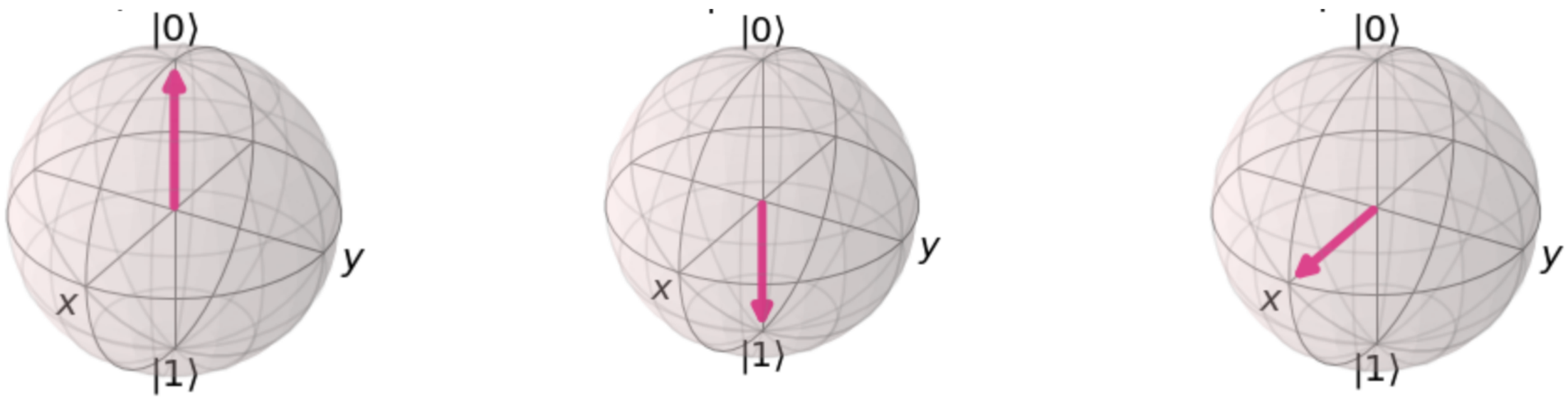
# Quantencomputer

## Was ist das? Was kann er? Wann kommt er?




*Prof. Dr. Sören Schlichting*
*Fakultät für Physik | Universität Bielefeld*
*sschlichting@physik.uni-bielefeld.de*

UNIVERSITÄT BIELEFELD

50 Jahre Fakultät für Physik

CRC-TR 211
Strong-interaction matter under extreme conditions

# Physik am Samstag

öffentlicher Vortrag von 10:00-11:00 (ca. 1h)

Hörsaal H-6

Quiz mit Preisverleihung 11:00 - 11:15 (ca. 15min)

Hörsaal H-6

Kaffeepause 11:15 - 11:30 (ca. 15min)

vor dem Hörsaal H-6

interaktive Quanten Computing Workshops 11:30 — 12:30 (ca. 1h)

Sammelpunkt vor dem Hörsaal H-6 um 11:30

Computerräume D01-012 und U0-139

# Quantencomputer & Quantenmechanik

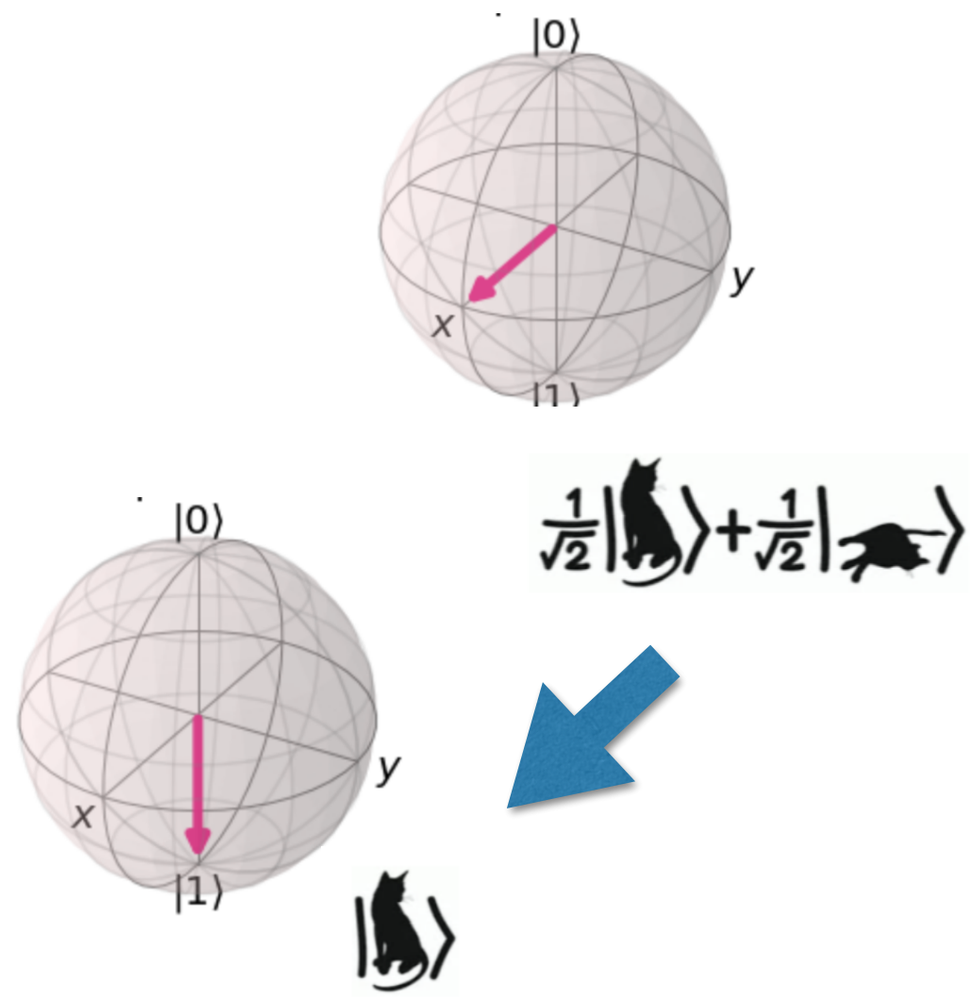
Ein Quantencomputer ist nicht einfach eine Weiterentwicklung eines klassischen Computers sondern ein neuartiges Konzept, das auf den Prinzipien der Quantenmechanik beruht

Beim heutigen Vortrag lernen wir einige
**Grundlagen der Quantenmechanik**

- Quantenzustand
- quantenmechanische Messung
- Verschränkung
- Interferenz

**anhand von Quantencomputern** kennen.

Beim anschliessenden Workshop besteht die Gelegenheit dies selbst auszuprobieren.



# Inhalte

Klassische & Quanteninformation

Bits & QBits, Quantenzustände, Quantenmessung

Quantengates und Quantenalgorithmen

Gates, Verschränkung, Interferenz, Grover Algorithmus

Quantenhardware

digitale & analoge Quantencomputer, Status & Ausblick

# Klassische- & QuantenInformation

Die Information in klassischen Computern ist gespeichert in sog. klassischen Bits, welche die binären Werte 0 oder 1 annehmen können

Da jedes klassische Bit nur zwei Werte annehmen kann, benötigt man zB 4Bits um Zahlen von 0-9 zu Speichern

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 1 |

$= 0x2^3+0x2^2+1x2^1+1x2^0$
$= 0x8+0x4+1x2+1x1$
$= 3$

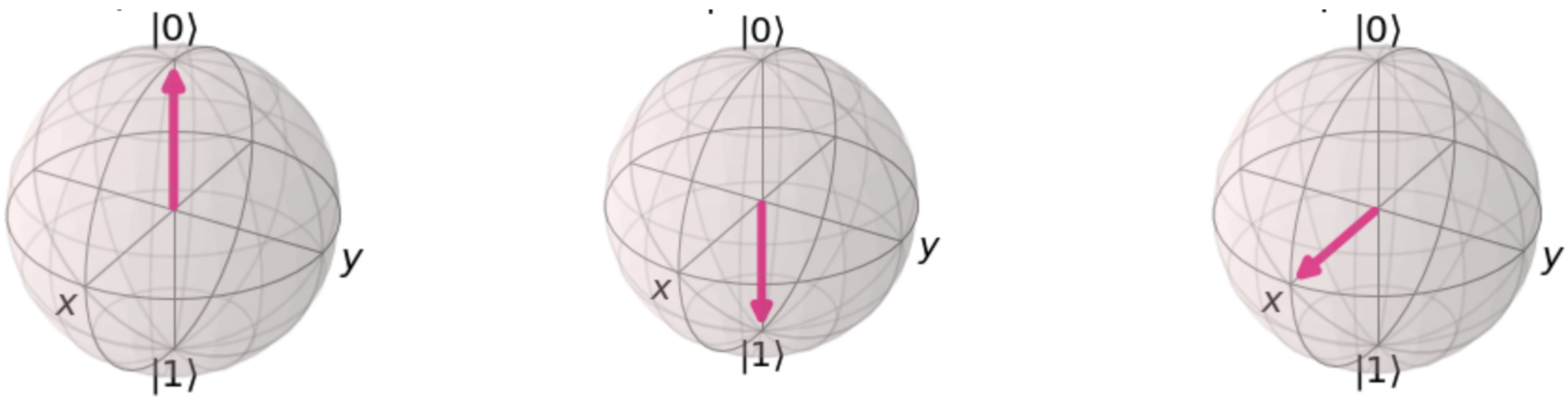
$= 0x2^3+1x2^2+0x2^1+1x2^0$
$= 0x8+1x4+0x2+1x1$
$= 5$

D.h. die obige Sequenz bedeutet

3 3 4 5 5

# Qubit

Die Information in Quantencomputern werden in sog. Qubits (“Quantenbits”) gespeichert, die den quantenmechanischen Zustand eines 2-Level Systems annehmen können. Eine Möglichkeit die Zustände eines Qubits darzustellen ist die sog. Bloch-Sphere




