Karlsruhe Institute of Technology

Grundlagen des Quantencomputers

Christian Tesch

Gliederung

1. Qubit und Quantenregister
2. Quantengatter
3. Mögliche Anwendungen für Quantencomputer
4. Praktische Implementierungen

Qubit

- Klassisches Bit:
  - 0 oder 1

- Quantenbit (kurz: Qubit):
  - Superposition aus Basiszuständen $|0\rangle$ und $|1\rangle$:

$$|\phi\rangle = a\,|0\rangle + b\,|1\rangle \qquad a, b \in \mathbb{C}$$

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

und $|0\rangle \perp |1\rangle$

Dekohärenz

- Zerstörung der Superposition eines Qubits durch Wechselwirkung mit der Umgebung
- Quantenmechanische Effekte nur innerhalb Dekohärenzzeit nutzbar
- Größte Hürde auf dem Weg zum Quantencomputer

No Cloning Theorem

- Superpositionszustände können nicht kopiert werden
- Urpsrungszustand muss beim Kopieren verändert werden

Zustandsgemisch

- Keine vollständigen Informationen über Zustand

  z.Bsp. aufgrund von:

  - Messungenauigkeiten
  - Ensemblemessung

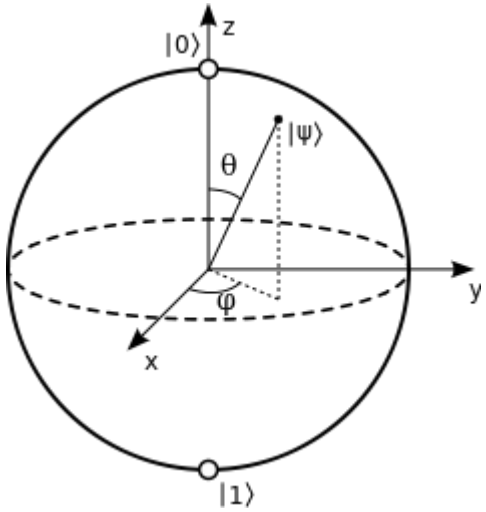
- Darstellung über Dichtematrix $\hat{\rho}$:

$$\hat{\rho} = \sum p_i \left|\phi_i\right\rangle \left\langle\phi_i\right|$$

Bloch Sphere

- Darstellung des Zustands in Kugelkoordinaten

$$|\phi\rangle = cos\frac{\theta}{2}|0\rangle + e^{i\phi}sin\frac{\theta}{2}|1\rangle$$



- Obere Halbkugel:
  - Höhere Wahrscheinlichkeit $|0\rangle$ zu erhalten
- Untere Halbkugel
  - Höhere Wahrscheinlichkeit $|1\rangle$ zu erhalten

Quantenregister

- Zustände mit mehreren Qubits

- z.Bsp. Zwei-Qubit-Quantenregister:
  - Mögliche Basiszustände:

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

  - Werden aus Tensorprodukt der einzelnen Basiszustände gebildet

d.h. : $|01\rangle = |0\rangle \otimes |1\rangle$

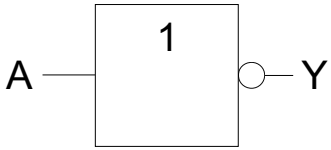
- Üblich ist Dezimaldarstellung bei größeren Registern:
  - z.Bsp.: $|01101\rangle = |13\rangle$

Verschränkung

- „spukhafte Fernwirkung“
- Verschränkter Zustand: $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Messung an erstem Qubit legt Zustand des zweiten Qubit fest
- Widerspricht Lokalitätsprinzip

