Quantum Computation + Quantum Information

(basierend auf Nielsen + Chuang book)

Fundamentale Konzepte? Wie funktioniert ein Quantencomputer? Wie schnell ist er?

1. Shor Algorithm

- quantum Revolution 1920's

since 70s: complete control over single quantum systems (before macroscopic systems)

why? Hands! Often most profound insights: develop new Methods for probing a new regime of Nature

ex: - radio astronomy
- low T physics

dito quantum control: just taking first steps along these lines

- computer science

abstract model: Turing Machine ("universal Turing Machine")
(deterministic) ↳ simulate any other (Turing) Machine algorithmic

↓

mathematical concept of computation

church-Turing Hypothesis: equivalence between algorithms performed on real physical device and rigorous mathematical concept of Universal Turing Machine

„Any algorithm which can be simulated efficiently using a Turing machine"
(probabilistic)

↓

field of: computational complexity

efficient: polynomial in size of Problem

inefficient: superpolynomial, typically exponential

1985: Deutsch: ∃ computational device capable of efficiently simulating any physical system?

laws of physics: ultimately quantum mechanical → computing device based on quantum mechanics?

more powerful than classical C.?

Yes: Shor 1994: - finding prime factors of integer } efficient on QC, not on classical C.
- „discrete logarithm"

Grover 1995: - search through unstructured space

parallel: 1982: Richard Feynman: simulating quantum systems on classical computers is inefficient → build computers based on quantum?

other problems faster on QC? don't know – stay tuned!

Quantenrechner

Hauptbestandteile des „quanten Schaltkreismodells eines Computers":

1. klassische Ressourcen (nicht qm)

Quantenrechner besteht aus a) klassischen und b) quantenmechanischen Komponenten. Prinzipiell sind keine klassischen Teile notwendig, aber gewisse Aufgaben werden einfacher wenn Teile der Rechnung klassisch erfolgen können.
z.B. Quanten error-correction

2. angemessener Zustandsraum

von qubits (= quanten Bits, see below) $\to 2^n$-dim. Hilbertraum, mit Produktzustandsbasis $|x_1, \ldots, x_n\rangle$, wo $x_i = \{0,1\}$

3. Fähigkeit, Zustände zu präparieren

Man nimmt an, dass ein beliebiger Basiszustand $|x_1, \ldots, x_n\rangle$ in höchstens n Schritten zubereitet werden kann.

4. Fähigkeit, Quanten-Logikoperationen auszuführen („perform quantum gates")

Quanten-Logikoperationen müssen auf einer beliebigen Untermenge von Qubits ausführbar sein, und eine „universelle" Familie von Operationen muss ausführbar sein.

5. Fähigkeit, Messungen an der Rechnungszustandsbasis auszuführen

Messungen (zum „Auslesen" der Resultate) können in der Zustandsbasis an einem oder mehreren Qubits ausgeführt werden.

Quantum Bits (= Qubits)

Bit = fundamentale Informationseinheit im klassischen Computer

analog dazu: quanten Bit = Qubit : quantenmechanische, fundamentale Informationseinheit

Information ist immer verknüpft mit einer physikalischen Repräsentation, aber es ist hilfreich, zunächst das qubits als mathematische Objekte mit gewissen Eigenschaften zu beschreiben, die allen physikalischen Realisierungen gemeinsam ist.

klassisches Bit: Zustand entweder 0 oder 1

qubit: quantenmechanische Zustände $|0\rangle$ und $|1\rangle$ (Dirac Notation)

Unterschied: qubit kann, im Gegensatz zum klassischen Bit, nicht nur im Zustand 0/$|0\rangle$ oder 1/$|1\rangle$ sein, sondern auch in einem beliebigen Überlagerungszustand:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \text{(2-niveau System) qm} \qquad (24)$$