Zustand |0>

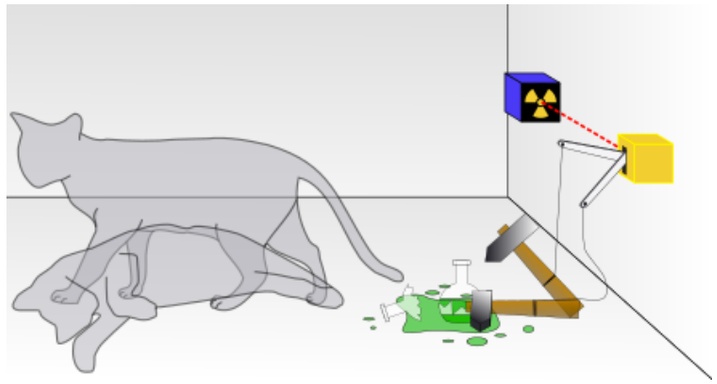
Zustand |1>

Superposition von Zuständen |0> und |1>

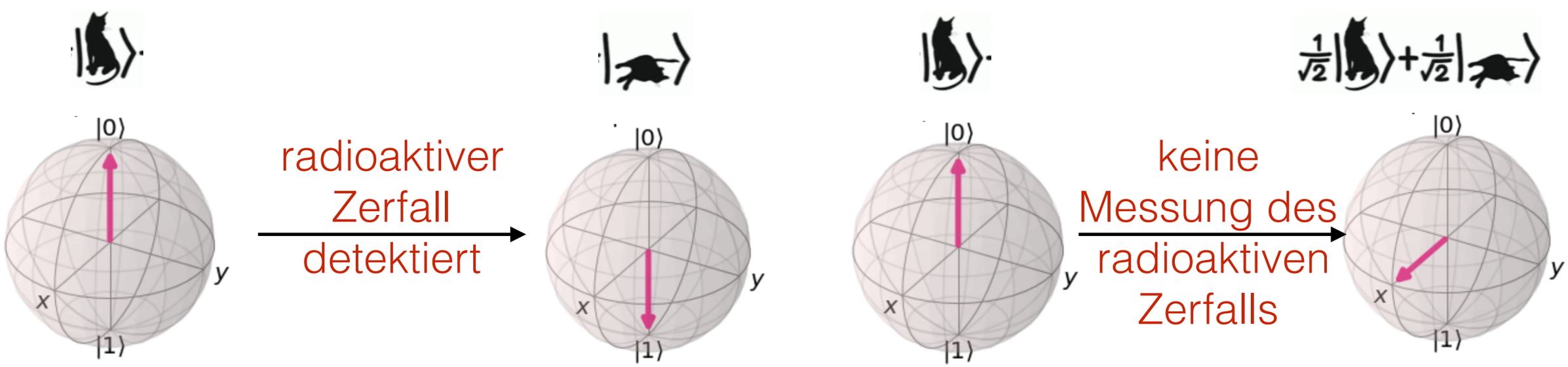
Neben den Zuständen |0> und |1> können Qubits beliebige Kombinationen (“Superposition”) dieser beiden Zustände annehmen, d.h. das Qubit kann gleichzeitig im Zustand |0> und |1> sein

# Schrödingers Katze

Die Tatsache dass ein Quantensystem eine Überlagerung mehrerer Zustände annehmen kann ist eine Besonderheit der Quantenmechanik und führt zu paradoxen Situationen wenn man dies auf klassische Objekte überträgt



**Schrödingers Katze** — Gedankenexperiment bei dem eine Katze durch nach dem radioaktiven Zerfall eines Atomkerns in einer Überlagerung aus tot und lebendig ist



# Qubit vs. klassiches Bit

Da ein Qubit nicht nur |0> oder |1> sein kann, kann es mehr Informationen speichern als ein klassisches Bit

Dieser Effekt wird immer signifikanter je mehr Qubits wir betrachten

Die Quantenmechanischen Zustände eines System von Qubits werden durch eine Quantenmechanische Wellenfunktion beschrieben die beliebige Überlagerungen der Basiszustände beschreibt

$$|\Psi >= a_0|0 > +a_1|1 >$$ 1-Qubit

$$|\Psi >= a_{00}|00 > +a_{01}|01 > +a_{10}|10 > +a_{11}|11 >$$ 2-Qubit

wobei das Betragsquadrat $|a|^2$ der Koeffizienten a die Wahrscheinlichkeit angibt mit denen sich das Quantensystem in dem entsprechenden Basiszustand befindet

# Qubit vs. klassiches Bit

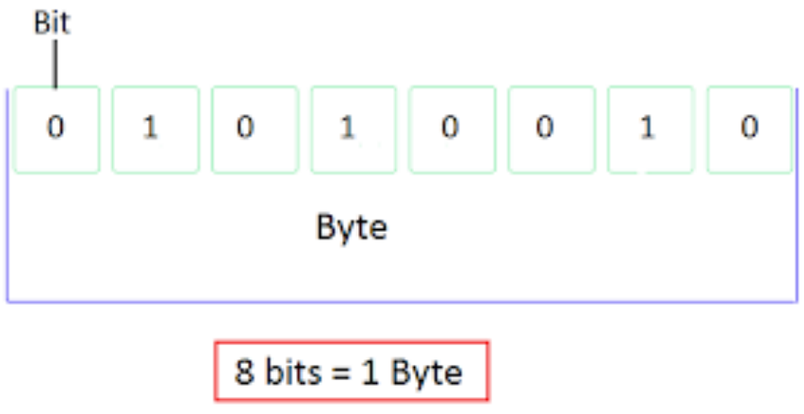
Es ist zwar klassisch möglich ein Qubit (mit gewisser Präzision) darzustellen, allerdings sind dafür wesentlich mehr klassische Bits notwendig

$$N_{\text{bits}} = 2^{N_{\text{qubits}}} \times 2 \times 64$$

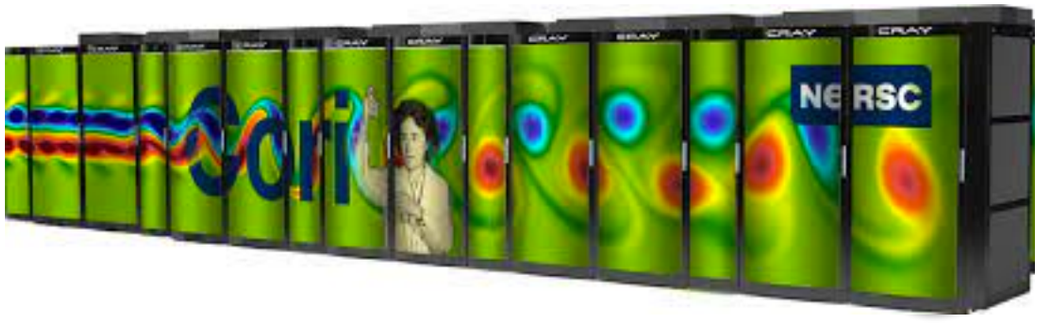
#Basis Quantenzustände #Bits/komplexe Zahl (double precision)

Dieses exponentielle Verhalten ~$2^{N_{\text{qubits}}}$ führt sehr schnell zu einem enormen Speicherbedarf

| | |
|---|---|
| 1 Qubit | 32 B |
| 10 Qubit | 16 kB |
| 50 Qubits | 18.014 TB |
| … | |



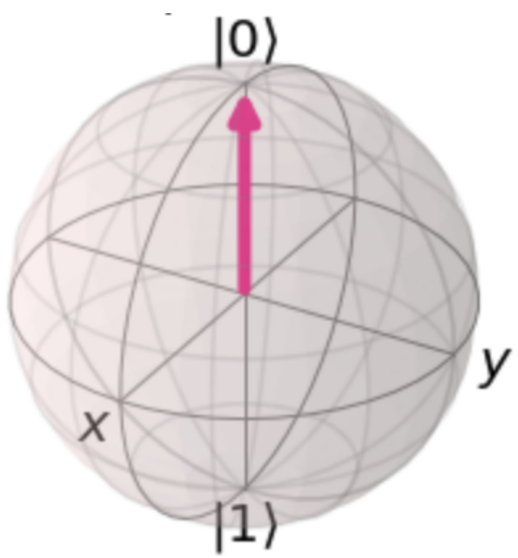

Bis zu ~50 Qubits können auf den besten klassischen Großrechnern simuliert werden

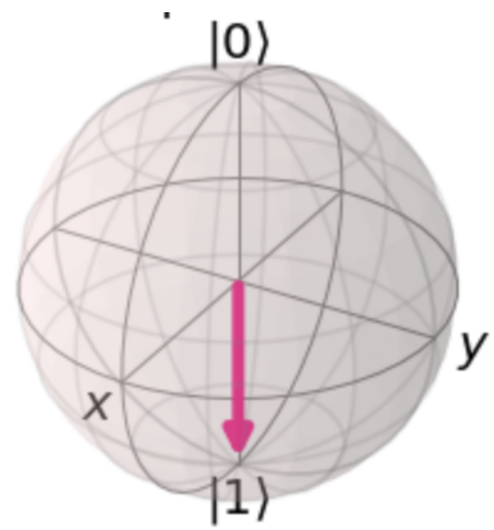


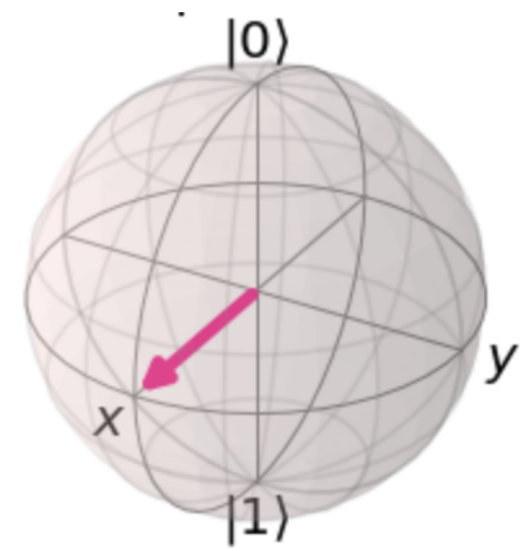
# Quantenmechanische Messung

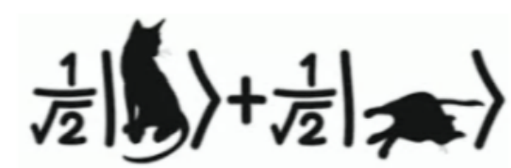
Wenn wir den Zustand eines Qubits messen, kann jede einzelne Messung immer nur 0 oder 1 ergeben.