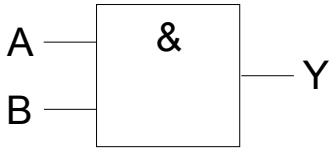
Klassische Gatter

NOT-Gatter



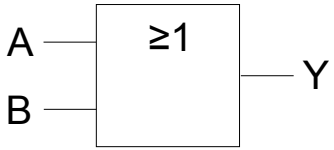
$$Y = \bar{A}$$

AND-Gatter



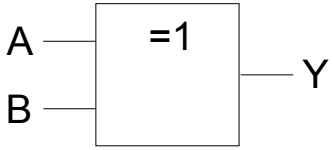
$$Y = A \wedge B$$

OR-Gatter



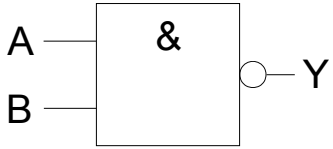
$$Y = A \vee B$$

XOR-Gatter



$$Y = A \oplus B$$

NAND-Gatter



$$Y = \overline{A \wedge B}$$

Klassische Gatter

- Anzahl Eingabebits ≠ Anzahl Ausgabebits

- Information geht verloren

→ Reduktion der Zustände von 4 auf 2

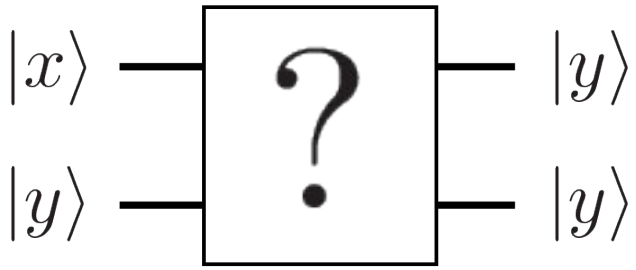
→ Reduktion der Entropie um $\Delta S = k_b \; ln(2)$

→ Abgabe von Wärme $Q = S \; T = k_b \; T \; ln(2)$

(Neumann-Landauer-Grenze)

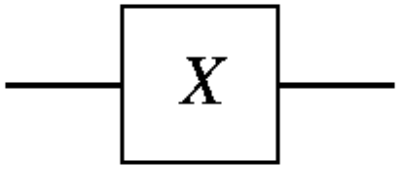
Quantengatter

- Quantengatter = unitäre Operation
- Reversibel
- Kein Informationsverlust → keine Wärmeabgabe aufgrund Entropie
- No-Cloning-Theorem:
  Kopieren nicht möglich mit reversiblen Operationen
- Erschwert Fehlerkorrektur



Ein-Qubit-Gatter

Pauli-X/Y/Z-Gatter

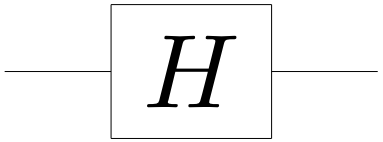


$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

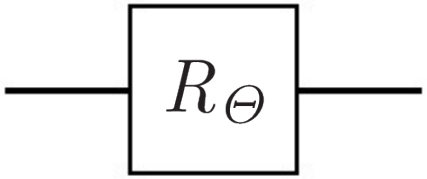
$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

Hadamard-Gatter



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

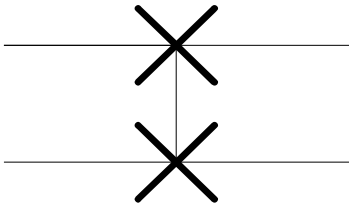
Phase-Shift-Gatter



$$R_\Theta = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\Theta} \end{bmatrix}$$

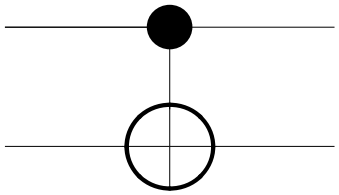
Quantengatter über mehrere Qubits

SWAP-Gatter



$$SWAP = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

CNOT-Gatter

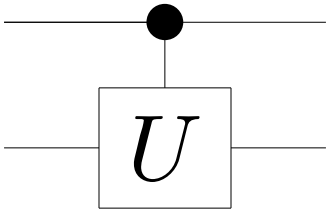


$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$|x, y\rangle \rightarrow |x, x \oplus y\rangle$$

