoperatoren (hvis egenverdier bestemmer energierne af systemet), τ er tiden (fordi vi allerede bruger t) og $\hbar$ er Plancks konstant.

For at lave kvantefaseestimeringsalgoritmen bruger vi to sæt af qubits som vi kalder **register 1 og 2**. Register 1 har t qubits og det er ved at måle på dette register at vi i sidste ende vil få estimatet af ϕ . Register 2 har så mange qubits det kræver at opskrive tilstanden $|u\rangle$ (dette afhænger af hvilken operator U er). Figur 11 giver en diagrammatisk illustration af kvantefaseestimeringsalgoritmen.

Bemærk

Bemærk at vi vil opskrive en samlet tilstand for de to registre på formen $|j\rangle|u\rangle$ hvor $|j\rangle$ lever i det første register og $|u\rangle$ lever i det andet. Systemets tilstand vil typisk være en superposition af sådanne tilstande.

Lad os kaste os ud i det. De skridt der tilsammen udgør kvantefaseestimeringsalgoritmen er opsummeret i tabellen Figur 12:

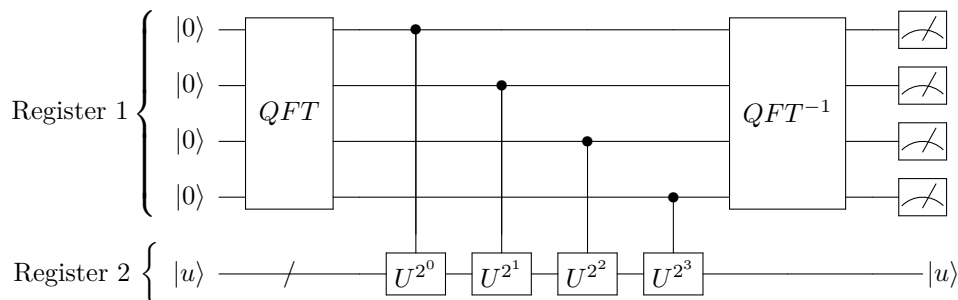
Opgave 15

Check at kvantefouriertransformationen af $|0\rangle$ i anden linje i tabellen i Figur 12 er korrekt. Check også den inverse kvantefouriertransformation i næstsidste linje.

Opgave 16

Vis, at for $t = 1$ (dvs. hvis der kun er en qubit i register 1) så er tilstanden efter den inverse kvantefouriertransformation $\frac{1}{2}((1 + e^{i\phi})|0\rangle + (1 - e^{i\phi})|1\rangle)|u\rangle$.

For en **unitær operator** U gælder følgende: $UU^\dagger = U^\dagger U = 1$, hvor † er hermitisk konjugering, altså kompleks konjugering og transponering.



Figur 11. Kvantefaseestimeringsalgoritmen for $t = 4$. De øverste 4 qubits udgør det første register, og det er resultatet af at måle på disse der giver estimatet af fasen ϕ . Informationen om ϕ bliver overført til register 1 via t kontrollerede operationer med hhv. $U^{2^0} \dots U^{2^{t-1}}$ på det andet register der er i egentilstanden $|u\rangle$ (Bemærk her at “/” indikerer at dette register består af flere qubits, vi tegner det blot som en enkelt streg). Hvis kontrol-qubitten, indikeret ved $\bullet$, er $|1\rangle$ vil den kontrollerede operation anvende operatoren i firkanten på den qubit firkanten er afsat på.

Starttilstanden	$ 0\rangle u\rangle$	lokaliseret ved 0
QF-transform	$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} j\rangle u\rangle$	delokaliseret i Fourier rummet
Kontrollerede U	$\frac{1}{\sqrt{2^t}} \sum_{j=0}^{2^t-1} e^{i\phi j} j\rangle u\rangle$	delokaliseret med faser
QF $^{-1}$ -transform	$\frac{1}{2^t} \sum_{j,k=0}^{2^t-1} e^{i(\phi - 2\pi \frac{k}{2^t})j} k\rangle u\rangle$	top for k så $2\pi k/2^t$ nær ϕ
Måling	$ k'\rangle u\rangle$	resultat er k' , estimat af ϕ er $2\pi k'/2^t$

Figur 12. De skridt der udgør kvantefaseestimeringsalgoritmen.