D.h. bei jeder Messung muss sich das Qubit für einen der beiden Zustände |0> oder |1> entscheiden






Die Wahrscheinlichkeit ergibt sich durch das Betragsquadrat der Amplitude

**0 zu 100%**

**1 zu 100%**

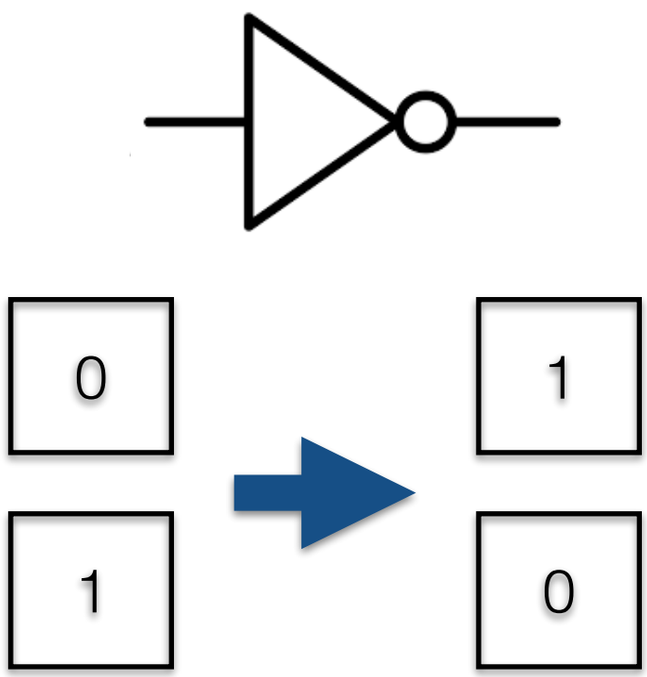
**0 zu 50%**
**1 zu 50%**

# Klassiche- und Quantengates

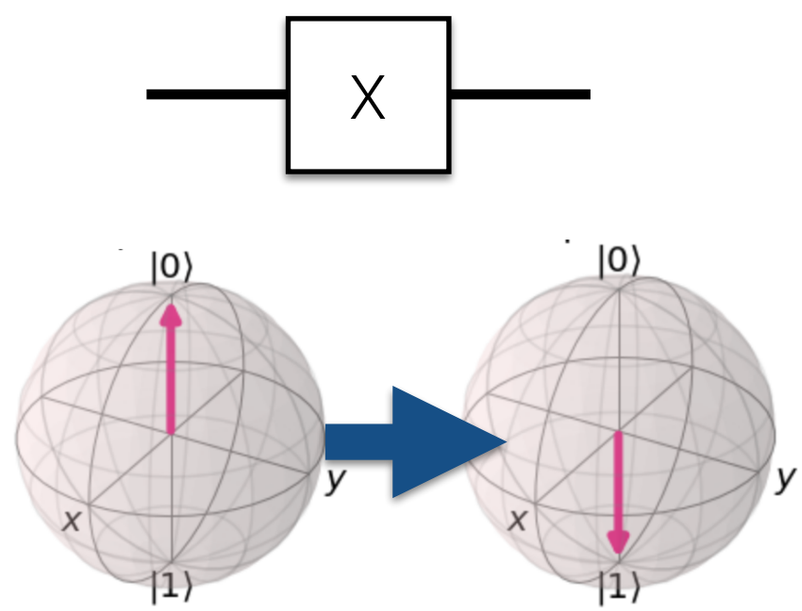
Diese Informationen sind natürlich nur dann nützlich wenn man sie manipulieren, also etwas mit Ihnen machen kann

Beim klassischen Computer macht man das mit logischen Gates, beim Quantencomputer mit Quantengates

NOT Gate



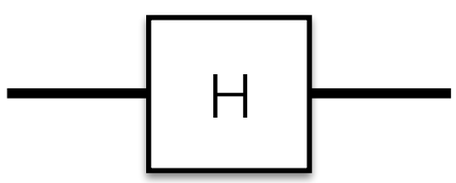

X-Gate

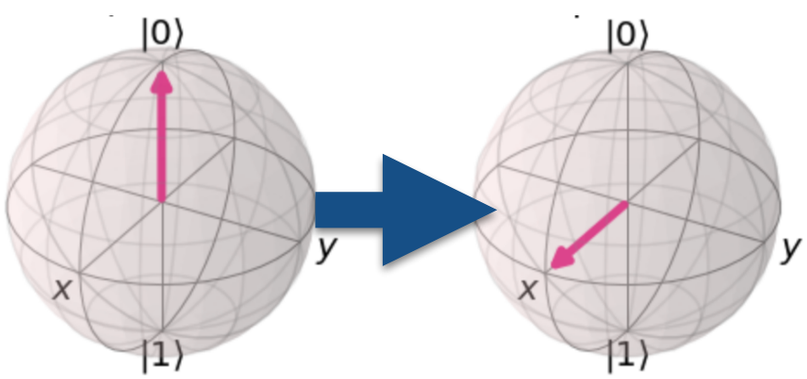


# Klassiche- und Quantengates

Da ein Qubit viel mehr Informationsgehalt besitzt als ein klassisches Bit gibt es neben den Analogons zu klassischen Gates auch spezielle Quantengates wie z.B. das H-Gate oder Rx-Gate