$|\alpha|^2 + |\beta|^2 = 1$ Normierung

(wie schon besprochen), d.h. qubit = Einheitsvektor im 2D komplexen Vektorraum

klassisch: Messung des Bits möglich / trivial

qubit: gegeben 1 qubit ist es bemerkenswerterweise nicht möglich, den quantenzustand des Qubits zu messen, d.h. α und β zu bestimmen. Bei Messung erhalten wir entweder $|0\rangle$ mit Wahrscheinlichkeit $|\alpha|^2$ oder $|1\rangle$ mit Wahrscheinlichkeit $|\beta|^2$. Trotzdem hat ein $|\psi\rangle$ wie (24) echte, verifizierbare Konsequenzen, welche für die Stärke / Geschwindigkeit eines Quantencomputers wesentlich sind.

Beispiel: $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ (25)

$\xrightarrow{\text{Messung, Kollaps } |\psi\rangle}$ entweder $|0\rangle$ 50% Wahr.

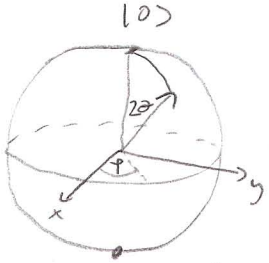
oder $|1\rangle$ 50% Wahr.

nach der Messung ist der Rest der Information verloren.

Realisierungen:
- Polarisationszustände eines Photons
- Spin (Kernspin, Elektronspin, z.B. in einem Quantendot)
- Atomorbitale, z.B. Grund- und Angeregter Zustand

Nützliche Visualisierung: Blochsphäre, wie besprochen.

$$|\psi\rangle = e^{i\gamma}\left(\cos\tfrac{\vartheta}{2}|0\rangle + e^{i\varphi}\sin\tfrac{\vartheta}{2}|1\rangle\right) \qquad (26)$$



die Gesamtphase α spielt keine Rolle (weil nicht direkt beobachtbar), d.h. die in einem Qubit gespeicherte Information ist durch zwei (kontinuierliche) Winkel $\vartheta \in [0, 90°]$ und $\varphi \in [0, 2\pi)$ beschrieben, die bei individueller Messung verloren geht. (Projektion auf $|0\rangle$ oder $|1\rangle$)

Aber: könnte man unendlich viele $|\psi\rangle$ Zustände erzeugen und messen, so könnte die volle Information (ϑ, φ) gewonnen werden

Mehrere Qubits

Zwei Qubits: $\{|0\rangle_1, |1\rangle_1\}$ und $\{|0\rangle_2, |1\rangle_2\}$ Zustands basis:

$$|00\rangle = |0\rangle_1 |0\rangle_2 \,, \quad |01\rangle = |0\rangle_1 |1\rangle_2 \quad \text{etc.}$$

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \qquad (27)$$

analog zu 1 Qubit: bei Messung: Kollaps auf $|00\rangle$ mit $|\alpha_{00}|^2$ Wahrsch. etc.

Messung nur eines Teilsystems ist auch möglich, z.B. nur des 1. qubit:

ergibt $|0\rangle_1$ mit Wahr. $|\alpha_{00}|^2 + |\alpha_{01}|^2$ $\rightarrow |\psi_{\text{post meas.}}\rangle = \dfrac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$ (28)

oder $|1\rangle_1$ mit Wahr. $|\alpha_{10}|^2 + |\alpha_{11}|^2$ $\rightarrow$ analog ↑

n Qubits: Basiszustände $|x_1 x_2 \ldots x_n\rangle$ (Produktbasis)

2^n Zustände mit 2^n $\alpha_{\ldots}$ Amplituden

Bsp. $n = 500$ $\rightarrow 2^n$ größer als Anzahl Atome im UNIVERSUM !

„Hilbert Space is a BIG place" Carlton Caves

Zeigt wohlmöglich das enorme Potential von Quantenrechnern auf!

Quantenrechner

Analog zum klassischen Computer, der aus elektrischen Logikschaltkreisen aufgebaut ist, wird beim Quantenrechner die Information in den Qubits mithilfe von „quantenlogik Operationen" verarbeitet. („quantum gates") Einige Beispiele von solchen „quantum gates" besprechen wir nun.

