

# Seminar über Quantum Computing

*Qubits, gates and networks*<sup>a</sup>

Lars Fischer

Universität Siegen

---

<sup>a</sup>Folien auf <http://www.larsfischer.de.vu>

# Inhaltsverzeichnis

<b>1</b>	<b>Qubits, Quantum registers</b>	<b>3</b>
<b>2</b>	<b>Quantum logic gates, quantum networks</b>	<b>20</b>
2.1	Das Hadamard Gate . . . . .	23
2.2	Das Phase-Shift Gate . . . . .	31
2.3	Das Controlled-NOT Gate . . . . .	37
2.4	Das Controlled-Phase-Shift Gate .	44
2.5	Controlled-U-Gate . . . . .	47
<b>3</b>	<b>Reversible Gatter und Univ. Gatter</b>	<b>51</b>

# 1 Qubits, Quantum registers

# Von Bits und Bytes

- Bit ist kleinste Informationseinheit

# Von Bits und Bytes

- Bit ist kleinste Informationseinheit
- ein Bit befindet sich in genau *einem* von zwei möglichen Zuständen

# Von Bits und Bytes

- Bit ist kleinste Informationseinheit
- ein Bit befindet sich in genau *einem* von zwei möglichen Zuständen
- Bytes bestehen aus Bits

# Von Bits und Bytes

- Bit ist kleinste Informationseinheit
- ein Bit befindet sich in genau *einem* von zwei möglichen Zuständen
- Bytes bestehen aus Bits
- ein Byte der Länge  $n$  kann dann einen von  $2^n$  verschiedenen Werten speichern

# Von Bits und Bytes

- Bit ist kleinste Informationseinheit
- ein Bit befindet sich in genau *einem* von zwei möglichen Zuständen
- Bytes bestehen aus Bits
- ein Byte der Länge  $n$  kann dann einen von  $2^n$  verschiedenen Werten speichern
- Darstellung einer Dezimalzahl in einem Byte der Länge 3:  $6_d = 110_b$



# Qubits

**Definition:** Ein Qubit ist ein *Quanten-System*, das zwei Quanten-Zustände einnehmen kann oder eine Überlagerung der beiden.

# Qubits

**Definition:** Ein Qubit ist ein *Quanten-System*, das zwei Quanten-Zustände einnehmen kann oder eine Überlagerung der beiden.

Diese beiden Quanten-Zustände bezeichnet man mit  $|0\rangle$  und  $|1\rangle$ .  $\{|0\rangle, |1\rangle\}$  bildet eine *Orthonormalbasis* des Zustandsraums des Qubits.

# Zustand eines Qubits

Man fasst die möglichen Zustände eines Qubits als Vektorraum (Zustands-Vektorraum) auf.

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle ,$$

mit  $\alpha, \beta \in \mathbb{C}$  und  $|\alpha|^2 + |\beta|^2 = 1$

# Zustand eines Qubits

Man fasst die möglichen Zustände eines Qubits als Vektorraum (Zustands-Vektorraum) auf.

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle ,$$

$$\text{mit } \alpha, \beta \in \mathbb{C} \text{ und } |\alpha|^2 + |\beta|^2 = 1$$

$$\text{bzw. } |\Psi\rangle = e^{i\phi} (\cos\gamma |0\rangle + e^{i\psi} \sin\gamma |1\rangle)$$

# Zustand eines Qubits

Man fasst die möglichen Zustände eines Qubits als Vektorraum (Zustands-Vektorraum) auf.

$$|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle ,$$

$$\text{mit } \alpha, \beta \in \mathbb{C} \text{ und } |\alpha|^2 + |\beta|^2 = 1$$

$$\text{bzw. } |\Psi\rangle = e^{i\phi} (\cos\gamma |0\rangle + e^{i\psi} \sin\gamma |1\rangle)$$

**Definition:** Ist  $\alpha \cdot \beta \neq 0$  so ist der Zustand  $\Psi$  eine Überlagerung (Superposition) der Quantenzustände.

# Koordinaten-Schreibweise:

Die Basis  $\{|0\rangle, |1\rangle\}$  ist fest, so lässt sich der Zustands-Vektor eines Qubits  $|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$  schreiben als:

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

Die Basisvektoren  $|0\rangle$  und  $|1\rangle$  schreiben sich als:

$$\begin{pmatrix} 1 \\ 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

# Realisierungen von Qubits

- Photonen: zwei Polarisierungen
- Atome: Spin des Atomkerns
- Ionenfalle: zwei verschiedenen Energie-Zustände des Atoms

# Quanten-Register

**Definition:** Eine Einheit von  $n$  Qubits heißt Quanten-Register der Größe  $n$  (quantum register).



# Quanten-Register

**Definition:** Eine Einheit von  $n$  Qubits heißt Quanten-Register der Größe  $n$  (quantum register).

Ist  $V_{qb}$  der Vektorraum, der Zustände eines Qubits, so ist der Vektorraum  $V_{qr}$ , der Zustände eines Quanten-Registers der Größe  $n$ :

$$V_{qr} = \bigotimes_{i=1}^n V_{qb}$$

# Kompakt-Schreibweise

Hat eine Zahl die dezimale Darstellung  $a_d$  und die binäre Darstellung  $a_n \dots a_0$ , so vereinbart man die kompaktere Darstellung  $|a_d\rangle$  oder  $|a_n \dots a_0\rangle$ , anstelle von

$$|a_n\rangle \otimes |a_{n-1}\rangle \otimes \dots \otimes |a_1\rangle \otimes |a_0\rangle$$

Man sagt auch, das Quanten-Register wurde mit dem Wert  $|a_d\rangle$  präpariert.