Bemærk I opgaven ovenfor er tilstanden af det første register inden vi måler præcist som i det simpleste eksempel på kvanteinterferens i afsnit 6!

Inden vi ser hvordan kvanteinterferensen kommer i stand for flere qubits, så lad os lige knytte an til de Fourier multipliers vi så på i Kapitel III.

AFSNIT 14

Kvante-fourier multiplier

De kontrollerede unitære operationer, i den tredje linje af tabellen i Figur 12, tilføjer hvad der for den klassiske Fouriertransformation svarer til en Fourier multiplier. Denne kvante-fourier multiplier, $e^{i\phi j}$, svarer præcist til den klassiske Fourier multiplier, $e^{i\phi_0 m}$, vi så på i kapitel III. Lige som den klassiske Fourier multiplier skifter et periodisk signal med ϕ_0 , skifter kvante-fourier multiplieren, $e^{i\phi j}$, i kvantefaseestimerings-algoritmen, start tilstanden $|0\rangle$ til en tilstand der er superposition af $|k\rangle$ hvor der er konstruktiv interferens for $2\pi k/2^t$ tæt på ϕ ;

$$|0\rangle \xrightarrow{\text{QFT}} \frac{1}{\sqrt{2}} |j\rangle \xrightarrow{\text{cU}} \frac{1}{\sqrt{2}} \cdot e^{i\phi j} |j\rangle \xrightarrow{\text{QFT}^{-1}} |k\rangle, \text{ hvor } 2\pi k/2^t \sim \phi.$$

AFSNIT 15

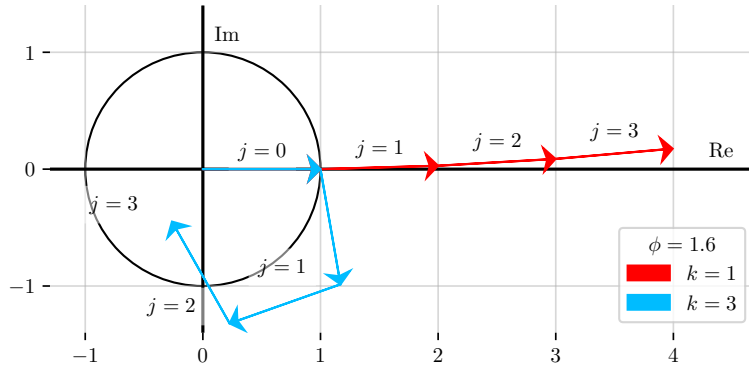
Konstruktiv kvanteinterferens udpeger fasen

Lad os tage et nærmere kig på den dobbeltsum

$$\sum_{j,k=0}^{2^t-1} e^{i(\phi - 2\pi \frac{k}{2^t})j} |k\rangle \quad (15.1)$$

vi har fået efter den inverse kvantefourier transformation – det er nemlig **lige her kvanteinterferensen sker**. For at se hvordan den virker så bemærk at j kun optræder i eksponenten og ikke andre steder. Derfor, når vi tager summen over j , så vil disse faser have en stærk tendens til at gå ud mod hinanden og når vi dividerer summen med 2^t (se linje 4 af algoritmen) bliver det samlede bidrag meget lille. Dette sker for alle værdier af k med mindre $2\pi k/2^t$ er meget tæt på ϕ . For hvis dette er tilfældet vil alle de 2^t led i summen over j være meget tæt på 1. Så når $2\pi k/2^t$ er meget tæt på ϕ er summen over j af størrelsesorden 2^t , som vi så dividerer med 2^t og får et resultat af størrelsesorden 1. Dette gør at der er overvældende sandsynlighed for at en måling vil give en værdi k' hvor $2\pi k'/2^t$ er en god approksimation til ϕ .

