Kvantdatorer & kvantprogrammering

Martin Jirlow

2020-03-04

Lite om mig

- Har haft intresse för datorer hela mitt liv.
- Började programmera när jag var 11 år gammal.
- Jobbade ett år efter gymnasiet med bildbehandling.
- Studerar nu första året på Teknisk Matematik på Chalmers.

Vad är en kvantdator?

Vad är en kvantdator?

En kvantdator:

Vad är en kvantdator?

En kvantdator:

- Har kvantbitar istället för vanliga bitar

Vad är en kvantdator?

En kvantdator:

- Har kvantbitar istället för vanliga bitar
- Utför operationer direkt på minnet

Vad är en kvantdator?

En kvantdator:

- Har kvantbitar istället för vanliga bitar
- Utför operationer direkt på minnet
- Är väldigt svåra att bygga

Vad är en kvantdator?

En kvantdator:

- Har kvantbitar istället för vanliga bitar
- Utför operationer direkt på minnet
- Är väldigt svåra att bygga
- **Är inte alltid bättre!**

En kvantdator löser inte allt

Det är ett vanligt missförstånd att kvantdatorer är snabbare en klassiska datorer i allmänhet. Detta stämmer inte!

En kvantdator löser inte allt

Det är ett vanligt missförstånd att kvantdatorer är snabbare en klassiska datorer i allmänhet. Detta stämmer inte!

Kvantdatorer kan utnyttja kvantmekaniska fenomen för att lösa vissa problem på helt nya sätt.

En kvantdator löser inte allt

Det är ett vanligt missförstånd att kvantdatorer är snabbare en klassiska datorer i allmänhet. Detta stämmer inte!

Kvantdatorer kan utnyttja kvantmekaniska fenomen för att lösa vissa problem på helt nya sätt. Detta kräver helt nya algoritmer och sätt att tänka kring programmering.

Problem kvantdatorer är bra på

Kvantdatorer är självklart bra på att simulera system som själva är kvantmekaniska, exempelvis atomer, molekyler, magnetism och spinsystem.

Problem kvantdatorer är bra på

Kvantdatorer är självklart bra på att simulera system som själva är kvantmekaniska, exempelvis atomer, molekyler, magnetism och spinsystem. Utöver detta har man upptäckt andra problem som kan förbättras med kvantdatorer, till exempel:

- Primtalsfaktorisering av stora tal
- Enkryptering
- Kommunikation (superdense coding)
- Många fler problem...

Kort om kvantmekanik

Kvantmekanik

- En övergripande teori

Kvantmekanik

- En övergripande teori
- Upptäcktes gradvis av ett flertal forskare under 1900-talet
  - Max Planck (kvantisering av svartkroppstrålning, 1900)
  - Albert Einstein (fotoelektriska effekten, 1905)
  - Erwin Schrödinger
  - Werner Heisenberg

Kvantmekanik

- En övergripande teori
- Upptäcktes gradvis av ett flertal forskare under 1900-talet
  - Max Planck (kvantisering av svartkroppstrålning, 1900)
  - Albert Einstein (fotoelektriska effekten, 1905)
  - Erwin Schrödinger
  - Werner Heisenberg
- Beskriver hur materia och energi beter sig i mikrokosmos

Kvantmekanik

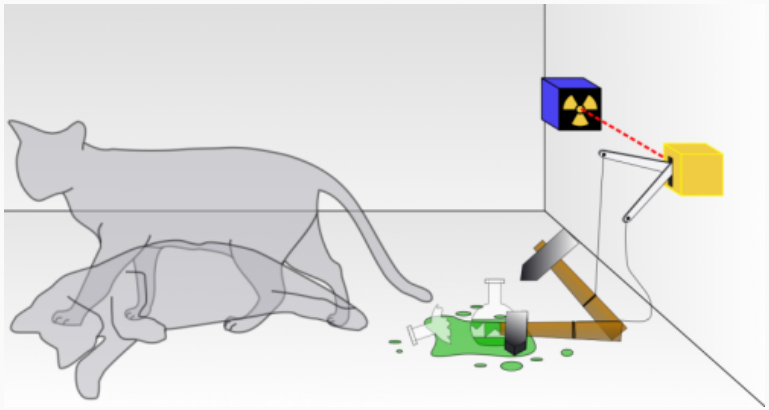
- En övergripande teori
- Upptäcktes gradvis av ett flertal forskare under 1900-talet
  - Max Planck (kvantisering av svartkroppstrålning, 1900)
  - Albert Einstein (fotoelektriska effekten, 1905)
  - Erwin Schrödinger
  - Werner Heisenberg
- Beskriver hur materia och energi beter sig i mikrokosmos
- Kan enbart göra statistiska förutsägningar

Kvantmekanik

- En övergripande teori
- Upptäcktes gradvis av ett flertal forskare under 1900-talet
  - Max Planck (kvantisering av svartkroppstrålning, 1900)
  - Albert Einstein (fotoelektriska effekten, 1905)
  - Erwin Schrödinger
  - Werner Heisenberg
- Beskriver hur materia och energi beter sig i mikrokosmos
- Kan enbart göra statistiska förutsägningar
- Kvantobjekt är både partiklar och vågor (Våg-partikeldualiteten)

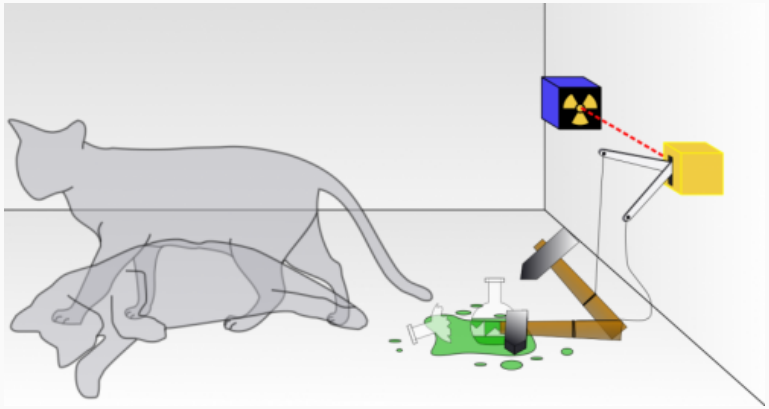
Superposition

- Ett viktigt begrepp: superposition.



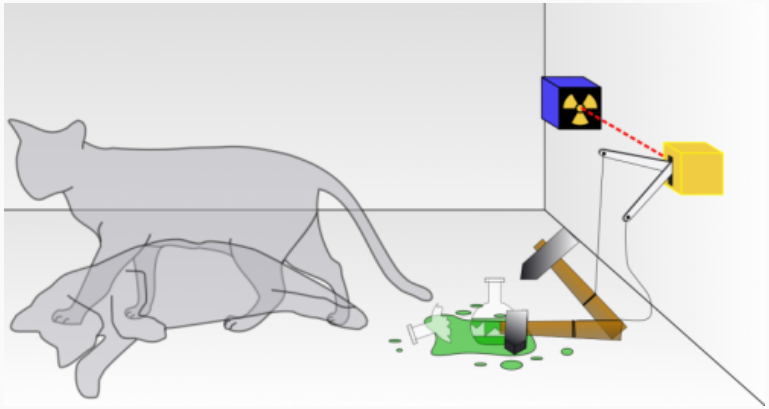
Superposition

- Ett viktigt begrepp: superposition.
- En kvantpartikel kan befinna sig mellan olika tillstånd. Den beter sig då som en våg och beskrivs med en vågfunktion.



Superposition

- Ett viktigt begrepp: superposition.
- En kvantpartikel kan befinna sig mellan olika tillstånd. Den beter sig då som en våg och beskrivs med en vågfunktion.
- Om vi däremot försöker mäta vilket tillstånd partikeln befinner sig i, så kommer vågfunktionen kollapsa till ett av de möjliga tillstånden enligt någon sannolikhet.



Sammanflätning

Ett annat viktigt koncept är sammanflätning. Två kvantpartiklar kan vara sammanflätade, vilket innebär att egenskaper hos den ena kvantpartikeln beror av den andra.

Sammanflätning

Ett annat viktigt koncept är sammanflätning. Två kvantpartiklar kan vara sammanflätade, vilket innebär att egenskaper hos den ena kvantpartikeln beror av den andra.

Om två kvantpartiklar som är sammanflätade befinner sig i en superposition så kommer de båda kollapsa tillsammans.

Sammanflätning

Ett annat viktigt koncept är sammanflätning. Två kvantpartiklar kan vara sammanflätade, vilket innebär att egenskaper hos den ena kvantpartikeln beror av den andra.

