Faktorisering med hjälp av kvantberäkningar

Lars Engebretsen 2004-11-19

Bakgrund

Vanliga datorer styrs av klassiska fysikens lagar.

Vanliga datorer kan simuleras av turingmaskiner i polynomisk tid.

Kanske kan vi lösa svårare problem med kvantmekanik?

Vi behöver en vettig modell som dessutom går att implementera.

Modellen bör kunna lösa svårare problem än ”vanliga” datorer.

Vad är en kvantdator?

Klassisk programmering: C, C++, Java, källkod och kompilering:
`g++ -O4 gurka.cc`; `javac apelsin.java`; `./a.out`; `gdb`; `...`

Såsmåningom hoppas vi på något liknande för kvantdatorer.

Tekniken är nu mycket mer primitiv, söker analogier till turingmaskinen.

Ett "kvantprogram": matematiska operationer på ett matematiskt objekt.

Detta kan (ska kunna) realiseras fysiskt i laboratorium.

Vad är en kvantdator?

Man kan tänka på kvantdatorn på två sätt.

1) En klump materia i ett laboratorium.
   Beräkning: Utsätt klumpen för olika magnetfält.

2) Ett matematiskt objekt (en funktion).
   Beräkning En följd av matematiska operationer efter vissa regler.

Vi kommer att använda det senare idag.

Modell – översikt

Informationslagring: Vågfunktionen, en linjärkombination av tillstånd.

Programsteg: Lokala unitära transformationer av vågfunktionen.

Mätning: Vi frågar systemet vilket tillstånd det är i.
Slumpvis svar som beror på vågfunktionen.

En mätning förstör nästan all information som finns i vågfunktionen.

Modell – kvantbiten

En kvantbit beskrivs av två bastillstånd: $|0\rangle$ och $|1\rangle$.

Kvantbiten kan vara i tillstånd $\alpha_0|0\rangle + \alpha_1|1\rangle$ så snart $\|\alpha_0\|^2 + \|\alpha_1\|^2 = 1$.

Ibland skriver vi $\alpha_0|0\rangle + \alpha_1|1\rangle$ som $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

Modell – kvantbiten

En kvantbit beskrivs av två bastillstånd: $|0\rangle$ och $|1\rangle$.

Kvantbiten kan vara i tillstånd $\alpha_0|0\rangle + \alpha_1|1\rangle$ så snart $\|\alpha_0\|^2 + \|\alpha_1\|^2 = 1$.

Ibland skriver vi $\alpha_0|0\rangle + \alpha_1|1\rangle$ som $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

Mätning: Vi frågar kvantbiten vilket tillstånd den är i.
Sannolikheten att vi får svaret $|i\rangle$ är $\|\alpha_i\|^2$.

Efter mätningen kollapsar kvantbiten till det tillstånd vi såg vid mätningen.

Modell – programsteg

Minsta byggstenen: Unitära operatorer.

Modell – programsteg

Minsta byggstenen: 2×2-matriser sådana att $A^* = A^{-1}$.

En matris A avbildar tillståndet $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ på $A \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

Modell – programsteg

Minsta byggstenen: 2×2-matriser sådana att $A^* = A^{-1}$.

En matris A avbildar tillståndet $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ på $A \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ avbildar $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ på $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

Modell – programsteg

Minsta byggstenen: 2×2-matriser sådana att $A^* = A^{-1}$.

En matris A avbildar tillståndet $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ på $A \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ avbildar varje tillstånd på sig själv.

Modell – programsteg

Minsta byggstenen: 2×2-matriser sådana att $A^* = A^{-1}$.

En matris A avbildar tillståndet $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ på $A \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ avbildar varje tillstånd på sig själv.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ avbildar $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ på $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_0 \end{pmatrix}$.

Modell – programsteg

Minsta byggstenen: 2×2-matriser sådana att $A^* = A^{-1}$.

En matris A avbildar tillståndet $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ på $A \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ avbildar varje tillstånd på sig själv.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ definierar $\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$.

Modell – programsteg

Minsta byggstenen: 2×2-matriser sådana att $A^* = A^{-1}$.

En matris A avbildar tillståndet $\begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$ på $A \begin{pmatrix} \alpha_0 \\ \alpha_1 \end{pmatrix}$.

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ avbildar varje tillstånd på sig själv.

$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ definierar $\alpha_0|0\rangle + \alpha_1|1\rangle \mapsto \alpha_1|0\rangle + \alpha_0|1\rangle$.

$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$ definierar $|0\rangle \mapsto \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$.

Modell – ett exempel

Systemet startar i tillstånd $|0\rangle$. Lägg på operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Modell – ett exempel

Systemet startar i tillstånd $|0\rangle$. Lägg på operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Systemet byter tillstånd till $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$.

Modell – ett exempel

Systemet startar i tillstånd $|0\rangle$. Lägg på operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Systemet byter tillstånd till $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$.

En mätning nu ger $|0\rangle$ och $|1\rangle$ med samma sannolikhet.

Modell – ett exempel

Systemet startar i tillstånd $|0\rangle$. Lägg på operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Systemet byter tillstånd till $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$.

En mätning nu ger $|0\rangle$ och $|1\rangle$ med samma sannolikhet.
Antag att vi mäter och ser $|1\rangle$. Efteråt vet vi att systemet är i tillstånd $|1\rangle$.

Modell – ett exempel

Systemet startar i tillstånd $|0\rangle$. Lägg på operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Systemet byter tillstånd till $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$.

En mätning nu ger $|0\rangle$ och $|1\rangle$ med samma sannolikhet.
Antag att vi mäter och ser $|1\rangle$. Efteråt vet vi att systemet är i tillstånd $|1\rangle$.

Använd A igen; systemet hamnar i tillstånd $\frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle$. Mät igen.

Modell – ett exempel

Systemet startar i tillstånd $|0\rangle$. Lägg på operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Systemet byter tillstånd till $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$.

En mätning nu ger $|0\rangle$ och $|1\rangle$ med samma sannolikhet.
Antag att vi mäter och ser $|1\rangle$. Efteråt vet vi att systemet är i tillstånd $|1\rangle$.

Använd A igen; systemet hamnar i tillstånd $\frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle$. Mät igen.

Mätningen ger $|0\rangle$ och $|1\rangle$ med samma sannolikhet.

Modell – ett liknande exempel

Samma början: Vi startar i $|0\rangle$ och kör operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Modell – ett liknande exempel

Samma början: Vi startar i $|0\rangle$ och kör operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Systemet byter tillstånd till $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$.

Modell – ett liknande exempel

Samma början: Vi startar i $|0\rangle$ och kör operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Systemet byter tillstånd till $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$.

Men nu kör vi A igen; Då hamnar vi i $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Modell – ett liknande exempel

Samma början: Vi startar i $|0\rangle$ och kör operatorn $A = \frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}$.

Systemet byter tillstånd till $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$.

Men nu kör vi A igen; Då hamnar vi i $\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

En mätning nu ger $|1\rangle$ med sannolikhet ett.

Modell – fler bitar

Vi behöver fler bitar än en. Bastillstånden blir då $|\mathrm{b}\rangle$ för binära strängar b.

Systemets tillstånd skrivs $\sum \alpha_{\mathrm{b}}|\mathrm{b}\rangle$ där $\sum \|\alpha_{\mathrm{b}}\|^2 = 1$.

Vid mätning ser vi $|\mathrm{b}\rangle$ med sannolikhet $\|\alpha_{\mathrm{b}}\|^2$.