Eksempel | Figur 13 viser hvordan summen over j i ligning 15.1 ser ud for forskellige værdier af k når $\phi = 1.6$ og $t = 2$. For $k = 1$ så er $2\pi \frac{k}{2^t} = 2\pi \frac{1}{4} = \frac{\pi}{2} \approx 1.6$, altså en perfekt approksimation af $\phi = 1.6$ hvis man afrunder til to cifre ($t = 2$). Altså er forskellen $(\phi - 2\pi \frac{k}{2^t})j$ lille for alle j , så alle led i summen tilføjer meget lidt til vinklen af resultatet. Hvis derimod $k = 3$ er $2\pi \frac{k}{2^t} = \frac{3\pi}{4} \approx 4.7$ er denne forskel stor. Hvert led i summen vil derfor drastisk skifte retning af summen som set i Figur 13.



Figur 13. Illustration af summen af de komplekse faser der indgår i dobbeltsummen (15.1). Summen over j er givet ved den samlede vektor for to fastholdte værdier af k .

Bemærk Bemærk at det er en konstruktiv kvanteinterferens der gør det meget sandsynligt at målingen giver en værdi k' hvor $2\pi k'/2^t$ er en god approksimation til ϕ . Mens der for værdier af k hvor $2\pi k/2^t$ ikke er tæt på ϕ er destruktiv kvanteinterferens.

AFSNIT 16

Korrekt til t decimaler

Hvor tæt skal $2\pi k/2^t$ være på ϕ for at denne konstruktive kvanteinterferens opstår? Uden at gå i for meget matematisk detalje kan vi få en intuition for dette ved at se

på dobbeltsummen (15.1). Vi vil gerne bestemme de værdier af k hvor summen over j giver noget af størrelsesorden 2^t (husk at vi dividerer summen med 2^t). For at dette er tilfældet må vi have at fasen $(\phi - 2\pi \frac{k}{2^t})j$ er tæt på nul, og dette skal gælde for alle værdier af $j = 0, \dots, 2^t - 1$ ellers får vi ikke konstruktiv interferens. Vi slutter altså at $\phi - 2\pi \frac{k}{2^t}$ skal være af størrelsesorden 2^{-t} . Målingen i slutningen af algoritmen vil derfor med stor sandsynlighed give en værdi k' hvor $2\pi \frac{k'}{2^t}$ er et estimat af ϕ der er korrekt til t (binære) decimaler.

AFSNIT 17

Virker også hvis $|u\rangle$ ikke er en egentilstand

Umiddelbart kan det måske syntes lidt kunstigt at man har en egentilstand $|u\rangle$ for U men ikke nogen egen værdi. Men vi behøver faktisk ikke have nogen præcis egentilstand af U for at kunne få nytte af kvantefaseestimeringen. For at se dette så bemærk at egentilstandene, $|u_i\rangle$, for den unitære operator U udgør en ortonormal basis (for Hilbert-rummet). Derfor kan en vilkårlig tilstand $|\psi\rangle$ skrives

$$|\psi\rangle = c_1|u_1\rangle + c_2|u_2\rangle + \dots \quad (17.1)$$

for passende komplekse koefficienter c_i . Og da alle operationer vi bruger er lineære, kan vi bruge kvantefaseestimeringsalgoritmen på tilstanden $|\psi\rangle$ ved at lade den virke på hvert led i summen for sig! Resultatet af målingen i slutningen af algoritmen vil da give et godt estimat af en af de faser der indgår i egen værdierne af U . Vi ved ikke hvilken det er, men sandsynligheden for at det er den i 'te egen værdi er proportional med $|c_i|^2$.

Eksempel Hvis vi for eksempel har, $U = e^{-iHt/\hbar}$, hvor H er systemets Hamiltonoperator og vores mål er at bestemme grundtilstandsenergien. Så skal vi blot kunne komme med et gæt, $|\psi\rangle$, der har et godt overlap, $\langle u_{\text{grundtilstand}} | \psi \rangle = c_{\text{grundtilstand}}$, med grundtilstanden $|u_{\text{grundtilstand}}\rangle$, da er sandsynligheden for at algoritmen estimerer grundtilstandsenergien til stor præcision proportional med $|c_{\text{grundtilstand}}|^2$.

