SJÄLVSTÄNDIGA ARBETEN I MATEMATIK

MATEMATISKA INSTITUTIONEN, STOCKHOLMS UNIVERSITET

Faktorisering med kvantdatorn

av

Jonas Pettersson

2012 - No 10

Faktorisering med kvantdatorn

Jonas Pettersson

Självständigt arbete i matematik 15 högskolepoäng, grundnivå

Handledare: Rikard Bögvad

2012

Sammanfattning

Denna uppsats kommer att behandla den teoretiska kvantdatorn och hur man med dess hjälp kan faktorisera stora heltal effektivt. Vi kommer att gå igenom hur kvantdatorn ska byggas upp och de matematiska representationerna av dess delar. Vi kommer också att gå igenom hur delarna kan användas för att lösa problemet med faktorisering av stora heltal. Datorerna som finns idag kan inte faktorisera effektivt men vi ska se hur kvantdatorn kan göra det. Vi avslutar uppsatsen med att beskriva en algoritm för hur faktorisering med en kvantdator går till och visar ett exempel. Uppsatsen baseras mycket på An Introduction to Quantum Computing av Phillip Kaye, Raymond Laflamme och Michele Mosca, se [1].

Innehåll

1 Introduktion

1.1 Datorer

Datorer är fysiska maskiner som hjälper oss att lösa problem med så kallade algoritmer. Vi beskriver i det här avsnittet vad en algoritm är och hur man jämföra olika algoritmer med varandra. Vi kommer också att gå igenom den kvantfysik som behövs för att förstå kvantdatorn, se [1] kapitel 1.

1.1.1 Datorn och algoritmer

Datorer används idag för att lösa uppgifter på en mängd områden, allt från enkla hushållsapparater till stora superdatorer. I datorer använder man ett binärt språk med två olika spänningslägen som representeras av ettor och nollor, så kallade bitar. För att utföra beräkningar skickas spänningar genom elektriska kretsar byggda av i huvudsak transistorer. De elektriska kretsarna representerar logiska grindar. En logisk grind är en elektrisk krets vars utvärde är en logisk funktion av kretsens invärden, till exempel NOT, AND och XOR. När en spänning skickas genom en krets så representeras det av att motsvarande logiska funktion appliceras på spänningens binära representation. Kretsarna/grindarna kan man koppla samman till större kretsar för att kunna göra beräkningar som $+, -, \cdot, /, mod$. Man kan sätta ihop en uppsättning av sådana större kretsar/beräkningar för att lösa mer komplexa uppgifter och har då en algoritm. En algoritm är alltså en mängd instruktioner för att lösa ett problem

Exempel 1. *Nedan ser vi pseudokoden till en algoritm för att beräkna hypotenusan. Pseudokod är kod som inte är beroende av ett programmeringsspråk utan bara beskriver vad algoritmen ska göra. Här beräknas* $\sqrt{x^2 + y^2}$ *av kateterna* x *och* y*, sedan sätts* z *till resultatet:*

```
hypo(x heltal, y heltal){
z:= sqrt((x*x) + (y*y));
}
```

1.1.2 Ordo

När vi jämför olika algoritmer är vi intresserade av att ha ett mått som visar om en algoritm är effektiv eller inte. Vi vill ha ett mått på hur mycket resurser det går åt för att köra en algoritm på en dator. Måttet kan till exempel vara tidsåtgång, antalet grindar som går åt eller hur mycket minne som behövs. Vi kommer att mäta hur mycket resurser som går åt för att köra algoritmer som funktioner av längden på det indata som används. Måttet vi är intresserade av är ett som ger en övre gräns för resursåtgången. Man bortser får konstanter och tar den dominerande termen i resursåtgången som mått. Till exempel kan två olika algoritmer för multiplikation av två n bitar

långa tal ha resursåtgång $3n^2+2$ respektive $4n^3+3n+6$. För stora n kommer n^3 och n^2 att dominera och vara en övre gräns för resursåtgångarna. Man säger att algoritmerna tillhör $O(n^2)$, respektive $O(n^3)$.

O står för ordo och är den beteckning man brukar använda för resursåtgången. Man tolkar det som att en algoritm är begränsad av funktionen $f(n)$ om den tillhör $O(f(n))$. $f(n)$ är alltså den dominerande termen då n blir stort. Med hjälp av O kan vi således undersöka och välja de algoritmer som löser våra problem effektivast. Man brukar dela in algoritmer i olika klasser med avseende på effektivitet. Om en algoritm har resursåtgång $O(n^c)$ för något tal c, säger man att den algoritmen är polynomiell med avseende på resursåtgången. På samma sätt säger man att en algoritm i $O(\log n)$ är logaritmisk, en i $O(n)$ är linjär och en i $O(c^n)$ är exponentiell för konstanten c.

Algoritmer som kräver exponentiell resursåtgång klassas som ineffektiva. Till exempel kan man inte faktorisera stora heltal effektivt. Den snabbaste heuristiska algoritmen man känner till idag för att faktorisera kallas General Number Field Sieve (GNFS). Det är den snabbast kända algoritmen för faktorisering av stora tal med en klassisk dator n och har resursåtgång $e^{O((\log n)^{\frac{1}{3}}(\log\log n)^{\frac{2}{3}})}$. Den kräver alltså exponentiellt med resurser. n i det här fallet består av $\log_2 n$ bitar.

Vi kommer att se en metod för att faktorisera mycket effektivare. Metoden kommer att använda kvantdatorn för att faktorisera med mycket mindre resursåtgång än den klassisk dator. Om man skulle lyckas göra det kan man till exempel knäcka RSA-krypteringen, se [11] kapitel 3. RSA har fått sitt namn av dess skapare, Ron Rivest, Adi Shamir, Leonard Adleman och bygger på att det är svårt att faktorisera stora heltal.

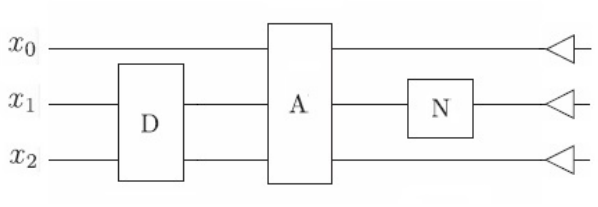
1.1.3 Rita kretsar

När vi visualisera en krets för att visa hur man ska koppla grindar och vilka indata som ska gå till vad ritar vi kretsscheman. Man ritar kretsar som geometriska figurer med linjer mellan. De geometriska figurerna representerar grindar och linjerna som kopplar samman grindarna representerar de vägar som data flödar genom. Alla grindarna presenteras vidare som rektanglar utom mätningar som presenteras av trianglar. Se figur 1 för exempel.

1.2 Kvantfysik

Kvantdatorn använder några viktiga egenskaper hos kvantfysiken. Vi går igenom dessa egenskaper med hjälp av ett vanligt exempel på ett kvantsystem[1]. Exemplet kommer att skildra ett experiment där den klassiska fysiken inte kan förklara fenomenet man observerar. Kvantfysiken behövs för att kunna förklara det som inträffar. Uppställningen i experimentet har gjorts på

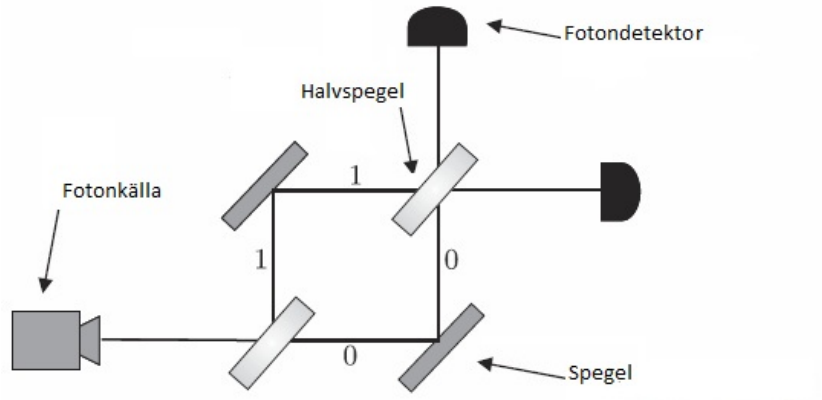
[1]Se avsnitt 1.6 i [1], [13] avsnitt 2.1.1(exempel 2.1.18 sid 65) och 2.10 i [15].



Figur 1: Kretsschema över operatorerna D, A och N med indata x_0, x_1 och x_2 och mätning av utdata.

riktigt och går under namnet Mach-Zehnder interferometer. Resultat kan tyckas konstigt och strider mot ens intuition till en början men vi kommer att förklara fenomenet man iakttar.

Exempel 2. *En uppställning med en fotonkälla, två speglar, två fotondetektorer och två halvspeglar(stråldelare) ställs upp. Halvspeglarna släpper igenom hälften av de fotoner som träffar dem och reflekterar hälften. Man börjar med att rikta en fotonkälla så att den skicka fotoner mot en halvspegel som delar upp fotonerna i två vägar. I de båda vägarna monteras en spegel. Sedan låter man dessa speglar reflekterar ihop fotonerna och ställer den andra halvspegeln där fotonerna korsar varandra. Den andra halvspegeln låter man reflektera ut fotonerna till varsin fotondetektor, se bild 2. En foton kan alltså ta två*

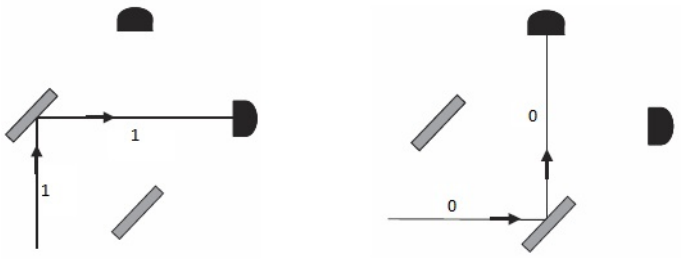


Figur 2: Uppställning med två halvspeglar, en fotonkälla, två speglar och två fotondetektorer.

möjliga vägar efter den första halvspegeln. Vägarna döps till 0 *och* 1*. Det är alltså med en sannolikhet på* $\frac{1}{2}$ *som en fotonen hamnar på en specifik väg. Fotonerna man skickar kommer alltså efter den första halvspegeln att delas upp i två vägar med lika många i vardera väg. Efter att fotonerna reflekterats ihop av speglarna och passerat den sista halvspegeln läser man av hur*

många fotoner varje fotondetektor träffats av. Det verkar ju rimligt att man skulle detektera hälften av fotonerna vid vardera fotondetektor. Men så är inte fallet! Det visar sig att alla fotoner hamnar vid en och samma detektor. Det här fenomenet går emot hur vi är vana att se på verkligheten med den klassiska fysiken. Men vi kan förstå vad som händer om vi använder oss av en kvantfysisk modell.

Om vi bortser från den andra halvspegeln en stund kommer varje foton att följa en av två vägar enligt den klassiska fysiken. Nämligen 0 *eller* 1 *beroende på om fotonen reflekteras eller inte av den första halvspegeln, se bild 3. Vi*



Figur 3: Till vänster ser vi 1-vägen och till höger 0-vägen.

kan se varje foton som ett system med 2 lägen där lägena motsvarar att fotonen befinner sig på väg 0 *eller* 1*. Vi representera lägena med en vektor (lägesvektor)*

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

för vägen 0 *och*

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

för vägen 1*. Vi kommer senare att gå igenom varför just dessa vektorer är lämpliga. Fotonkällan monterades så att varje foton vi skickar kommer att starta i väg* 0*. Fotonerna kommer helt godtyckligt att reflekteras till väg* 1 *eller stanna i väg* 0 *efter den första halvspegeln enligt den klassiska fysiken. Men, enligt kvantfysiken kan fotonerna befinna sig i en så kallad superposition mellan vägarna* 0 *och* 1*. Matematiskt beskriver vi en generell superposition av väg* 0 *och* 1 *som en linjära kombination*

$$\alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

av lägesvektorerna. Om man rent fysiskt mäter vilken väg en foton befinner sig på kommer resultatet att bero på α *och* β*. Närmare bestämt kommer en foton att befann sig på väg* 0 *med sannolikhet* $|\alpha|^2$ *och på väg* 1 *med sannolikhet* $|\beta|^2$ *enligt kvantfysiken. När fotonen passerar en halvspegeln innebär*

det att man multiplicerar lägesvektorn med matrisen (en rotationsmatris)

$$E := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

Den fotonen som alltså startar på 0*-vägen kommer efter första halvspegeln att hamna i följande läge:*

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \frac{i}{\sqrt{2}} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Det motsvarar att fotonen hamnar på 0*-vägen med sannolikhet* $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$ *och i* 1*-vägen med sannolikhet* $|\frac{i}{\sqrt{2}}|^2 = \frac{1}{2}$*. Matrisen* E *beskriver således vad som händer med en fotons läge då den passerar en halvspegel. Mäter vi inte fotonens läge utan låter den passera genom den andra halvspegeln fås följande*

$$\Big(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}\Big)\Big(\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}\Big) = \begin{pmatrix} 0 \\ i \end{pmatrix}.$$

Om vi mäter nu kommer vi, med sannolikhet $|i|^2 = 1$*, läsa av att fotonen gått* 1*-vägen. Vilket stämmer överens med vad man iakttar när man utför experimentet. Fenomenet kallas interferens och man säger att den andra halvspegeln har fått de två vägarna i superposition att interferera och slå ut* 0*-vägen.*

Det är egenskaper hos kvantsystem som de i exempel 2 vi kommer att utnyttja i konstruktionen av kvantdatorn. Man bör tillägga att kvantdatorn för tillfället till största delen existerar i teorin och laboratorium. Den matematiska teorin bakom kvantdatorn är dock fortfarande intressant.

2 Matematiska begrepp

För att beskriva en kvantdator behöver vi behöver ett smidigt sätt att skriva vektorer på som passar när man ska representera lägesvektorer som de i 2. En del begrepp från linjär algebra samt *tensorprodukt* kommer också att vara till stor hjälp.

2.1 Diracnotation

Vektorerna vi ska använda för att representera lägen hos olika kvantsystem kommer att skrivas i Diracnotation[2]. Den introducerades först av Paul Dirac på 30-talet och går också under namnet bra-ket-notation. En vektor φ skrivs i Diracnotation som $|\varphi\rangle$. Vektorerna vi använder kommer att skrivas i en bas vi refererar till som beräkningsbasen. Beräkningsbasen är en bas där basvektorerna består av en etta på en rad och nollor på resten av raderna. Basvektorerna för beräkningsbasen skrivs i Diracnotation som binära strängar mellan | och ⟩. Den binära strängen är det binära tal som motsvarar vilken rad ettan i basvektorn finns sig på. Första raden räknas som rad 0. Varje basvektor i ett 2^n-dimensionellt vektorrum skrivs alltså med en binär sträng om n siffror i Diracnotation, se exempel nedan.

Exempel 3. *Anta att vi har ett $2^3 = 8$-dimensionellt vektorrum med beräkningsbasen som bas. Då får vi basvektorernas matris representation och Diracnotation som:*

$$\begin{pmatrix}1\\0\\0\\0\\0\\0\\0\\0\end{pmatrix} = |000\rangle, \begin{pmatrix}0\\1\\0\\0\\0\\0\\0\\0\end{pmatrix} = |001\rangle, \cdots, \begin{pmatrix}0\\0\\0\\0\\0\\0\\0\\1\end{pmatrix} = |111\rangle$$

Att skriva vilken rad ettan står på som ett binärt tal i Diracnotation ger ett kompakt sätt att representera vektorerna på.

En vektor beskriven i beräkningsbasen skrivs som en linjär kombination av basvektorerna.

Exempel 4. *I ett vektorrum med dimension 4 får vi:*

$$\begin{pmatrix}1\\0\\\pi\\\frac{1}{2}\end{pmatrix} = |00\rangle + \pi|10\rangle + \frac{1}{2}|11\rangle$$

[2]Se [1] avsnitt 2.1, [15] 2.1, [17] 1.5, [16] 3.5 och [7] 4.2.

Lägena i de kvantsystemen vi kommer att jobba med beskrivs i beräkningsbasen. Kvantsystemen kommer alltså att beskrivas som 2^n-dimensionella vektorrum med beräkningsbasen som ortonormalbas.

2.2 Linjär algebra och Hilbertrum

2.2.1 Linjär algebra

Vi behöver några definitioner från den linjära algebran.

Definition 1. *En linjär operator på ett vektorrum $\mathcal{H}$ är en linjär avbildning $U : \mathcal{H} \mapsto \mathcal{H}$ av vektorrummet till sig självt.*

Vi identifierar U med sin matrisrepresentation i beräkningsbasen.

Definition 2. *Det Hermitiska konjugatet av en komplexvärd matris U är U transponerad med alla dess element utbyta mot respektive komplexa konjugat. Det Hermitiska konjugatet skrivs $U^\dagger$*[3]*.*

Exempel 5. *Om vi har*

$$U = \begin{pmatrix} \frac{1}{2} + \frac{i}{2} & \frac{1}{2} - \frac{i}{2} \\ -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix},$$

så kommer det Hermitiska konjugatet till U att vara

$$U^\dagger = \begin{pmatrix} \frac{1}{2} - \frac{i}{2} & \frac{i}{\sqrt{2}} \\ \frac{1}{2} + \frac{i}{2} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

Definition 3. *En unitär operator U definieras av egenskapen (för matrisen) att $U^{-1} = U^\dagger$, där $U^\dagger$ är det Hermitiska konjugatet till U*[4]*.*

Exempel 6. *Om vi har samma matris U som i exemplet innan där*

$$U = \begin{pmatrix} \frac{1}{2} + \frac{i}{2} & \frac{1}{2} - \frac{i}{2} \\ -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}, U^\dagger = \begin{pmatrix} \frac{1}{2} - \frac{i}{2} & \frac{i}{\sqrt{2}} \\ \frac{1}{2} + \frac{i}{2} & \frac{1}{\sqrt{2}} \end{pmatrix}$$

så får vi

$$UU^\dagger = \begin{pmatrix} \frac{1}{2} + \frac{i}{2} & \frac{1}{2} - \frac{i}{2} \\ -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{2} - \frac{i}{2} & \frac{i}{\sqrt{2}} \\ \frac{1}{2} + \frac{i}{2} & \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Alltså är $U^\dagger$ invers till U vilket betyder att U är unitär.