Quantengatter über mehrere Qubits

CU-Gatter



$$U = \begin{bmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{bmatrix}$$

$$CU = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{bmatrix}$$

Quantengatter über mehrere Qubits

Hadamard-Gatter über Quantenregister

$$H_n = \bigotimes_{i=1}^{n} H$$

z.Bsp.: $H_2 = H \otimes H$

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

H *nur auf erstes Qubit:*

$$H \otimes 1_2$$

H *nur auf zweites Qubit:*

$$1_2 \otimes H$$

$$= \frac{1}{2} \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

Universeller Satz von Quantengattern

- Satz von Quantengattern zur Darstelung aller möglicher Operationen
- Notwendig zur Realisierung von Quantencomputern
- Universeller Satz → jede Rechenoperation kann implementiert werden
- Ein möglicher Satz besteht z.Bsp. aus allen Ein-Qubit-Gatter und dem CNOT-Gatter

Problem von Deutsch

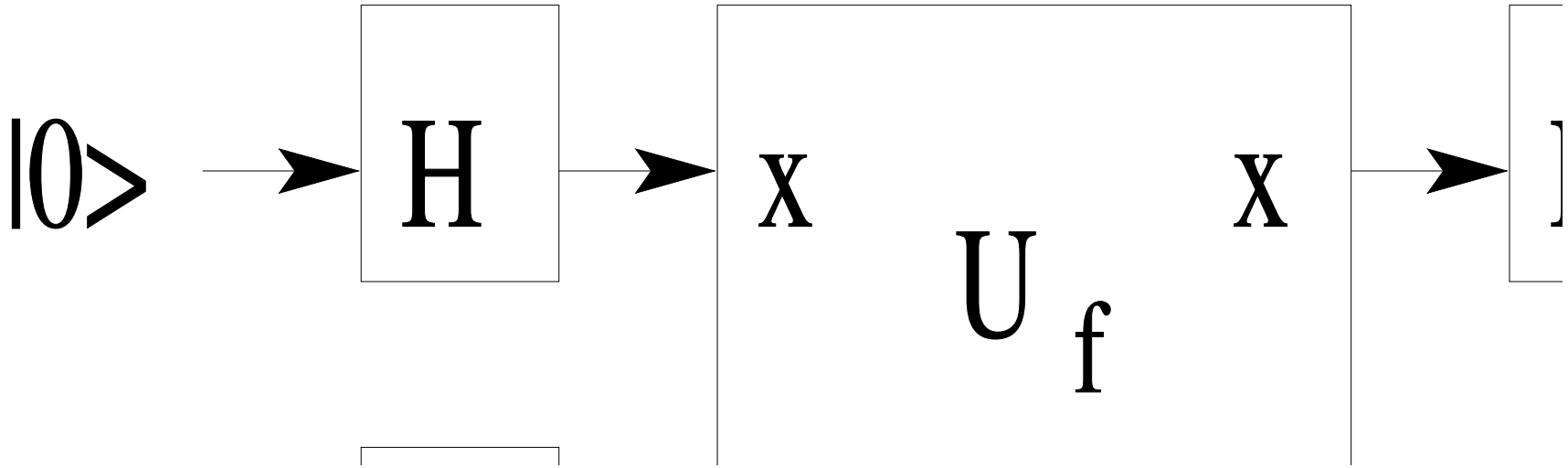
- Unbekannte Funktion $f: \{0,1\} \to \{0,1\}$
- Frage: Ist die Funktion konstant oder balanciert?
  - Konstant: $f(0) = f(1)$
  - Balanciert: $f(0) \neq f(1)$
- Beispiel: echte Münze oder Trickmünze
- Klassisch sind zwei Funktionsaufrufe nötig
- Quantencomputer benötigt nur einen