Om två kvantpartiklar som är sammanflätade befinner sig i en superposition så kommer de båda kollapsa tillsammans. Om vi mäter den ena av kvantpartiklarna så vet vi med säkerhet vad den andra kommer mätas till.

Kvantbitar

Kvantbitar

Klassisk bit

Kvantbit

Kvantbitar

Klassisk bit

- Har två möjliga tillstånd, $|0\rangle$ och $|1\rangle$

Kvantbit

- Har tillstånden $|0\rangle$ och $|1\rangle$, och superpositioner däremellan

Kvantbitar

Klassisk bit

- Har två möjliga tillstånd, $|0\rangle$ och $|1\rangle$
- Operationer görs med logiska grindar

Kvantbit

- Har tillstånden $|0\rangle$ och $|1\rangle$, och superpositioner däremellan
- Operationer görs med kvantgrindar

Kvantbitar

Klassisk bit

- Har två möjliga tillstånd, $|0\rangle$ och $|1\rangle$
- Operationer görs med logiska grindar
- Beskrivs oftast med elektriska spänningsskillnader

Kvantbit

- Har tillstånden $|0\rangle$ och $|1\rangle$, och superpositioner däremellan
- Operationer görs med kvantgrindar
- Beskrivs med kvantmekaniska egenskaper

Kvantbitar

Klassisk bit

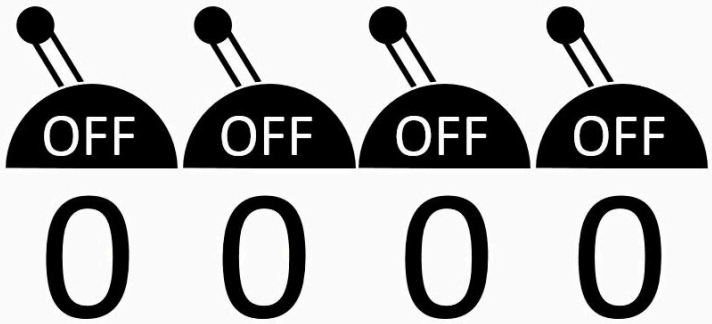
- Har två möjliga tillstånd, $|0\rangle$ och $|1\rangle$
- Operationer görs med logiska grindar
- Beskrivs oftast med elektriska spänningsskillnader
- Kan läsas utan att påverkas

Kvantbit

- Har tillstånden $|0\rangle$ och $|1\rangle$, och superpositioner däremellan
- Operationer görs med kvantgrindar
- Beskrivs med kvantmekaniska egenskaper
- **Mätning påverkar dess tillstånd**

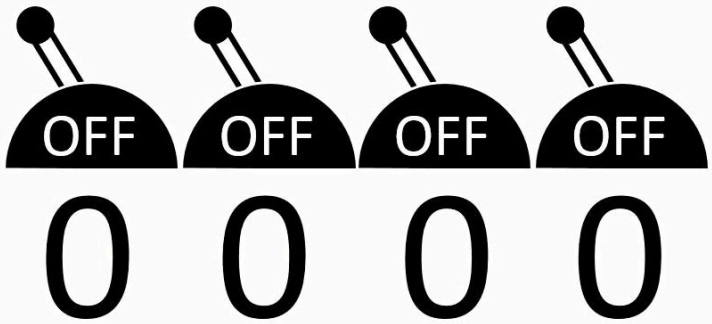
En klassisk bit

En klassisk bit kan ha tillstånd $|0\rangle$ och $|1\rangle$.



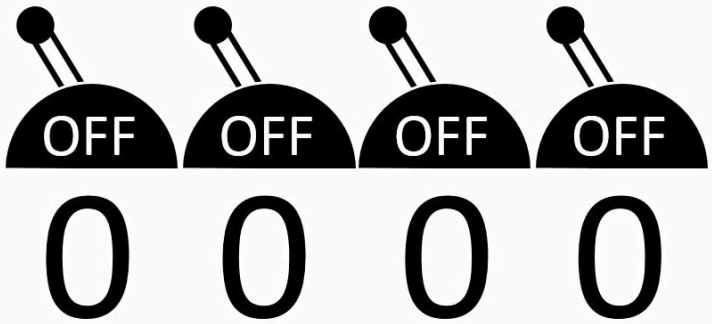
En klassisk bit

En klassisk bit kan ha tillstånd $|0\rangle$ och $|1\rangle$.
Det finns bara en operation vi kan göra med varje enskild bit: Vi kan vända på den.



En klassisk bit

En klassisk bit kan ha tillstånd $|0\rangle$ och $|1\rangle$.
Det finns bara en operation vi kan göra med varje enskild bit: Vi kan vända på den.
Detta görs med en logisk grind som kallas $\mathbf{NOT}$.



En kvantbit

En kvantbit kan också ha tillstånden $|0\rangle$ och $|1\rangle$...

En kvantbit

En kvantbit kan också ha
tillstånden $|0\rangle$ och $|1\rangle$...
och alla tillstånd däremellan:

$$a\,|0\rangle + b\,|1\rangle$$

så att

$$|a|^2 + |b|^2 = 1$$

En kvantbit

En kvantbit kan också ha
tillstånden $|0\rangle$ och $|1\rangle$...
och alla tillstånd däremellan:

$$a\,|0\rangle + b\,|1\rangle$$

så att

$$|a|^2 + |b|^2 = 1$$

a och b kan vara komplexa tal.
Detta bildar

En kvantbit

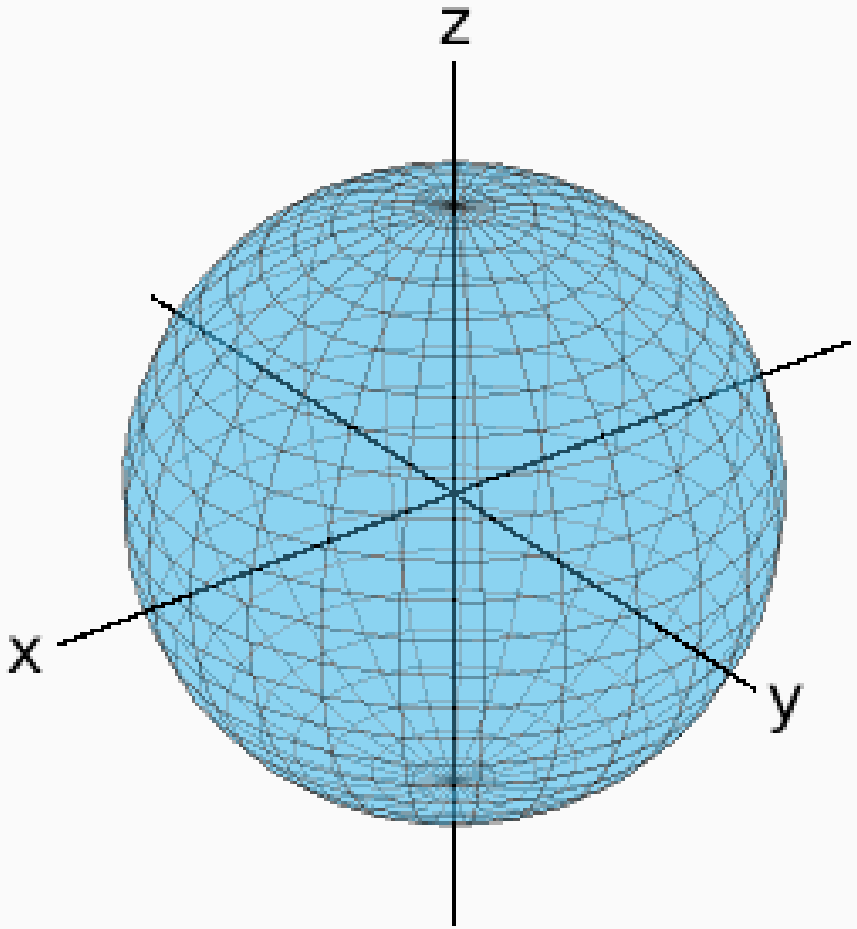
En kvantbit kan också ha tillstånden $|0\rangle$ och $|1\rangle$...
och alla tillstånd däremellan:

$$a\,|0\rangle + b\,|1\rangle$$

så att

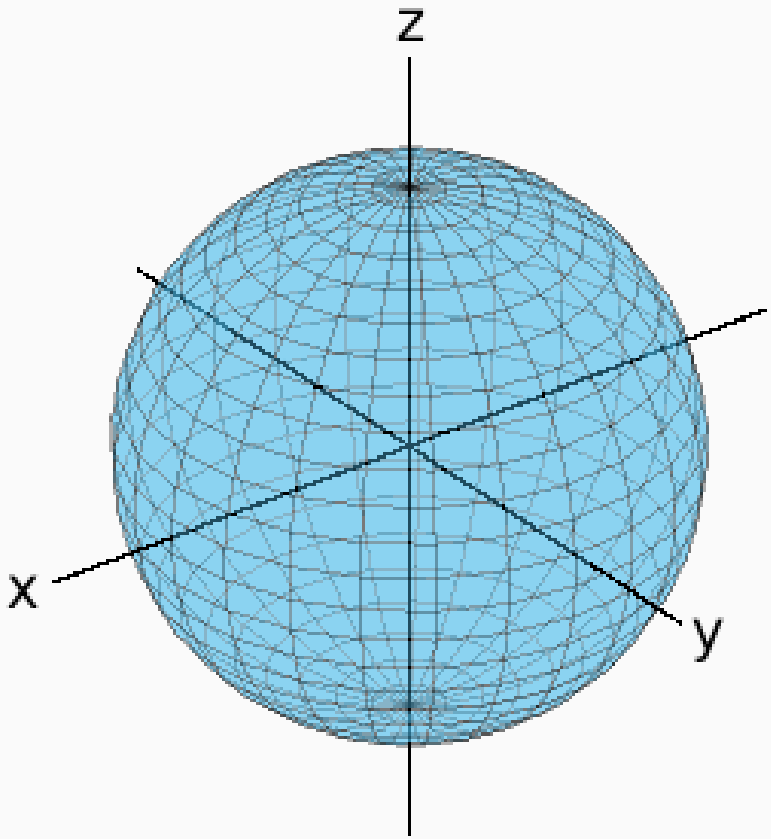
$$|a|^2 + |b|^2 = 1$$

a och b kan vara komplexa tal.
Detta bildar **en sfär!**



Blochsfären

Matematiken bakom kvantbitar är mest linjär algebra och utelämnas här.
Den viktiga bilden att ha är att en kvantbit kan ses som en sfär.

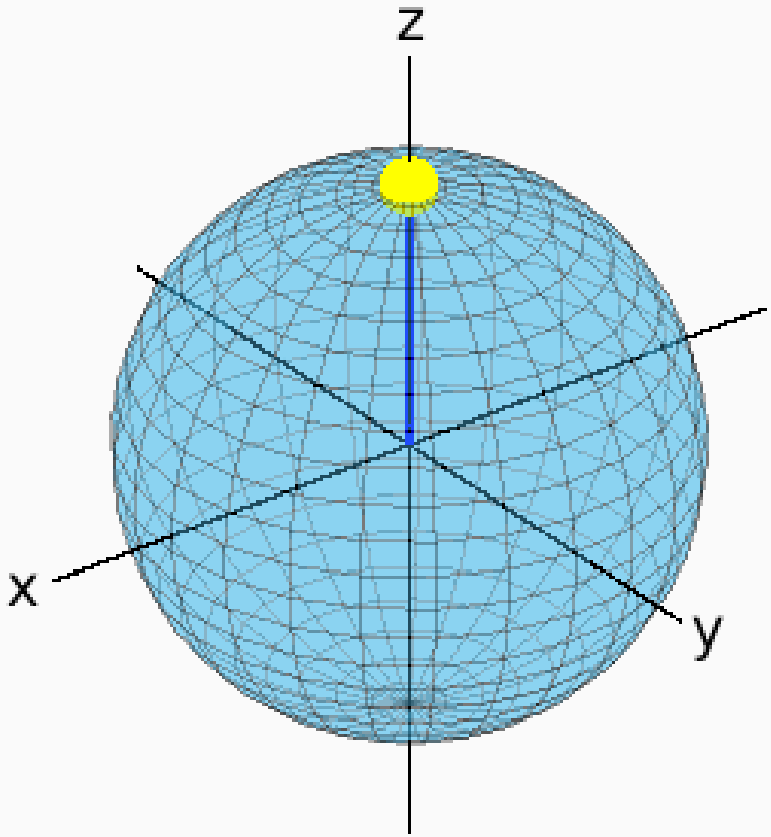


Blochsfären

Matematiken bakom kvantbitar är mest linjär algebra och utelämnas här.
Den viktiga bilden att ha är att en kvantbit kan ses som en sfär.

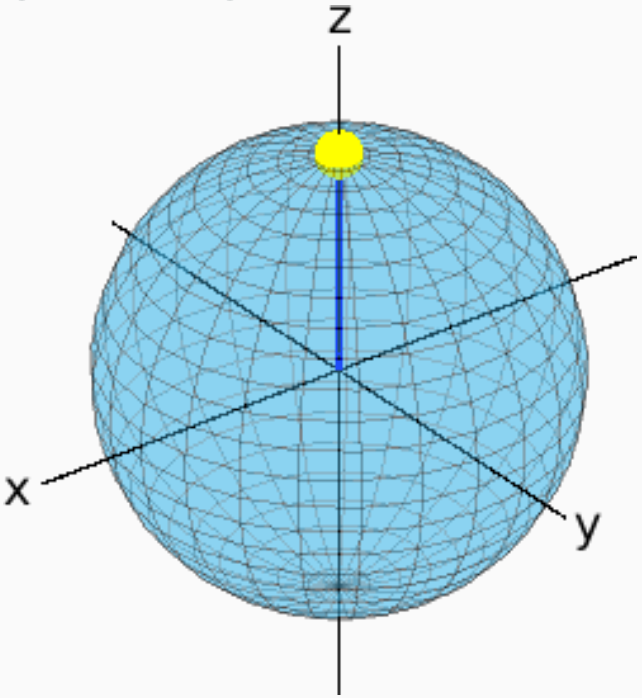
Tillståndet en specifik kvantbit är i beskrivs med en **punkt på sfären**.

Denna sfär kallas för Blochsfären.

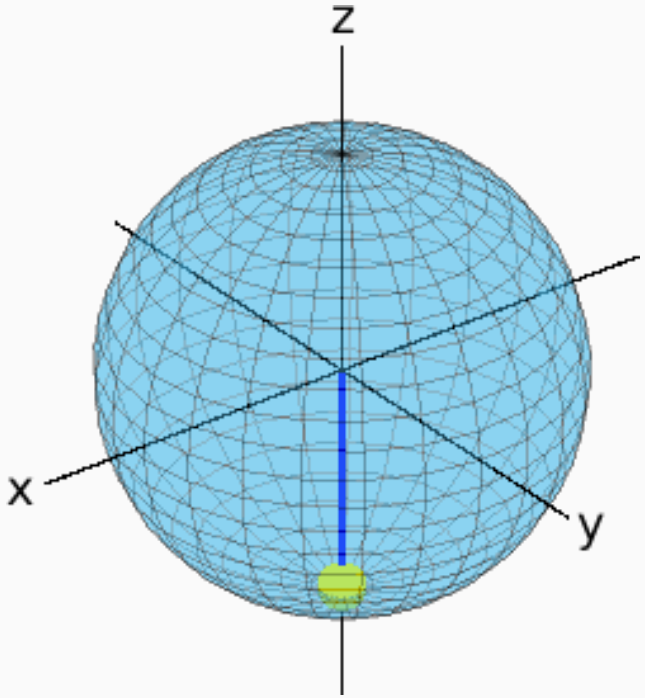


En kvantbit

Några vanliga tillstånd är:



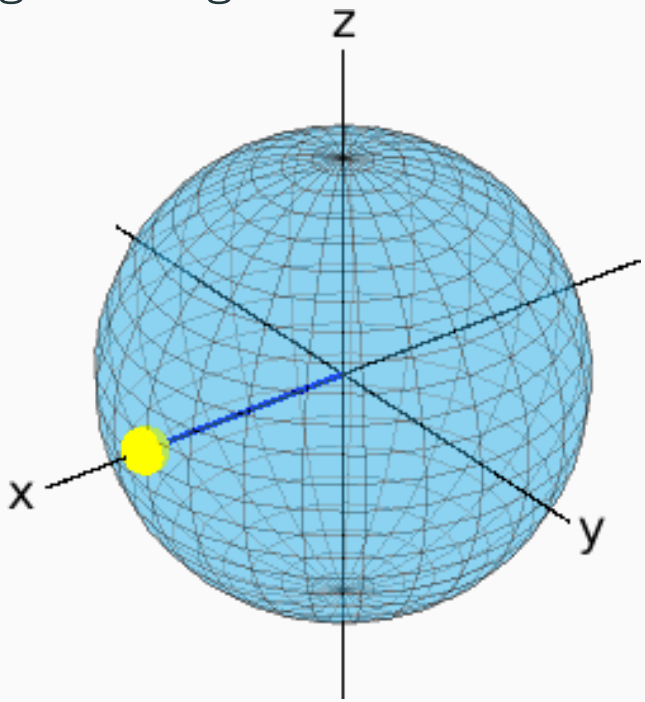
$|0\rangle$



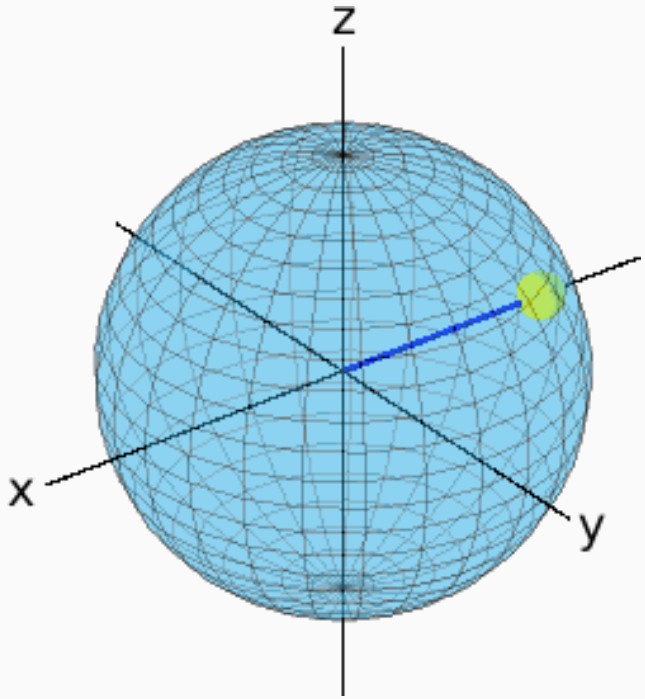
$|1\rangle$

En kvantbit

Några vanliga tillstånd är:



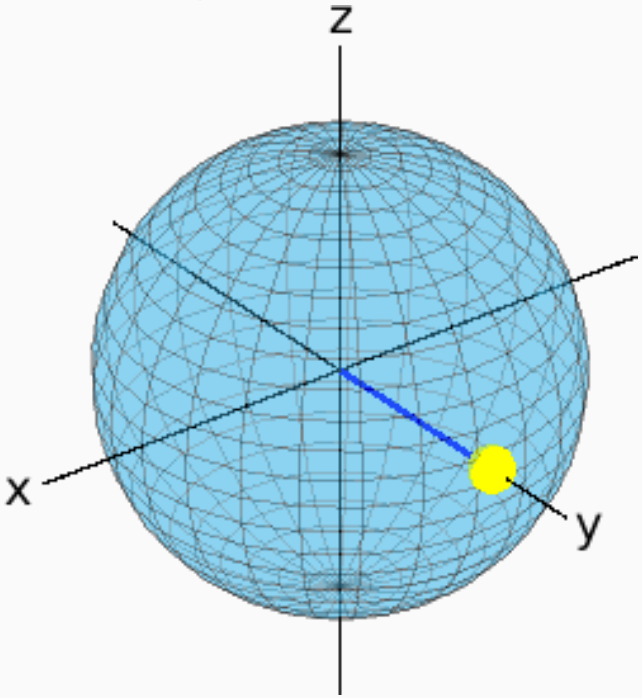
$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$



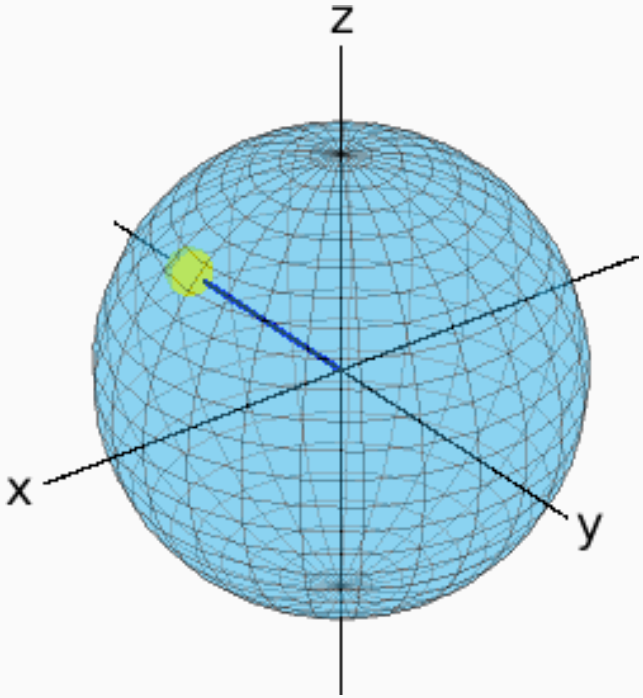
$$|-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

En kvantbit

Några vanliga tillstånd är:



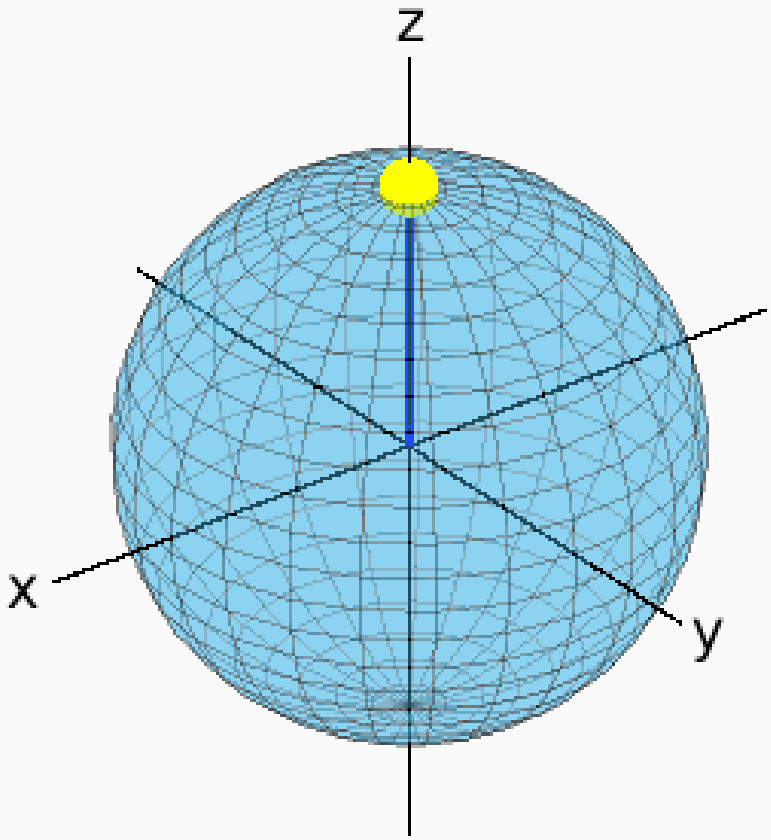
$$|\mu\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{i}{\sqrt{2}}|1\rangle$$



$$|\nu\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{i}{\sqrt{2}}|1\rangle$$

En kvantbit

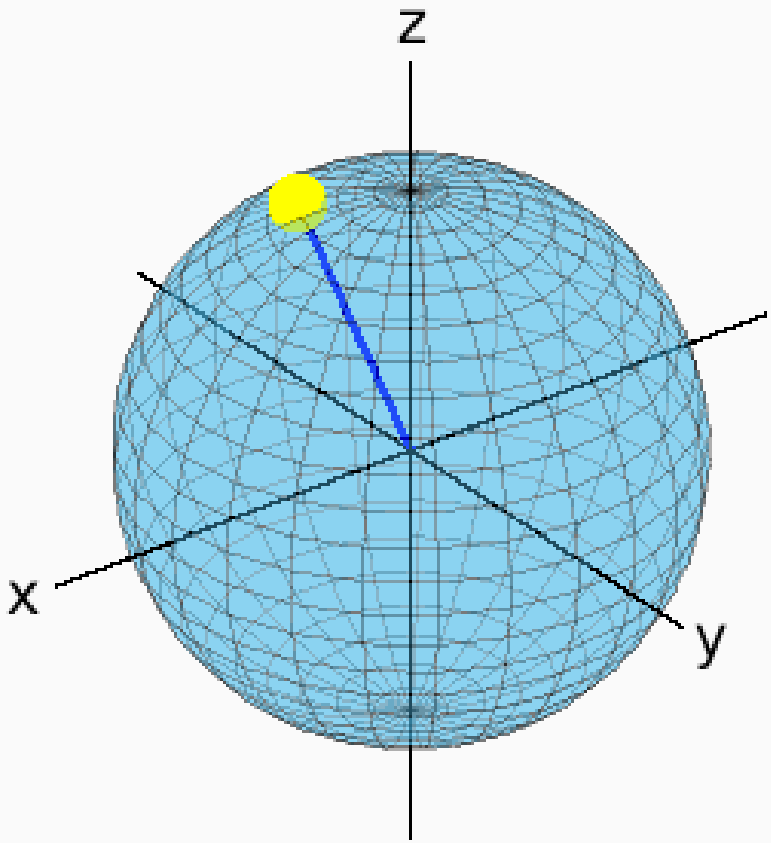
När vi mäter en kvantbit för att se vilket värde den har så kollapsar den till $|0\rangle$ eller $|1\rangle$, alltså nord- eller sydpolen på Blochsfären.