Einzelqubit Operationen („single qubit gates")

klassische Logikoperationen („gates") z.B. NOT:

	NOT
0	1
1	0

„Wahrheitstabelle"

gibt es ein quanten Analogon? offensichtlich $|0\rangle \to |1\rangle$ und $|1\rangle \to |0\rangle$, aber was soll mit Superpositionen geschehen?

wir fordern Linearität; (da QM allg. linear ist)

$$\alpha|0\rangle + \beta|1\rangle \xrightarrow{\text{QNOT}} \alpha|1\rangle + \beta|0\rangle \qquad (27)$$

oder $$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (\text{ist unitär } X^\dagger X = 1) \qquad (28)$$

d.h. quanten gates sind durch unitäre Matrizen dargestellt, die auf den Qubit-Zustandsvektoren wirken. (Unitär damit Normierung erhalten bleibt)

klassisch: das einzige nicht triviale Einzelbit gate = NOT

qm: mehrere nichttriviale Operationen, z.B.

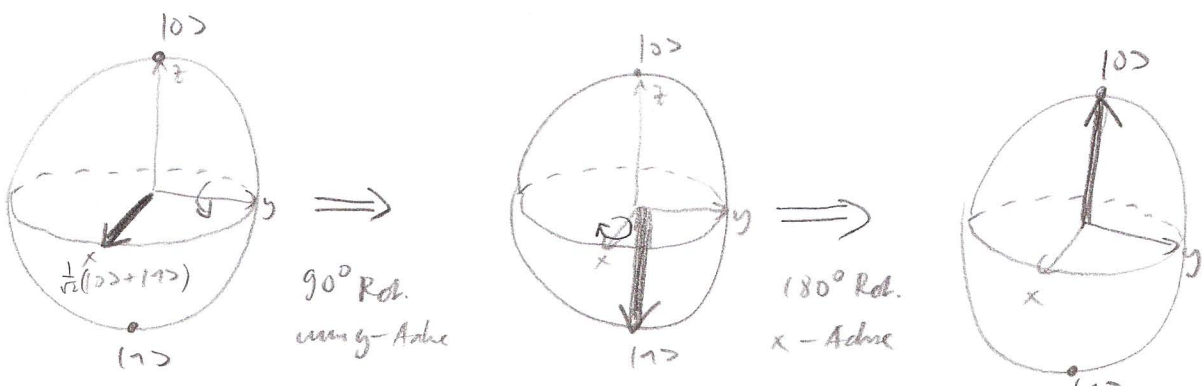
$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \sigma_z \qquad (29)$$

$$\text{Hadamard } H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad (30)$$

$H|0\rangle = (|0\rangle + |1\rangle)\frac{1}{\sqrt{2}}$ → „quadratwurzel NOT"

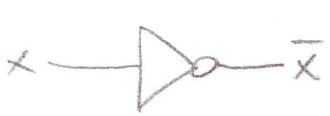
$H|1\rangle = (|0\rangle - |1\rangle)\frac{1}{\sqrt{2}}$ aber $H^2 = \mathbb{1}$, d.h. $H^2 \neq$ NOT

H auf Bloch-Sphäre: $H(|0\rangle + |1\rangle)\frac{1}{\sqrt{2}} = |0\rangle$

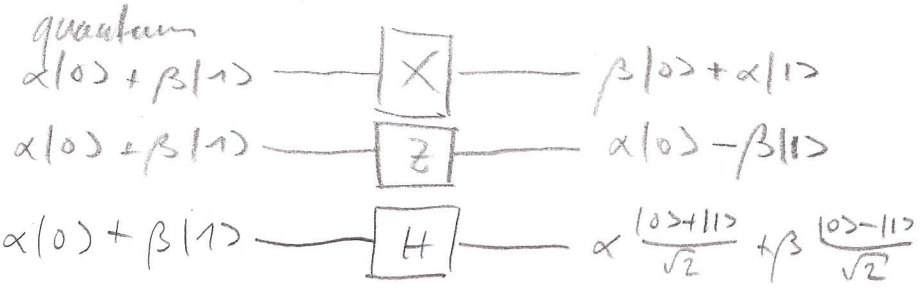


jede 1-Qubit Quantenoperation kann auf Blochsphäre visualisiert werden

klassisch



quantum



Da es unendlich viele 2×2 Matrizen (unitär) gibt, gibts ∞ viele Einzelqubit Op.