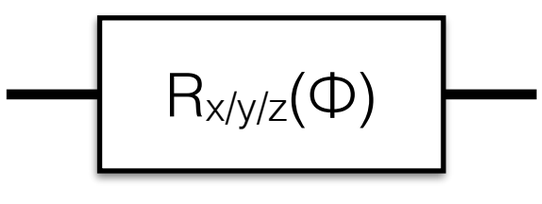
H-Gate

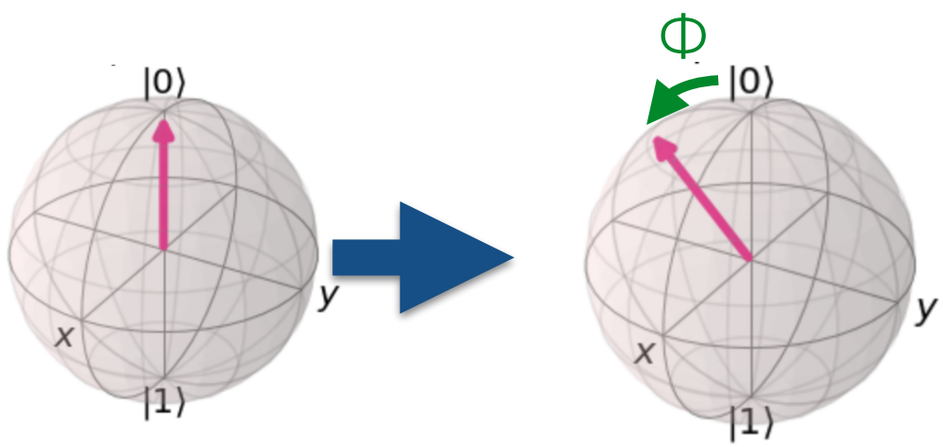



erzeugt Superposition von |0> und |1> Zustand

$R_{x/y/z}$-Gate



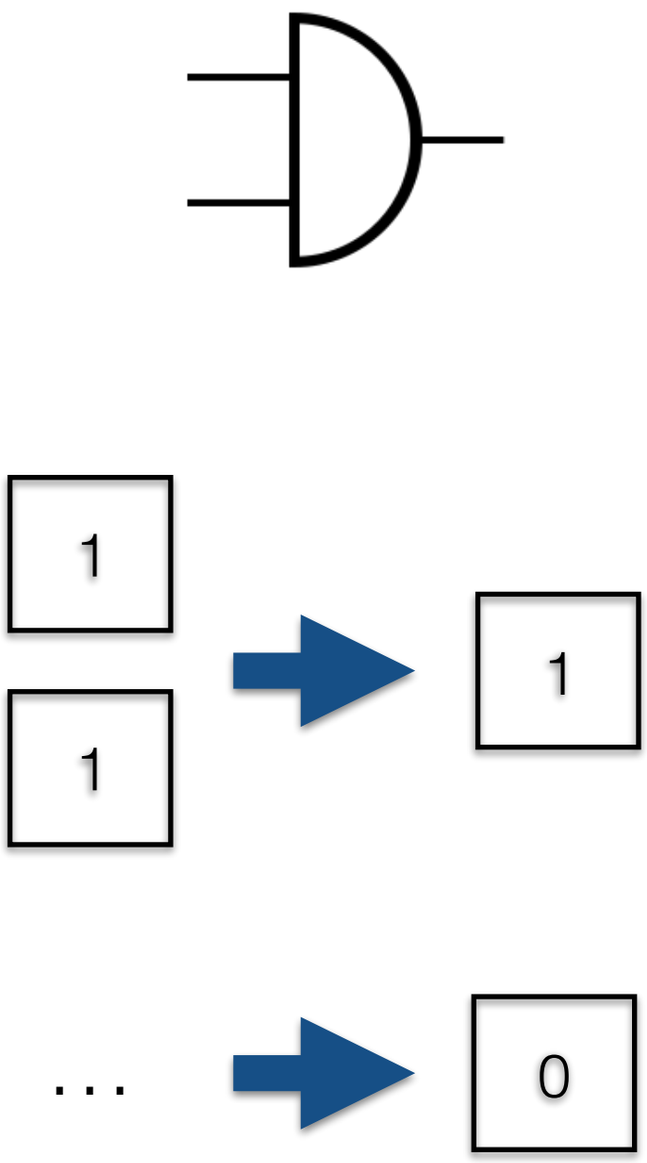




dreht Quantenzustand um Winkel Φ um x/y/z-Achse

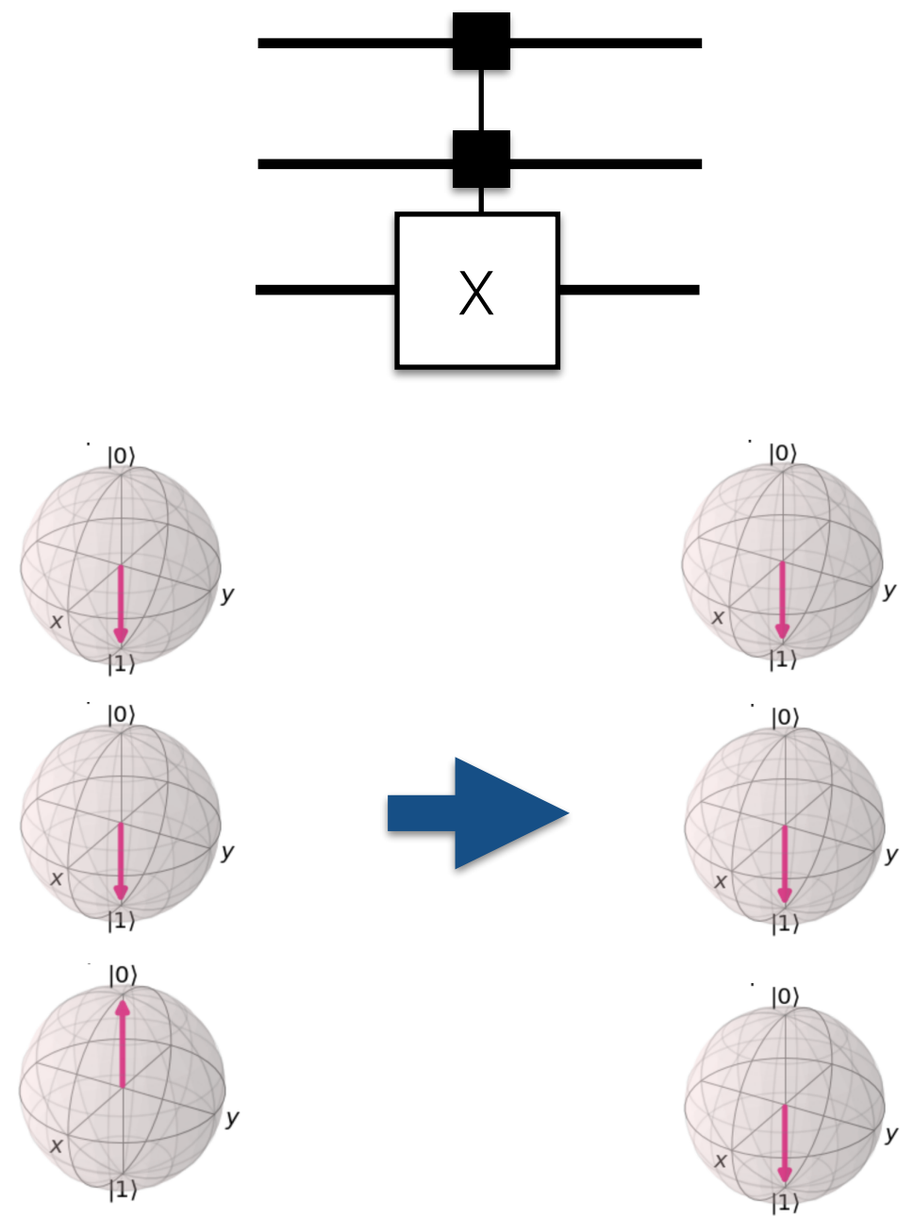
# Klassiche- und Quantengates

Damit klassische Bits und Qubits miteinander kommunizieren können benötigt man ausserdem Multi (Q)Bit Gates

AND-Gate




CCX-Gate



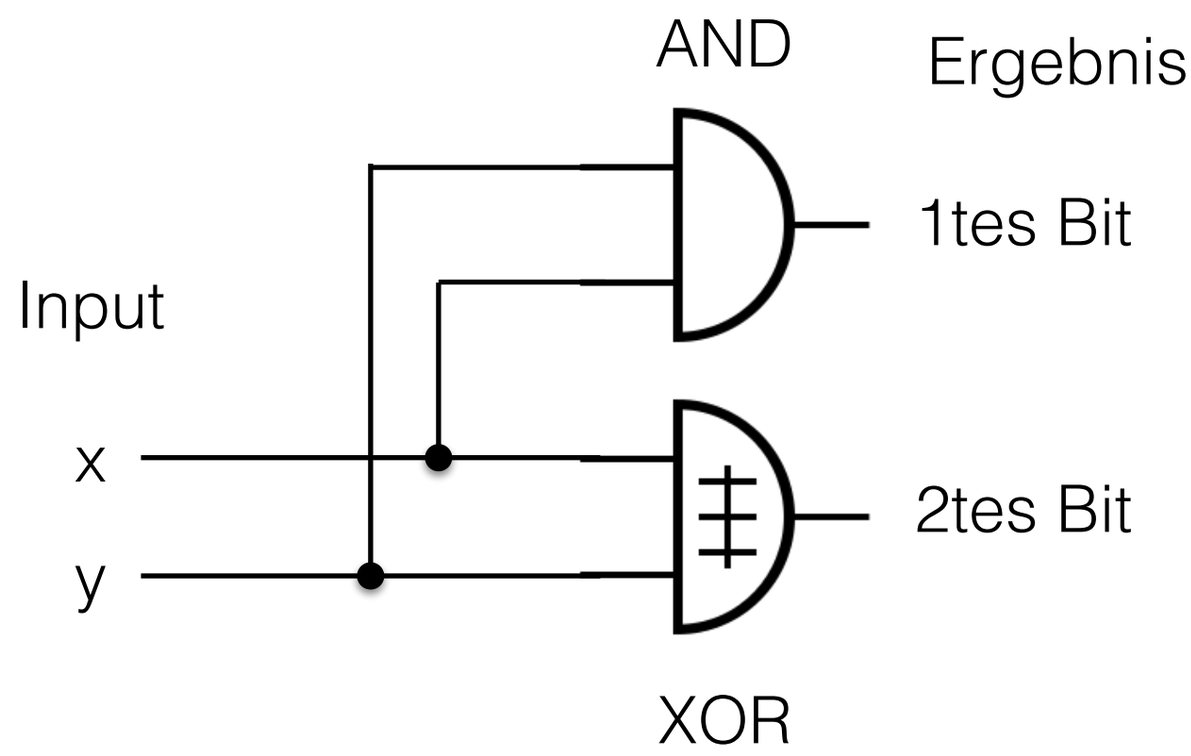
# Binäre Addition

Durch geschickte Kombination von Gates, lassen sich so auf klassischen und Quantencomputern Rechnungen durchführen

Einfachstes Beispiel ist die Addition von zwei Zahlen x,y mit Werten 0 oder 1

| Input x | | Input y | | Ergebnis | |
|---|---|---|---|---|---|
| 0 | + | 0 | = | 0 | 0 |
| 0 | + | 1 | = | 0 | 1 |
| 1 | + | 0 | = | 0 | 1 |
| 1 | + | 1 | = | 1 | 0 |

Klassischer Schaltkreis:

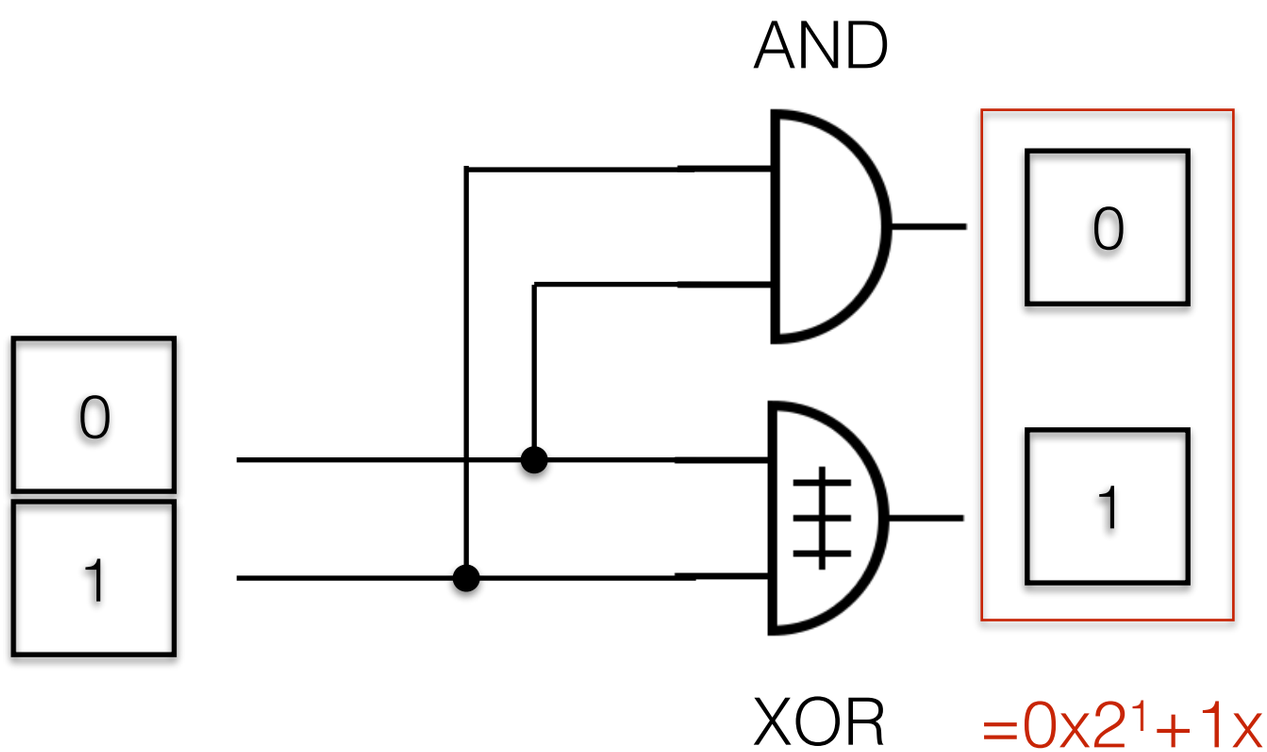


# Binäre Addition

Durch geschickte Kombination von Gates, lassen sich so auf klassischen und Quantencomputern Rechnungen durchführen