Opgave 17 Erstat $|u\rangle$ med $c_1|u_1\rangle + c_2|u_2\rangle$ i kvantefaseestimeringsalgoritmen afsnit 13 og gentag algoritmens skridt. Udnyt at alle operationer er lineære.

AFSNIT 18

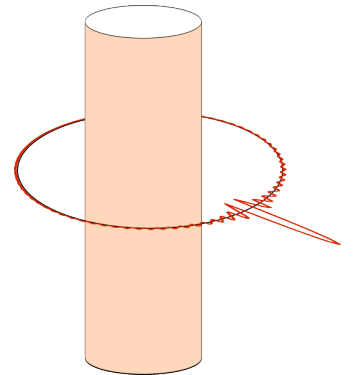
Fysisk intuition for kvantefaseestimerings-algoritmen

Som vi så i Afsnit 8 er det muligt at få en bedre forståelse af den simpleste kvantealgoritme ved at betragte et Mach-Zehnder interferometer. På samme vis er det muligt at opbygge en bedre fysisk intuition for kvantefaseestimerings-algoritmen ved at betragte en partikel på en ring med en lang spole i gennem, se Figur 14. Hvis man er nysgerrig efter at se detaljerne kan vi kan varmt anbefale at tage et kig i [7].

AFSNIT 19

Shors algoritme for primtalsfaktorisering

De bedste kendte klassiske algoritmer til at primtalsfaktorisere et helt tal med t bits menes at kræve $e^{O(t^{1/3} \log^{2/3} t)}$ operationer. Til sammenligning kan Shors algoritme for



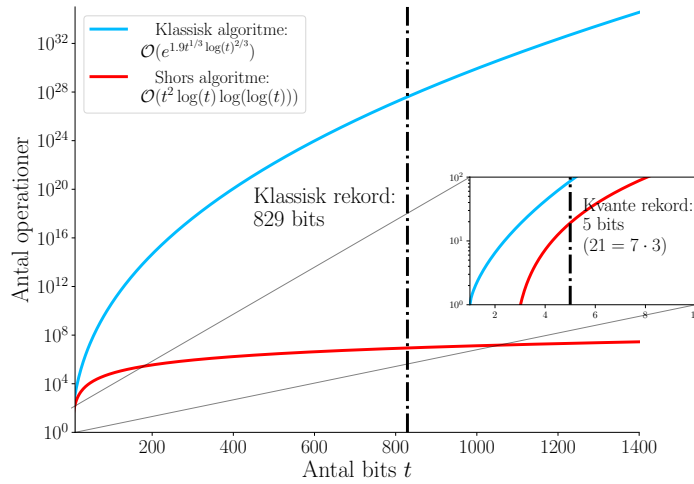
Figur 14. Bølgefunktionen for en partikel på en ring med en lang spole igennem. Dette systems tidsudvikling svarer til at udføre kvantefaseestimering og kan give en bedre intuition for algoritmen, se [7].

primtalsfaktorisering [5] løse den samme opgave med $O(t^2 \log(t) \log(\log(t)))$ operationer, se Figur 15¹ og [6] for detaljer. Med andre ord så kan en kvantecomputer primtalsfaktorisere eksponentielt hurtigere end en klassisk computer!

Shors algoritme består af flere trin, hvoraf det er kun *et trin* der skal udføres på en kvantecomputer, nemlig en kvantefaseestimering for den unitære operator der virker således

$$U|y\rangle = |xy(\bmod N)\rangle . \quad (19.1)$$

Hvordan denne unitære operator kommer i spil og hvilke andre trin der indgår i Shors algoritme en fantastisk tour de force i klassisk matematik og klassiske algoritmer. Vi kan varmt anbefale at brygge en stærk kop kaffe og dykke ned i detaljerne (se f.eks. [6]). Her vil vi blot bemærke at Shor også løser problemet med at finde en passende tilstand som det andet register skal starte i på en meget elegant måde: Shor benytter en superposition af egentilstande for U der giver $|1\rangle$ (i 10-tals notationen). Så det andet register skal blot startes i tilstanden $|1\rangle$.