[3] Se [4] kapitel 9, och [1] kapitel 2.
[4] Se [4] kapitel 9, [17] avsnitt 1.6, [15] avsnitt 2.5, och [1] kapitel 2.

2.2.2 Hilbertrum

Kvantsystemen vi ska jobba med kommer att beskrivas med komplexa vektorer i ändligtdimensionella vektorrum C^n. Med den inre produkten definierad som den komplexa Euklidiska inre produkten, se definition 4, är vektorrummen Hilbertrum[5]. Vi använder $\mathcal{H}$ för att beteckna Hilbertrum. Vi kommer inte att vinna något på att definiera rigoröst vad ett Hilbertrum är. Vi nöjer oss med att konstatera vektorrumen vi kommer att arbeta med är ändligtdimensionella Hilbertrum.

Definition 4. *Låt* $\mathbf{u}$*=(*u_1*,* u_2*,. . . ,* u_n*) och* $\mathbf{v}$*=(*v_1*,* v_2*,. . . ,* v_n*) är två komplexa vektorer i det n-dimensionella komplexa vektorrummet* C^n*. Om* $\overline{v}_1$*,* $\overline{v}_2$ *,. . . ,* $\overline{v}_n$ *är de komplexa konjugaten till* v_1*,* v_2*,. . . ,* v_n *så definierar*

$$\mathbf{u} \cdot \mathbf{v} = u_1\overline{v}_1 + u_2\overline{v}_2 + \cdots + u_n\overline{v}_n$$

den komplexa Euklidiska inre produkten.

Normen för en vektor $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ i ett Hilbertrum ges av

$$|\mathbf{u}| = \sqrt{\mathbf{u} \cdot \mathbf{u}} = \sqrt{u_1\bar{u}_1 + u_2\bar{u}_2 + \cdots + u_n\bar{u}_n}.$$

De unitära operatorerna vi gick igenom i föregående avsnitt har några viktiga egenskaper som är värda att nämna.

i För en unitär operator U och två komplexa vektorer $\mathbf{u}$ och $\mathbf{v}$ med samma dimension så gäller det att

$$U\mathbf{u} \cdot U\mathbf{v} = \mathbf{u} \cdot \mathbf{v}.$$

ii Alla egenvärden till en unitär operator U har absolutbelopp 1, det vill säga komplexa tal på formen $e^{2\pi i\varphi}$ $\varphi \in [0, 1]$.

iii Unitära operatorer bevarar normen hos vektorer de opererar på.

Nedan ser vi ett exempel på egenskap iii.

Exempel 7. *Om vi har samma* U *som i exempel 6 för unitära operatorer och* $\mathbf{u} = (1, i)$ *med normen* $|\mathbf{u}| = \sqrt{(1 \cdot 1 + i \cdot (-i)} = \sqrt{2}$ *så har vi*

$$U(\mathbf{u}) = \begin{pmatrix} \frac{1}{2} + \frac{i}{2} & \frac{1}{2} - \frac{i}{2} \\ -\frac{i}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 1(\frac{1}{2} + \frac{i}{2}) + i(\frac{1}{2} - \frac{i}{2}) \\ (-\frac{i}{\sqrt{2}}) + i(\frac{1}{\sqrt{2}}) \end{pmatrix} = \begin{pmatrix} 1 + i \\ 0 \end{pmatrix}.$$

Vi får vidare att normen blir

$$|U(\mathbf{u})| = \sqrt{(1 + i)(1 - i) + 0 \cdot 0} = \sqrt{2}$$

Alltså ser vi att normen bevaras efter att vi opererat på $\mathbf{u}$ *med den unitära operatorn* U*.*

[5]se [4] kapitel 9, [2] sid 542 och [15] avsnitt 2.3.

2.3 Tensorprodukter

För att kunna jobba med större kvantsystem behöver vi använda oss av tensorprodukt[6]. Tensorprodukt är ett sätt att kombinera vektorer, vektorrum eller linjära avbildningar med andra vektorer, vektorrum eller linjära avbildningar. Syftet är att kunna behandla flera vektorer som en vektor, flera vektorrum som ett vektorrum eller flera linjära avbildningar som en linjär avbildning. Tensorprodukt beräknas således mellan två eller flera vektorer, vektorrum eller linjära avbildningar. Operatorn för tensorprodukt skrivs $\otimes$.

Anta att vi har två Hilberrum $\mathcal{H}_1$ och $\mathcal{H}_2$ med dimension n respektive m och ortonormalbaserna $\{|u_l\rangle\}_{l\in\{1,\dots,n\}}$ för $\mathcal{H}_1$ och $\{|v_k\rangle\}_{k\in\{1,\dots,m\}}$ för $\mathcal{H}_2$. Då kommer tensorprodukten $\mathcal{H}_1 \otimes \mathcal{H}_2$ av vektorrummen $\mathcal{H}_1$ och $\mathcal{H}_2$ att vara ett nytt Hilberrum med nm dimensioner. $\mathcal{H}_1 \otimes \mathcal{H}_2$ sägs vara ett tensorproduktrum och har ortonormalbases $\{|u_l\rangle \otimes |v_k\rangle\}_{l\in\{1,\dots,n\},k\in\{1,\dots,m\}}$ där $|u_l\rangle \otimes |v_k\rangle$ är tensorprodukter mellan basvektorerna.

Tensorprodukten mellan två vektorer beräknas genom att multiplicera varje element i den första vektorn med varje element i den andra. Vi kan till exempel ha två vektorer med n respektive m dimensioner. Tensor produkten av dessa två ger nm nya element som bildar en ny vektor med dimension nm.

Exempel 8. *Om vi har 2 vektorer*

$$|\varphi_0\rangle = \alpha_0|0\rangle + \beta_0|1\rangle = \begin{pmatrix}\alpha_0\\ \beta_0\end{pmatrix}, |\varphi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle = \begin{pmatrix}\alpha_1\\ \beta_1\end{pmatrix}$$

så blir tensorprodukten av de två

$$|\varphi_0\rangle \otimes |\varphi_1\rangle = (\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) =$$

$$\alpha_0\alpha_1(|0\rangle \otimes |0\rangle) + \alpha_0\beta_1(|0\rangle \otimes |1\rangle) + \beta_0\alpha_1(|1\rangle \otimes |0\rangle) + \beta_0\beta_1(|1\rangle \otimes |1\rangle) =$$

$$\alpha_0\alpha_1|00\rangle + \alpha_0\beta_1|01\rangle + \beta_0\alpha_1|10\rangle + \beta_0\beta_1|11\rangle = \begin{pmatrix}\alpha_0\alpha_1\\ \alpha_0\beta_1\\ \beta_0\alpha_1\\ \beta_0\beta_1\end{pmatrix}.$$

Tensorprodukter uppfyller också följande axiom:

1. För godtyckliga $|\varphi_0\rangle \in \mathcal{H}_1, |\varphi_1\rangle \in \mathcal{H}_2$ och $c \in \mathbb{C}$,

$$c(|\varphi_0\rangle \otimes |\varphi_1\rangle) = (c|\varphi_0\rangle) \otimes |\varphi_1\rangle = |\varphi_0\rangle \otimes (c|\varphi_1\rangle)$$

[6]Se [1] avsnitt 2.6, [17] 2.1 och [6] del 1, kapitel 13.

2. För godtyckliga $|\varphi_0\rangle, |\psi_0\rangle \in \mathcal{H}_1$ och $|\varphi_1\rangle \in \mathcal{H}_2$,

$$(|\varphi_0\rangle \ + |\psi_0\rangle) \otimes |\varphi_1\rangle = |\varphi_0\rangle \otimes |\varphi_1\rangle + |\psi_0\rangle \otimes |\varphi_1\rangle$$

3. För godtyckliga $|\varphi_0\rangle \in \mathcal{H}_1$ och $|\varphi_1\rangle, |\psi_1\rangle \in \mathcal{H}_2$,

$$|\varphi_0\rangle \otimes (|\varphi_1\rangle \ + |\psi_1\rangle) = |\varphi_0\rangle \otimes |\varphi_1\rangle + |\varphi_0\rangle \otimes |\psi_1\rangle$$

Notationen $\otimes$ kommer ibland inte att skrivas ut för att få mer överskådliga uttryck. Istället för $|\varphi\rangle \otimes |\psi\rangle$ skriver vi $|\varphi\rangle|\psi\rangle$ eller $|\varphi\psi\rangle$ vilka representerar samma sak.

Tensorprodukt för linjära avbildningar beräknar man med avbildningsmatriser. Anta att vi har två linjära avbildningar $U \in \mathcal{H}_1$ och $V \in \mathcal{H}_2$ vilka har en $m \times n$ respektive $p \times q$ avbildningsmatris. Då kommer tensor produkten av U och V bli en ny linjär avbildning $U \otimes V$ på tensorproduktrummet $\mathcal{H}_1 \otimes \mathcal{H}_2$. $U \otimes V$ kommer att representeras av en $mp \times nq$ matris. Man beräknar avbildningsmatrisen för $U \otimes V$ genom att för varje element i U sätta man in matrisen V multiplicerad med elementet på den positionen i U:

$$U \otimes V = \begin{pmatrix} U_{11}V_{11} & \dots & U_{11}V_{1q} & \dots\dots & U_{1n}V_{11} & \dots & U_{1n}V_{1q} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ U_{11}V_{p1} & \dots & U_{11}V_{pq} & \dots\dots & U_{1n}V_{p1} & \dots & U_{1n}V_{pq} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ U_{m1}V_{11} & \dots & U_{m1}V_{1q} & \dots\dots & U_{mn}V_{11} & \dots & U_{mn}V_{1q} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ U_{m1}V_{p1} & \dots & U_{m1}V_{pq} & \dots\dots & U_{mn}V_{p1} & \dots & U_{mn}V_{pq} \end{pmatrix}$$

Om U och V är linjära avbildningar på $\mathcal{H}_1$ respektive $\mathcal{H}_2$, $|\varphi_0\rangle \in \mathcal{H}_1$ och $|\varphi_1\rangle \in \mathcal{H}_2$ så definieras $(U \otimes V)(|\varphi_0\rangle \otimes |\varphi_1\rangle)$ på $\mathcal{H}_1 \otimes \mathcal{H}_2$ av

$$(U \otimes V)(|\varphi_0\rangle \otimes |\varphi_1\rangle) \equiv U|\varphi_0\rangle \otimes V|\varphi_1\rangle.$$

Denna definition utvecklar vi linjärt över elementen i $\mathcal{H}_1 \otimes \mathcal{H}_2$ till

$$(U \otimes V)\Big(\sum_{kl} \lambda_{kl}|u_k\rangle \otimes |v_l\rangle\Big) \equiv \sum_{kl} \lambda_{kl} U|u_k\rangle \otimes V|v_l\rangle.$$

Vi har nu gått igenom den matematiska teori vi behöver för att beskriva en kvantdator.

3 Kvantdatorns delar

I det här kapitlet går vi igenom kvantdatorns delar. En klassisk dator har bitar, grindar och möjlighet att läsa av bitarna. En kvantdator byggs med motsvarande komponenter men komponenterna besitter lite andra egenskaper. Först beskrivs kvantbitar som motsvarar bitar. Sedan fortsätter vi med att beskriva kvantgrindar och tillslut en metod att läsa av kvantbitar.

3.1 Kvantbitar

3.1.1 Kvantbiten

I en vanlig dator representeras data binärt med så kallade bitar[7]. Samma princip används för att representera data i kvantdatorer men bitarna kallas då kvantbitar. Varje kvantbit är ett 2-dimensionellt kvantsystem. I en kvantbit används kvantsystemets läge för att representera data. Läget är det tillstånd som en kvantsystemet befinner sig i. Som vi såg i exempel 2 kan läget hos ett 2-dimensionellt kvantsystem beskrivas med basvektorerna

$$\begin{pmatrix}1\\0\end{pmatrix} = |0\rangle \; och \; \begin{pmatrix}0\\1\end{pmatrix} = |1\rangle.$$

Det är allmänt med dessa basvektorer man beskriver en kvantbits läge. Det generella läget kan beskrivas som

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

där α och β är komplexa tal och kallas sannolikhetsamplituder. α och β uppfyller också att $|\alpha|^2 + |\beta|^2 = 1$. En kvantbits läge beskrivs alltid med en enhetsvektor i ett Hilbertrum. En enhetsvektor är en vektor med längd 1. Vi kommer alltså bara att jobba med vektorer av längd 1. I exempel 2 kunde fotonerna befinna sig i en av två olika banor. Banorna representeras således av respektive enhetsvektor $|0\rangle$ och $|1\rangle$ i ett tvådimensionellt Hilbertrum och en foton i superposition som en linjär kombination av $|0\rangle$ och $|1\rangle$. När en foton i exempel 2 hade passerat den första halvspegeln så sa vi att den befann sig i en superposition mellan 0-vägen och 1-vägen. Kvantbitens läge som beskriver fotonen skrivs då som $\frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$.

Vi kommer att använda $|0\rangle$ och $|1\rangle$ (beräkningsbasen) som bas i Hilbertrumen genom nästan hela denna uppsats. Det hade givetvis gått bra med någon annan bas. En annan bas vi kommer att beröra lite kallas Hadamardbasen och har basvektorerna $|+\rangle$ och $|-\rangle$. Basvektorerna $|+\rangle$ och $|-\rangle$ skrivs i beräkningsbasen som $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ respektive $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

I exempel 2 kan man se varje foton som en kvantbit där lägena $|0\rangle$ och $|1\rangle$ beskriver vilken väg fotonen befinner sig på. Ett annat sätt att se på en

[7]Se [12] avsnitt 1, [16] 7.2, [13] 2.1.1, [17] 2.1, [14] kapitel 2 och 3 samt [1] kapitel 3.

kvantbit är som en foton där fotonens spinn talar om vilket läge den befinner sig i. Enligt kvantfysiken finns det en frihetsgrad hos partiklar som kallas spinn. Fotoner har ett spinn som kan vara upp, ner eller något mittemellan dem. Ett spinn mellan upp- och nerspinnet kallas för halvspinn. Uppspinnet beskrivs med $|0\rangle$ och nerspinnet med $|1\rangle$. Läget hos en foton med halvspinn beskrivs av en superposition mellan lägena för upp- respektive nerspinnet, alltså som $\alpha|0\rangle + \beta|1\rangle$. En kvantbit i superposition kan alltid skrivas som

$$|\psi\rangle = \cos(\tfrac{\theta}{2})|0\rangle + e^{i\varphi}\sin(\tfrac{\theta}{2})|1\rangle$$

med

$$|\cos(\tfrac{\theta}{2})|^2 + |e^{i\varphi}\sin(\tfrac{\theta}{2})|^2 = |\cos(\tfrac{\theta}{2})|^2 + |\sin(\tfrac{\theta}{2})|^2 = 1.$$

Lägesvektorer kan visualiseras som punkter på en tredimensionell enhetssfär, kallad *Blochsfär*[8]. En punkt på *Blochsfären* har koordinaterna

$$(x, y, z) = (\sin(\theta)\cos(\varphi), \sin(\theta)\sin(\varphi), \cos(\theta)),\ fr\ \theta, \varphi \in [0, 2\pi).$$

Anta att talet $e^{i\varphi}$ är ett komplext tal med norm 1 och α är någon godtycklig konstant sådan att $|\alpha|^2 + |\alpha|^2 = 1$. I lägen på formen

$$|\psi\rangle = \alpha|0\rangle + \alpha e^{i\varphi}|1\rangle$$

säger vi då att $e^{i\varphi}$ är den relativa fasen mellan basvektorerna $|0\rangle$ och $|1\rangle$.

Exempel 9. *Om vi har läget*

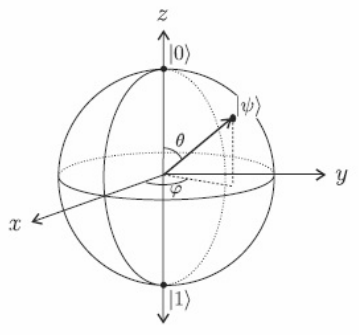
$$|-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

så är

$$-1 = e^{i\pi}$$

den relativa fasen mellan basvektorerna $|0\rangle$ *och* $|1\rangle$.

[8]Se figur 4 från [1] sid 43.



Figur 4: Lägesvektor visualiserad som en punkt på *Blochsfären*.

De system vi använder är stängda system. Det betyder att kvantbitarna inte kommer att utsättas för någon yttre påverkan i våra kretsar. Kretsarna bildar då slutna kvantsystem. Det kommer dock att finnas ett oundvikligt undantag, nämligen då vi vill läsa av informationen lagrad i kvantbitarna. Det gör man genom mätning och det går vi igenom senare i det här kapitlet.

3.1.2 Sammansatta system

I föregående avsnitt gick vi igenom hur en kvantbit beskrivs som ett enskilt 2-dimensionellt kvantsystem. För att kunna göra användbara beräkningar behöver vi system sammansatta av flera kvantbitar som kan interagera med varandra. Dessa system kallas sammansatta system och vi ska se hur vi kan beskriva dem[9].

Sammansatta system består av 2 eller fler kvantbitar vilka vi kan behandla som ett objekt. Anta att vi har ett sammansatta systemet som består av n kvantbitar. Beskrivs kvantbitarna av de tvådimensionella Hilbertrummen $\mathcal{H}_1, \mathcal{H}_2, \ldots, \mathcal{H}_n$ så beskrivs det sammansatta systemet av tensorproduktrummet $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_n$. Om den första, andra och upp till n:te kvantbiten befinner sig i läget $|\varphi_1\rangle, |\varphi_2\rangle, \ldots, |\varphi_n\rangle$ så beskrivs det samman satta systemets läge av tensorprodukten $|\varphi_1\rangle \otimes |\varphi_2\rangle \otimes \cdots \otimes |\varphi_n\rangle$.