Efter en mätning kollapsar systemet till det tillstånd vi såg.

Feynmans motivering av kvantberäkningar

Hur många bastillstånd finns det?

Två bitar: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
Tre bitar: $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$.

n bitar: 2^n bastillstånd!

Feynmans motivering av kvantberäkningar

Hur många bastillstånd finns det?

Två bitar: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$.
Tre bitar: $|000\rangle$, $|001\rangle$, $|010\rangle$, $|011\rangle$, $|100\rangle$, $|101\rangle$, $|110\rangle$, $|111\rangle$.

n bitar: 2^n bastillstånd!

Det tar exponentiell tid att simulera ett n-bitarsystem klassiskt.

Så kanske ger kvantberäkningar en exponentiell uppsnabbning?

Modell – operationer på två bitar

Operationer definieras, som tidigare, som unitära matriser.

Vilken transformation definieras av $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$?

$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \mapsto \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{11}|10\rangle + \alpha_{10}|11\rangle.$

Modell – operationer på två bitar

Operationer definieras, som tidigare, som unitära matriser.

Vilken transformation definieras av $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$?

$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \mapsto \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{11}|10\rangle + \alpha_{10}|11\rangle.$

Om den första biten är noll ändras inte den andra biten.
Om den första biten är ett negeras den andra biten.

Modell – sammanfattning

Information lagras som en vektor i ett komplext vektorrum.

Vektorrummet har 2^n dimensioner om vi har n kvantbitar.

Programmet består av unitära operationer på högst två kvantbitar åt gången.

Mått på komplexitet: Antal sådana operationer.

Vi får resultatet genom att mäta.

Vi ser $|b\rangle$ med sannolikhet $\|$koefficienten framför $|b\rangle\|^2$.

En mätning gör att vågfunktionen kollapsar.

Är modellen användbar?

Vad klarar vi av att göra i kvantmodellen?

Är modellen användbar?

Vad klarar vi av att göra i kvantmodellen?

Alla kvantberäkningar är reversibla; de kan alltså köras baklänges.

Därför finns inte operationer av typen "sätt x till 17".

Är modellen användbar?

Vad klarar vi av att göra i kvantmodellen?

Alla kvantberäkningar är reversibla; de kan alltså köras baklänges.

Därför finns inte operationer av typen "sätt x till 17".

Trots detta kan alla deterministiska beräkningar simuleras.

Huvudidé: NAND-grindar är universella; det räcker alltså att simulera dem. [$\mathrm{NAND}(x_1, x_2) = \neg(x_1 \wedge x_2)$.]

NAND-grindar kan simuleras reversibelt om man behåller indata.

Faktorisering

Vi vill dela upp N, ett tal med $\mathfrak{n}$ bitar, i primfaktorer.

Faktorisering

Vi vill dela upp N, ett tal med n bitar, i primfaktorer.

Välj ett slumpvis x och låt r vara dess ordning mod N; $x^r \equiv 1 \bmod N$.

Det är känt att $\gcd(x^{r/2} - 1, N)$ ofta är en icke-trivial faktor.

Faktorisering

Vi vill dela upp N, ett tal med n bitar, i primfaktorer.

Välj ett slumpvis x och låt r vara dess ordning mod N; $x^r \equiv 1 \bmod N$.

Det är känt att $\gcd(x^{r/2} - 1, N)$ ofta är en icke-trivial faktor.

Så om vi kan beräkna ordningen mod N så kan vi även faktorisera N.

Shors algoritm beräknar ordningen mod N i polynomisk tid.

Faktorisering

Vi vill dela upp N, ett tal med n bitar, i primfaktorer.

Välj ett slumpvis x och låt r vara dess ordning mod N; $x^r \equiv 1 \bmod N$.

Det är känt att $\gcd(x^{r/2} - 1, N)$ ofta är en icke-trivial faktor.

Så om vi kan beräkna ordningen mod N så kan vi även faktorisera N.

Shors algoritm beräknar ordningen mod N i polynomisk tid, dvs antalet operationer är polynomiskt i n.

Översikt av algoritmen

Shors algoritm har tre faser:

1. Konvertera $|0\rangle$ till en likformig fördelning.

Översikt av algoritmen

Shors algoritm har tre faser:

1. Konvertera $|0\rangle$ till en likformig fördelning.
   Kan göras genom att köra $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$ på varje kvantbit.

Översikt av algoritmen

Shors algoritm har tre faser:

1. Konvertera $|0\rangle$ till en likformig fördelning.
   Kan göras genom att köra $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$ på varje kvantbit.

2. Beräkna $x^a \bmod N$ givet x, a och N.

Översikt av algoritmen

Shors algoritm har tre faser:

1. Konvertera $|0\rangle$ till en likformig fördelning.
   Kan göras genom att köra $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$ på varje kvantbit.

2. Beräkna $x^a \bmod N$ givet x, a och N. Går att göra om vi behåller indata.

Översikt av algoritmen

Shors algoritm har tre faser:

1. Konvertera $|0\rangle$ till en likformig fördelning.
   Kan göras genom att köra $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$ på varje kvantbit.

2. Beräkna $x^a \bmod N$ givet x, a och N. Går att göra om vi behåller indata.

3. Beräkna fouriertransformen av a: $|a\rangle \mapsto 2^{-m/2}\sum_{c=0}^{2^m-1}\omega^{ac}|c\rangle$ där $\omega = e^{2\pi i/2^m}$.

Översikt av algoritmen

Shors algoritm har tre faser:

1. Konvertera $|0\rangle$ till en likformig fördelning.
   Kan göras genom att köra $\frac{1}{\sqrt{2}}\begin{pmatrix}1 & -1\\ 1 & 1\end{pmatrix}$ på varje kvantbit.

2. Beräkna $x^a \bmod N$ givet x, a och N. Går att göra om vi behåller indata.

3. Beräkna fouriertransformen av a: $|a\rangle \mapsto 2^{-m/2}\sum_{c=0}^{2^m-1}\omega^{ac}|c\rangle$ där $\omega = e^{2\pi i/2^m}$.
   Antag tillsvidare att detta går att göra.

Mer detaljerad version av algoritmen

Givet x and N vill vi beräkna ordningen av x mod N. N består av n bitar.

1. Skapa a genom att skapa $m = 3n$ likafördelade slumpbitar.
   Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |a\rangle|x\rangle|N\rangle$

Mer detaljerad version av algoritmen

Givet x and N vill vi beräkna ordningen av x mod N. N består av n bitar.

1. Skapa a genom att skapa $m = 3n$ likafördelade slumpbitar.
   Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |a\rangle|x\rangle|N\rangle$

2. Beräkna $x^a \bmod N$. Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |x^a\rangle|a\rangle|x\rangle|N\rangle$

Mer detaljerad version av algoritmen

Givet x and N vill vi beräkna ordningen av x mod N. N består av n bitar.

1. Skapa a genom att skapa $m = 3n$ likafördelade slumpbitar.
   Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |a\rangle|x\rangle|N\rangle$

2. Beräkna $x^a \bmod N$. Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |x^a\rangle|a\rangle|x\rangle|N\rangle$

3. Fouriertransformera a. $|a\rangle \mapsto 2^{-m/2} \sum_{c=0}^{2^m-1} \omega^{ac}|c\rangle$

Mer detaljerad version av algoritmen

Givet x and N vill vi beräkna ordningen av x mod N. N består av n bitar.

