Quantencomputer Programmierung

mail@AndreBetz.de

Klassischer vs. Quanten Computer

Klassische Computer:

- Besteht aus einzelnen Speicherzellen **Bits**
- Jedes Bit kann entweder Zustand **1** oder **0** haben
- Zu jedem Zeitpunkt ist der Computer einen aus **2^n** Zuständen, von 00…0 bis 11..1

Quantencomputer:

- Besteht aus einzelnen Speicherzellen **Qbits**
- Jedes Qbit kann den Zustand **1** oder **0** oder einen Mischung aus beiden haben
- Eine Mischung nennt man **Superspostion**

Eigenschaften von QBits:

Superposition:

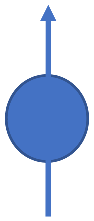
- Ein Objekt hat mehr als einen Zustand zur gleichen Zeit

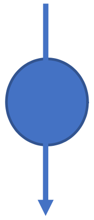
Verschränkung:

- Quantenobjekte paarweise erzeugt worden, sind verschränkt zB Kristalle spaltet Photon einer Energie in zwei Photonen niedriger Energie auf
- Getrennte Objekte haben eine Auswirkung aufeinander, ohne Verbindung

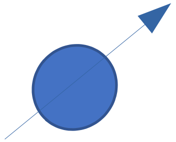
Es gibt keine Analogie dazu in der klassischen Welt.

Superposition 1

Zustand 1:  <=> |0>
Spin up

Zustand 0:  <=> |1>
Spin
down

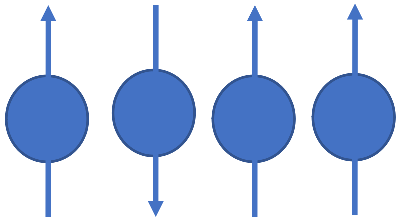
Orthogonale Pfeilrichtungen kennzeichnen den Zustand

Superposition:  <=> |0> + |1>

Pfeilrichtungen dazwischen kennzeichnen eine Superposition, in der alle möglichen Zustände gleichzeitig existieren. Erst durch eine Messung zerfällt der Elektronen Spin in exakt 0 oder exakt 1.

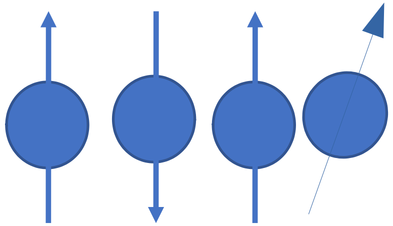
Superposition 2

Keine Superposition



<=> |1011> <=> |7>

Superposition



<=> |1011> + |1010> <=> |7> + |6>

Es gibt nach der Messung eine gewisse Wahrscheinlichkeit, dass der Zustand 7 oder 6 sein wird.
mit 4 Bits kann einer von 2^4 Zuständen dargstellt werden, Qbits können alle 2^4 Zustände haben.

Grenzen klassischer Computer – Beispiel

Reiseagentur:

- Gruppe aus 3 Personen zu transportieren (A,B,C)
- Gruppe soll auf zwei Taxis (0,1) aufgeteilt werden
- A und B sind befreundet, A und C, B und C nicht
- Bedingung: Maximiere Transport von befreundeten
- Klassische CPU braucht 2^3 Schritte, skaliert mit Anzahl der Personen $\mathbf{2}^{\mathbf{Personenzahl}}$
- Quantencomputer mit 3 Qbits benötigt 1 Schritt und benötigt auch bei einer höheren Personenzahl nur einen Rechenschritt

A	B	C	Score
0	0	0	-1
0	0	1	1
0	1	0	-1
0	1	1	-1
1	0	0	-1
1	0	1	-1
1	1	0	1
1	1	1	-1

Problemklassen

P-Probleme (Polynomialzeit):

Rechenzeit wächst proportional zur festen Potenz der Problemgrösse zB Ist eine Zahl eine Primzahl