Alla lägen i sammansatta system kan inte beskrivas som en tensorprodukt av de enskilda kvantbitarnas lägen. Om vi har ett 2-kvantbitsystem där båda kvantbitarna är oberoende av varandra så skapar varje kvantbit ett eget stängt system. Läget av 2-kvantbitsystemet kan då beskrivas som en tensorprodukt av de två Hilbertrummen för respektive kvantbit. Men om kvantbitarna tillåts interagera med varandra kommer båda att ingå i ett stängt system. När kvantbitarna interagerar med varandra säger man att de är sammanflätade. Säg att vi har två kvantbitar som är sammanflätade. Då kommer det stängda systemet att innehålla båda kvantbitarna och det är inte säkert att vi kan beskriva systemet som en tensorprodukt. Man säger att ett sammansatt läge är sammanflätat om det inte kan delas upp i en tensorprodukt av de separata kvantbitarnas lägen. Ändringar av en kvantbit i ett sammansatt läge kommer att påverka de andra kvantbitarna utan att man direkt gör något med dem och vice versa. Exempel 10 visar hur vi kan kolla om ett läge är sammanflätat.

Exempel 10. *Anta att vi har ett sammansatt system med 2 kvantbitar i läget*

$$|\varphi\rangle = \tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{\sqrt{2}}|10\rangle.$$

Läget går inte att skriva som en tensorprodukt av några lägesvektorer från de enskilda kvantbitarna. Man kan visa detta genom att bevisa att det inte existerar $\alpha_0, \beta_0, \alpha_1$ och β_1 sådana att

$$|\varphi\rangle = (\alpha_0|0\rangle + \beta_0|1\rangle) \otimes (\alpha_1|0\rangle + \beta_1|1\rangle) =$$

[9]Se kapitel 4 [14], avsnitt 3.3 i [1], 2.1.2 och 2.1.4 i [13] samt 2.13 [15].

$$= \alpha_0\alpha_1|00\rangle + \alpha_0\beta_1|01\rangle + \beta_0\alpha_1|10\rangle + \beta_0\beta_1|11\rangle.$$

Vi skulle få $\alpha_0\alpha_1 = \frac{1}{2}, \alpha_0\beta_1 = \frac{1}{2}, \beta_0\alpha_1 = \frac{1}{\sqrt{2}}$ *och* $\beta_0\beta_1 = 0$ *. Men om* $\beta_0\beta_1 = 0$ *så måste* $\beta_0 = 0$ *eller* $\beta_1 = 0$ *alternativt båda vara lika med noll. Om* $\beta_0 = 0$ *får vi* $\beta_0\alpha_1 = 0$ *vilket inte stämmer. Om* $\beta_1 = 0$ *får vi* $\alpha_0\beta_1 = 0$ *vilket inte heller stämmer, är båda noll får vi båda motsägelserna. Alltså är läget sammanflätat.*

Om vi däremot har läget

$$|\varphi\rangle = \tfrac{1}{2}|00\rangle + \tfrac{1}{2}|01\rangle + \tfrac{1}{2}|10\rangle \ + \tfrac{1}{2}|11\rangle$$

kan det skrivas som tensorprodukten

$$|\varphi\rangle = (\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle) \otimes (\tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle),$$

där $\alpha_0 = \beta_0 = \alpha_1 = \beta_1 = \frac{1}{\sqrt{2}}$.

3.2 Kvantgrindar

För att göra beräkningar i en vanlig dator använder man sig av grindar. Genom grindarna man skickar man bitar för att få den logiska operatorn som grinden realiserar utförd på bitarna. På samma sätt behövs det kvantgrindar som vi applicerar på kvantbitar[10]. En kvantgrind/operator som verkar på och utvecklar en lägesvektor gör detta linjärt. Dessa operatorer är linjära avbildningar och vi kommer att räkna på dem med deras avbildningsmatriser. Om vi har en godtycklig linjär avbildning U som avbildar $|\varphi_k\rangle$ till $U|\varphi_k\rangle$ får vi att

$$U\sum_k \alpha_k|\varphi_k\rangle = \sum_k \alpha_k U|\varphi_k\rangle.$$

Som vi går igenom i avsnitt 3.3 måste $\sum_k |\alpha_k|^2 = 1$ bevaras. De enda linjära avbildningarna som bevarar detta är de unitära, vilka bevarar normen hos vektorer. De unitära linjära avbildningarna vi är intresserade är de som avbildar från 1-kvantbitsystem till 1-kvantbitsystem. Dessa kan i Hilbertrummen som beskriver kvantbitar representeras av 2×2 matriser.

Det finns några vanliga grindar vi behöver. De första fyra är de så kallade Pauligrindarna (se [1] sid 63) vilka definieras:

$$I \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ X \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Y \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \ \textit{och} \ Z \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Grindarna X, Y och Z motsvarar rotationer av lägesvektorer kring x-,y- och z-axeln på Blochsfären. Vi ska mest lägga fokus på I och X. I identifierar den vanliga identitetsavbildningen och gör inget med det läge den avbildar. X identifierar NOT-grinden som representerar den logiska NOT-funktionen

[10] Se avsnitt 5.3 i [14], 2.3 i [17], 7.4 och 7.5 i [16], 4.1 i [15], 4.2 i [1] och 2.3.1 i [13].

och avbildar $|0\rangle$ till $|1\rangle$ och $|1\rangle$ till $|0\rangle$ eller mer generellt $\alpha|0\rangle + \beta|1\rangle$ till $\alpha|1\rangle + \beta|0\rangle$:

$$X(\alpha|0\rangle + \beta|1\rangle) \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \beta \\ \alpha \end{pmatrix} \equiv \alpha|1\rangle + \beta|0\rangle.$$

Det finns också en fasrotationsgrind som ändrar på den relativa fasen hos ett läge. Fasrotationsgrindar R definieras av matriser på formen

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{\varphi i} \end{pmatrix}.$$

Har man läget $\alpha|0\rangle + \beta|1\rangle$ och applicerar R får man

$$R(\alpha|0\rangle + \beta|1\rangle) = \begin{pmatrix} 1 & 0 \\ 0 & e^{\varphi i} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} \alpha 1 \\ \beta e^{\varphi i} \end{pmatrix} = \alpha|0\rangle + \beta e^{\varphi i}|1\rangle.$$

En annan mycket användbar grind är Hadamardgrinden. Den betecknas H och avbildar basvektorerna i beräkningsbasen på följande sätt:

$$H|0\rangle = \tfrac{1}{\sqrt{2}}|0\rangle + \tfrac{1}{\sqrt{2}}|1\rangle$$

$$H|1\rangle = \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle.$$

Hadamardgrinden är sin egen invers och har avbildningsmatrisen

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

som motsvarar en rotation på $\frac{\pi}{4}$ i det reella talplanet.

Det finns en annan klass av mycket användbara grindar, nämligen de kontrollerade grindarna. Detta är en typ av grind som har minst två kvantbitar som indata. En av dem styr om grinden ska göra något eller inte och kallas styrkvantbit eller styrläget. Om indata till den styrakvantbiten är $|1\rangle$ så appliceras grinden och är styrkvantbiten $|0\rangle$ gör den ingenting. De kontrollerade grindarna skrivs allmänt c-U där U är den avbildning som appliceraa. Ett bra exempel på en sådan är c-X eller $CNOT$ som är den kontrollerade versionen av NOT-grinden. Den avbildar på följande sätt:

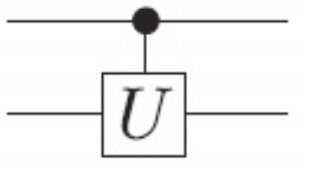
$$c-X|0\rangle|0\rangle = |0\rangle|0\rangle,\ c-X|0\rangle|1\rangle = |0\rangle|1\rangle$$

$$c-X|1\rangle|0\rangle = |1\rangle|1\rangle,\ c-X|1\rangle|1\rangle = |1\rangle|0\rangle.$$

Mer generellt för en grind c-U får vi

$$c-U|0\rangle|\phi\rangle = |0\rangle|\phi\rangle,\ c-U|1\rangle|\phi\rangle = |1\rangle U|\phi\rangle.$$

En sådan grind ritar vi i ett kretsschema som figur 5.



Figur 5: Kretsschema över en kontrollerad U-grind, den kvantbit som skickas genom linjen med den svarta pricken är styrkvantbiten.

Vi vet hur vi kan applicera linjära avbildningar på enskilda kvantbitar. Som vi nämnde tidigare är det av intresse att jobba med sammansatta system. Vi vill därför kunna göra grindar som verkar på mer än bara en kvantbit. Säg att man har ett sammansatt system av kvantbitar och vill applicera ett antal avbildningar på var och en av dem. Avbildningarna kan beskrivas som tensorprodukten av alla avbildningar man vill applicera. Man har då en avbildning som kan appliceras på det läge som beskriver det sammansatta systemets läge. På så sätt kan man sätta ihop avbildningar så att de appliceras på ett godtyckligt antal kvantbitar samtidigt.

Exempel 11. *Anta att vi har ett 2-kvantbitsystem och matar in läget* $|\varphi_0\rangle \otimes |\varphi_1\rangle$ *och vill utföra NOT-grinden* X *på den sista kvantbiten. Då kommer vi att implicit applicera* I *på den första kvantbiten. Alltså avbildas* $|\varphi_0\rangle \otimes |\varphi_1\rangle$ *till* $I|\varphi_0\rangle \otimes X|\varphi_1\rangle = (I \otimes X)(|\varphi_0\rangle \otimes |\varphi_1\rangle)$ *och den linjära avbildningen blir* $I \otimes X$*. Avbildningsmatrisen för* $I \otimes X$ *är*

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Vi har sätt hur man kan applicera kvantgrindar på kvantbitars lägen. I nästa avsnitt ska vi gå igenom hur vi kan tillgodogöra oss information om resultatet av kvantgrindars verkan på lägen.

3.3 Mätningar

De kvantsystem vi jobbar med är stängda, de påverkas således inte av någon yttre omgivning. Om vi vill tillgodogöra oss informationen i ett kvantsystem måste vi göra någon form av mätning. Det innebär att den yttre omgivningen kommer att påverka systemet och det förblir inte längre stängt. Mätningar är ett problem med kvantdatorn för de ändrar läget som systemet befinner sig i. När läget vid mätning ändras, förstörs informationen lagrad i systemet. Teorier för hur mätningar går till och vilka sätt man kan göra på ligger utan-

för den här uppsatsen. Vi nöjer oss därför med att konstatera några viktiga egenskaper hos en vanlig metod att mäta, kallad en Von Neumannmätning[11].

Hur systemet utvecklas när vi mäter det kan inte lägre beskrivas av en unitär operator. Det kommer inte att utvecklas med tiden som vi gick igenom i avsnitt 3.2. Anta att vi har ett system med N urskiljbara lägen $|0\rangle, |1\rangle, \ldots, |N-1\rangle$. Vi antar också att vi har en apparat som skickar ut ett värde i tillsammans med läget $|i\rangle$ när $|i\rangle$ är indata till apparaten. Värdet i är det index som talar om vilket av de möjliga resultaten av mättningen vi fått. I systemet vi nyss antog så kommer i vara något av talen $0, 1, \ldots, N-1$. Vi kan se det som att vi får värdet i på någon digital display med tillräcklig noggrannhet för att visa i.

Vi beskriver rent axiomatiskt vad som händer vid en mätning och det är erfarenhetsmässigt så här ett kvantsystem beter sig när man mäter det. Vi kommer här inte att gå in på den fysikaliska motivationen, den ligger utanför den här uppsatsen. Säg att vi har läget $|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle$ i ett lägesrum $\mathcal{H}_A$ med en given ortonormalbas $C = \{|\varphi_i\rangle\}$ för kvantsystemet A. En Von Neumannmätning av systemet A i läget $|\psi\rangle$ med avseende på basen C ger φ_i som resultat med sannolikhet $|\alpha_i|^2$ och lämnar systemet i läget $|\varphi_i\rangle$. Kom ihåg från avsnitt 3.1.1 att vi nämnde sannolikhetsamplituden för olika lägen. Det är alltså sannolikhetsamplituderna α_i i systemets lägen som avgör vilken utdata vi får när vi mäter. Eftersom summan av sannolikhetsamplituderna måste vara 1 måste de linjära avbildningarna bevara den summan med värde 1, alltså att $\sum_k |\alpha_k|^2 = 1$. Systemet kommer vid mätning att falla samman till ett av basläget $|\varphi_i\rangle$ och all information i resten av systemet går förlorad. Det enda vi får kvar är läget $|\varphi_i\rangle$ och värdet φ_i som vi kan läsa av på apparaten.

Säg att vi har ett sammansatt system i läget $|\psi\rangle = \sum_i \alpha_i |\varphi_i\rangle|\gamma_i\rangle$ från lägesrummet $\mathcal{H}_A \otimes \mathcal{H}_B$. En Von Neumannmätningen av system A ger oss värdet φ_i som resultat med sannolikhet $|\alpha_i|^2$ och lämnar systemet i läget $|\varphi_i\rangle|\gamma_i\rangle$.

Exempel 12. *Vi har ett 1-kvantbitsystem A med basen $\{|0\rangle, |1\rangle\}$ och läget*

$$|\psi\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \tfrac{1}{\sqrt{2}}|0\rangle - \tfrac{1}{\sqrt{2}}|1\rangle.$$

En mätning av A med apparaten som beskrevs tidigare kan ge två möjliga resultat. 0 som utdata och systemet lämnas i läget $|0\rangle$ med sannolikhet $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$ eller utdata 1 och läget $|1\rangle$ med sannolikhet $|-\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$. I det här fallet har båda baslägena samma sannolikhet så resultatet av mätningen är slumpmässig.

Exempel 13. *Anta att vi har ett 2-kvantbitsystem i den vanliga beräkningsbasen med läget*

$$|\psi\rangle = \sqrt{\tfrac{2}{12}}|00\rangle + \sqrt{\tfrac{1}{12}}|01\rangle - \sqrt{\tfrac{5}{12}}|10\rangle + \sqrt{\tfrac{4}{12}}|11\rangle.$$

[11] Se avsnitt 2.3.2 i [13], 3.4 och 4.5 i [1].

Gör vi två mätningar, en på varje kvantbit, kommer vi få följande resultat: 0 *och* 0 *med sannolikhet* $\frac{2}{12}$, 0 *och* 1 *med sannolikhet* $\frac{1}{12}$, 1 *och* 0 *med sannolikhet* $\frac{5}{12}$ *samt* 1 *och* 1 *med sannolikhet* $\frac{4}{12}$. *Om vi bara mäter den ena kvantbiten, säg den första, får vi resultatet* 0 *med sannolikhet* $\frac{2}{12} + \frac{1}{12} = \frac{3}{12}$ *och* 1 *med sannolikhet* $\frac{5}{12} + \frac{4}{12} = \frac{9}{12}$. *Skriver vi om* $|\psi\rangle$ *till*

$$|\psi\rangle = \sqrt{\tfrac{3}{12}}|0\rangle(\sqrt{\tfrac{2}{3}}|0\rangle + \sqrt{\tfrac{1}{3}}|1\rangle) + \sqrt{\tfrac{1}{12}}|1\rangle(\sqrt{\tfrac{5}{9}}|0\rangle + \sqrt{\tfrac{4}{9}}|1\rangle)$$

ser vi lättare vad vi får kvar efter en mätning. Den andra kvantbiten kommer att lämnas i en superposition $\sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$ *om vi mäter* 0 *och i* $\sqrt{\frac{5}{9}}|0\rangle + \sqrt{\frac{4}{9}}|1\rangle$ *om vi mäter* 1. *Hela systemet kommer att lämnas i* $|0\rangle \otimes (\sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle) = \sqrt{\frac{2}{3}}|00\rangle + \sqrt{\frac{1}{3}}|01\rangle$ *respektive* $|1\rangle \otimes (\sqrt{\frac{5}{9}}|0\rangle + \sqrt{\frac{4}{9}}|1\rangle) = \sqrt{\frac{5}{9}}|10\rangle + \sqrt{\frac{4}{9}}|11\rangle$ *efter en mätning.*

Till slut kan vi tillägga att när vi gör en mätning i en krets kommer, som vi såg i kapitel 1, det representeras av en triangel i kretsschemat, se figur 1. Vi har sett hur vi kan tillgodogöra oss information om ett kvantsystem genom att mäta det. Vi har också sett hur en sådan mätning påverkar systemet. Vi kan nu gå vidare och titta på några viktiga kvantalgoritmer.

4 Kvantalgoritmer

I det här kapitlet ska vi se på de algoritmer och tekniker som vi behöver för att kunna utföra vår faktoriseringsalgoritm. Vi går igenom hur vi tillgodogör oss egenvärden till en operators egenlägen(egenvektorer). Det kommer att visa sig att vi kan göra det genom att lagra egenvärden på ett specifikt sätt med en speciell algoritm och sedan läsa av det. Men först ska vi titta på en teknik som flyttar på egenvärdet.

4.1 Flytta egenvärden

Att flytta egenvärden är en teknik som används mycket i konstruktionen av kvantalgoritmer, se kapitel 6 i [1]. Det är ett verktyg som med kontrollerade grindar och axiom 1 för tensorprodukter kan lagra information om egenvärden styrkvantbiten. Om vi dessutom låter styrkvantbiten vara en superposition av $|0\rangle$ och $|1\rangle$ kan vi lagra informationen i den relativa fasen hos styrkvantbiten. Vi börjar med ett enkelt fall och går sedan vidare till ett mer generellt.

4.1.1 Flytta egenvärden med kontrollerad NOT-grinden

Om vi tittar på $c\text{-}X$ (den kontrollerade NOT-grinden) igen och applicerar den på 2 kvantbitar i Hadamardbasen får vi

$$c\text{-}X\Big(\Big(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\Big)\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)\Big) =$$

$$= \tfrac{1}{2}(c\text{-}X(|0\rangle|0\rangle) - c\text{-}X(|0\rangle|1\rangle) + c\text{-}X(|1\rangle|0\rangle) - c\text{-}X(|1\rangle|1\rangle))$$

$$= \tfrac{1}{2}(|0\rangle|0\rangle - |0\rangle|1\rangle + |1\rangle|1\rangle - |1\rangle|0\rangle) = \Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big).$$

Här har alltså rollerna på vilken kvantbit som påverkas ändrats på. Det beror på att $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ är ett egenläge till X med egenvärdet -1. Vi har

$$c\text{-}X\Big(|1\rangle\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)\Big) = |1\rangle\Big(X\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)\Big) =$$

$$|1\rangle((-1)\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)\Big) = (-1)|1\rangle\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big),$$

$$c\text{-}X\Big(|0\rangle\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)\Big) = (1)|0\rangle\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big).$$

Alltså

$$c\text{-}X\Big(|a\rangle\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)\Big) = (-1)^a|a\rangle\Big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\Big)$$

och för en styrkvantbit som är i en godtycklig superposition får vi

$$c\text{-}X(\alpha_0|0\rangle + \alpha_1|1\rangle)\Big(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big) = (\alpha_0|0\rangle - \alpha_1|1\rangle)\Big(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big).$$

Vi kan se det som att vi har applicerat c-X på ett egenläge och flyttat tillbaka egenvärdet framför styrkvantbiten. Om vi dessutom har en superposition som styrkvantbit hamnar egenvärdet i den relativa fasen hos styrkvantbiten. Tekniken att flytta fram egenvärdet framför styrkvantbiten kan generalliseras till andra grindar än CNOT-grinden som vi ska se i nästa avsnitt.