Einfachstes Beispiel ist die Addition von zwei Zahlen x,y mit Werten 0 oder 1

Klassischer Schaltkreis:




$=0x2^1+1x2^0=1$

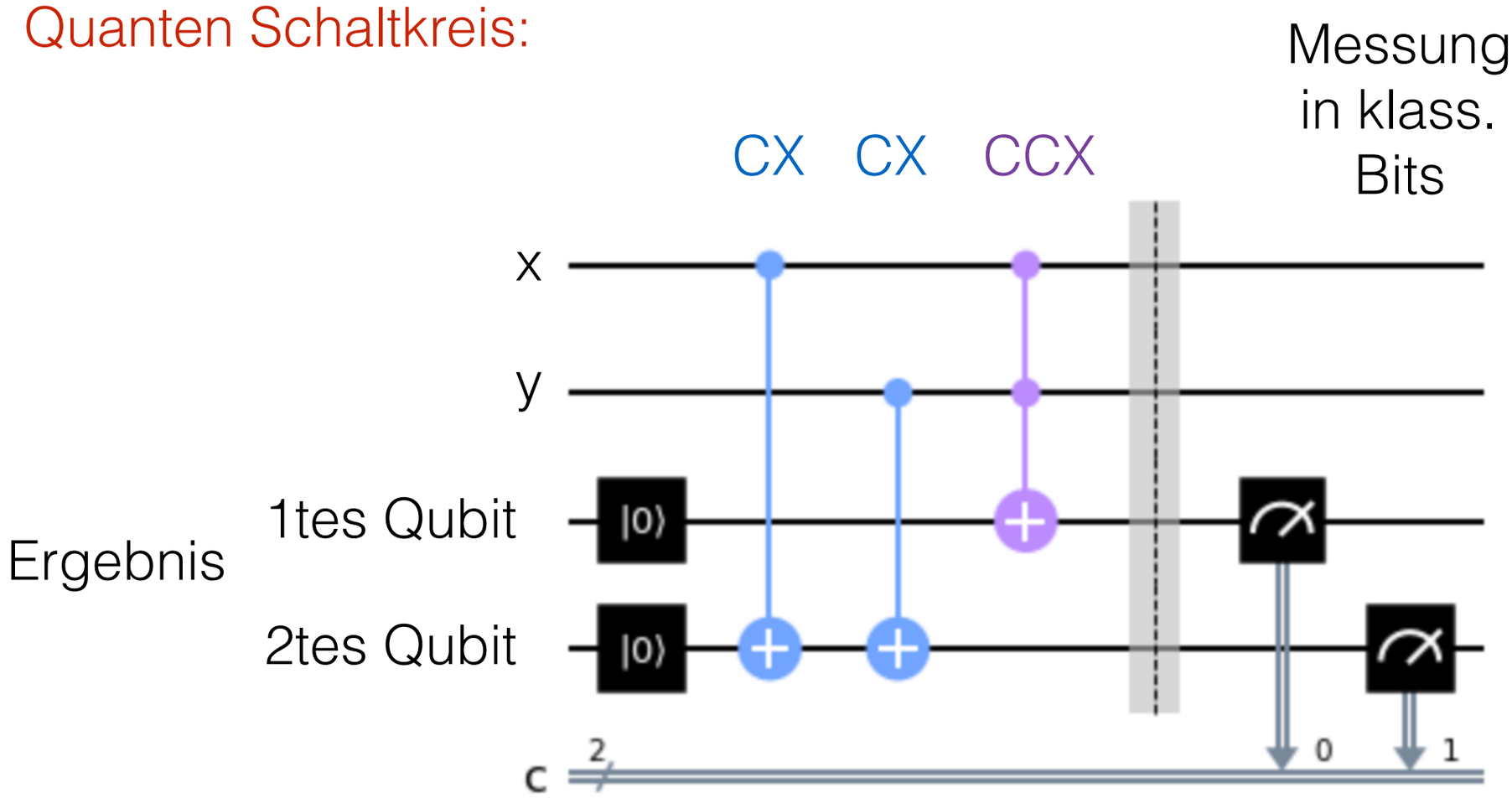
Wir erhalten also wie gewünscht 0+1=1!

# Binäre Addition

Durch geschickte Kombination von Gates, lassen sich so auf klassischen und Quantencomputern Rechnungen durchführen

Einfachstes Beispiel ist die Addition von zwei Zahlen x,y mit Werten 0 oder 1

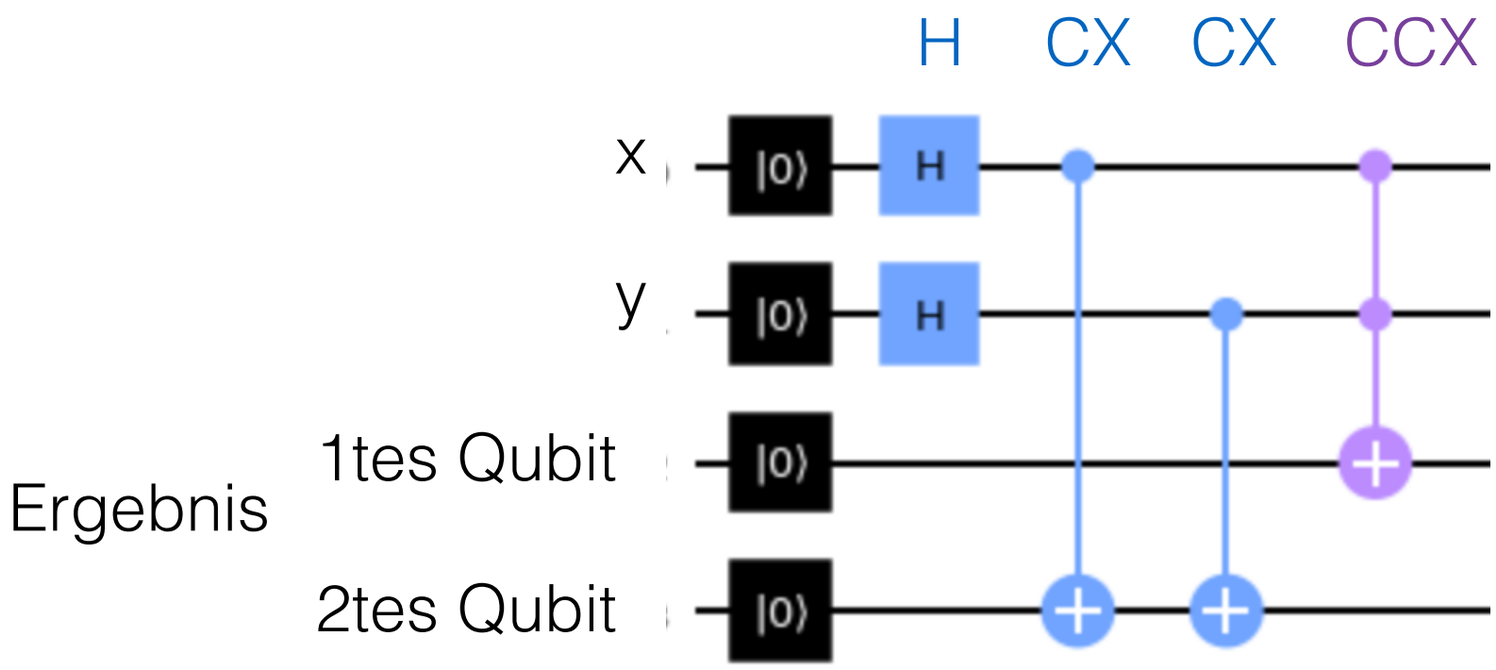
Quanten Schaltkreis:



# Quantenparallelismus

Der klassische Schaltkreis führt die Rechnung für jeden gegebenen Input einzeln aus. Der Quantenparallelismus nutzt aus, dass es durch quantenmechanische Überlagerungen möglich ist die Additionen 0+0,0+1,1+1,1+1 alle gleichzeitig auszuführen.

Dazu erstellen wir mit Hilfe des H-Gates einfach eine Überlagerung aller Basiszustände in den Qubits x,y und führen den gleichen Schaltkreis aus…




..so dass das Ergebnis für alle möglichen Inputs parallel bestimmt wird.

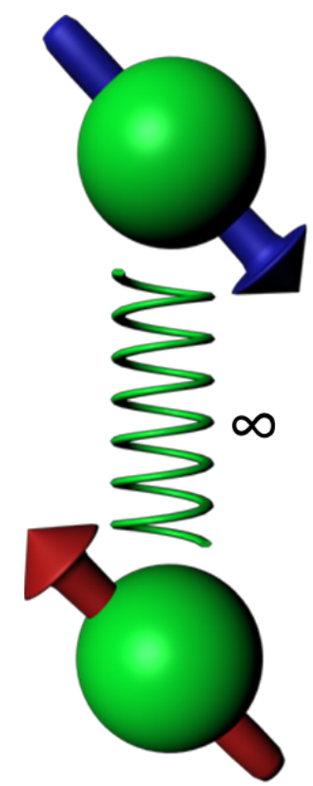
# Entanglement/Verschränkung

Wenn wir Systeme von mehreren Qubits betrachten, ist es möglich dass zwei oder mehrere Qubits miteinander verschränkt sind.

Das bedeutet insbesondere, dass man zB Zustände herstellen kann, bei denen die Einzelzustände von zwei Qubits immer gleich sind.

$$\frac{1}{\sqrt{2}}|00> + \frac{1}{\sqrt{2}}|11>$$

Dies führt dazu dass sich durch eine Messung des ersten Qubits, der Zustand des zweiten Qubits ändert, und in diesem Beispiel mit Sicherheit feststeht.