1. Skapa a genom att skapa $m = 3n$ likafördelade slumpbitar.
   Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |a\rangle|x\rangle|N\rangle$

2. Beräkna $x^a \bmod N$. Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |x^a\rangle|a\rangle|x\rangle|N\rangle$

3. Fouriertransformera a. Tillstånd: $2^{-m} \sum_{a=0}^{2^m-1} \sum_{c=0}^{2^m-1} \omega^{ac}|x^a\rangle|c\rangle|x\rangle|N\rangle$

Mer detaljerad version av algoritmen

Givet x and N vill vi beräkna ordningen av x mod N. N består av n bitar.

1. Skapa a genom att skapa $m = 3n$ likafördelade slumpbitar.
   Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |a\rangle|x\rangle|N\rangle$

2. Beräkna $x^a \bmod N$. Tillstånd: $2^{-m/2} \sum_{a=0}^{2^m-1} |x^a\rangle|a\rangle|x\rangle|N\rangle$

3. Fouriertransformera a. Tillstånd: $2^{-m} \sum_{a=0}^{2^m-1} \sum_{c=0}^{2^m-1} \omega^{ac}|x^a\rangle|c\rangle|x\rangle|N\rangle$

4. Mät tillståndet och beräkna r givet observationen av c.

Analys av algoritmen – intuition

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle |c\rangle |x\rangle |N\rangle$

Vad är sannolikheten att se ett visst $|x^k\rangle |c\rangle |x\rangle |N\rangle$?

Analys av algoritmen – intuition

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle|c\rangle|x\rangle|N\rangle$

Vad är sannolikheten att se ett visst $|x^k\rangle|c\rangle|x\rangle|N\rangle$?
Eftersom $x^k \equiv x^{k+r} \equiv x^{k+2r} \equiv \cdots$ bidrar flera a till samma $|x^k\rangle|c\rangle|x\rangle|N\rangle$.

Analys av algoritmen – intuition

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle|c\rangle|x\rangle|N\rangle$

Vad är sannolikheten att se ett visst $|x^k\rangle|c\rangle|x\rangle|N\rangle$?
Eftersom $x^k \equiv x^{k+r} \equiv x^{k+2r} \equiv \cdots$ bidrar flera a till samma $|x^k\rangle|c\rangle|x\rangle|N\rangle$.

$$\Pr[|x^k\rangle|c\rangle|x\rangle|N\rangle] = 2^{-2m} \left\| \sum_{a : x^a \equiv x^k} \omega^{ac} \right\|^2$$

Analys av algoritmen – intuition

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle|c\rangle|x\rangle|N\rangle$

Vad är sannolikheten att se ett visst $|x^k\rangle|c\rangle|x\rangle|N\rangle$?
Eftersom $x^k \equiv x^{k+r} \equiv x^{k+2r} \equiv \cdots$ bidrar flera a till samma $|x^k\rangle|c\rangle|x\rangle|N\rangle$.

$$\Pr[|x^k\rangle|c\rangle|x\rangle|N\rangle] = 2^{-2m} \left\| \sum_{a:x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \sum_j \omega^{(k+jr)c} \right\|^2$$

Analys av algoritmen – intuition

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle|c\rangle|x\rangle|N\rangle$

Vad är sannolikheten att se ett visst $|x^k\rangle|c\rangle|x\rangle|N\rangle$?
Eftersom $x^k \equiv x^{k+r} \equiv x^{k+2r} \equiv \cdots$ bidrar flera a till samma $|x^k\rangle|c\rangle|x\rangle|N\rangle$.

$$\Pr[|x^k\rangle|c\rangle|x\rangle|N\rangle] = 2^{-2m} \left\| \sum_{a:x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \sum_j \omega^{kc} \omega^{jrc} \right\|^2$$

Analys av algoritmen – intuition

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle |c\rangle |x\rangle |N\rangle$

Vad är sannolikheten att se ett visst $|x^k\rangle|c\rangle|x\rangle|N\rangle$?
Eftersom $x^k \equiv x^{k+r} \equiv x^{k+2r} \equiv \cdots$ bidrar flera a till samma $|x^k\rangle|c\rangle|x\rangle|N\rangle$.

$$\Pr[|x^k\rangle|c\rangle|x\rangle|N\rangle] = 2^{-2m} \left\| \sum_{a : x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \omega^{kc} \sum_j \omega^{jrc} \right\|^2$$

Analys av algoritmen – intuition

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle|c\rangle|x\rangle|N\rangle$

Vad är sannolikheten att se ett visst $|x^k\rangle|c\rangle|x\rangle|N\rangle$?
Eftersom $x^k \equiv x^{k+r} \equiv x^{k+2r} \equiv \cdots$ bidrar flera a till samma $|x^k\rangle|c\rangle|x\rangle|N\rangle$.

$$\Pr[|x^k\rangle|c\rangle|x\rangle|N\rangle] = 2^{-2m} \left\| \sum_{a:x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \sum_j \left(\omega^{rc}\right)^j \right\|^2.$$

När är denna summa stor?

Analys av algoritmen – intuition

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle|c\rangle|x\rangle|N\rangle$

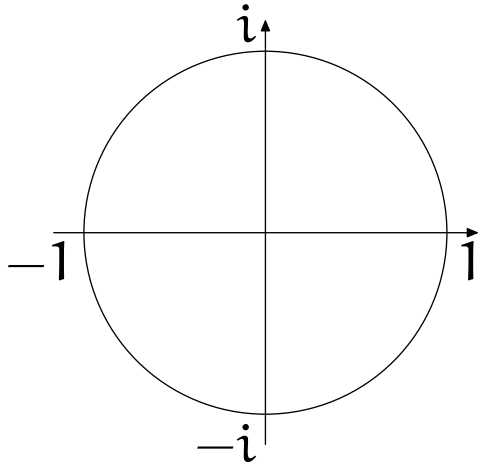
Vad är sannolikheten att se ett visst $|x^k\rangle|c\rangle|x\rangle|N\rangle$?
Eftersom $x^k \equiv x^{k+r} \equiv x^{k+2r} \equiv \cdots$ bidrar flera a till samma $|x^k\rangle|c\rangle|x\rangle|N\rangle$.

$$\Pr[|x^k\rangle|c\rangle|x\rangle|N\rangle] = 2^{-2m} \left\| \sum_{a:x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \sum_j \left(\omega^{rc}\right)^j \right\|^2.$$

När är denna summa stor? Studera $\| \sum_j (\omega^{rc})^j \|$.

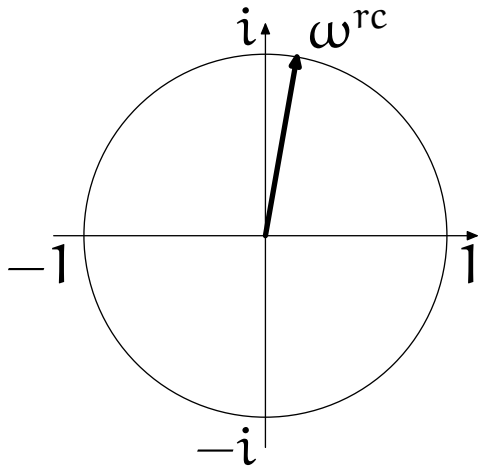
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