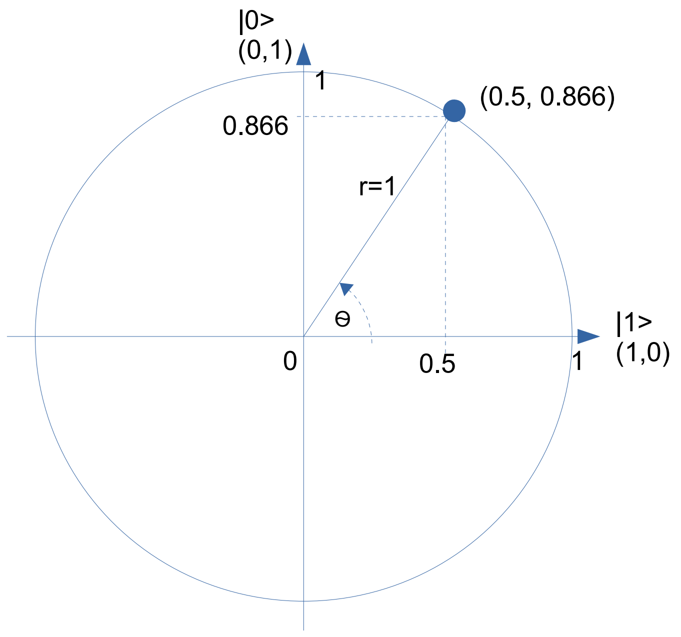
NP-Probleme (nichtdeterministisch Polynomial):

Rechenzeit wächst exponentiell zB Travelling Salesman wächst exponentiell mit Anzahl der Städte. Überprüfung ist wieder in Polynomialzeit. Quantencomputer können einige schnell lösen. Evtl P == NP?!

PSPACE:

Polynomial wachsender Speicher und exponentiell wachesende Rechenzeit. Schach und GO gehören dazu. Noch kein Akgorithmus für QC bekannt.

Quantum Bit- QBit



Wenn ein Qbit gemessen wird, wird mit einer bestimmten Wahrscheinlichkeit |0> oder |1> gemessen.

Wahrscheinlicht für |a> = $|a|^2$

Bedingung 1 = $|\ |0\rangle\ |^2 + |\ |1\rangle\ |^2$

|0> = $|0.5|^2 = 0.25 = 25\%$

|1> = $|0.866|^2 = 0.75 = 75\%$

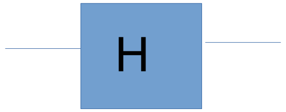
Darstellung als Verktor: $\vec{a} = \begin{pmatrix} x \\ y \end{pmatrix}$

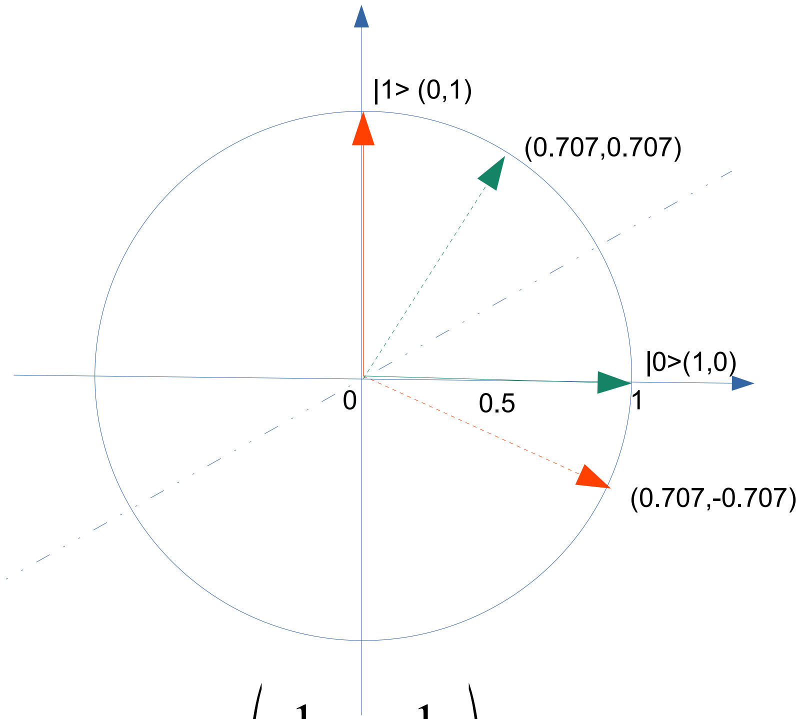
|0> = $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ |1> = $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Quantengatter