Diese Art der Verschränkung hat keine klassische Analogie aber vielfältige Anwendungen zB bei der Entwicklung von Quantenalgorithmen oder in der Quantenkommunikation

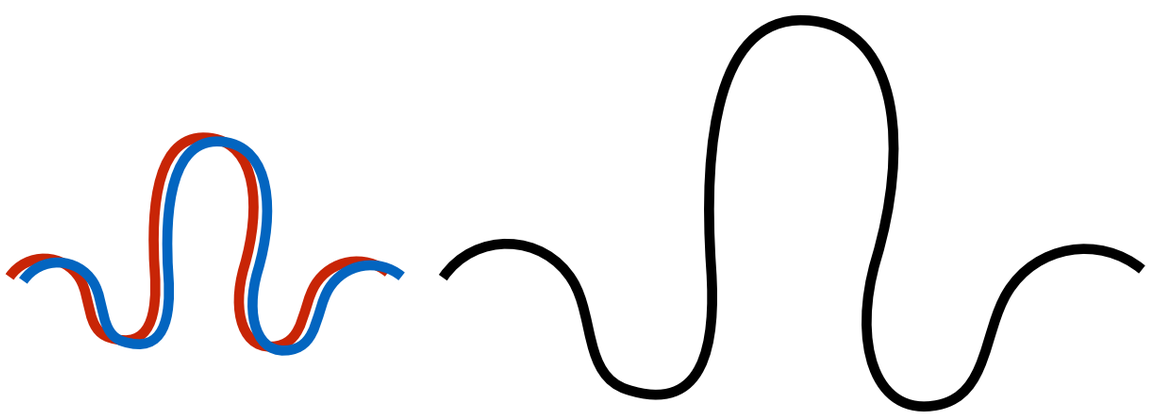
Nobelpreis 2022 an J. Clauser, A. Aspect, A. Zeillinger für Nachweis von Verschränkung an Photonen

# Interferenz

Ein weiteres wichtiges Konzept bei dem Design von Quantenalgorithmen, ist das man in der Quantenmechanik nicht mit Wahrscheinlichkeiten sondern mit Amplituden rechnet

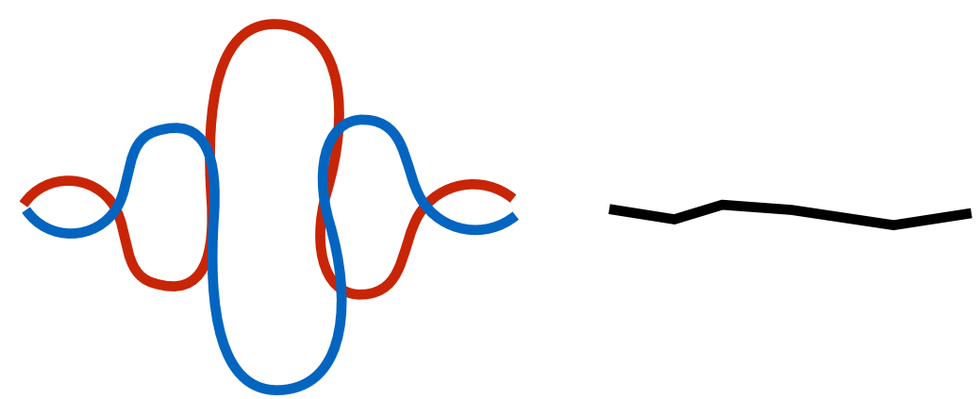
Während Wahrscheinlichkeiten immer positiv sind, können Amplituden zB auch negativ sein. Dies spiegelt den "Wellencharakter" der Quantenmechanik wieder, wodurch das Phänomen der Interferenz entstehen kann

konstruktive Interferenz



= aufschaukeln von Wellen

destruktive Interferenz



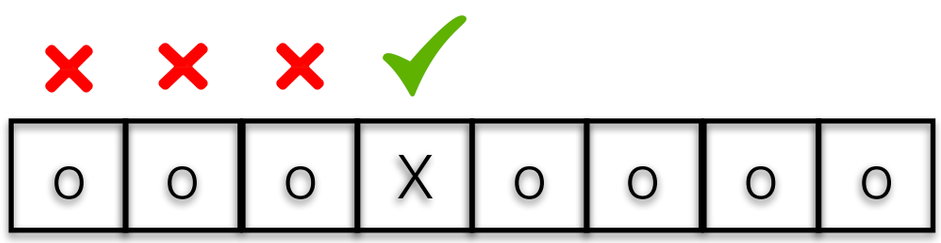
= auslöschen von Wellen

# Suchprobleme & Grover Algorithmus

Dieses Phänomen wird zB bei Such- oder Optimierungsproblemen ausgenutzt um aus vielen Zuständen den richtigen zu identifizieren.

Ein klassisches Suchproblem ist zB aus einer Liste von Elementen (o,o,o,X,o,o,o,o) das besondere Element zu identifizieren.

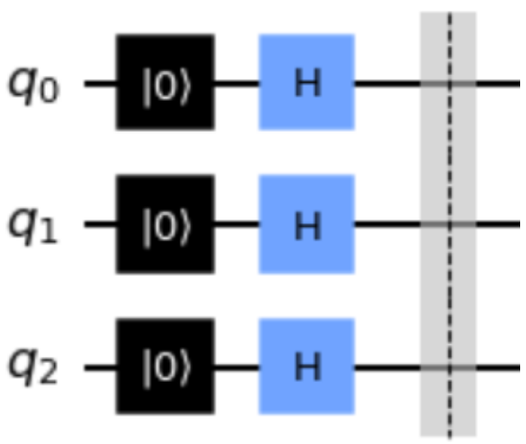
Ein klassischer Computer geht hierbei so vor, dass er sich der Reihe nach alle Elemente einzeln anschaut und überprüft, welches das besondere Element ist




Ein Quantencomputer kann dieses Problem mit Hilfe des Grover Algorithmus deutlich effizienter lösen, und so auch sehr große Suchprobleme lösen.

# Grover Algorithmus

Der Grover Algorithmus verwendet Manipulationen des Quantenzustands um **konstruktive Interferenz für das markierte Element und destruktive Interferenz für alle unmarkierten Elemente** herzustellen.

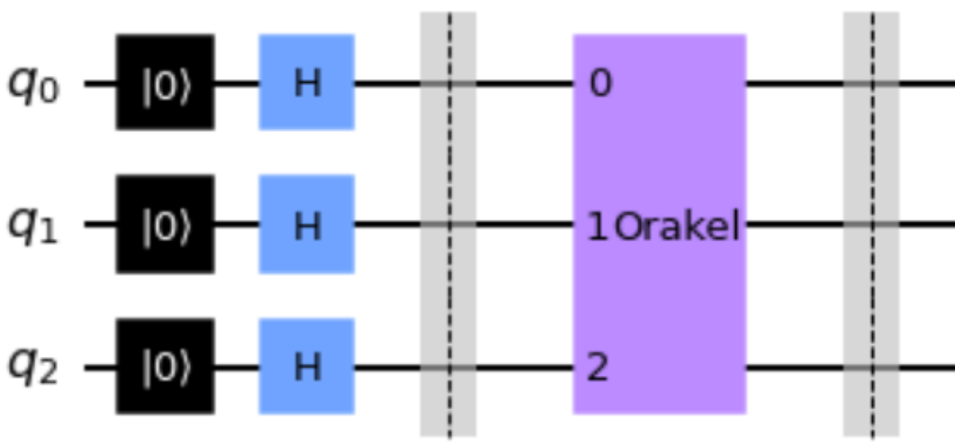



Damit alle Zustände gleichzeitig überprüft werden können erzeugt man zunächst eine Superposition aller Basiszustände

$$|\Psi >= \frac{1}{\sqrt{8}}|000 > + \frac{1}{\sqrt{8}}|001 > + \cdots + \frac{1}{\sqrt{8}}|111 >$$

# Grover Algorithmus

Der Grover Algorithmus verwendet Manipulationen des Quantenzustands um **konstruktive Interferenz für das markierte Element und destruktive Interferenz für alle unmarkierten Elemente** herzustellen.

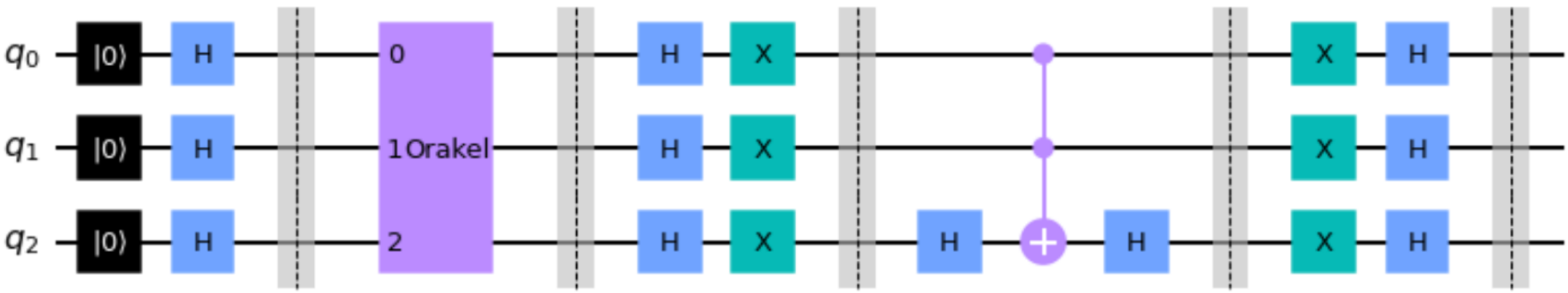



Durch ein entsprechendes Quantenguate das sog. “Orakel” wird der gesuchte Zustand (hier |001>) durch einen Vorzeichenwechsel markiert

$$|\Psi>= \frac{1}{\sqrt{8}}|000> - \frac{1}{\sqrt{8}}|001> + \cdots + \frac{1}{\sqrt{8}}|111>$$

# Grover Algorithmus

Der Grover Algorithmus verwendet nun das Orakel zusammen mit einer weiteren Manipulation des Quantenzustands um **konstruktive Interferenz für das markierte Element und destruktive Interferenz für alle unmarkierten Elemente** herzustellen.