Aber: jede unitäre Matrix U kann geschrieben werden

$$U = e^{i\alpha}\begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}\begin{pmatrix} \cos\gamma/2 & -\sin\gamma/2 \\ \sin\gamma/2 & \cos\gamma/2 \end{pmatrix}\begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix} \quad (31)$$

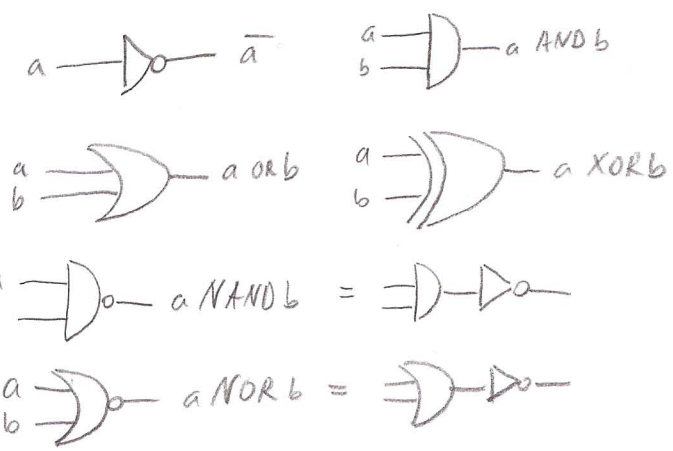
d.h. kann aus Operationen mit $\{\alpha, \beta, \gamma, \delta\}$ aufgebaut werden.

Weiter: mit gewissen fixen Werten $\{\alpha, \beta, \gamma\}$ können beliebig gute Näherungen jeder unitären Matrix U erreicht werden

Allg: jede beliebige quanten Operation (Rechnung) auf beliebig vielen Qubits kann immer aus einer endlichen, diskreten Menge von Operationen beliebig genau zusammengesetzt werden. Diese endliche, diskrete Menge heisst dann universell

Operationen an Mehreren Qubits „multiple qubit gates"

Klassisch

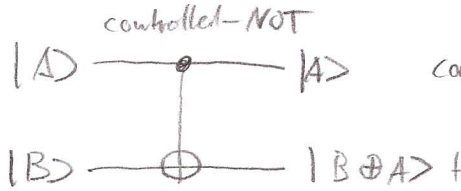


jede Funktion kann aus NAND zusammengesetzt werden: NAND: universell
(z.B. XOR allein oder sogar XOR + NOT: nicht universell) (paritätserhaltend)

quantenmechanisch

viele, exemplarisch:

controlled-NOT



(32)

$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$ in $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ Basis

↖ unitär

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

„falls control qubit = 0, dann target unverändert"

Verallgemeinertes XOR: $|A, B\rangle \xrightarrow{CNOT} |A, B \oplus A\rangle$ (33)

↑ Addition Modulo 2 = XOR

stellt sich heraus: keine Verallgemeinerung / quanten Analog zu NAND, OR etc weil diese „irreversibel" sind, d.h. nicht invertierbar. (Info verloren)
(z.B. gegeben die Ausgabe A⊕B des XOR, nicht möglich A und B zu bestimmen)
aber unitäre matrizen immer invertierbar. $U^{-1} = U^\dagger$, auch unitär

Quantencomputer: reversibel / invertierbar (wichtig für Verständnis wieviel Quantencomputer schnell)

Auch: Jedes n-qubit gate: kann aus CNOT und Einzelqubit gates konstruiert werden (34)