Figur 15. Antal operationer det kræver med den bedste kendte klassiske algoritme og med Shors algoritme at primtals faktorisere et tal med t bits. Bemærk den logaritmiske y-akse.

¹En liste af rekorder for faktoriseringsproblemet udført på klassiske computere kan findes på https://en.wikipedia.org/wiki/Integer_factorization_records. Rekorderne for kvantecomputere kan findes på https://en.wikipedia.org/wiki/Shors_algorithm under “Physical Implementation”.

Opsummering

Her afslutningsvis vil vi forsøge at binde de dele der er arbejdet med i noten sammen.

AFSNIT 20

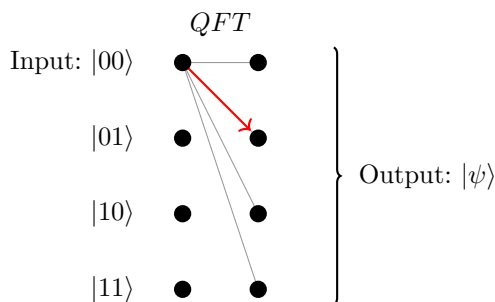
Superposition af alle veje giver mulig interferens

I dobbeltspalteforsøget, se Figur 1, lægger vi først amplituderne sammen og absolutkvadrerer derefter for at bestemme sandsynligheden. Summen af amplituderne giver mulighed for at der opstår positiv og destruktiv interferens. Vi lægger amplituderne for de to veje gennem dobbeltspalteforsøget sammen først da der ikke er nogen måde at afgøre hvilken vej partiklen har taget. Det samme grundlæggende kvantemekaniske princip udnyttes i kvantealgoritmer, her er vejen gennem dobbeltspalteforsøget blot erstattet af veje gennem superpositioner af kvantetilstande.

Eksempel | F.eks. vil kvantefouriertransformationen sende

$$|00\rangle \xrightarrow{QFT} \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle). \quad (20.1)$$

Kvantefouriertransformationen åbner hermed de 4 veje som resten af algoritmen efterfølgende skaber interferens mellem, se Figur 16.

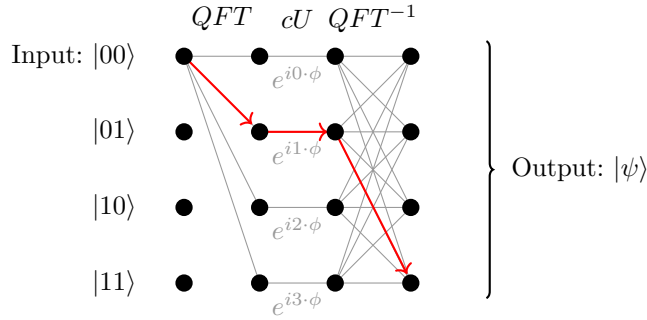


Figur 16. Kvantefouriertransformationen spreder tilstanden $|00\rangle$ ud på alle de fire mulige tilstande med 2 qubits og åbner dermed for 4 mulige veje. De grå linjer indikerer de mulige veje og den røde pil fremhæver en af disse.

Opgave 18 | Vis at der er lige stor sandsynlighed for at måle hvert af de 4 udfald 00, 01, 10 og 11 efter kvantefouriertransformationen af tilstanden $|00\rangle$.

Eksempel | Vi kan tænke de 2 qubits som det første register i kvantefaseestimeringsalgoritmen med $t = 2$. I Figur 17 har vi tilføjet de resterende skridt af kvantefaseestimeringsalgoritmen fra Figur 11 og 12. Outputtilstanden $|\psi\rangle$ er en superposition af de mulige veje og det er netop derfor kvanteinterferensen der udpeger løsningen kan opstå.