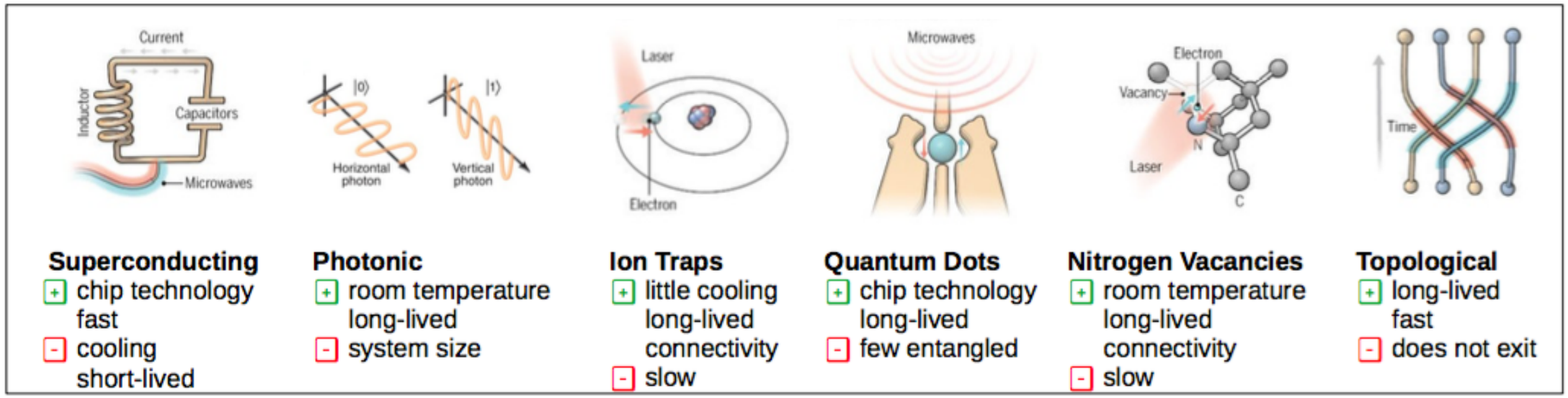

Die unterschiedlichen Vorzeichen nutzt man nun aus um konstruktive/ destruktive Interferenz zu erzeugen

$$|\Psi>= \frac{1}{\sqrt{32}}|000> + \frac{5}{\sqrt{32}}|001> + \cdots + \frac{1}{\sqrt{32}}|111>$$

so dass eine Messung mit ca. 78% Wahrscheinlichkeit das gesuchte Element ergeben würde

# Quantencomputer — Hardware

Bislang haben wir die theor. Eigenschaften eines idealen Quantencomputers besprochen. Bei der praktischen Realisierung eines solchen Systems werden verschiedene Ansätze verfolgt um ein solches Quantensystem zu realisieren.



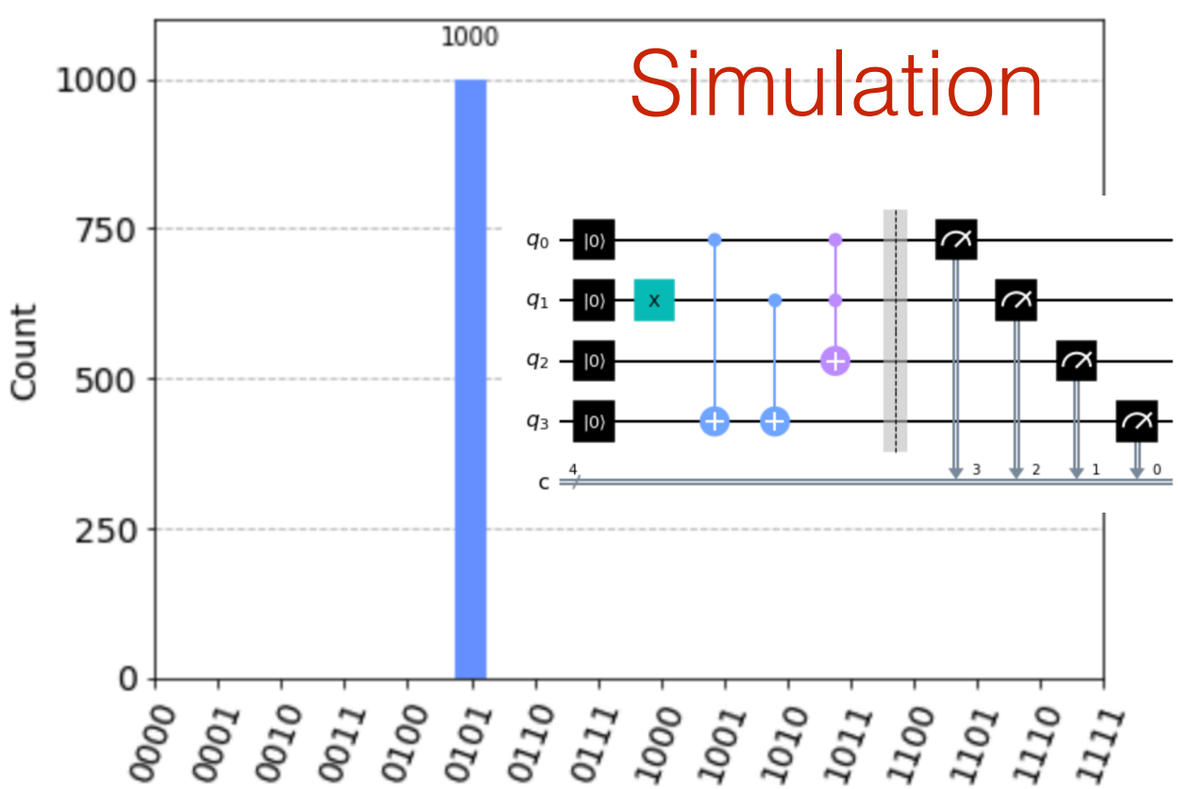
Neben den bislang besprochenen digitalen Quantencomputern gibt es noch sog. Quantensimulatoren (nicht universell programmierbar) für spezialiserte Anwendungen

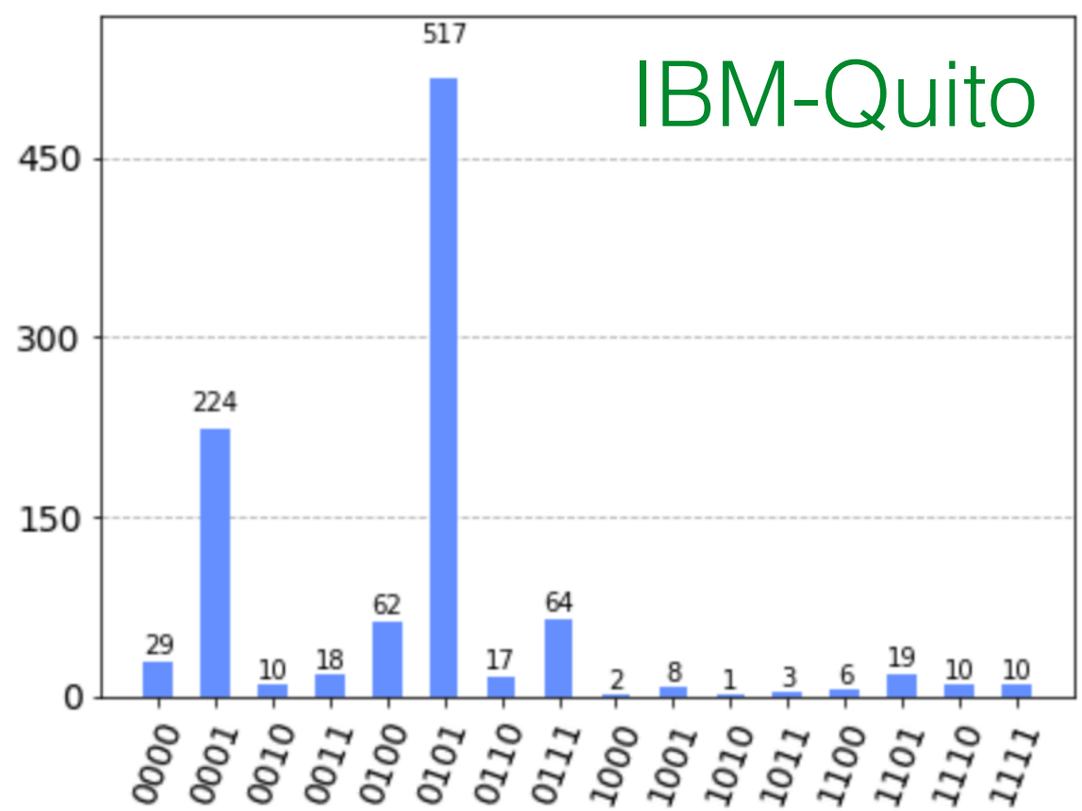
# Generelle Probleme von Quantencomputern

Die theoretischen Stärken eines Quantencomputers sind zugleich auch seine Schwächen bei der praktischen Entwicklung von Quantencomputern.

Eine hinreichend große Anzahl von hochsensiblen Qubits für eine hinreichend lange Dauer genügend gut von der Umgebung isoliert werden, und zugleich miteinander verbunden und programmierbar sein.