4.1.2 Flytta egenvärden med en 2-kvantbitgrind U_f

Anta att vi istället har en 2-kvantbitgrind U_f som implementerar någon godtycklig funktion $f : \{0,1\} \to \{0,1\}$ genom avbildningen $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. $\oplus$ står för den logiska operationen XOR. $y \oplus f(x)$ kan vi beräkna med en klassisk dator så vi kan implementera U_f. Säg att vi använder samma målkvantbit $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ som vi använde i förra avsnittet med den kontrollerade NOT-grinden. Då får vi

$$U_f\Big(|x\rangle\Big(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big)\Big) = \frac{U_f(|x\rangle|0\rangle) - U_f(|x\rangle|1\rangle)}{\sqrt{2}} =$$

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

Eftersom $f(x)$ bara kan anta värdena 0 och 1 tittar vi på vad resultatet blir i de fallen:

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

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

Vi kan sammanfatta resultaten och skriva läget som

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

Om vi flyttar tillbaka $(-1)^{f(x)}$ framför $|x\rangle$ kan vi skriva läget som

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

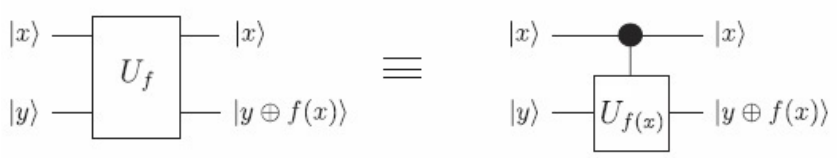
Om $|x\rangle$ är i superpositionen $(\alpha_0|0\rangle + \alpha_1|1\rangle)$ genererar U_f

$$U_f\Big((\alpha_0|0\rangle + \alpha_1|1\rangle)\Big(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big)\Big) =$$

$$= \Big((-1)^{f(0)}\alpha_0|0\rangle + (-1)^{f(1)}\alpha_1|1\rangle\Big)\Big(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\Big).$$

Det vi har gjort är att anta att vi har en 2-kvantbitgrind U_f som implementerar någon godtycklig funktion $f\{0,1\} \to \{0,1\}$, där $U_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. Om vi applicerar U_f på ett 2-kvantbitläge $|x\rangle\big(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\big)$ kan vi se U_f som en kontrollerad 1-kvantbitgrind som styrs av $|x\rangle$. Vi refererar till den kontrollerade som c-U_f som har en egenvektor $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$ med egenvärdet $(-1)^{f(x)} = e^{\pi i f(x)}$. Figur 6 visar kretsen för U_f och c-U_f, den är tagen från [1] sid 94.

För att sammanfatta vad vi kommit fram till: Vi har tittat på kontrollerade grindar och grindar vars effekt bestäms av indatats lägen. Vi har sett hur vi med hjälp av egenläget för dessa grindar kan koppla motsvarande egenvärdet till styrkvantbiten. Det är något vi kommer att ha stor nytta av i avsnitt 4.3. Då ska vi beskriva en algoritm för att få fram information om egenvärdet.



Figur 6: Kretsschema över U_f och c-U_f.

4.2 Kvantfouriertransformation

Kvantfouriertransformation är en viktig del i många algoriter till kvantdoatorn. Bland annat används dess invers för att läsa av den relativa fasen hos ett läge. Kvantfouriertransformation kan både koda in och läsa av information ur den relativa fasen. Vi börjar med att gå igenom hur den fungerar och hur vi bygger den. Sedan beskriver vi inversen och hur vi med den kan uppskatta den relativa fasen i ett läge.

4.2.1 QFT-grinden

Kvantfouriertransformation förkortas QFT från engelskans Quantum Fourier Transformation[12]. Den är en mycket användbar operation som spelar en viktig roll i faktoriseringsalgoritmen. QFT är ett sätt att koda in information om en lägesvektor i den relativa fasen till basvektorerna i ett kvantsystem. Vi börjar med att definiera den:

[12]Se (avsnitt 7.1.1 i [1], 10.3 i [16], 11.5.2 i [15], 5.7 i [14] och 3.2.2 i [13].

Definition 5. *Anta att vi i $\mathbb{C}^N$ har följande lägesvektor $|x\rangle = \sum_{i=0}^{N-1} x_i|i\rangle$ där $x_0, x_1, \ldots, x_{N-1} \in (0,1)$. N är alltså antalet baslägesvektorer och kan skrivas som 2^n där n är antalet kvantbitar i systemet. Kvantfouriertransformationen av $|x\rangle$ över de N baslägena $|0\rangle, |1\rangle, \ldots, |N-1\rangle$ definieras då som $|y\rangle = \sum_{i=0}^{N-1} y_i|i\rangle$ där*

$$y_k = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} x_j e^{2\pi i \frac{k}{N} j}.$$

$|y\rangle$ betecknas QFT_N och kan också skrivas som avbildningen med följande effekt på basvektorerna i $\mathbb{C}^N$

$$QFT_N : |x\rangle \longmapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i \frac{x}{N} y}|y\rangle.$$

Den har också en invers:

$$QFT_N^{-1} : |x\rangle \longmapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{-2\pi i \frac{x}{N} y}|y\rangle.$$

När vi skriver uttryck framöver så kommer vi att skriva talen i lägesvektorerna, alltså talet y i $|y\rangle$ binärt. Tal på formen $\phi = 0, x_1 x_2 x_3 \ldots$ skrivs också med basen 2, alltså är ϕ samma som

$$x_1 \cdot 2^{-1} + x_2 \cdot 2^{-2} + x_3 \cdot 2^{-3} + \ldots$$

För att förstå hur vi kan bygga en som utför QFT:n tittar vi först på ett 2-kvantbitsystem.

4.2.1.1 1 och 2 kvantbitar

Vi betraktar först effekten som en Hadamardgrind har på ett basläge i ett 1-kvantbitsystem:

$$H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} = \frac{|0\rangle + (-1)^0|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i\pi \cdot 0}|1\rangle}{\sqrt{2}},$$

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} = \frac{|0\rangle + (-1)^1|1\rangle}{\sqrt{2}} = \frac{|0\rangle + e^{i\pi \cdot 1}|1\rangle}{\sqrt{2}}.$$

Vi sammanfattar det som att vi kodar in 0 och 1 i den relativa fasen;

$$H|x\rangle = \frac{|0\rangle + (-1)^x|1\rangle}{\sqrt{2}} = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{xy}|y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i \frac{x}{2} y}|y\rangle. \quad (1)$$

Vi ser det som att H har kodat in den binära strängen $x \in \{0,1\}$ i läget $|x\rangle$ in i den relativa fasen mellan baslägena. Lägg märke till att (1) är ekvivalent med att utföra QFT_2 på $|x\rangle$. Eftersom H är sin egen invers får vi att

$$H\Big(\frac{|0\rangle + (-1)^x|1\rangle}{\sqrt{2}}\Big) = H\Big(\frac{|0\rangle + \frac{e^{2\pi i \frac{x}{2}}}{\sqrt{2}}|1\rangle}{\sqrt{2}}\Big) = |x\rangle.$$

Det blir som en avkodning av informationen som finns i fasen.

Anta nu istället att vi har läget $|x\rangle$ då x är den binära strängen x_1x_2. $|x\rangle$ är då en basvektor i ett 2-kvantbitsystem som beskrivs av ett fyrdimensionellt Hilbertrum med basvektorer $|00\rangle, |01\rangle, |10\rangle, |11\rangle$. Vi kan prova att koda in den på samma sätt med tensorpodukten av två H-grindar:

$$(H \otimes H)|x\rangle = (H \otimes H)|x_1x_2\rangle = H|x_1\rangle \otimes H|x_2\rangle$$

$$\Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{x_1}}{\sqrt{2}}|1\rangle\Big) \otimes \Big(\frac{1}{\sqrt{2}}|0\rangle + \frac{(-1)^{x_2}}{\sqrt{2}}|1\rangle\Big) =$$

$$\Big(\frac{|0\rangle + e^{2\pi i\frac{x_1}{2}}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i\frac{x_2}{2}}|1\rangle}{\sqrt{2}}\Big) =$$

$$\Big(\frac{|0\rangle + e^{2\pi i\cdot 0,x_1}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i\cdot 0,x_2}|1\rangle}{\sqrt{2}}\Big). \tag{2}$$

Om vi tittar på vad vi får om vi utför en QFT_4 på läget $|x_1x_2\rangle$:

$$QFT_4|x_1x_2\rangle = \frac{1}{\sqrt{4}}\sum_{y=0}^{4-1} e^{2\pi i\frac{x_1x_2}{4}y}|y\rangle =$$

$$\tfrac{1}{\sqrt{4}}\big(e^{2\pi i\frac{x_1x_2}{4}0}|00\rangle + e^{2\pi i\frac{x_1x_2}{4}1}|01\rangle + e^{2\pi i\frac{x_1x_2}{4}2}|10\rangle + e^{2\pi i\frac{x_1x_2}{4}3}|11\rangle\big) =$$

{ Vi byter nämnarna i bråken i exponenterna till deras binära motsvarighet}

$$\tfrac{1}{\sqrt{4}}\big(e^{2\pi i\frac{x_1x_2}{(100)_2}(0)_2}|00\rangle + e^{2\pi i\frac{x_1x_2}{(100)_2}(1)_2}|01\rangle + e^{2\pi i\frac{x_1x_2}{(100)_2}(10)_2}|10\rangle + e^{2\pi i\frac{x_1x_2}{(100)_2}(11)_2}|11\rangle\big)$$

$$= \tfrac{1}{\sqrt{2^2}}(|00\rangle + e^{2\pi i\cdot 0,x_1x_2}|01\rangle + e^{2\pi i\cdot x_1,x_2}|10\rangle + e^{2\pi i(x_1,x_2+0,x_1x_2)}|11\rangle).$$

I uttrycket ovan kan vi förenkla termen $e^{2\pi i\cdot x_1,x_2}$ på följande sätt:

$$e^{2\pi i\cdot x_1,x_2} = e^{2\pi i\cdot x_1}e^{2\pi i\cdot 0,x_2} = 1^{x_1}e^{2\pi i\cdot 0,x_2} = e^{2\pi i\cdot 0,x_2}.$$

Då har vi uttrycket

$$\tfrac{1}{\sqrt{2^2}}(|00\rangle + e^{2\pi i\cdot 0,x_1x_2}|01\rangle + e^{2\pi i\cdot 0,x_2}|10\rangle + e^{2\pi i(x_1,x_2+0,x_1x_2)}|11\rangle)$$

i vilket vi kan skriva om $e^{2\pi i(x_1,x_2+0,x_1x_2)}$ som

$$e^{2\pi i(x_1,x_2+0,x_1x_2)} = e^{2\pi i\cdot x_1,x_2}e^{2\pi i\cdot 0,x_1x_2} = e^{2\pi i\cdot 0,x_2}e^{2\pi i\cdot 0,x_1x_2} = e^{2\pi(0,x_2+0,x_1x_2)}.$$

Vi har då kvar uttrycket

$$\tfrac{1}{\sqrt{2^2}}(|00\rangle + e^{2\pi i\cdot 0,x_1x_2}|01\rangle + e^{2\pi i\cdot 0,x_2}|10\rangle + e^{2\pi i(0,x_2+0,x_1x_2)}|11\rangle) =$$

$$\Big(\frac{|0\rangle + e^{2\pi i\cdot 0,x_2}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i\cdot 0,x_1x_2}|1\rangle}{\sqrt{2}}\Big). \tag{3}$$

Vi ser att det enda som skiljer sig mellan (2) och (3) är att den relativa fasen mellan baslägena i en av kvantbitarna och ordningen på kvantbitarna. Det är till och med så att fasen endast skiljer sig om $x_2 = 1$. Ordningen är inget större problem, allt vi behöver göra är att läsa av resultatet omvänt. För att justera fasen i (2) får vi användning för fasrotationsoperatorn, i det här fallet R_2 som har avbildningsmatrisen

$$\begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^2}} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0,01)_2} \end{pmatrix}.$$

Om $x_2 = 1$ och vi applicerar R_2 på den andra kvantbiten i (2) får vi

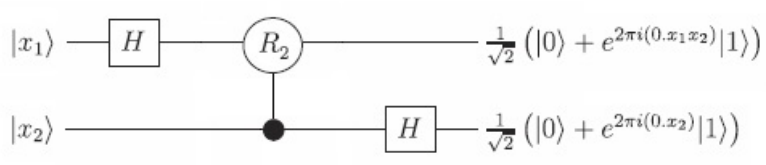
$$\begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0,0x_2)} \end{pmatrix} \Big(\frac{|0\rangle + e^{2\pi i 0,x_1}|1\rangle}{\sqrt{2}} \Big) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0,0x_2)} \end{pmatrix} \begin{pmatrix} 1 \\ e^{2\pi i(0,x_1)} \end{pmatrix} =$$

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ e^{2\pi i(0,x_1)} \end{pmatrix} = \Big(\frac{|0\rangle + e^{2\pi i 0,x_1 x_2}|1\rangle}{\sqrt{2}} \Big)$$

och har läget

$$\Big(\frac{|0\rangle + e^{2\pi i 0,x_1 x_2}|1\rangle}{\sqrt{2}} \Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i 0,x_2}|1\rangle}{\sqrt{2}} \Big).$$

Vi behöver bara ha en kontrollerad variant av R_2 som utförs om $x_2 = 1$ så har vi skapat en krets som utför QFT_4 på ett 2-kvantbitsystem. Figur 7 visar en sådan krets. Vi har nu sätt en idé för hur vi kan implementera QFT för



Figur 7: Kretsschema över QFT-kretsen för ett 2-kvantbitsystem.

2 kvantbitar och ska utveckla den till 3 kvantbitar.

4.2.1.2 3 kvantbitar Om vi har ett 3-kvantbitläge med läget $|x_1x_2x_3\rangle$ får vi på samma sätt som med 2-kvantbitläget att

$$(H \otimes H \otimes H)|x_1x_2x_3\rangle =$$

$$\Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_1}|1\rangle}{\sqrt{2}} \Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_2}|1\rangle}{\sqrt{2}} \Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_3}|1\rangle}{\sqrt{2}} \Big). \quad (4)$$

När vi i läget (4) applicerar en $c-R_2$ styrd av x_2 och en $c-R_3$ styrd av x_3 på den första kvantbiten får vi

$$\Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_1x_2x_3}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_2}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_3}|1\rangle}{\sqrt{2}}\Big).$$

Om vi sedan utför $c-R_2$ på den andra kvantbiten styrd av x_3 så får vi följande läge

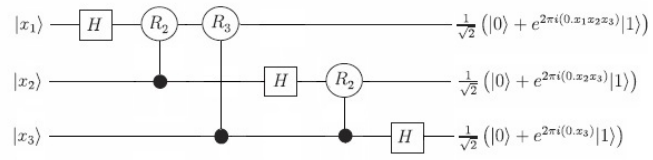
$$\Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_1x_2x_3}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_2x_3}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_3}|1\rangle}{\sqrt{2}}\Big).$$

Det är samma, bortsett från ordningen på kvantbitarna, som

$$QFT_8|x_1x_2x_3\rangle = \frac{1}{\sqrt{2^3}} \sum_{y=0}^{8-1} e^{2\pi i \frac{x_1x_2x_3}{8}y}|y\rangle =$$

$$\Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_3}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_2x_3}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_1x_2x_3}|1\rangle}{\sqrt{2}}\Big)$$

och kan realiseras med kretsen i figur 8. Vi har nu sett hur man kan implementera QFT för 2- respektive 3-kvantbitsystem och ska gå vidare till det generella fallet med n kvantbitar.



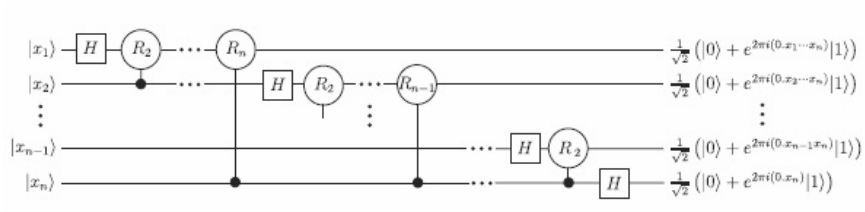
Figur 8: Kretsschema över QFT-kretsen för ett 3-kvantbitsystem.