- Klassische Computer brauchen nur ein universelles Gatter (zB NAND)
- Quantencomputer brauchen drei Gatter um universell zu sein, davon sind zwei unitär (H, Phasenschieber) und das dritte verschränkt ein zweites QBit (CNOT).
- Alle Gatter haben gemein, dass sie die Wahrscheinlichkeit verändern.
- Quantengatter müssen reversibel sein

Hadamard-Gatter



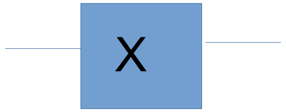


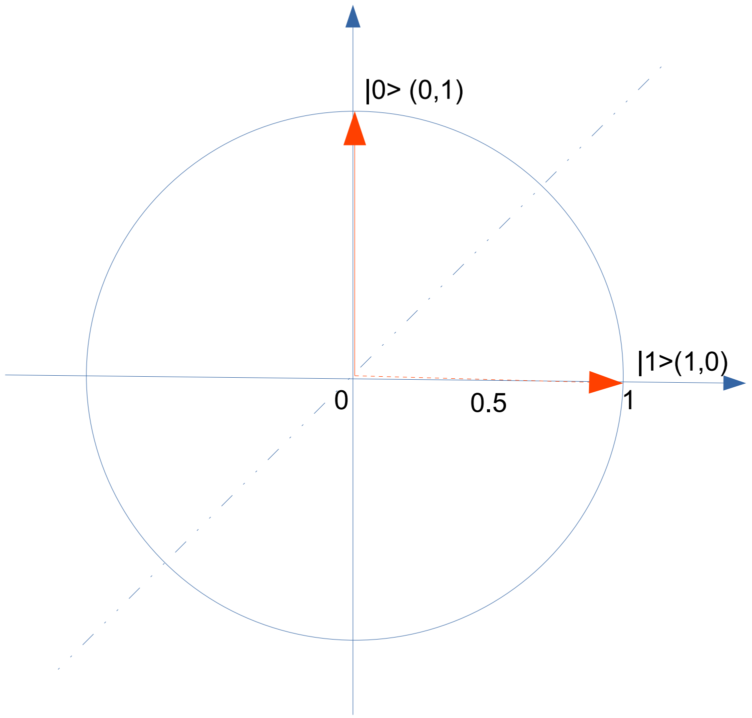
$$H = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}$$

- Wirkt nur auf ein QBit
- Erzeugt eine Superposition eines Zustandes |1> (0,1) zu (0.707, -0.707) oder |0> zu (0.707, 0.707)
- Zustand ist versteckt, da nach einer Messung zu 50% |0> oder |1> gemessen wird
- Nochmalige Anwendung des Gatters erzeugt wieder ursprünglichen Zustand
- Wird meist am Anfang eines Quantenalgorithmus gesetzt

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0.707 & -0.707 \end{pmatrix}$$

X-Gatter





- Wirkt nur auf ein QBit
- Pauli-X-Gatter genannt
- Tauscht Komponenten von |0> and |1>
- Wird benutzt, um ein QBit in den Zustand |1> zu setzen

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

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

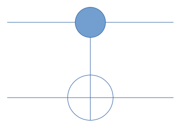
Darstellung verschränkter QBits

$|0> = \begin{pmatrix}0\\1\end{pmatrix}$ $|1> = \begin{pmatrix}1\\0\end{pmatrix}$ Und |AB> = |A> + |B> , wobei + Kronecker Produkt

Beispiel zwei verschränkter QBits

$|00> = \begin{pmatrix}1\\0\\0\\0\end{pmatrix}$ $|01> = \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$ $|10> = \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$ $|11> = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$