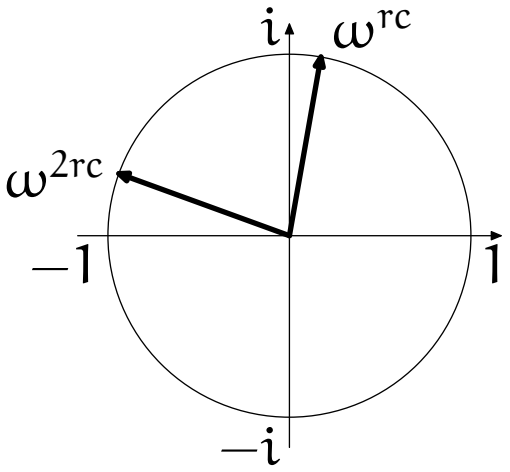
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



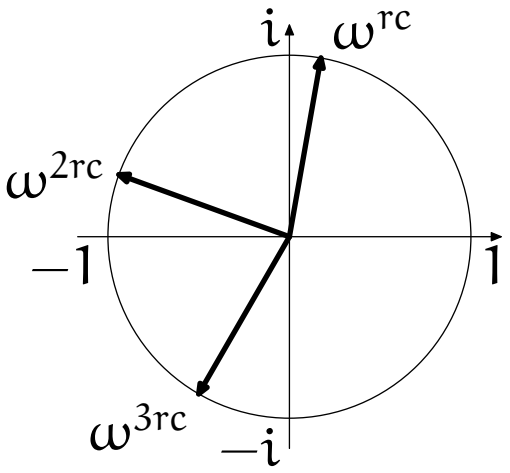
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



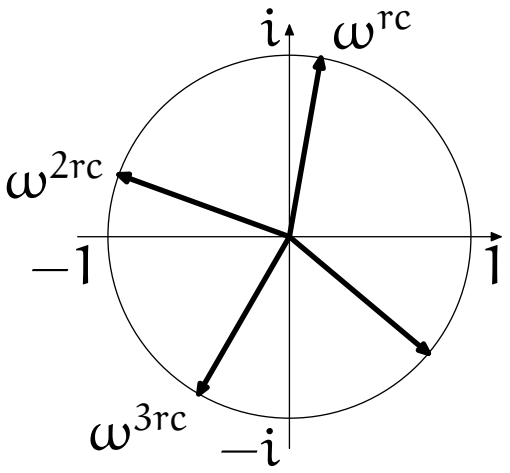
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



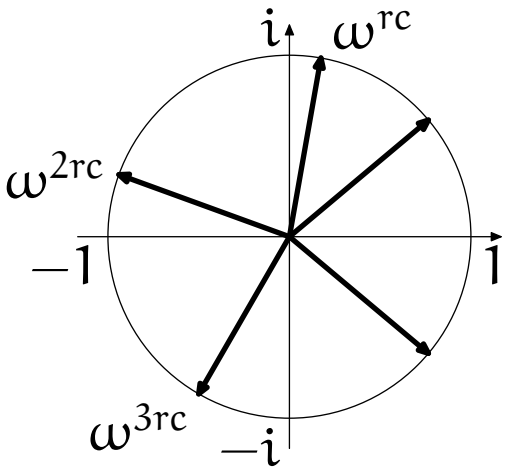
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



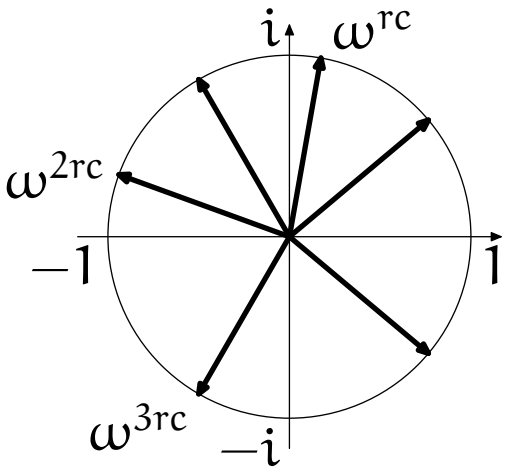
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



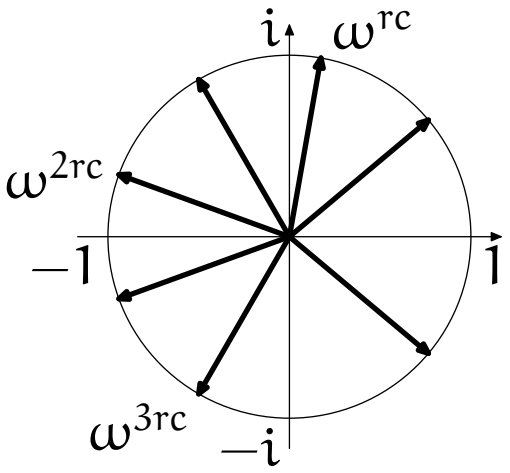
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



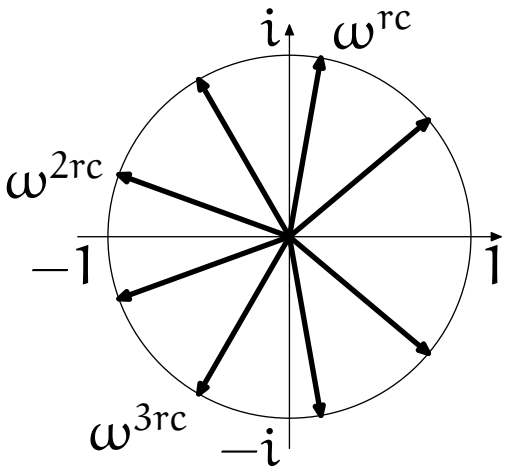
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



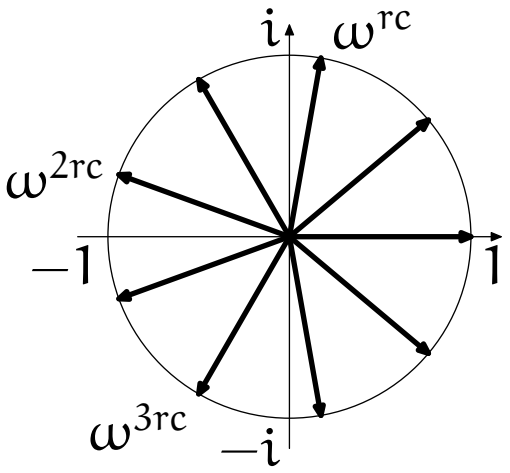
Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



Analys av algoritmen – summor av enhetsrötter

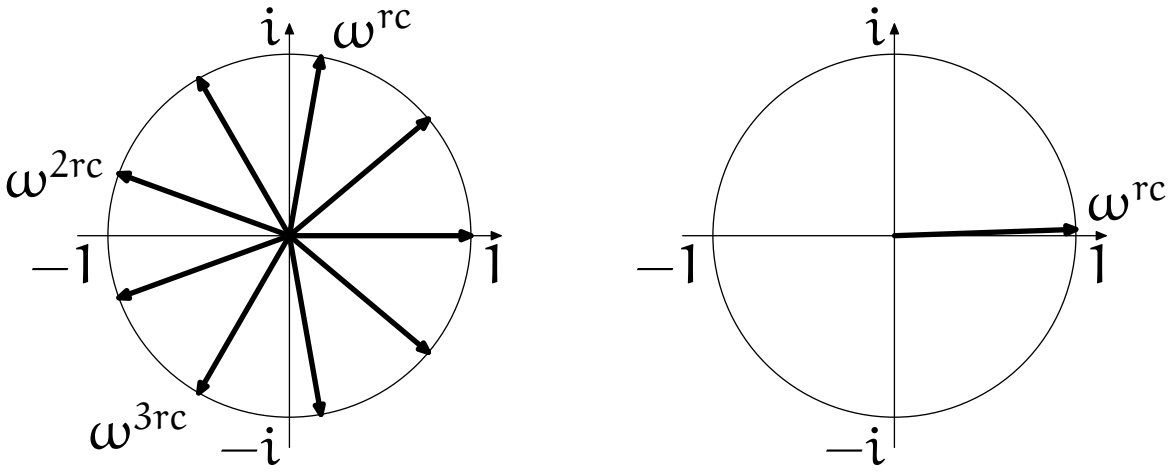
När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



$\| \sum_j (\omega^{rc})^j \|$ = längden av summan av ovanstående vektorer.