Bemærk Bemærk at diagrammet i Figur 17 er en naturlig udvidelse af det diagram vi havde for den simpleste kvantealgoritme i Figur 7.



Figur 17. Kvantefaseestimerings algoritmen for $t = 2$; de grå linjer indikerer de mulige veje for det første register. De røde pile viser én mulig vej. Output-tilstanden $|\psi\rangle$ er en superposition af alle de mulige veje og det er i denne superposition kvanteinterferensen sker.

AFSNIT 21

Konstruktiv interferens ved løsningen vi søger

Udfaldet af den afsluttende måling i kvantealgoritmen vil med stor sandsynlighed give et resultat der svarer til de tilstande hvor der skabes konstruktiv interferens. Tilsvarende er der meget lav sandsynlighed for, at udfaldet svarer til en tilstand med destruktiv interferens. For at dette fører til en nyttig beregning er det afgørende, at den konstruktive interferens peger på løsningen til det problem vi ønsker at løse.

Eksempel For kvantefaseestimeringen peger den konstruktive interferens på den fase vi ønsker at måle. Dette kommer i stand helt analogt til hvordan en klassisk Fourier multiplier kan benyttes til at forskyde et klassisk signal. I den klassiske Fourier multiplier er vi dog nødt til at kende den fase vi ønsker at forskyde signalet med, i kvantefaseestimeringsalgoritmen kommer den tilsvarende fase ind ved at lade operatoren virke på dens egentilstand, hvilket ikke kræver at vi kender fasen.

AFSNIT 22

Afslutning

Ambitionen med disse noter er at give en ide om hvad kvanteinterferens er og hvordan dette udnyttes i kvantealgoritmer. Emnet er selvfølgelig meget større end hvad der er dækket her og udvikles løbende. Vi håber at arbejdet med disse noter har givet både baggrund for og nysgerrigheden til at grave dybere.

Appendix

AFSNIT A

Implementering af kvantefouriertransformationen

For at give et indblik i hvordan kvantefouriertransformationen kan implementeres på en kvantecomputer med $O(2^t)$ af de grunliggende operationer, så lad os skitsere en kvantealgoritme der udfører den. Første skridt er at indse at kvantefouriertransformationen kan skrives på den faktorerede form

$$|l\rangle \rightarrow \frac{1}{\sqrt{2^t}} (|0\rangle + e^{2\pi i 2^{t-1} l/2^t} |1\rangle) (|0\rangle + e^{2\pi i 2^{t-2} l/2^t} |1\rangle) \dots (|0\rangle + e^{2\pi i 2^0 l/2^t} |1\rangle) . \quad (\text{A.1})$$

Bemærk Vigtigt, l et tal mellem 0 og 2^{t-1} der på venstresiden af (A.1) markerer hvilken tilstand $|l\rangle$ vi er ved at lave kvantefouriertransformationen af. På højresiden arbejder vi med det direkte produktrum af t qubits. Så når vi skal genfinde tilstanden $|j\rangle$ fra definitionen (11.1) så er den på højresiden i en binær repræsentation

$$j = j_1 j_2 \dots j_t \quad (\text{A.2})$$

hvor j_i enten er 0 eller 1. Med andre ord:

$$j = j_1 2^{t-1} + j_2 2^{t-2} + \dots + j_t 2^0 . \quad (\text{A.3})$$

Eksempel F.eks. hvis $t = 4$ og vi på højresiden vil identificere tilstanden $|9\rangle$ med $j = 9$, så er den repræsenteret ved $|1001\rangle$ på højresiden.

Opgave 19 Sammenlign udtrykket (A.1) med definitionen (11.1) og vis at vi får de rette koefficienter til tilstandene $|j\rangle$ med $j = 0$, $j = 1$ og $j = 2$. Prøv at generalisere derfra.