Diese Fehler führen zu inkorrekten Ergebnissen:



# Entwicklung von Quantencomputern

Durch den Einstieg kommerzieller Unternehmen hat es in den letzten Jahren signifikante Fortschritte bei der Entwicklung digitaler Quantencomputer gegeben

| Manufacturer | Name/Codename/Designation | Architecture | Layout | Socket | Fidelity | Qubits | Release date |
|---|---|---|---|---|---|---|---|
| IBM | IBM Osprey | Superconducting | N/A | N/A | N/A | 433 qubit | November 2022 |
| Xanadu | Borealis[7] | Photonics | N/A | N/A | N/A | 216 qb[7] | 2022[7] |
| IBM | IBM Eagle | Superconducting | N/A | N/A | N/A | 127 qubit | November 2021 |
| USTC | Jiuzhang | Photonics | N/A | N/A | N/A | 76 qb[5][6] | 2020 |
| Google | Bristlecone | Superconducting transmon | 6×12 lattice | N/A | 99% (readout) 99.9% (1 qubit) 99.4% (2 qubits) | 72 qb[3][4] | March 5, 2018 |
| IBM | IBM Manhattan [18] | Superconducting | QV32 [19] | N/A | N/A | 65 qb | |
| Google | Sycamore | Superconducting transmon | 9×6 lattice | N/A | N/A | 53 qb effective | 2019 |
| IBM | IBM Q 53 | Superconducting | N/A | N/A | N/A | 53 qb | October 2019 |

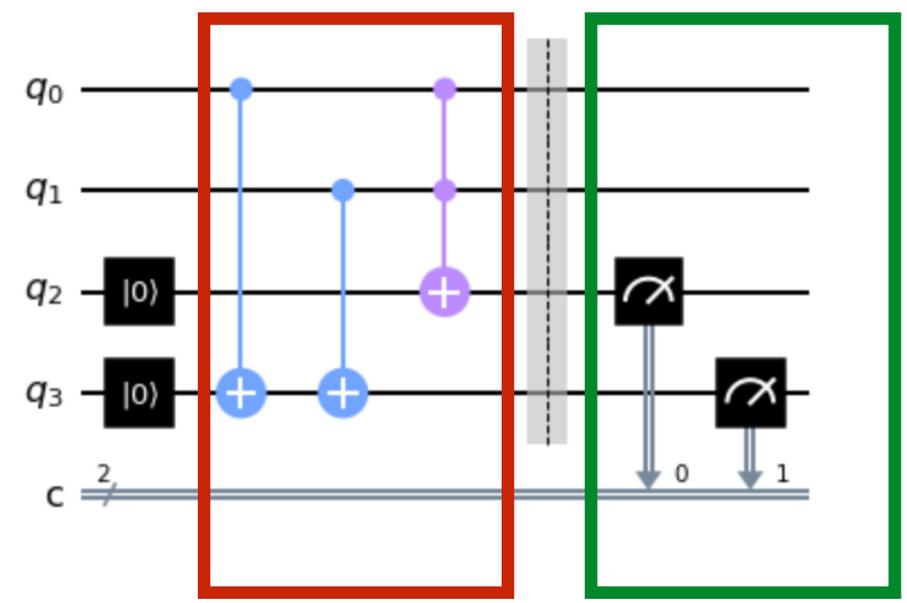
Das Problem bleibt jedoch weiterhin die Fehlerraten zu reduzieren (bzw. durch Mitigation oder Korrektur gering genug zu halten) um sinnvolle Rechnungen auf hinreichend grossen Systemen durchzuführen

# Generelle Probleme von Quantencomputern

Bei den Fehlern unterscheidet man zwischen verschiedenen Arten von Fehlern, die zwischen verschiedenen Geräten stark variieren können

-> Gate Fehler (speziell 2-Qubit)
typischerweise ~0.1 -10 %

-> Messfehler (2-Qubit)
typischerweise ~0.1 -1 %




Diese vermeintlich kleinen Fehler vervielfachen sich bei der Anwendung von mehreren Gates in einem Quantenalgorithmus

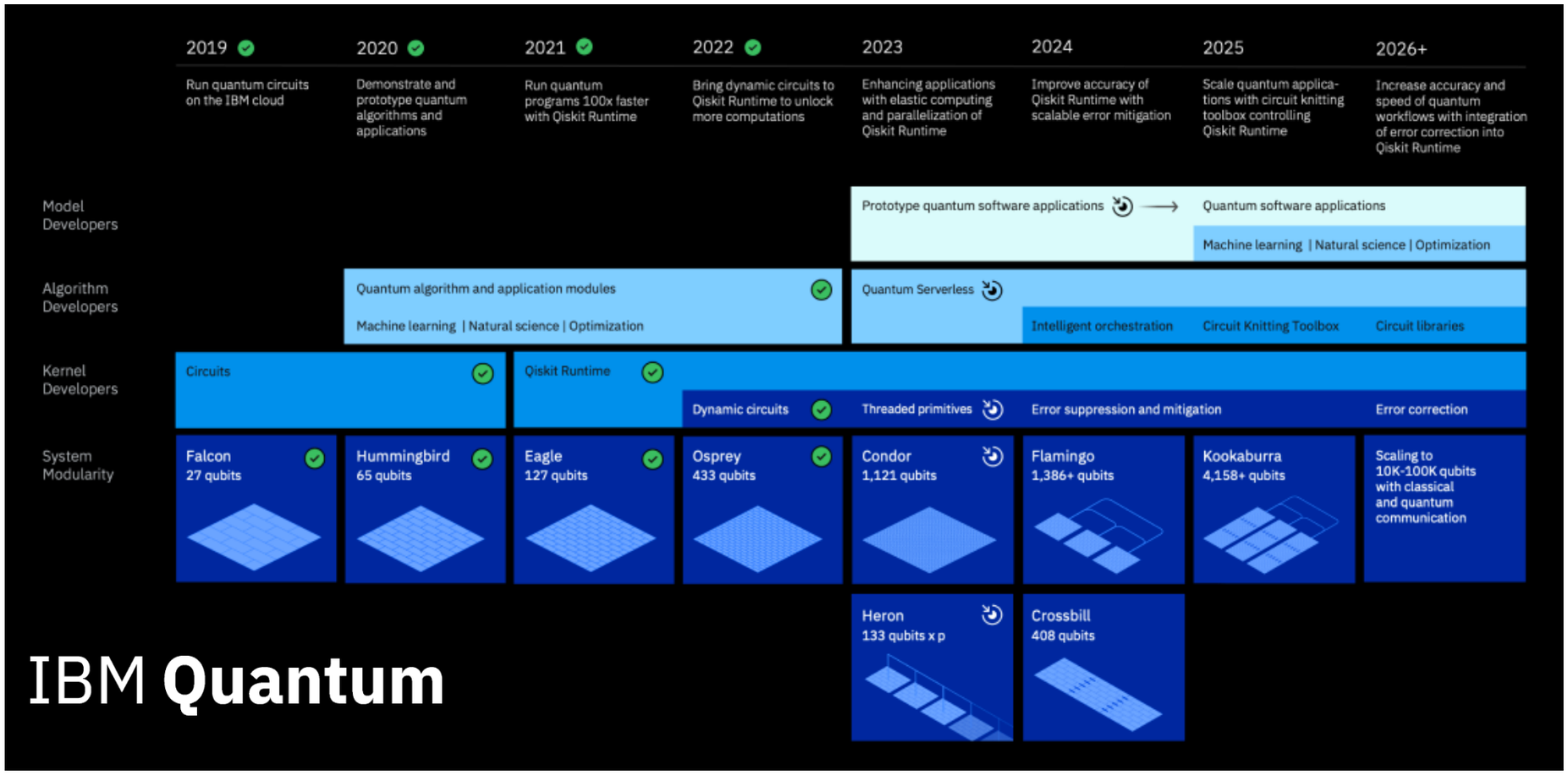
Bei 127 Gates mit einer Fehlerrate von 2% ist die Wahrscheinlichkeit das richtige Ergebnis zu bekommen lediglich 7.68 %

IBM Eagle 127
Qubits

| | |
|---|---|
| Status: ● Online | Avg. CNOT Error: 2.078e-2 |
| Total pending jobs: 0 jobs | Avg. Readout Error: 1.426e-2 |
| Processor type ⓘ: Eagle r3 | Avg. T1: 301.67 us |
| Version: 1.0.0 | Avg. T2: 160.92 us |
| Basis gates: CX, ID, RZ, SX, X | Providers with access: -- |

# Ausblick

Die Herausforderung ist es mit der Herstellung von Quantencomputern mit mehr Qubits gleichzeitig die Fehlerquote zu reduzieren, so dass diese Systeme sinnvoll genutzt werden können




Da noch nicht absehbar ist wann fehlertolerante Quantencomputer verfügbar sind, beschränkt sich der Nutzen zunächst auf ausgewählte Probleme bei denen Fehler korrigiert werden können oder tolerabel sind

# Zusammenfassung

Quantencomputer basieren auf den Grundsätzen der Quantenmechanik und nutzen bei der Lösung von Problemen quantenmechanische Phänomene wie z.B. Verschränkung und Superposition für die es keine klassischen Analogien gibt.

Damit stellen Quantencomputer eine interessante Technologie mit vielfältigen Anwendungen in Wissenschaft und Technik dar

klassische Such- und Optimierungsprobleme, Dynamik chem. Reaktionen, …

Die quantenmechanischen Eigenschaften eines Quantencomputers machen es zugleich schwierig ein solches System zu realisieren; der derzeitige Entwicklungsstand erlaubt es auf absehbare Zeit (noch?) nicht relevante Probleme auf einem Quantencomputer zu lösen.

Dennoch ist dies ein sehr aktives Forschungsgebiet, mit vielfältigen Möglichkeiten sowohl im Bereich der Hardwareentwicklung als auch in der Entwicklung von Anwendungen und Algorithmen von Quantencomputern.

# Weitere Ressourcen

Sollte dieser Vortrag Ihre Neugier zum Thema Quantencomputer geweckt haben empfehlen wir als weitere Ressourcen

IBM Quanten Computing Lab

IBM Quantum

https://quantum-computing.ibm.com/lab

Die Slides dieses Vortrags finden Sie auf meiner Webseite

www.kaiden.de

Gerne können Sie mich auch im Anschluss an den Vortrag persönlich oder per jederzeit per E-Mail kontaktieren

sschlichting@physik.uni-bielefeld.de