Analys av algoritmen – summor av enhetsrötter

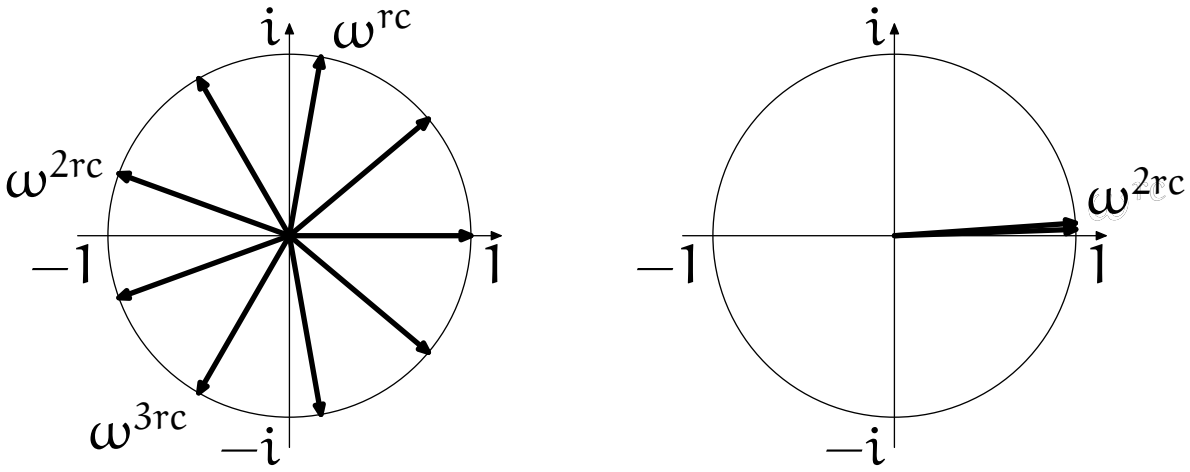
När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



$\| \sum_j (\omega^{rc})^j \|$ = längden av summan av ovanstående vektorer.

Analys av algoritmen – summor av enhetsrötter

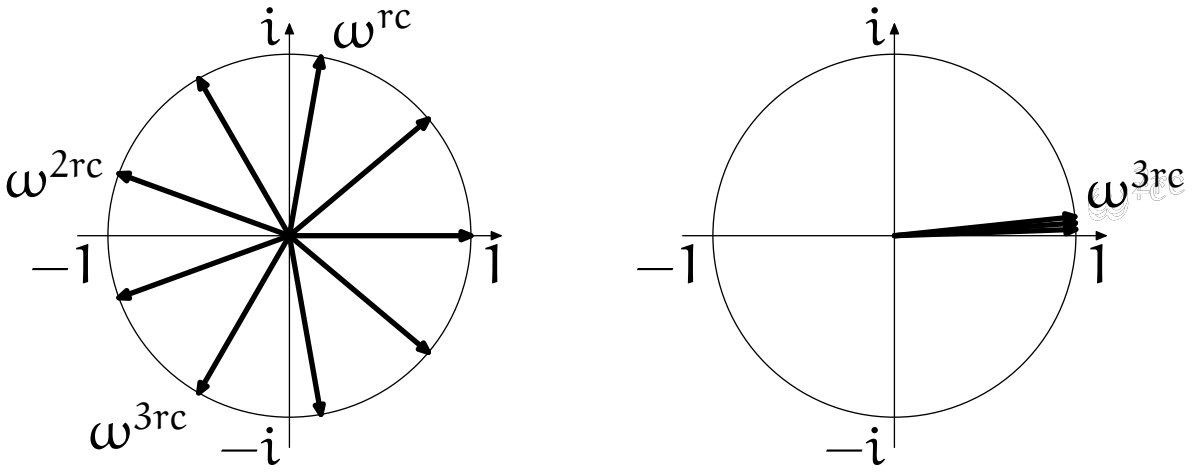
När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



$\| \sum_j (\omega^{rc})^j \|$ = längden av summan av ovanstående vektorer.

Analys av algoritmen – summor av enhetsrötter

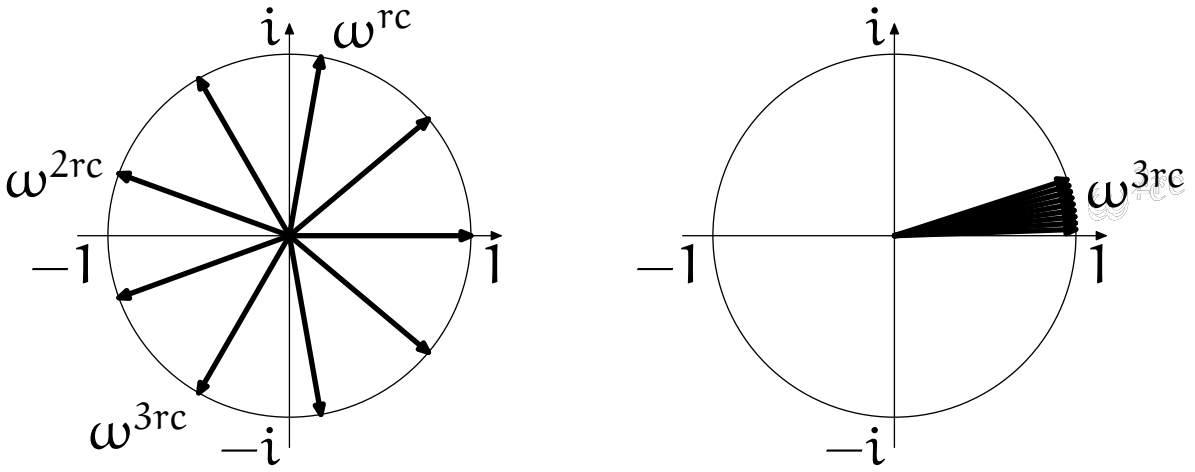
När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



$\| \sum_j (\omega^{rc})^j \|$ = längden av summan av ovanstående vektorer.

Analys av algoritmen – summor av enhetsrötter

När är $\| \sum_j (\omega^{rc})^j \|$ stort? (ω komplext tal med norm 1.)



$\| \sum_j (\omega^{rc})^j \|$ = längden av summan av ovanstående vektorer.

Analys av algoritmen – sammanfattning

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle |c\rangle |x\rangle |N\rangle$

$$\Pr[|x^k\rangle |c\rangle |x\rangle |N\rangle] = 2^{-2m} \left\| \sum_{a : x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \sum_j (\omega^{rc})^j \right\|^2 .$$

Stort om ω^{rc} är nära 1, dvs om $e^{2\pi i rc/2^m}$ är nära 1.

Analys av algoritmen – sammanfattning

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle |c\rangle |x\rangle |N\rangle$

$$\Pr[|x^k\rangle |c\rangle |x\rangle |N\rangle] = 2^{-2m} \left\| \sum_{a : x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \sum_j (\omega^{rc})^j \right\|^2 .$$

Stort om ω^{rc} är nära 1, dvs om $e^{2\pi i rc/2^m}$ är nära 1, dvs om $rc/2^m$ är nästan ett heltal.