En kvantbit

När vi mäter en kvantbit för att se vilket värde den har så kollapsar den till $|0\rangle$ eller $|1\rangle$, alltså nord- eller sydpolen på Blochsfären.

Sannolikheten att kollapsa till $|0\rangle$ beror på hur nära nordpolen kvantbiten är.

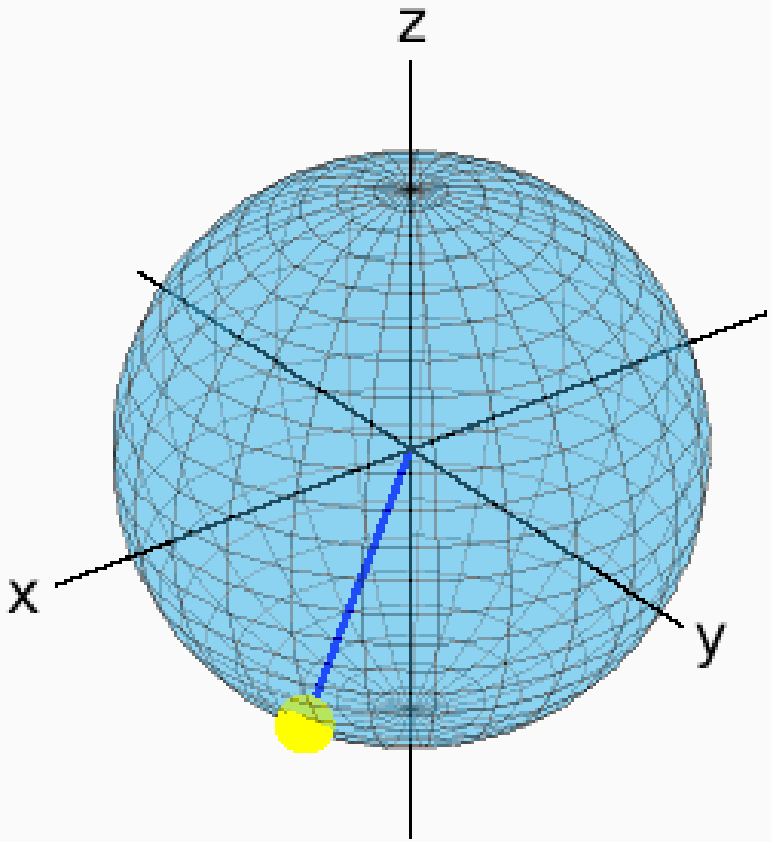


En kvantbit

När vi mäter en kvantbit för att se vilket värde den har så kollapsar den till $|0\rangle$ eller $|1\rangle$, alltså nord- eller sydpolen på Blochsfären.

Sannolikheten att kollapsa till $|0\rangle$ beror på hur nära nordpolen kvantbiten är.

Sannolikheten att kollapsa till $|1\rangle$ beror på hur nära sydpolen kvantbiten är.



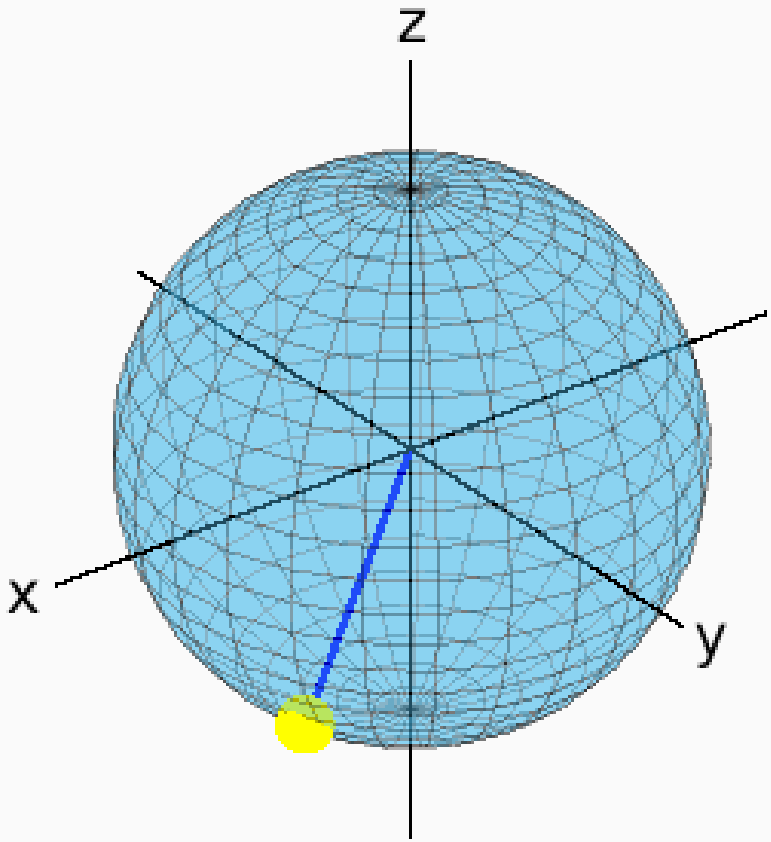
En kvantbit

När vi mäter en kvantbit för att se vilket värde den har så kollapsar den till $|0\rangle$ eller $|1\rangle$, alltså nord- eller sydpolen på Blochsfären.

Sannolikheten att kollapsa till $|0\rangle$ beror på hur nära nordpolen kvantbiten är.

Sannolikheten att kollapsa till $|1\rangle$ beror på hur nära sydpolen kvantbiten är.

$|+\rangle$, $|-\rangle$, $|\mu\rangle$, $|\nu\rangle$ kollapsar alltså alla till $|1\rangle$ 50% av gångerna.



Flera kvantbitar

Om vi har två kvantbitar som båda är $|0\rangle$ kan vi skriva detta som $|00\rangle$.

Flera kvantbitar

Om vi har två kvantbitar som båda är $|0\rangle$ kan vi skriva detta som $|00\rangle$.
Två kvantbitar kan sammanlagt befinna sig i fyra tillstånd:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

Flera kvantbitar

Om vi har två kvantbitar som båda är $|0\rangle$ kan vi skriva detta som $|00\rangle$.
Två kvantbitar kan sammanlagt befinna sig i fyra tillstånd:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

och alla superpositioner av dessa fyra tillstånd:

$$a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

Flera kvantbitar

Om vi har två kvantbitar som båda är $|0\rangle$ kan vi skriva detta som $|00\rangle$. Två kvantbitar kan sammanlagt befinna sig i fyra tillstånd:

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle$$

och alla superpositioner av dessa fyra tillstånd:

$$a\,|00\rangle + b\,|01\rangle + c\,|10\rangle + d\,|11\rangle$$

Hädanefter kommer vi inte skriva ut talen a, b, c och d då vi skriver ut superpositioner, för att göra det enklare att läsa och för att det viktigaste är att veta att vi har en superposition, inte exakta formen på den.

Kvantgrindar

Kvantgrindar på en kvantbit

Med klassiska bitar finns det endast en grind vi kan använda på en ensam bit, $\mathbf{NOT}$.

Kvantgrindar på en kvantbit

Med klassiska bitar finns det endast en grind vi kan använda på en ensam bit, **NOT**.

Då en kvantbit inte bara kan vara av och på utan oändligt många tillstånd däremellan så behöver vi betydligt fler grindar än **NOT** för att kunna nå en kvantbits fulla potential.

Kvantgrindar på en kvantbit

Med klassiska bitar finns det endast en grind vi kan använda på en ensam bit, $\mathbf{NOT}$.