Rechnung: Problem von Deutsch

- Präparation eines Zwei-Qubit Zustands
- Anwendung der Hadamard Transformation
- Funktion f „kontrolliert“ anwenden auf zweites Qubit
- Erneute Anwendung der Hadamard-Transformation
- Messung: möglicher Ausgang:

  - $|01\rangle$: f ist konstant
  - $|11\rangle$: f ist balanciert

Schaltkreis Problem von Deutsch



Shor-Algorithmus

- Faktorisierung von Zahlen
  - 2001: Faktorisierung von 15 durch IBM
  - 2011: Faktorisierung von 21 an der University of Bristol
- Laufzeit schneller als beim klassischen Computer
- Kann RSA-Verschlüsselung knacken

Grover Algorithmus

- Suche in unsortierten Datenbanken mit N Einträgen

- Laufzeit:
  - klassischer Computer: $\mathcal{O}(N)$
  - Quantencomputer: $\mathcal{O}(\sqrt{N})$

- DES Brute Force:
  - Klassischer Computer: ca. 317 Jahre
  - Quantencomputer: ca. 1,5 Minuten

Kryptographie

- Quantenkommunikation mittels Qubits

- Lauschangriff kann festgestellt werden
  - Lauscher misst → zerstört Superposition
  - Lauscher kann aufgrund von No-Cloning-Theorem keine Kopie erstellen

DiVincenzo Kriterien

- Wohldefinierte Qubits, System muss skalierbar sein
- Präparation der Qubits in reine Zustände
- Ausreichend lange Dekohärenzzeit
- Universeller Quantengatter Satz
- Qubits alle einzeln messbar

Kriterien für die Quantenkommunikation

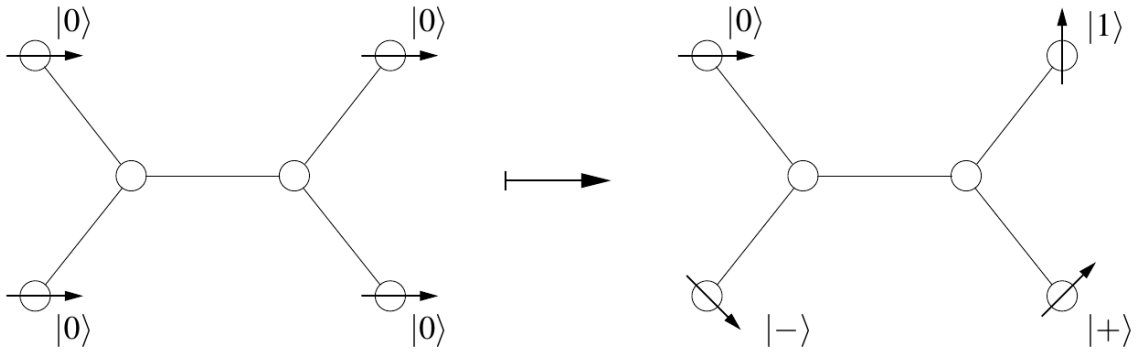
- Stationäre Qubits in bewegliche Qubits überführen
- Austausch beweglicher Qubits an entfernten Orten

Ionenfallen Quantencomputer

- Ionen gefangen in elektromagnetischem Feld
- Grundzustand und angeregter Zustand entsprechen den zwei Basiszuständen
- Universeller Satz von Gattern implementierbar
- Skalierbar
- Vielversprechender Ansatz

NMR - Quantencomputer

- Moleküle als Quantenregister
- Kernspin der Atome als Qubits
- Nicht skalierbar



Kryptographie

- Keine eigentlichen Quantencomputer
- Reine Kommunikation
- Photonen als bewegliche Qubits
- Systeme sind bereits kommerziell erhältlich

Literatur

- Quantum Computing – A Short Course from Theory to Experiment, J. Stolze, D. Suter
- Quantum Computing verstehen, M.Homeister
- Explorations in Quantum Computing, Colin P. Williams