CNOT-Gatter



- Controlled NOT
- Arbeitet mit zwei QBits |AB>
- Mögliche Varianten |00>, |01>, |10>, |11>
- QBit A kontrolliert QBit B, wenn QBit A |1> ist, wird QBit B vertauscht.
- Beispiel: |10> - |11>

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

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

Quantum Bit- QBit

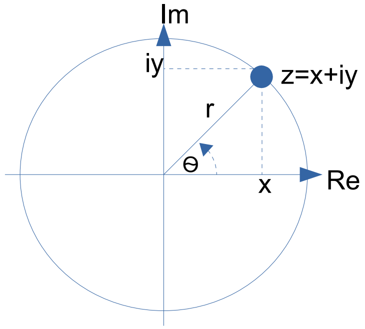
$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Zustand eines Qbits: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

α, β sind komplexe Zahlen und sind die Wahrscheinlichkeitsamplitude
mit $\alpha = \alpha_{real} + i\alpha_{imag}$ und $\beta = \beta_{real} + i\beta_{imag}$

Wahrscheinlichkeitsbedingung: $1^2 = |\alpha|^2 + |\beta|^2$

Die Wahrscheinlichkeit den Zustand $|0\rangle$ zu messen liegt bei $|\alpha|^2$ und $|1\rangle$ bei $|\beta|^2$

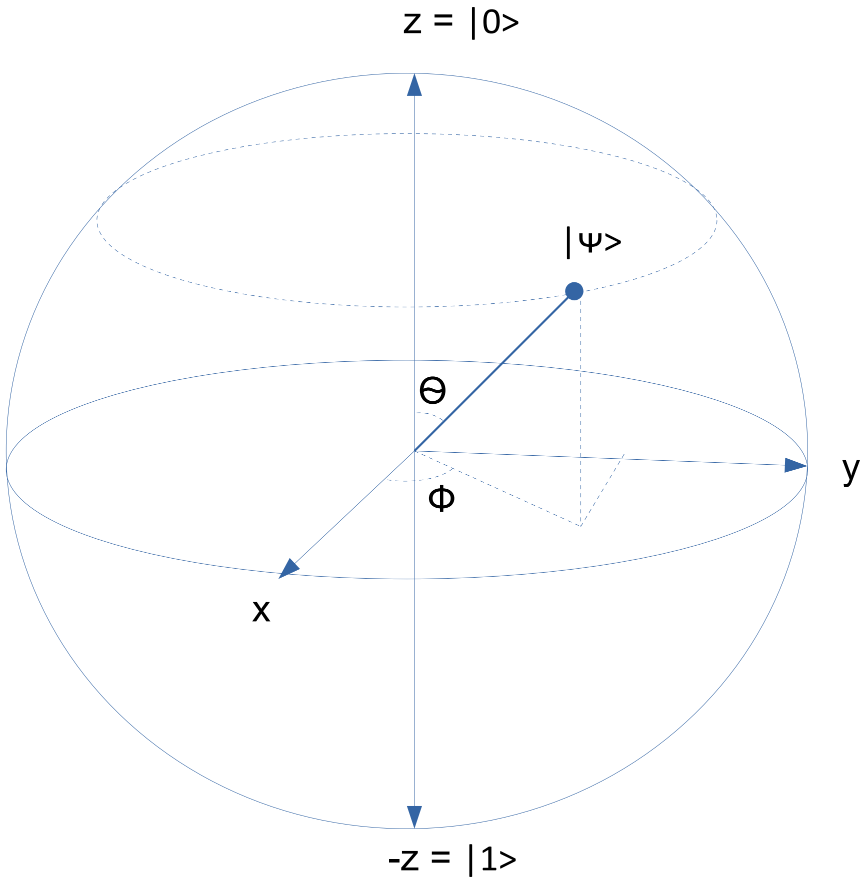


$x = r \cos(\Theta)$
$iy = r \sin(\Theta)$

$r = |z| = \sqrt{x^2 + y^2}$

$z = x + iy = r\,(\cos(\Theta) + i \sin(\Theta)) = r\, e^{i\Theta}$

Blochkugel



- |Ψ> Bezeichnet den Zustand des Qbits
- Radius ist 1