Då en kvantbit inte bara kan vara av och på utan oändligt många tillstånd däremellan så behöver vi betydligt fler grindar än $\mathbf{NOT}$ för att kunna nå en kvantbits fulla potential.

Vi börjar med att definiera fyra kvantgrindar för en bit: $\mathbf{X}$, $\mathbf{Z}$, $\mathbf{S}$ och $\mathbf{H}$.

Kvantgrinden X

Kvantgrinden $\mathbf{X}$ är kvantbitens motsvarighet till $\mathbf{NOT}$.

Kvantgrinden X

Kvantgrinden $\mathbf{X}$ är kvantbitens motsvarighet till $\mathbf{NOT}$. Det gäller alltså att

$$\mathbf{X}\,|0\rangle = |1\rangle$$
$$\mathbf{X}\,|1\rangle = |0\rangle\,.$$

Kvantgrinden X

Kvantgrinden $\mathbf{X}$ är kvantbitens motsvarighet till $\mathbf{NOT}$. Det gäller alltså att

$$\mathbf{X}\,|0\rangle = |1\rangle$$
$$\mathbf{X}\,|1\rangle = |0\rangle\,.$$

Men vad händer om kvantbiten inte är i tillstånden $|0\rangle$ eller $|1\rangle$?

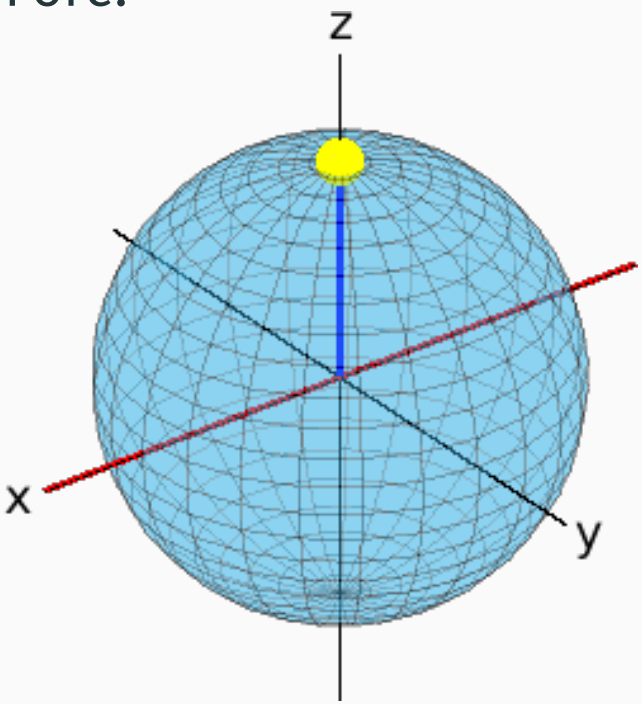
Kvantgrinden X

Jo, $\mathbf{X}$ roterar kvantbiten på Blochsfären $180°$ moturs runt x-axeln!

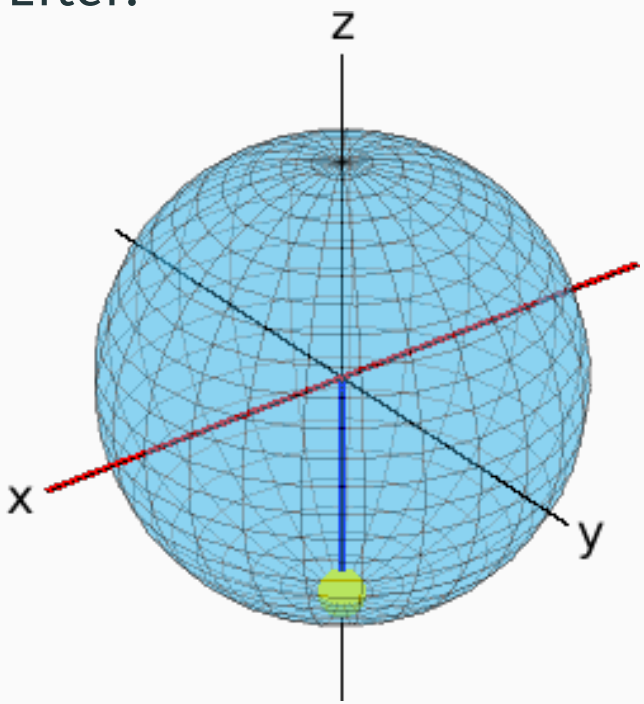
Kvantgrinden X

Jo, $\mathbf{X}$ roterar kvantbiten på Blochsfären $180°$ moturs runt x-axeln!

Före:



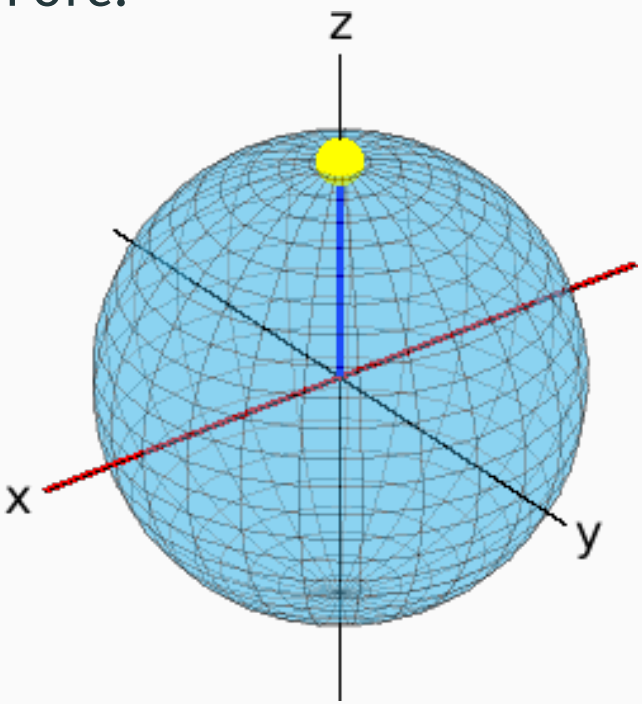
Efter:



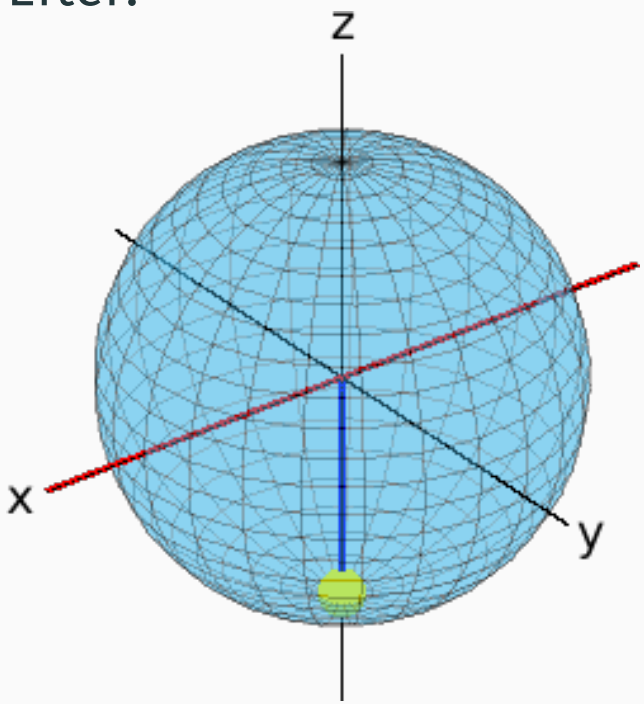
Kvantgrinden X

Jo, $\mathbf{X}$ roterar kvantbiten på Blochsfären $180°$ moturs runt x-axeln!

Före:



Efter:

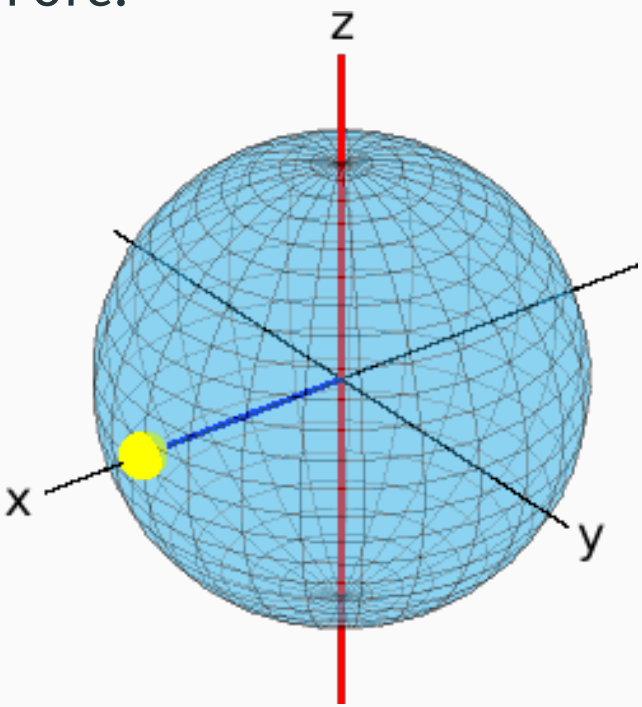


Generellt gäller att de flesta enbitskvantgrindar är rotationer på Blochsfären.