4.2.1.3 n kvantbitar Om vi bygger ut kretsen vi byggt till en som opererar på lägen i ett n-kvantbitsystem får vi kretsen i figur 9 från [1] sid 117. Den kretsen kommer med läget $|x_1x_2\ldots x_n\rangle$ som indata att generera läget

$$\Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_1\ldots x_n}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_2\ldots x_n}|1\rangle}{\sqrt{2}}\Big) \otimes \cdots \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0,x_n}|1\rangle}{\sqrt{2}}\Big).$$

Bortsett från ordningen som vi kunde lösa har vi en fungerande krets för att realisera QFT_{2^n} om vi kan visa följande likhet:

$$QFT_{2^n}|x_1x_2\ldots x_n\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x_1x_2\ldots x_n}{2^n}y}|y\rangle =$$



Figur 9: Kretsschema över QFT-kretsen för ett n-kvantbitsystem.

$$\Big(\frac{|0\rangle + e^{2\pi i \frac{x_1 x_2 \dots x_n}{2^n} 2^{n-1}}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \frac{x_1 x_2 \dots x_n}{2^n} 2^{n-2}}|1\rangle}{\sqrt{2}}\Big) \otimes \dots$$
$$\otimes \Big(\frac{|0\rangle + e^{2\pi i \frac{x_1 x_2 \dots x_n}{2^n} 2}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \frac{x_1 x_2 \dots x_n}{2^n}}|1\rangle}{\sqrt{2}}\Big) =$$
$$\Big(\frac{|0\rangle + e^{2\pi i \cdot 0, x_n}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0, x_{n-1} x_n}|1\rangle}{\sqrt{2}}\Big) \otimes \dots$$
$$\otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0, x_2 \dots x_n}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0, x_1 \dots x_n}|1\rangle}{\sqrt{2}}\Big). \tag{5}$$

Istället för (5) kommer vi att bevis en mer generell likhet som täcker in (5). Vi byter också ut bråken i exponenterna mot ett godtyckligt långt binärt uttryck i decimalform. Vi får för $\phi = 0, x_1 x_2 \dots$

$$\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n - 1} e^{2\pi i \phi y}|y\rangle =$$

$$\Big(\frac{|0\rangle + e^{2\pi i \phi 2^{n-1}}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \phi 2^{n-2}}|1\rangle}{\sqrt{2}}\Big) \otimes \dots$$
$$\dots \otimes \Big(\frac{|0\rangle + e^{2\pi i \phi 2}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \phi}|1\rangle}{\sqrt{2}}\Big) =$$
$$\Big(\frac{|0\rangle + e^{2\pi i \cdot 0, x_n x_{n+1} \dots}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0, x_{n-1} x_n \dots}|1\rangle}{\sqrt{2}}\Big) \otimes \dots$$
$$\dots \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0, x_2 x_3 \dots}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0, x_1 x_2 \dots}|1\rangle}{\sqrt{2}}\Big). \tag{6}$$

Vi kommer att bevisa (6) med ett induktionsbevis. För att göra det lite lättare att följa med i omskrivningarna konstaterar vi tre saker.

Omskrivningar till beviset

(a) Om vi har en fas

$$e^{2\pi i(x_1x_2\ldots x_i,x_{i-1}\ldots)}$$

kan den skrivas om till

$$e^{2\pi i(x_1x_2\ldots x_i)+(0,x_{i-1}\ldots)} =$$

$$e^{2\pi i(x_1x_2\ldots x_i)}e^{2\pi i(0,x_{i-1}\ldots)} = 1e^{2\pi i(0,x_{i-1}\ldots)} = e^{2\pi i(0,x_{i-1}\ldots)}.$$

Det är samma förenkling vi såg i (3)

(b) Anta att variabeln y i den relativa fasen $e^{2\pi i\phi y}$ i termerna hos (6) skrivs i basen 2 som den binära strängen $y_ny_{n-1}\ldots y_1 = y_n2^{n-1}+y_{n-1}2^{n-2}+\cdots+y_1$. Vidare kan vi om $\phi = 0, x_1x_2\ldots$ göra följande omskrivning:

$$\phi y = \phi(y_n2^{n-1} + y_{n-1}2^{n-2} + \cdots + y_1) =$$

$$\phi y_n2^{n-1} + \phi y_{n-1}2^{n-2} + \cdots + \phi y_1 =$$

$$y_n(x_1x_2\ldots x_{n-1}, x_n\ldots) + y_{n-1}(x_1x_2\ldots x_{n-2}, x_{n-1}\ldots) + \ldots$$

$$\cdots + y_2(x_1, x_2\ldots) + y_1(0, x_1x_2\ldots).$$

Som med det vi vet från (a) förkortas exponenterna till

$$y_n(0, x_nx_{n-1}\ldots) + y_{n-1}(0, x_{n-1}x_{n-2}) + \ldots$$

$$\cdots + y_1(0, x_1x_2\ldots).$$

(c) För den halvan av de 2^n baslägena $|y\rangle$ i termerna hos (6) på formen $|1y_{n-1}\ldots y_1\rangle$, alltså där $y \geq 2^{n-1}$, har vi

$$e^{2\pi i\phi(1y_{n-1}\ldots y_1)}|1y_{n-1}\ldots y_1\rangle =$$

$$e^{2\pi i(\phi 2^{n-1}+\phi y_{n-1}2^{n-2}+\cdots+\phi y_1)}|1y_{n-1}\ldots y_1\rangle =$$

$$e^{2\pi i\phi 2^{n-1}}e^{2\pi i\phi(y_{n-1}\ldots y_1)}|1y_{n-1}\ldots y_1\rangle =$$

$$e^{2\pi i(x_1x_2\ldots x_{n-1},x_n\ldots)}e^{2\pi i\phi(y_{n-1}\ldots y_1)}|1y_{n-1}\ldots y_1\rangle =$$

$$e^{2\pi i(0,x_n\ldots)}e^{2\pi i\phi(y_{n-1}\ldots y_1)}|1y_{n-1}\ldots y_1\rangle.$$

Uttrycket ovan kan nu med axiomen för tensorprodukter skrivas om till

$$e^{2\pi i(0,x_n\ldots)}|1\rangle \otimes e^{2\pi i\phi(y_{n-1}\ldots\phi y_1)}|y_{n-1}\ldots y_1\rangle.$$

För de resterande 2^{n-1} termerna där $y_n = 0$ får vi

$$e^{2\pi i\phi(0y_{n-1}\ldots y_1)}|0y_{n-1}\ldots y_1\rangle = e^{2\pi i\phi(y_{n-1}\ldots y_1)}|0y_{n-1}\ldots y_1\rangle =$$

$$|0\rangle \otimes e^{2\pi i\phi(y_{n-1}\ldots y_1)}|y_{n-1}\ldots y_1\rangle$$

Så enligt axiomen för tensorprodukter kan (6) skrivas som

$$\Big(\frac{|0\rangle + e^{2\pi i(0,x_n\ldots)}|1\rangle}{\sqrt{2}}\Big) \otimes \frac{1}{\sqrt{2^{n-1}}}\sum_{y=0}^{2^{n-1}} e^{2\pi i\phi y}|y\rangle.$$

Sats och bevis till QFT

Sats 1. *För godtyckligt långa värden* $\phi = 0, x_1x_2\ldots$ *och* $n \in \mathbb{Z}^+ \setminus \{0\}$ *gäller* (6).

Bevis. Vi bevisar (6) med hjälp av induktion.
Induktionsbas:
n=1

$$\sum_{y=0}^{1} e^{2\pi i\phi y}|y\rangle = \Big(\frac{|0\rangle + e^{2\pi i(0,x_1x_2\ldots)}|1\rangle}{\sqrt{2}}\Big)$$

n=2

$$\frac{1}{\sqrt{4}}\sum_{y=0}^{4-1} e^{2\pi i\phi y}|y\rangle = \Big(\frac{|0\rangle + e^{2\pi i\cdot 0,x_2x_3\ldots}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i\cdot 0,x_1x_2\ldots}|1\rangle}{\sqrt{2}}\Big)$$

Så (6) gäller för $n = 1$ och $n = 2$.
Induktionshypotes:
Vi antar att (6) gäller för $n = k$ för något godtyckligt heltal $0 < k$.
n=k

$$\frac{1}{\sqrt{2^k}}\sum_{y=0}^{2^k-1} e^{2\pi i\phi y}|y\rangle =$$

$$\Big(\frac{|0\rangle + e^{2\pi i\phi 2^{k-1}}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i\phi 2^{k-2}}|1\rangle}{\sqrt{2}}\Big) \otimes \ldots$$

$$\cdots \otimes \Big(\frac{|0\rangle + e^{2\pi i\phi 2}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i\phi}|1\rangle}{\sqrt{2}}\Big) =$$

$$(\frac{|0\rangle + e^{2\pi i0\cdot,x_kx_{k+1}\cdots}|1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle + e^{2\pi i\cdot 0,x_{k-1}x_k\cdots}|1\rangle}{\sqrt{2}}) \otimes \ldots$$

$$\cdots \otimes (\frac{|0\rangle + e^{2\pi i\cdot 0,x_2x_3\cdots}|1\rangle}{\sqrt{2}}) \otimes (\frac{|0\rangle + e^{2\pi i\cdot 0,x_1x_2\cdots}|1\rangle}{\sqrt{2}}).$$

Induktionssteg:
Vi vill nu visa att(6) gäller för $n = k + 1$.
n=k+1

$$\frac{1}{\sqrt{2^{k+1}}}\sum_{y=0}^{2^{k+1}-1} e^{2\pi i\phi y}|y\rangle = \frac{1}{\sqrt{2^{k+1}}}(|00\ldots00\rangle + e^{2\pi i\phi}|00\ldots01\rangle + \ldots$$

$$\cdots + e^{2\pi i\phi(2^{k+1}-2)}|11\ldots10\rangle + e^{2\pi i\phi(2^{k+1}-1)}|11\ldots11\rangle) =$$

$$= \frac{1}{\sqrt{2^{k+1}}}(|00\ldots00\rangle + e^{2\pi i\phi(1)}|00\ldots01\rangle + \ldots$$

$$\cdots + e^{2\pi i\phi(11\ldots10)}|11\ldots10\rangle + e^{2\pi i\phi(11\ldots11)}|11\ldots11\rangle) =$$

{Vi utvecklar exponenterna enl. (b)}

$$\tfrac{1}{\sqrt{2^{k+1}}}(|00\ldots00\rangle + e^{2\pi i(0,x_1x_2\ldots)}|00\ldots01\rangle + \ldots$$

$$\ldots + e^{2\pi i((0,x_{k+1}x_{k+2}\ldots)+(0,x_kx_{k+1}\ldots)+\cdots+(0,x_3x_4\ldots)+(0,x_2x_3\ldots))}|11\ldots10\rangle +$$

$$e^{2\pi i((0,x_{k+1}x_{k+2}\ldots)+(0,x_kx_{k+1}\ldots)+\cdots+(0,x_2x_3\ldots)+(0,x_1x_2\ldots))}|11\ldots11\rangle) =$$

{Vi använder oss nu av (c) för att bryta ut $|0\rangle + e^{2\pi i(0,x_{k+1}x_{k+2}\ldots)}|1\rangle$ och får}

$$\Big(\frac{|0\rangle + e^{2\pi i\cdot 0,x_{k+1}x_{k+2}\cdots}|1\rangle}{\sqrt{2}}\Big) \otimes \tfrac{1}{\sqrt{2^k}}(|0\ldots00\rangle + e^{2\pi i(0,x_1x_2\ldots)}|0\ldots01\rangle + \ldots$$

$$\ldots + e^{2\pi i((0,x_kx_{k+1}\ldots)+\cdots+(0,x_3x_4\ldots)+(0,x_2x_3\ldots))}|1\ldots10\rangle +$$

$$e^{2\pi i((0,x_kx_{k+1}\ldots)+\cdots+(0,x_2x_3\ldots)+(0,x_1x_2\ldots))}|1\ldots11\rangle) =$$

{ Nu använder oss av (b) baklänges}

$$\Big(\frac{|0\rangle + e^{2\pi i\phi 2^k}|1\rangle}{\sqrt{2}}\Big) \otimes \tfrac{1}{\sqrt{2^k}}(|0\ldots00\rangle + e^{2\pi i\phi}|0\ldots01\rangle + \ldots$$

$$\ldots + e^{2\pi i\phi(2^k-2)}|1\ldots10\rangle + e^{2\pi i\phi(2^k-1)}11\ldots11\rangle) =$$

$$\Big(\frac{|0\rangle + e^{2\pi i\phi 2^k}|1\rangle}{\sqrt{2}}\Big) \otimes \frac{1}{\sqrt{2^k}}\sum_{y=0}^{2^k-1} e^{2\pi i\phi y}|y\rangle =$$

$$\Big(\frac{|0\rangle + e^{2\pi i\phi\cdot 2^k}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i\phi\cdot 2^{k-1}}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi\cdot i\phi 2^{k-2}}|1\rangle}{\sqrt{2}}\Big) \otimes \ldots$$

$$\ldots \otimes \Big(\frac{|0\rangle + e^{2\pi i\phi\cdot 2}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i\phi}|1\rangle}{\sqrt{2}}\Big)$$

Detta tillsammans med principen för induktion visar att (6) gäller för godtyckliga heltal $n > 0$. □

Nu vet vi hur vi ska implementera QFT_{2^n}. Vi kan på så sätt koda in information i den relativa fasen till basvektorer i ett system. Med hjälp av unitära 1-kvantbitgrindar och utifrån det vi vet kan vi lätt skapa dess invers $QFT_{2^n}^{-1}$. Det gör vi genom att gå igenom kretsen baklänges och byta ut alla grindar mot deras inverser. Inversens krets kommer alltså att bestå av samma Hadamardgrindar fast med fasrotationsgrindar R_n^{-1} som justerar fasen med $e^{-\frac{2\pi i}{2^n}}$. $QFT_{2^n}^{-1}$ kommer som resultat att ge oss en uppskattning av fasen i ett läge i omvänd ordning. I nästa avsnitt studerar vi inversen mer detaljerat.

4.2.2 Inversen och fasuppskattning

När vi faktoriserar kommer vi utnyttja den relativa fasen i lägena hos kvantbitar[13]. $QFT_{2^n}^{-1}$ ger oss som vi ska se en uppskattning av den relativa fasen. Det är här vi får användning av inversen till QFT_{2^n}. Vi påminner om hur QFT^{-1} ser ut,

$$QFT_{2^n}^{-1} : |x\rangle \longmapsto \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{-2\pi i \frac{x}{2^n} y} |y\rangle.$$

Betrakta läget

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x_1 x_2 \dots x_n}{2^n} y} |y\rangle$$

för en godtycklig sekvens $x_1 \dots x_n$ av ettor och nollor. Utför vi $QFT_{2^n}^{-1}$ på $|\psi\rangle$ kommer vi att få följande:

$$QFT_{2^n}^{-1}|\psi\rangle = QFT_{2^n}^{-1} \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x_1 x_2 \dots x_n}{2^n} y} |y\rangle = |x_n x_{n-1} \dots x_1\rangle.$$

Vi får alltså värdet på $x_1 \dots x_n$ i omvänd ordning, kom ihåg hur det var för QFT. Den omvända ordningen löser vi igen genom att döpa om $x_n x_{n-1} \dots x_1$. För att göra det lite tydligare går igenom ett exempel.

Exempel 14. *Säg att vi har läget*

$$|\psi\rangle = \frac{1}{\sqrt{2^3}} \sum_{y=0}^{2^3-1} e^{2\pi i \frac{x_1 x_2 x_3}{2^3} y} |y\rangle =$$

$$\Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_3}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_2 x_3}|1\rangle}{\sqrt{2}}\Big) \otimes \Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_1 x_2 x_3}|1\rangle}{\sqrt{2}}\Big)$$

och $QFT_{2^3}^{-1}$ implementerad på ett 3-kvantbitläge. Se figur 10 hämtad från [1] sid 115 för. $QFT_{2^3}^{-1}$:s kretsschema.

Om vi applicerar $QFT_{2^3}^{-1}$ på $|\psi\rangle$ kommer en Hadamardgrind att appliceras på den första kvantbiten och avbilda dess läge till

$$H\Big(\frac{|0\rangle + e^{2\pi i 0.x_3}|1\rangle}{\sqrt{2}}\Big) = |x_3\rangle.$$

På den andra kvantbiten kommer vi först att applicera rotationsgrinden R_2^{-1} om $x_3 = 1$ och sedan en Hadamardgrind. Kom ihåg från förra avsnittet att R_k^{-1} multiplicerar den relativa fasen med $e^{2\pi i \frac{1}{2^k}}$. Vi har två olika sätt $QFT_{2^3}^{-1}$ kan avbilda den andra kvantbitens läge:

[13] Se avsnitt 11.5.3 i [15] och 7.1 i [1].

1. ***För*** $x_3 = 0$***:***

$$H\Big(R_{2^2}^{-1}\Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_2x_3}|1\rangle}{\sqrt{2}}\Big)\Big) = H\Big(R_{2^2}^{-1}\Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_20}|1\rangle}{\sqrt{2}}\Big)\Big) =$$

$$= H\Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_2}|1\rangle}{\sqrt{2}}\Big) = |x_2\rangle$$

2. ***För*** $x_3 = 1$***:***

$$H\Big(R_{2^2}^{-1}\Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_2x_3}|1\rangle}{\sqrt{2}}\Big)\Big) = H\Big(R_{2^2}^{-1}\Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_21}|1\rangle}{\sqrt{2}}\Big)\Big) =$$

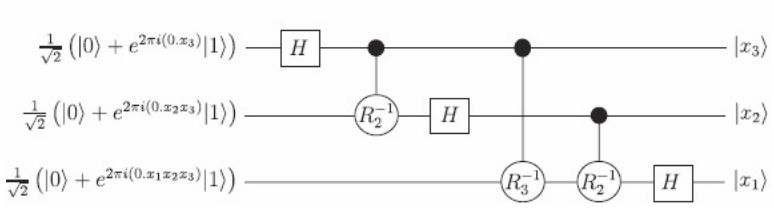
$$= H\Big(\frac{|0\rangle + e^{-2\pi i \cdot 0.01}e^{2\pi i \cdot 0.x_21}|1\rangle}{\sqrt{2}}\Big) = H\Big(\frac{|0\rangle + e^{2\pi i(0.x_21 - 0.01}|1\rangle}{\sqrt{2}}\Big) =$$

$$H\Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_2}|1\rangle}{\sqrt{2}}\Big) = |x_2\rangle$$

Den tredje kvantbitens läge avbildar vi på samma sätt som den andra kvantbitens läge men drar också bort x_2 *om den är 1. Vi får läget*

$$H\Big(R_2^{-1}\Big(R_3^{-1}\Big(\frac{|0\rangle + e^{2\pi i \cdot 0.x_1x_2x_3}|1\rangle}{\sqrt{2}}\Big)\Big)\Big) = |x_1\rangle.$$

Resultat av att applicera $QFT_{2^3}^{-1}$ *på* $|\psi\rangle$ *blir alltså läget* $|x_3x_2x_1\rangle$ *som vi får vända på för att få det korrekta värdet på* $x_1x_2x_3$*.*



Figur 10: Kretsschema över $QFT_{2^3}^{-1}$-kretsen för ett 3-kvantbitsystem.