Analys av algoritmen – sammanfattning

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle |c\rangle |x\rangle |N\rangle$

$$\Pr[|x^k\rangle |c\rangle |x\rangle |N\rangle] = 2^{-2m} \left\| \sum_{a:x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \sum_j (\omega^{rc})^j \right\|^2.$$

Stort om ω^{rc} är nära 1, dvs om $e^{2\pi i rc/2^m}$ är nära 1, dvs om $rc/2^m$ är nästan ett heltal, dvs om $c2^{-m}$ är nära d/r för något heltal d.

Analys av algoritmen – sammanfattning

Tillstånd när vi mäter: $2^{-m} \sum_{c=0}^{2^m-1} \sum_{a=0}^{2^m-1} \omega^{ac} |x^a\rangle |c\rangle |x\rangle |N\rangle$

$$\Pr[|x^k\rangle |c\rangle |x\rangle |N\rangle] = 2^{-2m} \left\| \sum_{a:x^a \equiv x^k} \omega^{ac} \right\|^2 = 2^{-2m} \left\| \sum_j (\omega^{rc})^j \right\|^2.$$

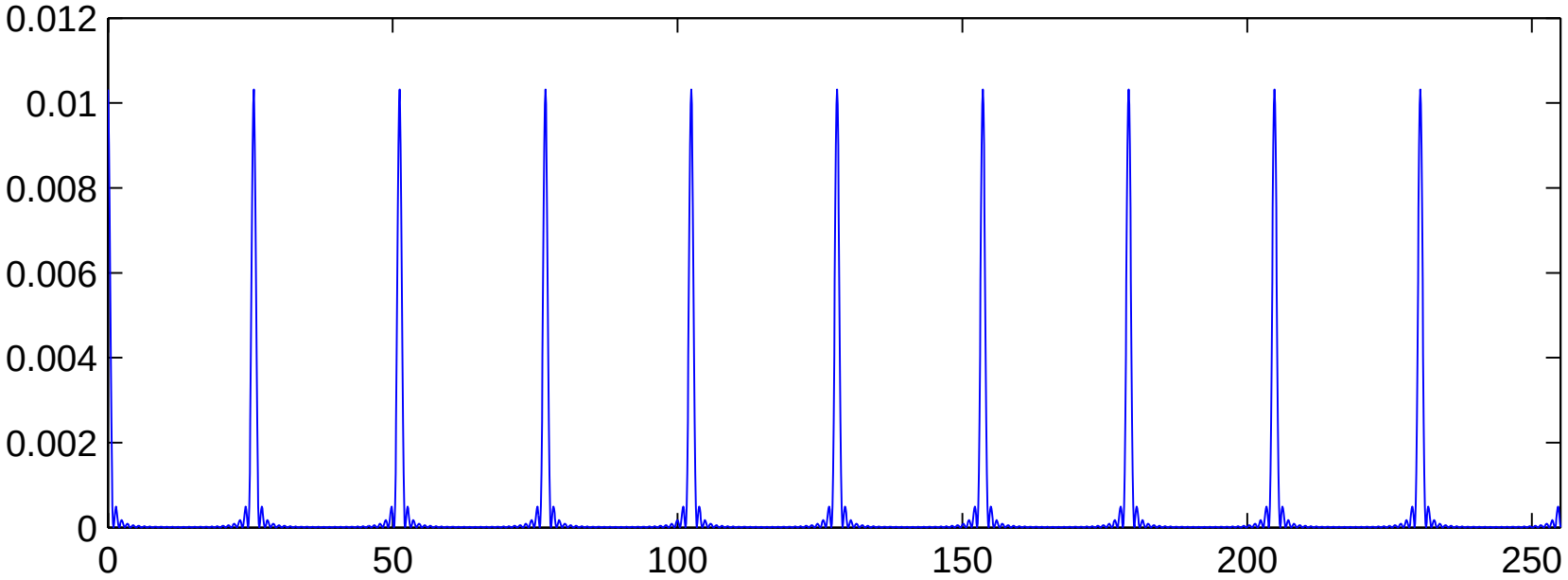
Stort om ω^{rc} är nära 1, dvs om $e^{2\pi i rc/2^m}$ är nära 1, dvs om $rc/2^m$ är nästan ett heltal, dvs om $c2^{-m}$ är nära d/r för något heltal d.

Vi observerar c och vet m, så vi får en approximation till d/r.

Om approximationen är bra kan vi beräkna d och r.

Analys av algoritmen – sannolikheten att se ett visst c

Figuren nedan visar $\Pr[c]$ då $r = 10$ och $m = 8$.



Med hög sannolikhet är $\left\| \frac{c}{2^m} - \frac{d}{r} \right\| \leq \frac{1}{2^{m+1}}$; detta räcker.

Fouriertransformen

Vi vill implementera $|a\rangle \mapsto 2^{-m/2} \sum_{c=0}^{2^m-1} e^{2\pi i ac/2^m} |c\rangle$

Fouriertransformen

Vi vill implementera $|a\rangle \mapsto 2^{-m/2} \sum_{c=0}^{2^m-1} e^{2\pi i ac/2^m} |c\rangle$

En kvantbit: $|a\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{c=0}^{1} e^{2\pi i ac/2} |c\rangle = \frac{1}{\sqrt{2}} \sum_{c=0}^{1} (-1)^{ac} |c\rangle$

Fouriertransformen

Vi vill implementera $|a\rangle \mapsto 2^{-m/2} \sum_{c=0}^{2^m-1} e^{2\pi i ac/2^m} |c\rangle$

En kvantbit: $|a\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{c=0}^{1} e^{2\pi i ac/2} |c\rangle = \frac{1}{\sqrt{2}} \sum_{c=0}^{1} (-1)^{ac} |c\rangle$

$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$;

Fouriertransformen

Vi vill implementera $|a\rangle \mapsto 2^{-m/2} \sum_{c=0}^{2^m-1} e^{2\pi i ac/2^m} |c\rangle$

En kvantbit: $|a\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{c=0}^{1} e^{2\pi i ac/2} |c\rangle = \frac{1}{\sqrt{2}} \sum_{c=0}^{1} (-1)^{ac} |c\rangle$

$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$; $\quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Fouriertransformen

Vi vill implementera $|a\rangle \mapsto 2^{-m/2} \sum_{c=0}^{2^m-1} e^{2\pi i ac/2^m} |c\rangle$

En kvantbit: $|a\rangle \mapsto \frac{1}{\sqrt{2}} \sum_{c=0}^{1} e^{2\pi i ac/2} |c\rangle = \frac{1}{\sqrt{2}} \sum_{c=0}^{1} (-1)^{ac} |c\rangle$

$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$; $\quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

Detta kan göras med rotationen $R = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

Fouriertransformen av två kvantbitar – verktyg

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

Vi kommer att behöva rotationerna från enbitsfallet: R_k roterar bit k.

Vi kommer också att behöva byta fas: $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$

Fouriertransformen av två kvantbitar – verktyg

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

Vi kommer att behöva rotationerna från enbitsfallet: R_k roterar bit k.

Vi kommer också att behöva byta fas: $S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & i \end{pmatrix}$

$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \mapsto \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + i\alpha_{11}|11\rangle$.