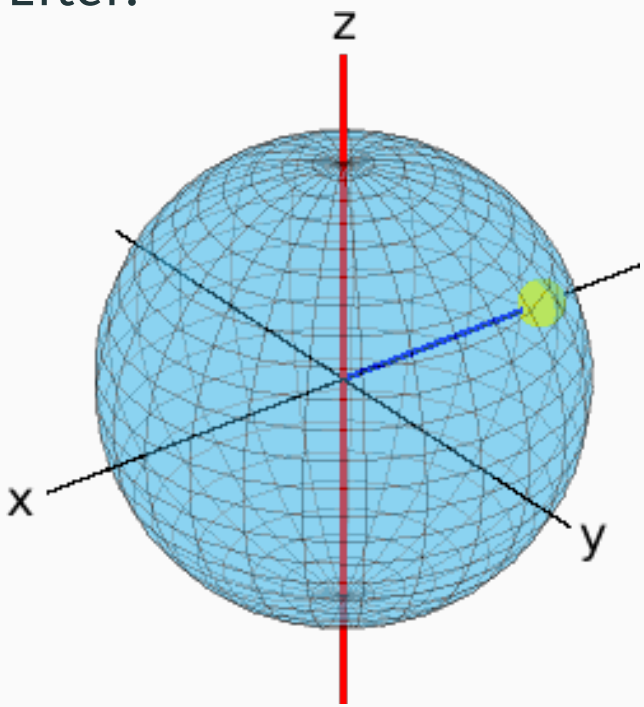
Kvantgrinden Z

På samma sätt är $\mathbf{Z}$ en $180°$-rotation moturs runt z-axeln!

Före:



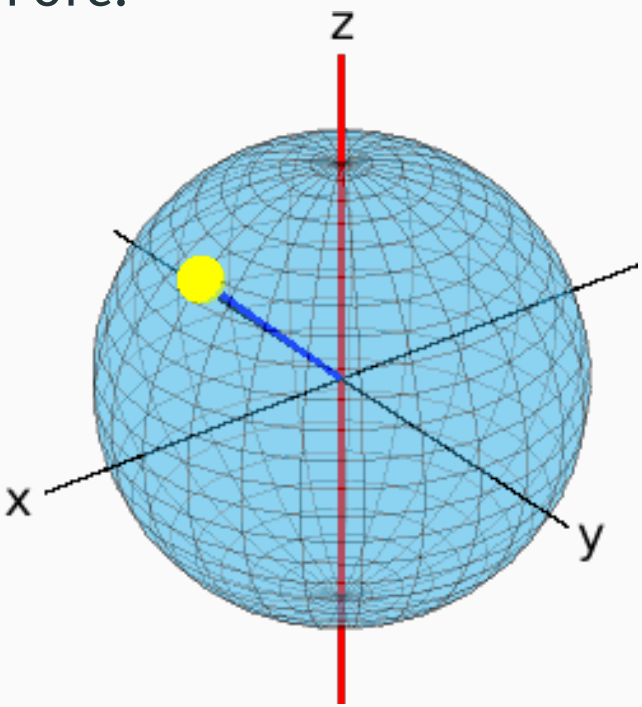
Efter:



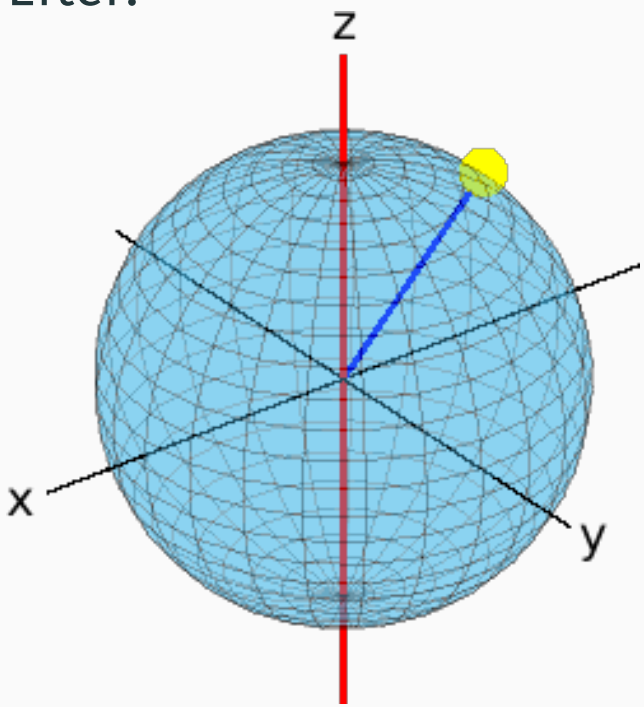
Kvantgrinden Z

På samma sätt är $\mathbf{Z}$ en $180°$-rotation moturs runt z-axeln!

Före:



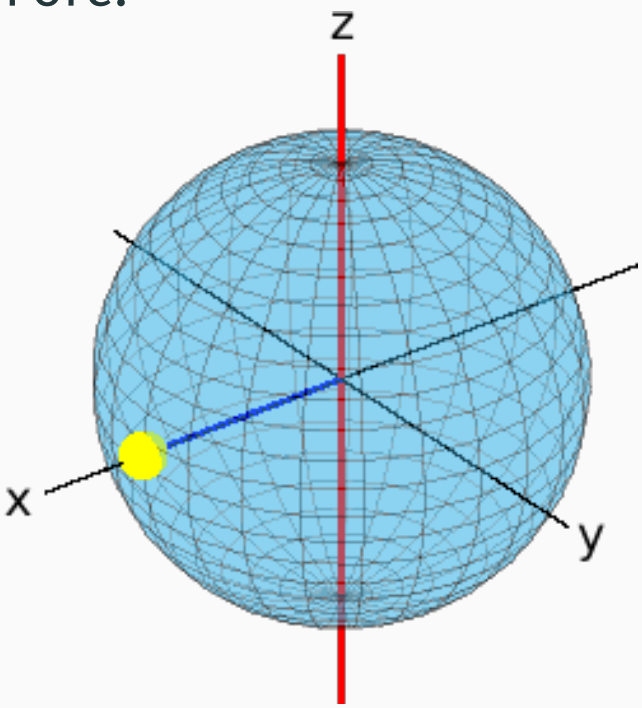
Efter:



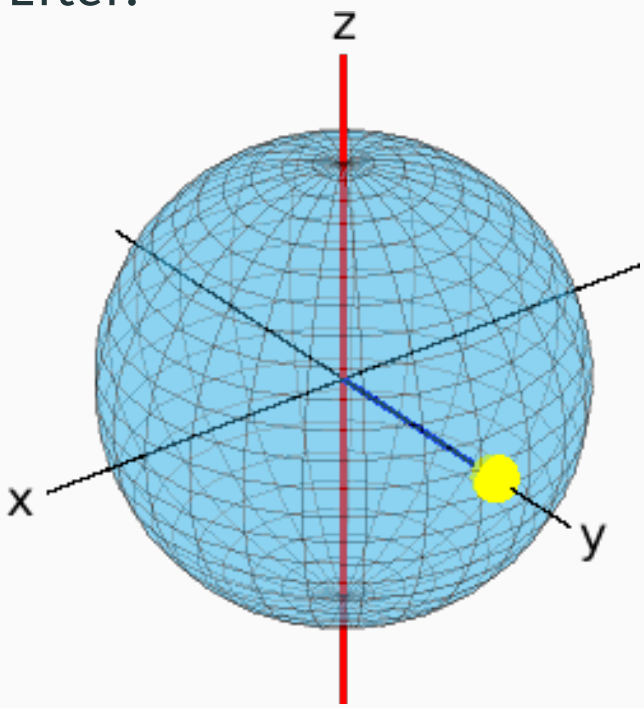
Kvantgrinden S

$\mathbf{S}$ är $\sqrt{\mathbf{Z}}$, vilket ger en $90°$-rotation moturs runt z-axeln.