Vi vet hur vi kan få fram information om ett tal ϕ i en relativ fas $e^{2\pi i\phi}$ om ϕ är på formen $\frac{x}{2^n}$ för något heltal $x \in \{0, 1, \ldots, 2^n - 1\}$. För andra värden på ϕ som inte är en heltalsmultipel av $\frac{1}{2^n}$ kommer vi att få en uppskattning $\frac{x}{2^n}$ av ϕ. Uppskattningen betecknar vi $\widetilde{\phi}$. Om vi implementerar $QFT_{2^n}^{-1}$ med n kvantbitar så kommer de olika uppskattningarna $\widetilde{\phi}$ av ϕ vi kan få från $QFT_{2^n}^{-1}$ att vara tal $\frac{x}{2^n}$ där $x \in \{0, 1, \ldots, 2^n - 1\}$. Med sannolikhet $\frac{4}{\pi^2}$ (se [1] avsnitt 7.1.1 för motiveringen till just denna sannolikhet) kommer vi få den uppskattning $\widetilde{\phi} = \frac{x}{2^n}$ som ligger närmast ϕ. Om ϕ ligger precis mitt emellan $\frac{x}{2^n}$ och $\frac{x+1}{2^n}$ så kommer vi få $\widetilde{\phi} = \frac{x}{2^n}$ eller $\widetilde{\phi} = \frac{x+1}{2^n}$ med sannolikhet $\frac{8}{\pi^2}$ (se [1] avsnitt 7.1.1 för motiveringen till denna sannolikhet).

Exempel 15. *Om vi vill uppskatta*

$$\phi = \frac{1}{6} = (0.166666666\ldots)_{10} = (0.001010101\ldots)_2$$

i läget

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\phi i y}|y\rangle =$$

med $QFT_{2^n}^{-1}$*, så börjar vi med att välja* $n = 7$*. I avsnitt 5.2 går vi igenom hur vi ska välja* n *på ett bra sätt men låt oss tro att* $n = 7$ *duger i det här fallet. Då kommer* $QFT_{2^7}^{-1}$ *att kunna ge en uppskattningar* $\frac{x}{2^7}$ *där* $x \in \{0, 1, \ldots, 2^7-1\}$*. Uppskattningen* $\frac{21}{2^7}$ *är den uppskattning av* $\frac{1}{6}$ *som ligger närmast* $\frac{1}{6}$ *där*

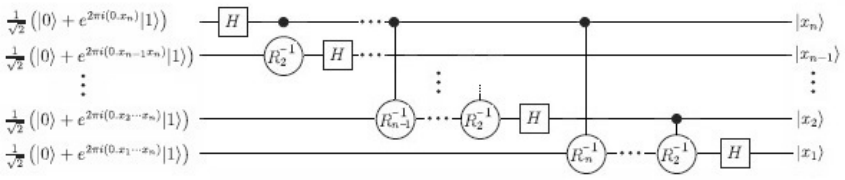
$$\frac{(21)_{10}}{(2^7)_{10}} = \frac{(21)_{10}}{(128)_{10}}(0.1640625)_{10} = (0.0010101)_2 = \frac{(10101)_2}{(10000000)_2} < \frac{(1)_{10}}{(6)_{10}}.$$

$QFT_{2^7}^{-1} : |\psi\rangle$ *kommer alltså att ge*

$$QFT_{2^7}^{-1}\Big(\frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\phi i y}|y\rangle\Big) = |0010101\rangle.$$

När vi mäter kollapsar systemet och mätinstrumentet visar värdet 0010101*. Värdet* 0010101 *ska tolkas som* $(\frac{0010101}{10000000})_2 = (\frac{21}{128})_{10}$

Detta gås igenom mer noggrant i [1] avsnitt 7.1.1 för den som vill veta mer. Figur 11 visar kretsschemat ser ut för inversen $QFT_{2^n}^{-1}$.



Figur 11: Kretsschema över $QFT_{2^n}^{-1}$-kretsen för ett n-kvantbitsystem.

4.3 Egenvärdesuppskattning

I det här avsnittet går vi igenom en algoritm för hur man med hjälp av QFT kan uppskatta egenlägens motsvarande egenvärden till en operator U[14]. Algoritmen kallas egenvärdesuppskattningsalgoritmen och förkortas EUA. I avsnitt 4.1 gick vi igenom hur man flyttar egenvärden. Det gör vi med en kontrollerad grind c-U av en operator U som vi applicerar på ett egenläge

[14]Se [1] avsnitt 7.2, [17] 3.7 och [15] 11.5.3.

$|\varphi\rangle$. Egenvärdet flyttas då till styrkvantbiten. Nu ska vi se hur vi kan använda egenvärdesförflyttning för att uppskatta egenvärden till en operator med motsvarande egenlägen.

Anta att vi har en n-kvantbitoperator U med egenläget $|\varphi\rangle$ och motsvarande egenvärde $e^{2\pi i\omega}$. Om vi implementerar c-U och låter c-U operera på $|\varphi\rangle$ med en superposition $\alpha_0|0\rangle + \alpha_1|1\rangle$ som styrkvantbit får vi

$$c\text{-}U((\alpha_0|0\rangle + \alpha_1|1\rangle)(|\varphi\rangle)) = c\text{-}U(\alpha_0|0\rangle|\varphi\rangle) + c\text{-}U(\alpha_1|1\rangle|\varphi\rangle)$$

$$(\alpha_0|0\rangle|\varphi\rangle) + \alpha_1|1\rangle U(|\varphi\rangle)) = (\alpha_0|0\rangle + e^{2\pi i\omega}\alpha_1|1\rangle)(|\varphi\rangle).$$

Vi vet att vi kan läsa av ω i egenvärdet med QFT^{-1} men då måste ω finnas i ett läge på formen

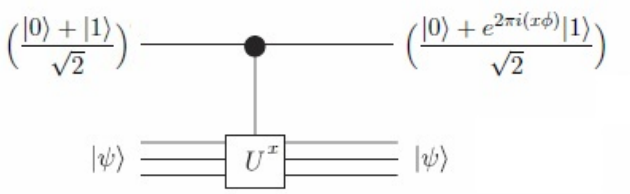
$$\frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^{n-1}} e^{2\pi i\omega y}|y\rangle =$$

$$\Big(\frac{|0\rangle + e^{2\pi i(2^{n-1}\omega)}|1\rangle}{\sqrt{2}}\Big)\Big(\frac{|0\rangle + e^{2\pi i(2^{n-2}\omega)}|1\rangle}{\sqrt{2}}\Big)\cdots\Big(\frac{|0\rangle + e^{2\pi i(\omega)}|1\rangle}{\sqrt{2}}\Big). \qquad (7)$$

För att kunna skapa detta läge behöver vi först konstatera att $|\varphi\rangle$ också är ett egenläge till U^x med egenvärdet $e^{x2\pi i\omega}$. U^x är den operator som applicerar U x antal gånger på ett n-kvantbitläge. Den kontrollerade varianten c-U^x med styrkvantbit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ gör alltså följande

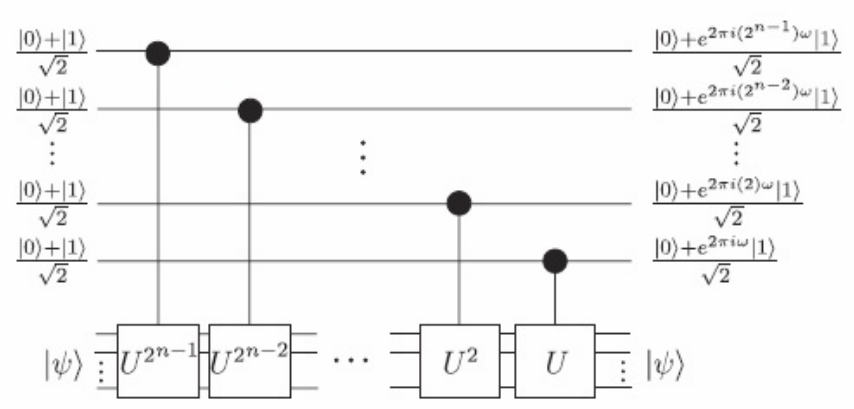
$$c\text{-}U^x\Big(\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big)|\varphi\rangle\Big) = \Big(\frac{|0\rangle + e^{2\pi i(x\omega)}|1\rangle}{\sqrt{2}}\Big)|\varphi\rangle.$$

Ovan har vi använt $|+\rangle$ från Hadamardbasen som styrkvantbit. Kretsen för c-U^x illustreras i Figur 12. Vi ser att lägesvektorn för kontrollkvantbiten liknar de från kvantbitarna i (7). Om vi sätter $x = 2^j$ för $j \in \{0, \ldots, n-1\}$ kan vi skapa varje kvantbits läge i (7) med n stycken c-U^{2^j}-grindar, se figur 13 och 14 för kretsen. Vi behöver alltså följande kontrolläge

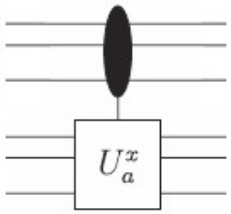


Figur 12: Kretsschema över operatorn c-U^x.

$$\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big)\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big)\cdots\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big) = \Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big)^{\otimes n} \qquad (8)$$



Figur 13: Kretsschema över operatorerna c-U^x.



Figur 14: Kompaktare sätt att rita kretsen i figur 13.

där varje kvantbit används som kontrollkvantbit till en av grindarna c-U^{2^j}. Läget (8) skapar vi lätt genom att applicera QFT_{2^n} på läget $|0\ldots0\rangle = |0\rangle^{\otimes n}$:

$$QFT_{2^n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1} e^{2\pi i\frac{0}{2^n}y}|y\rangle =$$

$$\Big(\frac{|0\rangle + e^{2\pi i\frac{0}{2^n}2^{n-1}}|1\rangle}{\sqrt{2}}\Big)\Big(\frac{|0\rangle + e^{2\pi i\frac{0}{2^n}2^{n-2}}|1\rangle}{\sqrt{2}}\Big)\cdots\Big(\frac{|0\rangle + e^{2\pi i\frac{0}{2^n}2}|1\rangle}{\sqrt{2}}\Big) =$$
$$\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big)\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big)\cdots\Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big) = \Big(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\Big)^{\otimes n}.$$

När vi sedan applicerar alla c-U^{2^j} på egenläget $|\varphi\rangle$ kommer styrläget att bli på samma form som (7). I ett styrläge på formen (7) kan vi uppskatta ω med $QFT_{2^n}^{-1}$.

Vi har alltså en n-kvantbitoperator U och den kontrollerade versionen c-U med egenläge $|\varphi\rangle$ och motsvarande egenvärde $e^{2\pi i\omega}$. Vi förbereder läget

$|0\rangle^{\otimes n}|\varphi\rangle$ där $|0\rangle^{\otimes n}$ ska vara styrläge och $|\varphi\rangle$ målläge. Applicerar vi EUA av U på läget $|0\rangle^{\otimes n}|\varphi\rangle$ kommer först QFT_{2^n} appliceras på läget $|0\rangle^{\otimes n}$ och avbilda det till $(\frac{|0\rangle+|1\rangle}{\sqrt{2}})^{\otimes n}$. Sedan applicerar alla n stycken $c\text{-}U^{2^j}$ för $j \in \{0, \ldots, n-1\}$ på läget $|\varphi\rangle$ med $(\frac{|0\rangle+|1\rangle}{\sqrt{2}})^{\otimes n}$ som styrläge. Appliceringen av $c\text{-}U^{2^j}$ flyttar egenvärdena $e^{2\pi i\omega 2^j}$ till styrläget. Styrläget ser då ut som läget (7). Sist appliceras $QFT_{2^n}^{-1}$ på styrläget att uppskatta ω i egenvärdena. EUA ger följande avbildning

$$|0\rangle|\varphi\rangle \to |\widetilde{\omega}\rangle|\varphi\rangle.$$

Värdet $\widetilde{\omega}$ är uppskattningen av ω, kom ihåg från avsnitt 4.2.2 att $QFT_{2^n}^{-1}$ ger en uppskattning. Mäter vi styrläget efter att utfört EUA kommer vi att få uppskattningen $\widetilde{\omega}$. Tanken är att vi i nästa kapitel ska skapa en operator U med egenvärden som innehåller information som hjälper oss att faktorisera tal.

5 Talteori

I det här kapitlet ska vi till en början gå igenom grundläggande talteori[15]. Vi går igenom vad *ordningen* av tal är. Sedan visar vi att vi med ordningen för vissa tal kan faktorisera. Vi kommer sedan att visar hur vi kan få fram bråk med information om ordningen från EUA. Ur dessa bråk kan vi då erhålla ordningen med hjälp av teorin om kedjebråk som avslutar kapitlet.

5.1 Faktorisering av heltal

Innan vi motiverar varför ordningen av tal är av intresse ska vi definiera den.

Definition 6. *Låt a och N vara positiva heltal med $SGD(a, N) = 1$. Ordningen definieras då som det minsta positiva heltalet r sådan att*

$$a^r \equiv 1 \bmod N$$

Vi kommer också att ha hjälp av *treregeln*. Om man har ett tal så är det delbart med 3 om summan av talets siffor är delbart med 3.

Exempel 16. *Vi har talet $288 = 3 \cdot 96$ så får vi att*

$$2 + 8 + 8 = 18,\ 3|18 \Rightarrow 3|288.$$

5.1.1 Den klassiska delen

En del steg i faktoriseringen av heltal kan vi göra på en klassik dator. De stegen går vi igenom i det här avsnittet. När vi vill faktorisera ett heltal så är det först några saker vi bör tänka på. Ska vi faktorisera positiva heltal vill vi hitta en faktor M_1 till heltalet M, dividera ut M_1 och så vi får ett till tal M_2 sådant att $M = M_1 \times M_2$. Sedan går vi vidare och faktoriserar ut M_1 och M_2 tills vi bara har primtalsfaktorer kvar. Alla jämna heltal har den triviala primtalsfaktorn 2. Problemet reduceras därför till att faktorisera udda heltal. Ska vi faktorisera ett heltal börjar vi med att faktorisera ut alla faktorer 2. Det udda talet vi får kvar kallar vi N.

Är N ett primtal är vi klara, därför testar vi först om så är fallet. Vi kan testa det effektivt med en klassisk dator genom att försöka dividera N med alla heltal från 3 till $\sqrt{N}$. Går någon division jämnt ut är N ett primtal och vi är klara. Är N inte ett primtal fortsätter vi med att testa om N är ett primtal upphöjt i något positivt heltal k.

Vi kan snabbt testa det genom att först utesluta basen 3 med treregeln. Vidare så har vi att om $N = p^k$ för något primtal p och något positivt heltal

[15]Se [1] avsnitt 7.3.2, i [17] 3.4 och 3.5, i [16] 10.3, i [15] 11.5.1, i [3] kapitel 8 och i [11] kapitel 2 och 3.

k gäller det att $k \log_2 p = \log_2 N$. Om $5 \leq p$ så har vi att $2 \leq \log_2 5 \leq \log_2 p$ och

$$k = \frac{\log_2 N}{\log_2 p} \leq \frac{\log_2 N}{\log_2 5} \leq \frac{\log_2 N}{2}.$$

Om $N = p^k$ och $5 \leq p$ kommer alltså k att uppfylla olikheten $2 \leq k \leq \frac{\log_2 N}{2}$. Tar vi nu k:te roten ut N för alla k:na och resultatet är ett primtal så är N ett primtal upphöjt i k. I det fallet har vi hittat alla faktorer och är därmed klara. Är N inte ett primtal upphöjt i k går vi vidare.

Nu vill vi hitta två faktorer N_1 och N_2 till N där $2 < N_1 < N$, $2 < N_2 < N$ och $N = N_1 \times N_2$. För att göra det väljer vi ett slumpmässigt $a < N$. Är $SGD(a, N) > 1$ har vi hittat en icketrivial faktor och är klara. SGD kan man beräkna effektivt med den utvecklade euklidiska algoritmen på en klassisk dator. Om $SGD(a, N) = 1$ kommer vi inte längre med en klassisk dator om vi vill faktorisera effektivt. Kan vi däremot hitta ordningen r av a så att $a^r \equiv 1 \bmod N$ kan vi fortsätta och faktorisera klart.

5.1.2 Varför ordningen

Senare i kapitlet går vi igenom hur vi kan hitta ordningen med hjälp av kvantdatorn. Nu visar vi hur vi kan använda oss av ordningen när vi faktoriserar. Anta att vi vet ett effektivt sätt att beräkna ordningen r på. Då kan vi använda r för att hitta en icketrivial faktor på följande vis;
Börja med att kolla om r är udda. Om så är fallet börjar vi om, vi vill nämligen titta på kvadratrötter $a^{r/2}$. Är r jämn gäller följande:

$$a^r \equiv 1 \bmod N \Leftrightarrow a^r - 1 \equiv 0 \bmod N \Rightarrow (a^{r/2} + 1)(a^{r/2} - 1) \equiv 0 \bmod N.$$

Är $a^{r/2} \equiv 1, -1 \bmod N$ så börjar vi om med ett annat a. Annars sätter vi $b = SGD((a^{r/2} - 1), N)$. Då gäller det att b måste vara en äkta gemensam faktor till $a^{r/2} - 1$ och N. För det kan inte vara så att $b = N$, för då är $a^{r/2} - 1 \equiv 0 \bmod N$. Det är ekvivalent med att $a^{r/2} \equiv 1 \bmod N$ vilket vi redan uteslutit. Det kan inte häller vars så $b = 1$ för då existerar det heltal u och v sådana att

$$(a^{r/2} - 1)u + Nv = 1. \tag{9}$$

Multiplicerar vi (9) med $a^{r/2} + 1$ på båda sidorna får vi

$$(a^r - 1)u + (a^{r/2} + 1)Nv = a^{r/2} + 1.$$

Eftersom $N|(a^r - 1)$ så måste det vara så att $N|a^{r/2} + 1$. Det betyder att $a^{r/2} + 1 \equiv 0 \bmod N$, vilket är ekvivalent med att $a^{r/2} \equiv -1 \bmod N$ som vi också uteslutit. Alltså är b en äkta delare till N och vi kan faktorisera upp N till b och N_1. Sedan fortsätter vi att på samma sätt faktorisera b och N_1 tills vi bara har primtalsfaktorer kvar. Analogt kan vi kolla $b = SGD(a^{\frac{r}{2}} + 1, N)$. Samtliga beräkningar i det här avsnittet förutom att hitta ordningen av a kan göras effektivt med en klassisk dator. Det är alltså ordningen vi behöver kvantdatorns hjälp att hitta.