Som næste skridt, lad os som for j også skrive l op som et binært tal

$$l = l_1 2^{t-1} + l_2 2^{t-2} + \dots + l_t 2^0 . \quad (\text{A.4})$$

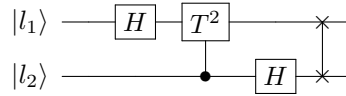
Bemærk nu at $e^{2\pi i 2^{t-1} l/2^t}$, der står i den første parentes på højresiden af (A.1), kun afhænger af den sidste binære decimal, l_t , da

$$e^{2\pi i 2^{t-1} l/2^t} = e^{2\pi i 2^{t-1} (l_1 2^{t-1} + l_2 2^{t-2} + \dots + l_t 2^0)/2^t} = e^{2\pi i l_t/2} = e^{\pi i l_t} \quad (\text{A.5})$$

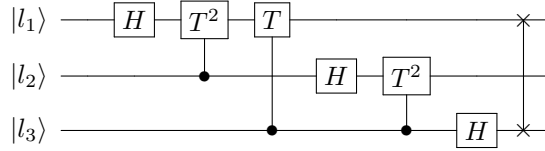
da alle de andre led i summen altid giver faktorer af 1 (brug at $e^{2\pi i} = e^0 = 1$). Fasen $e^{\pi i l_t}$ er 1 hvis $l_t = 0$ og -1 hvis l_t er 1. Så det første led på højresiden af (A.1) kan fås ved at lade H virke på den t 'te qubit. I det næste led på højresiden af (A.1) har vi $e^{2\pi i 2^{t-2} l/2^t}$ der tilsvarende kun afhænger af de sidste to binære decimaler l_{t-1} og l_t .

Hvis vi et øjeblik nøjes med betragte to qubits så kan vi få kvantefouriertransformationen fra algoritmen i Figur 18.

Umiddelbart virker det måske ikke som om dette kan give en eksponentiel fordel men lad os også tage et kig på hvad der sker, hvis vi har 3 qubits. Nu kan kvantefouriertransformationen udføres ved algoritmen i Figur 19. Med lidt god vilje kan man måske



Figur 18. Kvantefouriertransformationen for to qubits. Den kontrollerede T^2 operation, ser om l_2 er 1 og i så fald virker den med T^2 på den øverste qubit. Den sidste operation længst til højre ombytter de to qubits.



Figur 19. Kvantefouriertransformationen for 3 qubits.

nu begynde at ane den struktur der fører til at vi kan lave kvantefouriertransformationen for t qubits med $O(t^2)$ operationer. Den fulde struktur af algoritmen kan findes i f.eks. [6].

Litteratur

- [1] R.P. Feynmann og A.R. Hibbs, "Quantum Mechanics and Path Integrals", McGraw-Hill Colleges, New York, (1965).
- [2] "Introduction to Quantum Information Science" af Artur Ekert, Timothy Hosgood, Alastair Kay og Chiara Macchiavello, som kan findes på <https://qubit.guide/index>.
- [3] R. Cleve, A. Ekert, C. Macchiavello and M. Mosca "Quantum algorithms revisited", Proc. R. Soc. Lond. A.454: 339–354 (1998). <https://arxiv.org/abs/quant-ph/9708016>
- [4] A.Y. Kitaev, "Quantum measurements and the Abelian stabilizer problem," Electr. Coll. Comput. Complex. 3, article no. 3 (1996), <https://arxiv.org/abs/quant-ph/9511026>.
- [5] P.W. Shor "Algorithms for quantum computation: Discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of Computer Science. IEEE Comput. Soc. Press. pp. 124–134, (1994). P.W. Shor "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". SIAM Journal on Computing. 26 (5): 1484–1509 (1997), [arXiv:quant-ph/9508027](https://arxiv.org/abs/quant-ph/9508027).
- [6] M.A. Nielsen and I.L. Chuang, "Quantum Computation and Quantum Information": 10th Anniversary Edition. Cambridge University Press (2010). doi:10.1017/CBO9780511976667.
- [7] K. Splittorff, Quantum Phase Estimation and the Aharonov-Bohm effect, [arXiv:2407.11179](https://arxiv.org/abs/2407.11179).