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
$|01\rangle \mapsto \frac{1}{2}(|00\rangle$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
$|01\rangle \mapsto \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
$|01\rangle \mapsto \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$
$|10\rangle \mapsto \frac{1}{2}(|00\rangle$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
$|01\rangle \mapsto \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$
$|10\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
$|01\rangle \mapsto \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$
$|10\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
$|11\rangle \mapsto \frac{1}{2}(|00\rangle$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
$|01\rangle \mapsto \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$
$|10\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
$|11\rangle \mapsto \frac{1}{2}(|00\rangle - i|01\rangle - |10\rangle + i|11\rangle)$

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
$|01\rangle \mapsto \frac{1}{2}(|00\rangle + i|01\rangle - |10\rangle - i|11\rangle)$
$|10\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
$|11\rangle \mapsto \frac{1}{2}(|00\rangle - i|01\rangle - |10\rangle + i|11\rangle)$

Vi kan multiplicera med i genom att byta fas.
Samla därför termer som innehåller i.

Fouriertransformen av två kvantbitar – intuition

Vi vill implementera $|a\rangle \mapsto \frac{1}{2}\sum_{c=0}^{3} e^{2\pi i ac/4}|c\rangle = \frac{1}{2}\sum_{c=0}^{3} i^{ac}|c\rangle$.

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$
$|01\rangle \mapsto \frac{1}{2}(|00\rangle - |10\rangle) + i\frac{1}{2}(|01\rangle - |11\rangle)$
$|10\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
$|11\rangle \mapsto \frac{1}{2}(|00\rangle - |10\rangle) + i\frac{1}{2}(-|01\rangle + |11\rangle)$

Vi kan multiplicera med i genom att byta fas.
Samla därför termer som innehåller i.

Notera att i enbart dyker upp om bit noll är 1 i VL.
Rotation av bit ett ändrar $|b_1 b_0\rangle$ till ungefär $|0 b_0\rangle \pm |1 b_0\rangle$.

Fouriertransformen av två kvantbitar – konstruktion

Rotera först bit ett (R_1):

$|00\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$; $\quad |01\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle$

$|10\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle$; $\quad |11\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle$

Fouriertransformen av två kvantbitar – konstruktion

Rotera först bit ett (R_1):

$$|00\rangle \mapsto \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|10\rangle; \quad |01\rangle \mapsto \tfrac{1}{\sqrt{2}}|01\rangle + \tfrac{1}{\sqrt{2}}|11\rangle$$
$$|10\rangle \mapsto \tfrac{1}{\sqrt{2}}|00\rangle - \tfrac{1}{\sqrt{2}}|10\rangle; \quad |11\rangle \mapsto \tfrac{1}{\sqrt{2}}|01\rangle - \tfrac{1}{\sqrt{2}}|11\rangle$$

Byt sedan fas ($S \circ R_1$):

$$|00\rangle \mapsto \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|10\rangle; \quad |01\rangle \mapsto \tfrac{1}{\sqrt{2}}|01\rangle + i\tfrac{1}{\sqrt{2}}|11\rangle$$
$$|10\rangle \mapsto \tfrac{1}{\sqrt{2}}|00\rangle - \tfrac{1}{\sqrt{2}}|10\rangle; \quad |11\rangle \mapsto \tfrac{1}{\sqrt{2}}|01\rangle - i\tfrac{1}{\sqrt{2}}|11\rangle$$

Fouriertransformen av två kvantbitar – konstruktion

Rotera först bit ett (R_1):

$$|00\rangle \mapsto \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|10\rangle; \quad |01\rangle \mapsto \tfrac{1}{\sqrt{2}}|01\rangle + \tfrac{1}{\sqrt{2}}|11\rangle$$
$$|10\rangle \mapsto \tfrac{1}{\sqrt{2}}|00\rangle - \tfrac{1}{\sqrt{2}}|10\rangle; \quad |11\rangle \mapsto \tfrac{1}{\sqrt{2}}|01\rangle - \tfrac{1}{\sqrt{2}}|11\rangle$$

Byt sedan fas ($S \circ R_1$):

$$|00\rangle \mapsto \tfrac{1}{\sqrt{2}}|00\rangle + \tfrac{1}{\sqrt{2}}|10\rangle; \quad |01\rangle \mapsto \tfrac{1}{\sqrt{2}}|01\rangle + \mathrm{i}\tfrac{1}{\sqrt{2}}|11\rangle$$
$$|10\rangle \mapsto \tfrac{1}{\sqrt{2}}|00\rangle - \tfrac{1}{\sqrt{2}}|10\rangle; \quad |11\rangle \mapsto \tfrac{1}{\sqrt{2}}|01\rangle - \mathrm{i}\tfrac{1}{\sqrt{2}}|11\rangle$$

Mönstermatchning – vi vill egentligen ha:

$$|00\rangle \mapsto \tfrac{1}{2}(|00\rangle + |01\rangle) + \tfrac{1}{2}(|10\rangle + |11\rangle); \quad |01\rangle \mapsto \tfrac{1}{2}(|00\rangle - |10\rangle) + \mathrm{i}\tfrac{1}{2}(|01\rangle - |11\rangle)$$
$$|10\rangle \mapsto \tfrac{1}{2}(|00\rangle - |01\rangle) + \tfrac{1}{2}(|10\rangle - |11\rangle); \quad |11\rangle \mapsto \tfrac{1}{2}(|00\rangle - |10\rangle) - \mathrm{i}\tfrac{1}{2}(|01\rangle - |11\rangle)$$

Fouriertransformen av två kvantbitar – konstruktion

$S \circ R_1$ ger:

$|00\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$; $\quad |01\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle + i\frac{1}{\sqrt{2}}|11\rangle$

$|10\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle$; $\quad |11\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle - i\frac{1}{\sqrt{2}}|11\rangle$

Fouriertransformen av två kvantbitar – konstruktion

$S \circ R_1$ ger:

$|00\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle; \quad |01\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle + i\frac{1}{\sqrt{2}}|11\rangle$

$|10\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle; \quad |11\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle - i\frac{1}{\sqrt{2}}|11\rangle$

Rotera nu bit noll ($R_0 \circ S \circ R_1$):

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle) + \frac{1}{2}(|10\rangle + |11\rangle); \quad |01\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle) + i\frac{1}{2}(|10\rangle - |11\rangle)$

$|10\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle) - \frac{1}{2}(|10\rangle + |11\rangle); \quad |11\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle) - i\frac{1}{2}(|10\rangle - |11\rangle)$

Fouriertransformen av två kvantbitar – konstruktion

$S \circ R_1$ ger:

$|00\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle; \quad |01\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle + i\frac{1}{\sqrt{2}}|11\rangle$

$|10\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle; \quad |11\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle - i\frac{1}{\sqrt{2}}|11\rangle$

Rotera nu bit noll ($R_0 \circ S \circ R_1$):

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle) + \frac{1}{2}(|10\rangle + |11\rangle); \quad |01\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle) + i\frac{1}{2}(|10\rangle - |11\rangle)$

$|10\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle) - \frac{1}{2}(|10\rangle + |11\rangle); \quad |11\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle) - i\frac{1}{2}(|10\rangle - |11\rangle)$

Mönstermatchning – vi vill egentligen ha:

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle) + \frac{1}{2}(|10\rangle + |11\rangle); \quad |01\rangle \mapsto \frac{1}{2}(|00\rangle - |10\rangle) + i\frac{1}{2}(|01\rangle - |11\rangle)$

$|10\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle) + \frac{1}{2}(|10\rangle - |11\rangle); \quad |11\rangle \mapsto \frac{1}{2}(|00\rangle - |10\rangle) - i\frac{1}{2}(|01\rangle - |11\rangle)$