5.1.3 Uppskattning av ordningen av tal

De algoritmer vi hittills gått igenom kan användas för att ta reda på ordningen r av ett tal a[16]. Betrakta operatorn U_a med följande avbildning:

$$U_a|s\rangle \longmapsto |sa \bmod N\rangle \; s < N$$

$$U_a|s\rangle \longmapsto |s\rangle \; 0 \leq s \geq N.$$

U_a implementeras med n kvantbitar så att $2^n > N$ Vi kommer endast att studera U_a på lägena $\{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$. Eftersom $a^r \equiv 1 \bmod N$ fås, om U_a appliceras r gånger,

$$U_a^r|s\rangle \longmapsto |sa^r \bmod N\rangle = |s\rangle.$$

Vilket är ekvivalent med att

$$U_a^r|s\rangle \Leftrightarrow I|s\rangle.$$

Det innebär att U_a är en "r:te rot av identitetsoperatorn", det vill säga $U_a^r = I$. Egenvärdena till I är 1. Eftersom U_a^r har samma egenvärden som I kommer U_a att ha egenvärden som är r:te rötter av 1. Följande lemma från [2], sid 365, visar detta.

Lemma 1. *Låt r vara ett positivt heltal, U en operator med egenläge $\boldsymbol{x}$ och motsvarande egenvärde λ. Då gäller det att U^r har egenläget $\boldsymbol{x}$ med motsvarande egenvärde λ^r.*

Bevis. Vi har att

$$U\mathbf{x} = \lambda\mathbf{x} \Rightarrow U^r\mathbf{x} = U^{r-1}(U\mathbf{x}) = U^{r-1}\lambda\mathbf{x} = \lambda U^{r-2}(U\mathbf{x}) = \lambda^2 U^{r-2}\mathbf{x} = \ldots$$

$$\cdots = \lambda^{r-1}(U\mathbf{x}) = \lambda^{r-1}(\lambda\mathbf{x}) = \lambda^r\mathbf{x}.$$

□

Sats 2. *Egenvärdena till en operator U som uppfyller $U^r = I$ är vara r:te rötter av 1.*

Bevis. Om λ är ett egenvärde till U med motsvarande egenläge $\mathbf{x}$ och $U^r = I$ så fås (enligt lemma 1) att

$$U^r\mathbf{x} = \lambda^r\mathbf{x} \Leftrightarrow I\mathbf{x} = \lambda^r\mathbf{x}.$$

Identitetsoperatorns egenvärden är $\lambda^r = 1$. Det betyder att U har egenvärden $\lambda = \sqrt[r]{1}$ till motsvarande egenläget $\mathbf{x}$. $\sqrt[r]{1}$ är tal på formen $e^{2\pi i\frac{k}{r}}$ för $k \in \{0, 1, \ldots, r-1\}$. □

[16] Se avsnitt 7.3.3 i [1], 1.5 i [5] och 11.5.1 i [15].

Anta att vi har följande läge

$$|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^s \bmod N\rangle. \tag{10}$$

Om U_a appliceras på (10) så får vi följande

$$U_a|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} U_a|a^s \bmod N\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^{s+1} \bmod N\rangle =$$

$$\frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r}(s+1-1)} |a^{s+1} \bmod N\rangle =$$

$$e^{2\pi i \frac{k}{r}} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r}(s+1)} |a^{s+1} \bmod N\rangle =$$

{ Eftersom $e^{-2\pi i \frac{k}{r} r}|a^r \bmod N\rangle = e^{-2\pi i \frac{k}{r} 0}|a^0 \bmod N\rangle$ får vi }

$$e^{2\pi i \frac{k}{r}} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^s \bmod N\rangle = e^{2\pi i \frac{k}{r}} |u_k\rangle.$$

Det betyder att $|u_k\rangle$ är en egenvektor till U_a med egenvärde $e^{2\pi i \frac{k}{r}}$. I avsnitt 4.3 såg vi hur man får en uppskattning av egenvärden med EUA. EUA kommer med operatorn U_a och egenläget $|u_k\rangle$ att ge en uppskattning $\frac{\widetilde{k}}{r}$ av $\frac{k}{r}$ genom läget

$$|0\rangle|u_k\rangle \longmapsto |\tfrac{\widetilde{k}}{r}\rangle|u_k\rangle.$$

Hur vi kan använda $\frac{\widetilde{k}}{r}$ för att få fram ordningen r går vi igenom i avsnitt 5.2. Egenläget $|u_k\rangle$ kan inte skapas för något godtyckligt $k \in \{0, \ldots, r-1\}$ utan att veta r. Däremot räcker det, som vi snart ska se, att förbereda en likformig superpositionen som innehåller varje egenvärde. Betrakta den likformiga superpositionen

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle = \frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{-2\pi i \frac{k}{r} s} |a^s \bmod N\rangle.$$

Vi visa följande lemma:

Lemma 2. *Om*

$$|u_k\rangle = \frac{1}{\sqrt{r}} \sum_{s=0}^{r-1} e^{2\pi i \frac{k}{r} s} |a^s \bmod N\rangle,$$

gäller även att

$$\frac{1}{\sqrt{r}} \sum_{k=0}^{r-1} |u_k\rangle = |1\rangle$$

Bevis. Vi har läget

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}\frac{1}{\sqrt{r}}\sum_{s=0}^{r-1}e^{2\pi i\frac{k}{r}s}|a^s \bmod N\rangle. \tag{11}$$

Observera att

$$|a^s \bmod N\rangle = |1\rangle \Leftrightarrow s \equiv 0 \bmod r.$$

Amplituden för $|1\rangle$ i läget (11) är summan av termerna $\frac{1}{\sqrt{r}}\frac{1}{\sqrt{r}}e^{2\pi i\frac{k}{r}s}$ där $s \equiv 0 \bmod r$. I (11) finns bara ett sådant värde på s och det är $s = 0$. Vi har att

$$\frac{1}{\sqrt{r}}\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}e^{2\pi i\frac{k}{r}0} = \frac{1}{r}\sum_{k=0}^{r-1}1 = 1.$$

Amplituden för $|1\rangle$ är 1 alltså måste amplituden för alla andra lägestermer i (11) vara 0. Det vill säga

$$\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle = |1\rangle$$

givet att (11) faktiskt är ett läge. □

Detta betyder att EUA avbildar på följande sätt

$$|0\rangle|1\rangle = |0\rangle\Big(\frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|u_k\rangle\Big) = \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|0\rangle|u_k\rangle \longmapsto \frac{1}{\sqrt{r}}\sum_{k=0}^{r-1}|\widetilde{\frac{k}{r}}\rangle|u_k\rangle.$$

EUA kommer alltså att generera ett läge som är en superposition ev egenlägena sammanflätade med sina egenvärden. Tittar vi på det första läget, det vill säga styrläget, innehåller det en likformig fördelning av uppskattningar $\widetilde{\frac{k}{r}}$ av egenvärdena för $k \in \{0, \ldots, r-1\}$. Mäter vi styrläget kommer fasuppskattningen generera ett x sådant att $\frac{x}{2^n}$ är en uppskattning av $\frac{k}{r}$ för ett slumpat $k \in \{0, \ldots, r-1\}$.

EUA kommer att köra $U_a^{2^j}$ för $j \in \{0, 1, \ldots, n-1\}$, där appliceras U_a 2^j gånger för alla $j \in \{0, \ldots, n-1\}$. Det kräver en exponentiell resursåtgång. Men att applicera U_a 2^j gånger är samma sak som att applicera $U_{a^{2^j}}$ en gång. Talet a^{2^j} kan förberedas snabbt, med en klassisk dator, genom upprepad kvadrering. Vi kommer alltså bara att behöva applicera $U_{a^{2^j}}$ en gång för varje j. $U_{a^{2^j}}$ appliceras således bara n gånger vilket är inom polynomiell resursåtgång.

Vi en operator U_a som gör följande avbildning

$$U_a|s\rangle \longmapsto |sa \bmod N\rangle,$$

och $s < N$. Med den och EUA kan vi få fram en uppskattning med information om ordningen r av a modulo N. Uppskattningen blir ett rationellt tal med som kan skrivas med r som nämnare. Det viktiga är att vi får någon heltalsmultipel av $\frac{1}{r}$. Med sådana kan vi ta reda på r med hjälp av kedjebråk.

5.2 Kedjebråk

Ur uppskattningen $\widetilde{\frac{k}{r}}$ i avsnitt 5.1.2 kan vi, som vi ska se, ta reda på värdet av r med kedjebråk. Först konstaterar vi några saker om kedjebråk[17].

Sats 3. *Om vi har ett rationellt tal $\frac{x}{2^n}$, där x är ett heltal, så finns en sekvens $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_m}{b_m} = \frac{x}{2^n}$ av $O(n)$ rationella approximationer. Dessa kallas konvergenter och har följande egenskaper:*

i) $a_1 < a_2 < \cdots < a_m, b_1 < b_2 < \cdots < b_m$.

ii) Alla konvergenter kan beräknas med polynomiell resursåtgång.

iii) Om ett tal $\frac{k}{r}$ uppfyller

$$|\frac{x}{2^n} - \frac{k}{r}| \leq \frac{1}{2r^2},$$

så finns $\frac{k}{r}$ bland konvergenterna till $\frac{x}{2^n}$.

Sats 3 implicerar följande:

1. Anta att vi mätter den närmaste uppskattningen $\frac{x}{2^n}$ av $\frac{k}{r}$ och $2^n \geq 2r^2$. Då kan det som mest finnas en konvergent $\frac{a_i}{b_i}$ skiljd från $\frac{x}{2^n}$ sådan att $|\frac{x}{2^n} - \frac{a_i}{b_i}| \leq \frac{1}{2r^2}$ och $b_i \leq r$.
2. Om $2^n \geq 2r^2$ och $|\frac{x}{2^n} - \frac{a_i}{b_i}| \leq \frac{1}{2^n}$ så kommer $\frac{a_i}{b_i} = \frac{k}{r}$ att vara den enda konvergenten av $\frac{x}{2^n}$ med $b_i \leq 2^{\frac{(n-1)}{2}}$.

Vi visar med ett exempel.

Exempel 17. *Säg att vi mäter en uppskattning $\frac{k}{r} = \frac{9}{11}$, där $k = 9$, $r = 11$. För att kunna isolera $\frac{9}{11}$ bland uppskattningens konvergenter måste $2^n \geq 2 \cdot 11^2 = 242$. Vi sätter $n = 8$ som ger $2^8 = 256 \geq 242$. Uppskattningarna av $\frac{9}{11}$ att vara tal $\frac{x}{256}$ för $x \in \{0, 1, \ldots, 255\}$. $x = 209$ger den bästa uppskattningen av $\frac{9}{11}$ där*

$$\frac{209}{256} \leq \frac{9}{11}.$$

Vi kan nu skriva $\frac{209}{256}$ som ett kedjebråk:

$$\frac{209}{256} = 0 + \frac{1}{1 + \frac{1}{4 + \frac{1}{2 + \frac{1}{4 + \frac{1}{5}}}}}.$$

Kedjebråk kan skrivas på formen $[b_0; b_1, \ldots, b_n]$ där

$$[b_0; b_1, \ldots, s_n] = b_0 + \frac{1}{b_1 + \frac{1}{\ddots + \frac{1}{b_n}}}.$$

[17] Se [1] kapitel 7, [9] kapitel 1 och [8] kapitel 1 för mer information.

Vi kan då skriva $\frac{209}{256} = [0; 1, 4, 2, 4, 5]$. *Konvergenterna* $\frac{a_i}{b_i}$ *till* $\frac{209}{256}$ *får vi genom att beräkna avkortade kedjebråk:*

$$[0;1] = 0 + \frac{1}{1} = \frac{1}{1} =: \frac{a_1}{b_1}$$

$$[0;1,4] = 0 + \frac{1}{1+\frac{1}{4}} = \frac{4}{5} =: \frac{a_2}{b_2}$$

$$[0;1,4,2] = 0 + \frac{1}{1+\frac{1}{4+\frac{1}{2}}} = \frac{9}{11} =: \frac{a_3}{b_3}$$

$$[0;1,4,2,4] = 0 + \frac{1}{1+\frac{1}{4+\frac{1}{2+\frac{1}{4}}}} = \frac{40}{49} =: \frac{a_4}{b_4}$$

$$[0;1,4,2,4,5] = 0 + \frac{1}{1+\frac{1}{4+\frac{1}{2+\frac{1}{4+\frac{1}{5}}}}} = \frac{209}{256} =: \frac{a_5}{b_5}$$

Vi ser att det ursprungliga värdet $\frac{9}{11}$ *finns med bland konvergenterna men låt oss ignorera det för tillfället. Täljarna* $a_1, \ldots, a_m$ *och nämnarna* $b_1, \ldots b_m$ *som sats 3 talar om motsvarar talen* $1, 4, 9, 40$ *och* 209 *respektive* $1, 5, 11, 49$ *och* 256 *i det här fallet. Sats 3 säger att tal* $\frac{k}{r}$ *som uppfyller*

$$|\frac{x}{2^n} - \frac{k}{r}| \leq \frac{1}{2r^2}$$

finns med bland konvergenterna till $\frac{x}{2^n}$. *I det här fallet finns talen*

$$\frac{1}{1}\ dr\ r = 1,\ 2r^2 = 2,\ \left|\frac{209}{256} - \frac{1}{1}\right| = \frac{47}{256} \leq \frac{1}{2}$$

$$\frac{4}{5}\ dr\ r = 5,\ 2r^2 = 50,\ \left|\frac{209}{256} - \frac{4}{5}\right| = \frac{21}{1280} \leq \frac{1}{32}$$

$$\frac{9}{11}\ dr\ r = 11,\ 2r^2 = 242,\ \left|\frac{209}{256} - \frac{9}{11}\right| = \frac{5}{2816} \leq \frac{1}{242}$$

$$\frac{209}{256}\ dr\ r = 256,\ 2r^2 = 131072,\ \left|\frac{209}{256} - \frac{209}{256}\right| = 0 \leq \frac{1}{131072}$$

bland konvergenterna som uppfyller olikheten. Den första följden ur sats 3 sa att om vi mäter den närmaste uppskattningen till $\frac{k}{r}$ *finns det som mest en konvergent* $\frac{a_i}{b_i} \neq \frac{x}{2^n}$ *som uppfyller* $b_i \leq r$ *och*$|\frac{x}{2^n} - \frac{a_i}{b_i}| \leq \frac{1}{2r^2}$ *I det här fallet ska* $b_i \leq 11$ *och*

$$\left|\frac{209}{256} - \frac{a_i}{b_i}\right| \leq \frac{1}{2 \cdot 11^2} = \frac{1}{2 \cdot 11^2} = \frac{1}{242}.$$

Vi får för varje konvergent

$$\left|\frac{209}{256}-\frac{1}{1}\right| = \frac{47}{256} \not\leq \frac{1}{2\cdot 11^2} = \frac{1}{242}$$
$$\left|\frac{209}{256}-\frac{4}{5}\right| = \frac{21}{1280} \not\leq \frac{1}{2\cdot 11^2} = \frac{1}{242}$$
$$\left|\frac{209}{256}-\frac{9}{11}\right| = \frac{5}{2816} \leq \frac{1}{2\cdot 11^2} = \frac{1}{242}$$
$$\left|\frac{209}{256}-\frac{40}{49}\right| = \frac{1}{12544} \leq \frac{1}{2\cdot 11^2} = \frac{1}{242}$$
$$\left|\frac{209}{256}-\frac{209}{256}\right| = 0 \leq \frac{1}{2\cdot 11^2} = \frac{1}{242}.$$

där bara $\frac{9}{11}$ *uppfyller* $|\frac{209}{256}-\frac{a_i}{b_i}| \leq \frac{1}{2\cdot 11^2}$ *och* $b_i \leq 11$.

Enligt den andra följden ur sats 3 kommer det om $2^n \geq 2\cdot r^2$ *och* $|\frac{x}{2^n}-\frac{k}{r}| \leq \frac{1}{2^n}$ *endast att existera en konvergent* $\frac{a_i}{b_i} = \frac{k}{r}$ *av* $\frac{x}{2^n}$ *med* $b_i \leq 2^{\frac{n-1}{2}}$. *Vi har* $n = 8$ *och* $2^8 = 256 \geq 242 = 2\cdot 11^2$. *Följande konvergenter* $\frac{a_i}{b_i}$ *uppfyller* $|\frac{209}{256}-\frac{a_i}{b_i}| \leq \frac{1}{256}$*:*

$$\left|\frac{209}{256}-\frac{9}{11}\right| = \frac{5}{2816} \leq \frac{1}{256}$$
$$\left|\frac{209}{256}-\frac{40}{49}\right| = \frac{1}{12544} \leq \frac{1}{256}$$
$$\left|\frac{209}{256}-\frac{209}{256}\right| = 0 \leq \frac{1}{256}.$$

Av dessa är det bara $\frac{9}{11}$ *som uppfyller* $11 \leq 2^{\frac{(8-1)}{2}} (\approx 11.3)$*. Vi har således hittat ett sätt som möjliggör för oss att se vilken konvergent som motsvarar det ursprungliga talet* $\frac{k}{r}$.

Vi kan hitta $\frac{k}{r}$ bland konvergenterna genom att finna den konvergent $\frac{a_i}{b_i}$ som uppfyller $b_i \leq 2^{\frac{n-1}{2}}$ och

$$\left|\frac{x}{2^n}-\frac{a_i}{b_i}\right| \leq \frac{1}{2^n}.$$

De uppskattningar vi mäter då vi beräknar ordningen kommer att vara den decimala representationen av $\frac{k}{r}$ för något godtyckligt k. Tittar vi på bråket som motsvarar den decimala representationen av $\frac{k}{r}$ kan det vara ett förkortat bråk om k och r har gemensamma faktorer. Vi kan därmed inte ta reda på exakt vilket bråk som talet vi fått kommer ifrån och inte heller r. Men tar vi fram två uppskattningar för $\frac{k_1}{r}$ och $\frac{k_2}{r}$ i decimalform kan vi snabbt hitta reducerade bråk $\frac{c_1}{r_1} = \frac{k_1}{r}$ och $\frac{c_2}{r_2} = \frac{k_2}{r}$, där $SGD(c_1, r_1) = SGD(c_2, r_2) = 1$. Då kommer r att vara en multipel av r_1 och r_2. Vi har följande sats.

