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 $\mathbf{2^n}$ 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 **Supersposition**

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

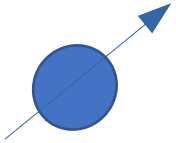
Es gibt keine Analogie dazu in der klassischen Welt.

Superposition 1

Zustand 1:  <=> |0>
Spin up

Zustand 0:  <=> |1>
Spin down

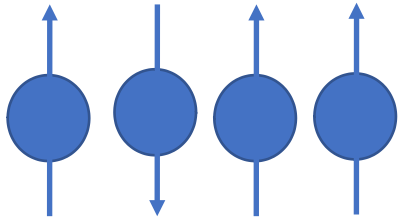
Orthogonale Pfeilrichtungen kennzeichnen den Zustand

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.

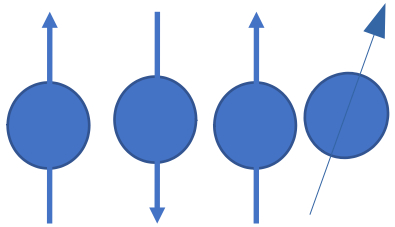
Superposition 2

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 $\mathbf{2^{Personenzahl}}$
- 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

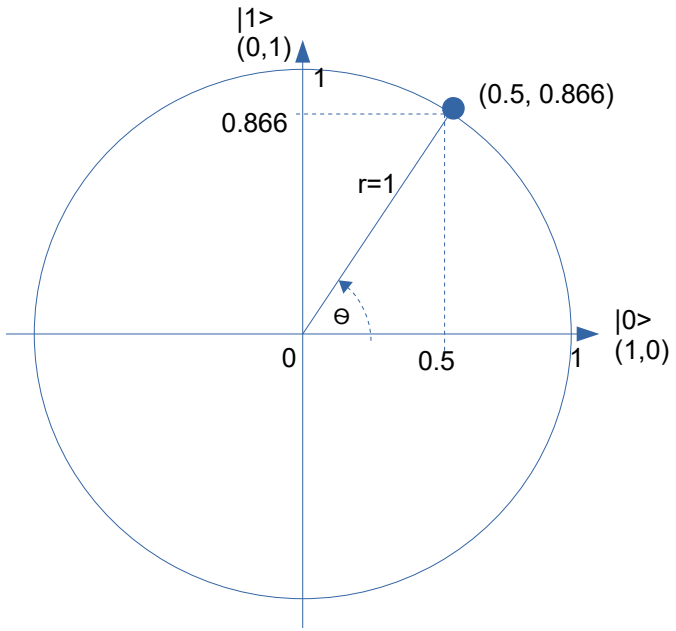
NP-Probleme (nichtdeterministisch Polynomial):

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 $|a\rangle = |a|^2$

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

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

Quantum Bit- QBit

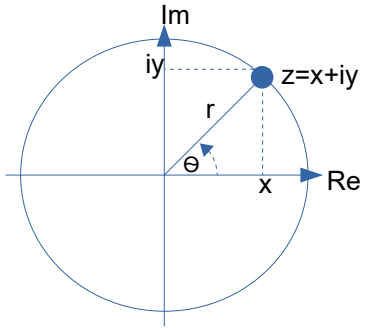
$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

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 $|\beta|^2$

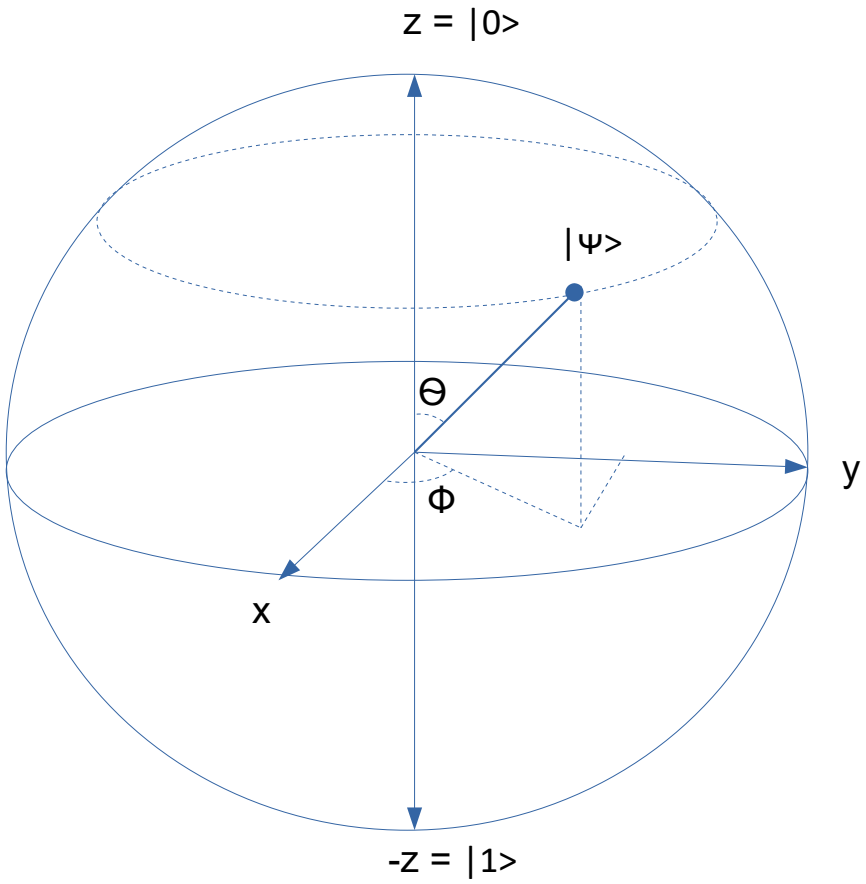


$x = r \cos(\Theta)$
$iy = r \sin(\Theta)$

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

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

Blochkugel



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