Före:



Efter:



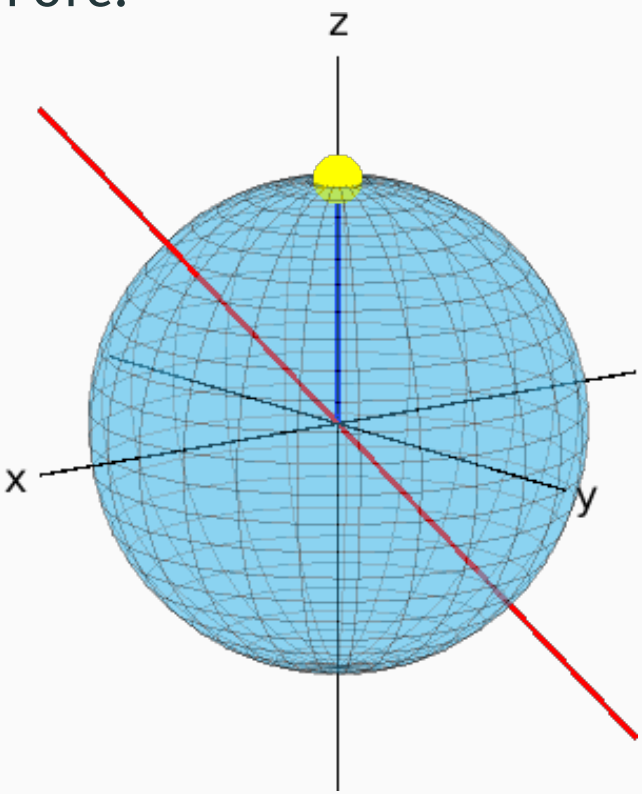
Hadamardgrinden (H)

Grinden $\mathbf{H}$ kallas för Hadamardgrinden (Hadamard gate) och är lite annorlunda. Även denna är en $180°$-rotation moturs, men runt linjen $z = x$ genom origo.

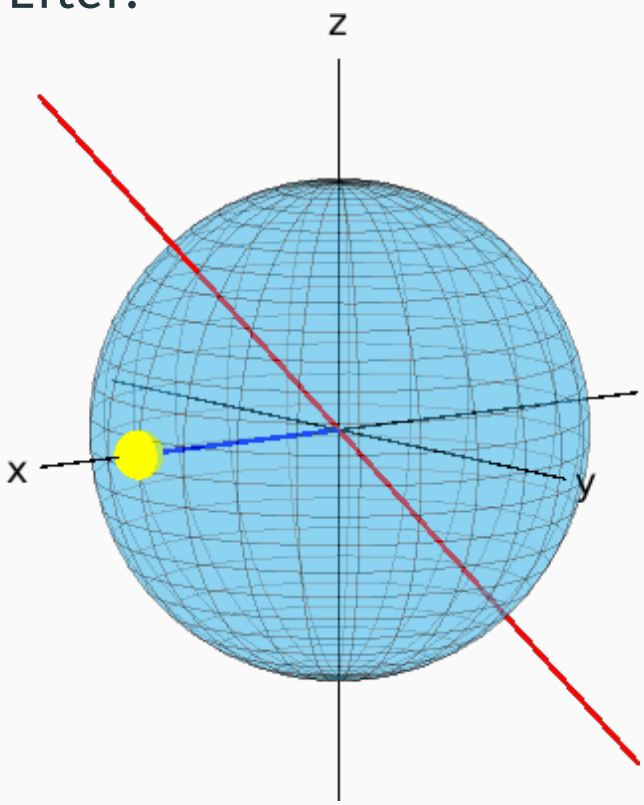
Hadamardgrinden (H)

Grinden $\mathbf{H}$ kallas för Hadamardgrinden (Hadamard gate) och är lite annorlunda. Även denna är en $180°$-rotation moturs, men runt linjen $z = x$ genom origo.

Före:



Efter:



Hadamardgrinden (H)

Hadamardgrinden är intressant eftersom den flyttar en kvantbit i något av tillstånden $|0\rangle$ eller $|1\rangle$ till en superposition på ekvatorn, nämligen $|+\rangle$ respektive $|-\rangle$. Detta går även åt andra hållet:

$$\mathbf{H}\,|0\rangle = |+\rangle$$
$$\mathbf{H}\,|1\rangle = |-\rangle$$
$$\mathbf{H}\,|+\rangle = |0\rangle$$
$$\mathbf{H}\,|-\rangle = |1\rangle$$

En kvantgrind på två bitar

Slutligen vill vi att kvantbitarna ska kunna interagera med varandra.
Då behöver vi grindar som beror på flera kvantbitar.

En kvantgrind på två bitar

Slutligen vill vi att kvantbitarna ska kunna interagera med varandra. Då behöver vi grindar som beror på flera kvantbitar. I klassiska datorer finns det många logiska grindar för detta, exempelvis **NAND**, **AND**, **XOR**, etc.

En kvantgrind på två bitar

Slutligen vill vi att kvantbitarna ska kunna interagera med varandra. Då behöver vi grindar som beror på flera kvantbitar. I klassiska datorer finns det många logiska grindar för detta, exempelvis **NAND**, **AND**, **XOR**, etc.

På kvantbitar kommer vi endast ta upp en sådan grind: **CNOT**.

Kvantgrinden CNOT

CNOT Står för Controlled NOT. Grinden tar två kvantbitar, en *target* och en *control*.

Kvantgrinden CNOT

CNOT Står för Controlled NOT. Grinden tar två kvantbitar, en *target* och en *control*.

Det grinden gör är att den flippar *target* mellan $|0\rangle$ och $|1\rangle$, men endast om *control* är $|1\rangle$.

Sammanflätning av kvantbitar

Sammanflätning av kvantbitar

Vi har nu allt vi behöver för att kunna sammanfläta två kvantbitar. Genom att kombinera en Hadamardgrind och en $\mathbf{CNOT}$-grind så kan vi skapa en sammanflätning:

Sammanflätning av kvantbitar

Vi har nu allt vi behöver för att kunna sammanfläta två kvantbitar. Genom att kombinera en Hadamardgrind och en $\mathbf{CNOT}$-grind så kan vi skapa en sammanflätning:

$$|00\rangle \Rightarrow \mathbf{H}(|0\rangle)\,|0\rangle = (|0\rangle + |1\rangle)\,|0\rangle = |00\rangle + |10\rangle$$

$$|00\rangle + |10\rangle \xrightarrow{\mathbf{CNOT}} |00\rangle + |11\rangle$$

Sammanflätning av kvantbitar

Vi har nu allt vi behöver för att kunna sammanfläta två kvantbitar. Genom att kombinera en Hadamardgrind och en $\mathbf{CNOT}$-grind så kan vi skapa en sammanflätning:

$$|00\rangle \Rightarrow \mathbf{H}(|0\rangle)\,|0\rangle = (|0\rangle + |1\rangle)\,|0\rangle = |00\rangle + |10\rangle$$
$$|00\rangle + |10\rangle \xrightarrow{\mathbf{CNOT}} |00\rangle + |11\rangle$$

Tillståndet $|00\rangle + |11\rangle$ är en sammanflätning. Vi har en superposition, men om vi mäter en av kvantbitarna så vet vi med säkerhet att den andra kommer ha samma värde. Superpositionen kan bara kollapsa till $|00\rangle$ eller $|11\rangle$.

Dagens utmaningar

Dagens utmaningar

Många problem finns fortfarande inom dagens kvantforskning. Till exempel:

Dagens utmaningar

Många problem finns fortfarande inom dagens kvantforskning. Till exempel:

- Kvantdatorer är svåra att bygga, kräver en superkyld miljö och det blir svårare ju fler kvantbitar du behöver.

Dagens utmaningar

Många problem finns fortfarande inom dagens kvantforskning. Till exempel:

- Kvantdatorer är svåra att bygga, kräver en superkyld miljö och det blir svårare ju fler kvantbitar du behöver.
- Dagens kvantbitar är instabila. Kvantalgoritmer längre en ett visst antal grindar kan inte användas utan att kvantbitarna blir instabila och man inte längre kan veta vilket tillstånd de befinner sig i.

Dagens utmaningar

Många problem finns fortfarande inom dagens kvantforskning. Till exempel:

- Kvantdatorer är svåra att bygga, kräver en superkyld miljö och det blir svårare ju fler kvantbitar du behöver.
- Dagens kvantbitar är instabila. Kvantalgoritmer längre en ett visst antal grindar kan inte användas utan att kvantbitarna blir instabila och man inte längre kan veta vilket tillstånd de befinner sig i.
- Vi har för få kvantbitar!

Tack för att ni lyssnat!