Fouriertransformen av två kvantbitar – konstruktion

$S \circ R_1$ ger:

$|00\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$; $|01\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle + i\frac{1}{\sqrt{2}}|11\rangle$

$|10\rangle \mapsto \frac{1}{\sqrt{2}}|00\rangle - \frac{1}{\sqrt{2}}|10\rangle$; $|11\rangle \mapsto \frac{1}{\sqrt{2}}|01\rangle - i\frac{1}{\sqrt{2}}|11\rangle$

Rotera nu bit noll ($R_0 \circ S \circ R_1$):

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle) + \frac{1}{2}(|10\rangle + |11\rangle)$; $|01\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle) + i\frac{1}{2}(|10\rangle - |11\rangle)$

$|10\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle) - \frac{1}{2}(|10\rangle + |11\rangle)$; $|11\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle) - i\frac{1}{2}(|10\rangle - |11\rangle)$

Mönstermatchning – vi vill egentligen ha:

$|00\rangle \mapsto \frac{1}{2}(|00\rangle + |01\rangle) + \frac{1}{2}(|10\rangle + |11\rangle)$; $|01\rangle \mapsto \frac{1}{2}(|00\rangle - |10\rangle) + i\frac{1}{2}(|01\rangle - |11\rangle)$

$|10\rangle \mapsto \frac{1}{2}(|00\rangle - |01\rangle) + \frac{1}{2}(|10\rangle - |11\rangle)$; $|11\rangle \mapsto \frac{1}{2}(|00\rangle - |10\rangle) - i\frac{1}{2}(|01\rangle - |11\rangle)$

Vi är nästan klara, vi behöver bara byta ordning på bitarna i HL!

Fouriertransformen – generella fallet

Transformen av två kvantbitar kan skrivas $R_0 \circ S \circ R_1 \circ$ (bitvändning).
Detta går att generalisera.

Fouriertransformen – generella fallet

Transformen av två kvantbitar kan skrivas $R_0 \circ S \circ R_1 \circ$ (bitvändning).
Detta går att generalisera.

Vi använder operationerna R_k – operera med $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ på bit k – och

$S_{k\ell}$ – operera med $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^{\ell-k}} \end{pmatrix}$ på bitarna k och ℓ.

Fouriertransformen – generella fallet

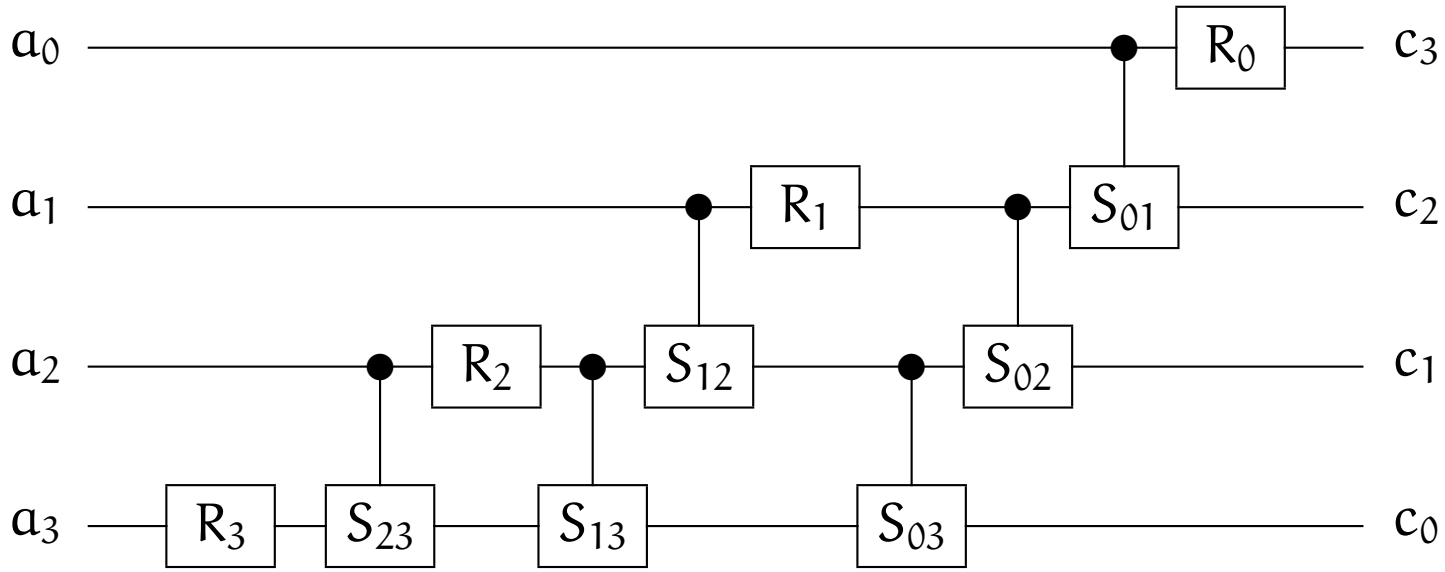
Transformen av två kvantbitar kan skrivas $R_0 \circ S \circ R_1 \circ$ (bitvändning).
Detta går att generalisera.

Vi använder operationerna R_k – operera med $\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ på bit k – och

$S_{k\ell}$ – operera med $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{2\pi i/2^{\ell-k}} \end{pmatrix}$ på bitarna k och ℓ.

Transformen av n bitar kan då skrivas
$R_0 \circ S_{0,1} \circ \cdots \circ S_{0,n-1} \circ R_1 \circ \cdots \circ R_{n-3} \circ S_{n-3,n-2} \circ S_{n-3,n-1} \circ R_{n-2} \circ S_{n-2,n-1} \circ R_{n-1}$.

Fouriertransformen – grafiskt schema



Antal operationer: $O(n^2)$.

Avslutning

Vi kan faktorisera i polynomisk tid med kvantberäkningar.

Är modellen realistisk?

Avslutning

Vi kan faktorisera i polynomisk tid med kvantberäkningar.

Är modellen realistisk? Svårt att säga. . .

Avslutning

Vi kan faktorisera i polynomisk tid med kvantberäkningar.

Är modellen realistisk? Svårt att säga. . .

Det verkar svårt att bygga datorer enligt modellen.
Rekord för närvarande: 7 bitar, faktorisera 15.
(*Nature* 414, ss 883–887, 2001.)

Avslutning

Vi kan faktorisera i polynomisk tid med kvantberäkningar.

Är modellen realistisk? Svårt att säga. . .

Det verkar svårt att bygga datorer enligt modellen.
Rekord för närvarande: 7 bitar, faktorisera 15.
(*Nature* 414, ss 883–887, 2001.)

Å andra sidan har den klassiska datorn utvecklas en hel del sedan turingmaskinen introducerades – kanske ska vi inte bygga kvantdatorer exakt enligt modellen?

Avslutning

Vi kan faktorisera i polynomisk tid med kvantberäkningar.

Är modellen realistisk? Svårt att säga. . .

Det verkar svårt att bygga datorer enligt modellen.
Rekord för närvarande: 7 bitar, faktorisera 15.
(*Nature* 414, ss 883–887, 2001.)

Å andra sidan har den klassiska datorn utvecklas en hel del sedan turingmaskinen introducerades – kanske ska vi inte bygga kvantdatorer exakt enligt modellen?

Ett modellproblem: Hur stoppar vi in indata i kvantbitarna? Kräver att bitarna tvingas till ett specifikt tillstånd.