Sats 4. *Låt r, k_1 och k_2 vara positiva heltal där k_1 och k_2 är godtyckligt och oberoende valda från $\{0, 1, \ldots, r-1\}$. Vidare låt c_1, r_1, c_2, r_2 vara heltal där $SGD(c_1, r_1) = SGD(c_2, r_2) = 1$ samt $\frac{k_1}{r} = \frac{c_1}{r_1}$ och $\frac{k_2}{r} = \frac{c_2}{r_2}$. Då är $r = MGM(r_1, r_2)$ med en sannolikhet på minst $\frac{6}{\pi^2}$. Talen c_1, r_1, c_2, r_2 och r kan beräknas inom $O(\log^2 r)$.*

Bevis. Eftersom att r är en multipel av både r_1 och r_2 så gäller det att $MGM(r_1, r_2)|r$. För att visa att $r = MGM(r_1, r_2)$ räcker det att visa att $r|MGM(r_1, r_2)$. För enkelhetens skull säger vi att k_1 och k_2 är valda godtyckligt och oberoende från $\{1, 2, \ldots, r\}$ då

$$k_1 = 0 \Rightarrow \frac{0}{r} = \frac{c_1}{r_1} \Rightarrow c_1 = 0, r_1 = 1$$

$$k_1 = r \Rightarrow \frac{r}{r} = \frac{c_1}{r_1} \Rightarrow c_1 = 1, r_1 = 1.$$

Alltså $r_1 = 1$ i båda fallen. Vi kan också notera följande

$$k_1 = SGD(r, k_1)c_1,\ r_1 = \frac{c_1 r}{k_1} = \frac{r}{SGD(r, k_1)}$$

$$k_2 = SGD(r, k_2)c_2,\ r_2 = \frac{c_2 r}{k_2} = \frac{r}{SGD(r, k_2)}.$$

Om $SGD(r, k_1)$ och $SGD(r, k_2)$ är relativt prima så kommer faktorerna vi dividerar bort från r för att få r_1 att finnas kvar i r_2 och vice versa. Vi har att $r|MGM(r_1, r_2)$ vilket betyder att $r = MGM(r_1, r_2)$.

Sannolikheten att få $SGD(r, k_1) = 1$ och $SGD(r, k_2) = 1$ är $\prod_{p|r}(1 - \frac{1}{p^2})$, det vill säga alla primtal p som delar r. $\prod_{p|r}(1 - \frac{1}{p^2})$ är strikt större än $\prod_p(1 - \frac{1}{p^2})$, alltså produkten över alla primtal. $\prod_p(1 - \frac{1}{p^2})$ kan visas vara lika med inversen till Riemanzetafunktionen för heltalet 2, som skrivs$\zeta(2)$. $\zeta(2)$ har värdet $\frac{\pi^2}{6}$. Sannolikheten att $r = MGM(r_1, r_2)$ är således strikt större än $\frac{6}{\pi^2}$. □

För att kunna ta reda på r måste vi göra två uppskattningar av ordningen för ett tal. Utifrån dessa kan vi sedan med stor sannolikhet beräkna r och slutföra faktoriseringen. När vi tar fram ordningen r behöver vi på förhand välja ett n som möjliggör detta. I kapitel 3 i [10] beskriver man *Lagrangessats* för grupper. Säg att vi har en ändlig grupp med N stycken element. Ordningen r för godtyckliga element a i gruppen delar då N. Implicit betyder det att $r \leq N$. Eftersom vi kommer att leta efter ordningen bland tal a sådana att $SGD(a, N) = 1$ så kommer dessa att bilda en grupp under vanlig multiplikation, se [10] sid 99. Eftersom gruppen består av tal där $SGD(a, N) = 1$, kommer gruppen att ha färre än N element (då vi konstaterat att N inte är ett primtal). Ordningen r kommer således att dela ett tal mindre än N. Vi kan därför sätta en övre gräns $r < N$. Sats 3 sa att

olikheten $2r^2 \leq 2^n$ måste vara uppfylld för att med säkerhet kunna isolera rätt konvergent, så

$$2r^2 < 2 \cdot N^2 \leq 2^n \Rightarrow N^2 \leq 2^{n-1} \Leftrightarrow 2 \cdot \log_2 N \leq n - 1 \Leftrightarrow 2 \cdot \log_2 N + 1 \leq n$$

Om vi väljer $n = 2 \cdot log_2 N + 1$ får vi att

$$2r^2 \leq 2^n = 2^{2 \cdot log_2 N + 1} = 2N^2.$$

Eftersom N inte kommer att vara en exponent av 2 så avrundar vi uppåt och sätter $n = \lceil 2 \cdot log_2 N + 1 \rceil$. Valet av n till $\lceil 2 \cdot log_2 N + 1 \rceil$ kommer att vara tillräckligt för att få önskat resultat. Detta är den sista pusselbiten i algoritmen.

6 Algoritmen

Vi ska nu sammanfatta allt vi gått igenom och beskriva den algoritm som med kvantdatorns hjälp kan faktorisera heltal. Den första faktoriseringsalgoritmen avsedd att köras på en kvantdator beskrevs först 1994 av Peter Shor och heter Shor's algoritm[18]. Den algoritm vi går igenom en algoritm som skiljer sig lite ifrån Shor's, men ger samma resultat. Den kommer att göra det med polynomiell resursårgång istället för exponentiell som de kända nuvarande algoritmerna behöver. Vi beskriver faktoriseringsalgoritem i fem grupper av steg. Varje grupp av steg kan antingen utföras av en klassisk dator eller en kvantdator. Figur 15 från sid 137 i [1] visar kretsen som ska utföras av kvantdatorn. Följande är en algoritm för att faktorisera ett heltal N^*:

i. Kan utföras av klassisk dator

   1. Faktorisera ut triviala primtalsfaktorer 2 så vi får kvar ett udda heltal N.
   2. Kontrollera om N är ett primtal, om så är fallet är vi klara, annars gå vidare
   3. Kontrollera om N är något primtal upphöjt till ett positivt heltal, är det fallet är vi klara, annars gå vidare.
   4. Välj ett godtyckligt tal a sådant att $1 < a < N$.
   5. Beräkna $SGD(N, a)$.
   6. Om $d = SGD(N, a) \neq 1$ är vi klara. Faktorisera N till $N_1 \times d$ och kör om algoritmen på N_1 och d. Är $SGD(N, a) = 1$ gå vidare till kvantdatorn för att hitta ordningen r så att $a^r = 1 \bmod N$

ii. Kräver kvantdator

[18] Se [1] avsnitt 7.3.4, [16] 10.4 samt [17] 3.4 och 3.5.

7. Välj n så att $2r^2 \leq 2^n$, $n = \lceil 2 \cdot log_2 N + 1 \rceil$ duger.
8. Skapa ett styrläge med n kvantbitar och sätt det till $|0\rangle^{\otimes n}$.
9. Skapa ett målläge med n kvantbitar och sätt det till $|1\rangle = |0 \ldots 01\rangle$, kalla det målläget.
10. Applicera QFT_{2^n} på styrlägett, som vi såg i avsnitt 4.3, och få läget $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}$.
11. Applicera $c\text{-}U_a^{2^j}$, där $U_a^{2^j}|s\rangle \mapsto |sa^{2^j} \bmod N\rangle$, för varje $j \in \{0, \ldots, n-1\}$] på målläget $|1\rangle$ med styrläget $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes n}$. Det flyttar in $U_a^{2^j}$:s egenvärden i den relativa fasen hos styrläget.
12. Applicera $QFT_{2^n}^{-1}$ på styrläget.
13. Mät styrläget för att få uppskattningen $\frac{x_1}{2^n}$ av en multipel $\frac{k}{r}$ för något godtyckligt $k \in \{0, 1, \ldots, r-1\}$.

iii. Kan utföras av klassik dator

14. Använd det vi kan om kedjebråk för att hitta r_1 och c_1 bland konvergenterna till $\frac{x_1}{2^n}$ så att $|\frac{x_1}{2^n} - \frac{c_1}{r_1}| \leq \frac{1}{2^n}$ och $r_1 \leq 2^{\frac{n-1}{2}}$. Hittas inga sådana så skicka ”FAIL” som utdata och börja om vid steg 7.

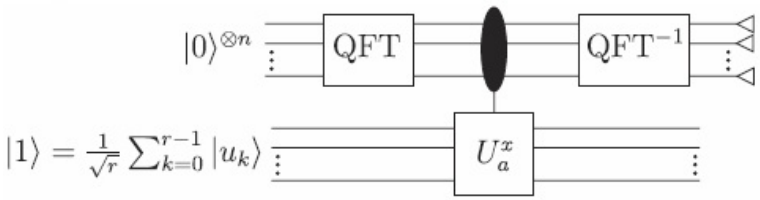
iv. Kräver kvantdator

15. (Görs också av kvantdatorn) Gör om steg 7-13 och använd kedjebråk för att hitta r_2 och c_2 så att $|\frac{x_2}{2^n} - \frac{c_2}{r_2}| \leq \frac{1}{2^n}$ och $r_2 \leq 2^{\frac{n-1}{2}}$. Hittas inga sådana så skicka ”FAIL” som output och börja om vid steg 4.

v. Kan utföras av klassik dator

16. Beräkna $r = MGM(r_1, r_2)$.
17. Beräkna $a^r \bmod N$, om resultat är 1 fortsätt, annars skicka ”FAIL” som utdata och börja om vid steg 4.
18. Om r är udda, börja om vid steg 4.
19. Om $a^{\frac{r}{2}} \equiv -1 \bmod N$ eller $a^{\frac{r}{2}} \equiv 1 \bmod N$, börja om vid steg 4.
20. Beräkna $b = SGD(a^{\frac{r}{2}} \pm 1, N)$ för att få en icketrivial faktor till N.
21. Faktorisera N till $N_1 \times b$ och upprepa från steg 2 med både N_1 och b tills N är helt faktoriserat till primtal.

Steg 8-12 är som synes EUA för operatorn U_a som avbildar $|s\rangle$ till $|as \bmod N\rangle$. Det tidskrävande momentet i algoritmen är att utföra $c - U_a^{2^j}$ opera-



Figur 15: Kretsen som ger oss tillräckligt med information att hitta ordningen.

tionerna. Lyckligtvis behöver vi inte applicera operatorn så många gånger. Som vi såg i 5.1.2, behöver vi bara förbereda a^{2^j}. a^{2^j} är ett tal mellan 0 och $N-1$ som vi kan förbereda genom upprepad kvadrering av a. Kvantkretsen för $c\text{-}U_a^{2^j}$ kommer således bara att utföra multiplikationer med a^{2^j} mod N. Det finns standardtekniker för att utföra denna multiplikation med resursårgång $O((\log N)^2 \log\log N \log\log\log N)$. QFT kräver resursåtgång $O((\log N)^2)$ så hela algoritmen för att faktorisera kommer bara att kräva resursåtgång $O((\log N)^2 \log\log(N) \log\log\log(N))$, se [1] sid 138. Om vi jämför med den bästa idag kända algoritmen som kräver $e^{O((\log N)^{\frac{1}{3}}(\log\log N)^{\frac{2}{3}})}$, ser vi att vi har en betydligt effektivare algoritm. För att göra det tydligare ska vi visa ett exempel.

Exempel 18. *Vi hoppar över steg 1-6 och utgår från att vi ska faktorisera* 21. *Vi väljer ett godtyckligt a bland de a:n som uppfyller* $SGD(21, a) = 1$*, alltså från* $\{2, 4, 5, 8, 10, 13, 16, 17, 19, 20\}$*, till exempel* 10. *Vi lätt se att ordningen r måste vara* 6 *men vi ska se hur vi får fram det med kvantdatorn. Vi börjar vid steg 7:*

7. *Välj n till* $\lceil 2 \cdot log_2 21 + 1 \rceil$ *alltså* $n = 10$.
8. *Skapa ett styrläget* $|0\rangle^{\otimes 10} = |0000000000\rangle$
9. *Skapa ett målläget* $|1\rangle = |0000000001\rangle$
10. *Applicera* $QFT_{2^{10}}$ *på styrläget så att det lämnas i läget* $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes 10}$
11. *Applicera* $c\text{-}U_a^{2^j}$ *för* $= 0, 1, \ldots 9$*, alltså* $2^j = 1, 2, 4, 8, 16, 32, 64, 128, 256, 512$ *på målläget* $|00\ldots01\rangle$ *med styrläget* $\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)^{\otimes 10}$ *. Egenvärdena* $e^{2\pi i \frac{k}{6} 2^x}$ *kommer att flyttas till den relativa fasen i styrläget. Styrläget kommer att lämnas i läget* $\left(\frac{|0\rangle+e^{2\pi i \frac{k}{6}2^0}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle+e^{2\pi i \frac{k}{6}2^1}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle+e^{2\pi i \frac{k}{6}2^2}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle+e^{2\pi i \frac{k}{6}2^3}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle+e^{2\pi i \frac{k}{6}2^4}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle+e^{2\pi i \frac{k}{6}2^5}|1\rangle}{\sqrt{2}}\right) \otimes$

$\left(\frac{|0\rangle+e^{2\pi i\frac{k}{6}2^6}|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle+e^{2\pi i\frac{k}{6}2^7}|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle+e^{2\pi i\frac{k}{6}2^8}|1\rangle}{\sqrt{2}}\right)\otimes\left(\frac{|0\rangle+e^{2\pi i\frac{k}{6}2^9}|1\rangle}{\sqrt{2}}\right)$ *för något slumpat* $k \in \{0,1,2,3,4,5\}$.

12. *Applicera* $QFT_{2^{10}}^{-1}$ *på styrläget för att få en uppskattning av* $\frac{k}{6}$.

13. *Mät styrläget för att få uppskattningen* $\frac{x_1}{2^{10}}$ *av* $\frac{k}{6}$ *för säg* $k = 5$. *Vi fick uppskattningen* $\frac{853}{2^{10}}$ *till* $\frac{5}{6}$ *som också är den bästa.*

14. *Hitta tal* c_1 *och* r_1 *bland konvergenterna till* $\frac{853}{2^{10}}$ *sådana att* $|\frac{853}{2^{10}} - \frac{c_1}{r_1}| \leq \frac{1}{2^{10}} = \frac{1}{1024}$ *och* $r_1 \leq 2^{\frac{10-1}{2}} \approx 22$. *Konvergenten* $\frac{5}{6}$ *är den enda som uppfyller de villkoren så vi får* $c_1 = 5$ *och* $r_1 = 6$.

15. *Upprepa steg 7-14. Säg att vi mätte en uppskattning av* $\frac{2}{6}$ *och fick approximationen* $\frac{341}{1024}$ *och tal* $c_2 = 1$ *och* $r_2 = 3$.

16. *Beräkna* $MGM(r_1, r_2) = MGM(6, 3) = 6$.

17. *Beräkna* $10^6 = 1000000 \equiv 1 \bmod 21$.

18. 6 *är ej udda så vi fortsätter.*

19. $10^{\frac{6}{2}} = 10^3 = 1000 \not\equiv -1, 1 \bmod 21$ *så vi fortsätter.*

20. *Beräkna* $SGD(1000 - 1, 21) = 3$

21. *Faktorisera bort* 3 *från* 21 *och börja om från steg 1 med* 7 *respektive* 3.

I exemplet ovan har vi ett litet tal N som vi faktoriserar. Algoritmen kommer till sin användning när vi vill faktorisera väldigt stora heltal N. Stora heltal använder man i till exempel RSA-kryptering. Om man lyckas att bygga en kvantdator kommer man således att kunna knäcka krypteringar som bygger på svårigheten att faktorisera stora tal snabbt.

Man har fram till idag i laboratoriemiljö lyckats att bygga små kvantdatorer med olika metoder[19]. En metod som verkar lovande är en teknik då man använder jonfällor. Där fångas joner i ett vakuum och används som byggstenar till kvantdatorn. Frågan är bara hur lång tid det tar innan vi har dem på skrivbordet.

[19] Se [15] kapitel 14 och [16] avsnitt 12.4 och kapitel 11.

Referenser

[1] Kaye, P. Laflamme, R. & Mosca M (2007), An Introduction to Quantum Computing, Oxford University press

[2] Anton, H. & Rorres, C. (2005), Elementary Linear Algebra, Drexel University, Nionde utgåvan

[3] Norman, L. Biggs (2002), Discrete Mathematics, Oxford University press, andra utgåvan

[4] Dym, H. (2007), Linear Algebra in Action, American Mathimatical Society

[5] Saff, E. B. & Snider, A. D. (2003), Fundamentals of Complex Analysis, Pearson Education International, tredje utgåvan

[6] Hogben, L. (2007), Handbook of Linear Algebra, Chapman & Hall/CRC

[7] Harald, J. Müller-Kirsten W. (2006), Introduction to Quantum Mechanics: Schrödinger Equation and Path Integral, World Scientific Publishing

[8] Rockett, A. M. Szüsz, P (1992), Continued Fractions, World Scientific Publishing

[9] Lorentzen, L. Waadeland, H. (1992), Continued Fractions with Applications, Elsevier Sience Publishers B.V.

[10] Beachy, J. A. Blair, W. D. (2006), Abstract Algebra, Waveland Press Inc, tredje utgåvan

[11] Hoffstein, J. Pipher, J. Silverman, J. H. (2008), An Introduction to Mathematical Cryptography, Springer Science+Business Media LLC

[12] Rippe, L. (2006), Quantum Computation with Naturally Trapped Sub-Nanometre-Spaced Ions, Doktorsavhandling, Lunds Universitet Fysiska Institutionen

[13] Gruska, J. (1999), Quantum Computing, McGraw-Hill Publishing Company

[14] Le Bellac, M. (2006), A Short Intruduction to Quantum Information and Quantum Computation, Cambridge University Press

[15] Vedral, V. (2006), Introduction to Quantum Information Science, Oxford University Press

[16] Blümel, R. (2010), Foundations of Quantum Mechanics From Photons to Quantum Computers, Jones and Barlett Publishing LLC

[17] Pittenger, O. A. (2000), An Introduction to Quantum Computing Algorithms, Birkhäuser Boston