# Bsp: Zustand eines Q.-Registers

Daten werden binär gespeichert: Soll die Zahl  $6_d$  in einem Quanten-Register der Größe 3 gespeichert werden, so werden die binären Ziffern in den Qubits des Quanten-Registers gespeichert:

# Bsp: Zustand eines Q.-Registers

Daten werden binär gespeichert: Soll die Zahl  $6_d$  in einem Quanten-Register der Größe 3 gespeichert werden, so werden die binären Ziffern in den Qubits des Quanten-Registers gespeichert:

$$\begin{aligned} |1\rangle \otimes |1\rangle \otimes |0\rangle &= \\ |110_b\rangle &= |6_d\rangle \end{aligned}$$

# Computational basis

Zu einem Quanten-Register der Größe  $n$  gibt es  $2^n$  Basisvektoren des Tensorproduktes  $V_{qr}$ . Diese  $2^n$  Ausdrücke bilden eine Basis des Zustandsraumes des Quanten-Registers der Größe  $n$  – die computational basis.

# Computational basis

Zu einem Quanten-Register der Größe  $n$  gibt es  $2^n$  Basisvektoren des Tensorproduktes  $V_{qr}$ . Diese  $2^n$  Ausdrücke bilden eine Basis des Zustandsraumes des Quanten-Registers der Größe  $n$  – die computational basis.

Interpretation:

- alle binären Ausdrücke der Länge  $n$  ( $\{0, 1\}^n$ )
- die Zahlen  $0, \dots, 2^n - 1$

# Quanten-Register der Größe 3

Ein Quanten-Register der Größe 3 hat diese 8 Basisvektoren:

$$\begin{aligned} |0_d\rangle &= |000_b\rangle, & |1_d\rangle &= |001_b\rangle, \\ |2_d\rangle &= |010_b\rangle, & |3_d\rangle &= |011_b\rangle, \\ |4_d\rangle &= |100_b\rangle, & |5_d\rangle &= |101_b\rangle, \\ |6_d\rangle &= |110_b\rangle, & |7_d\rangle &= |111_b\rangle, \end{aligned}$$

# Superposition

Im Gegensatz zu dem klassischen Register kann ein Quanten-Register nicht nur einen Wert speichern, sondern auch die Überlagerung von mehreren Zuständen:



# Beispiel zur Superposition

Überlagerung im höchstwertigen Qubit des Quanten-Registers: statt  $|0\rangle$  oder  $|1\rangle$ :

$$\left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle\right)$$

$$\left(\frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle\right) \otimes |0\rangle \otimes |0\rangle$$

$$= \frac{1}{\sqrt{2}} (|0\rangle \otimes |0\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2}} (|1\rangle \otimes |0\rangle \otimes |0\rangle)$$

$$= \frac{1}{\sqrt{2}} (|100_b\rangle + |000_b\rangle) = \frac{1}{\sqrt{2}} (|4_d\rangle + |0_d\rangle)$$

# Alles zugleich...

Besonders interessant ist die Überlagerung aller möglichen Zustände: man präpariert jedes Qubit mit der Überlagerung  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ :

# Alles zugleich...

Besonders interessant ist die Überlagerung aller möglichen Zustände: man präpariert jedes Qubit mit der Überlagerung  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ :

$$\begin{aligned} & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ &= \left(\frac{1}{\sqrt{2}}\right)^3 (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \end{aligned}$$

# Alles zugleich...

$$\begin{aligned} \dots &= \left(\frac{1}{\sqrt{2}}\right)^3 \left[ \left( |0\rangle \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \right) + \right. \\ &\quad \left. \left( |1\rangle \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \right) \right] = \\ \dots &= \left(\frac{1}{\sqrt{2}}\right)^3 \left[ |000_b\rangle + |001_b\rangle + |010_b\rangle + |011_b\rangle + \right. \\ &\quad \left. |100_b\rangle + |101_b\rangle + |110_b\rangle + |111_b\rangle \right] \end{aligned}$$

# Alles zugleich

$$= \left( \frac{1}{\sqrt{2}} \right)^3 \left[ |0_d\rangle + |1_d\rangle + |2_d\rangle + |3_d\rangle + \right. \\ \left. |4_d\rangle + |5_d\rangle + |6_d\rangle + |7_d\rangle \right]$$

- 
- 
- 

# Zusammenfassung

# Zusammenfassung

- Qubits

# Zusammenfassung

- Qubits
- Quanten-Register



# Zusammenfassung

- Qubits
- Quanten-Register
- computational basis

# Zusammenfassung

- Qubits
- Quanten-Register
- computational basis
- Superposition in einem Quanten-Register

## 2 Quantum logic gates, quantum networks

# Quantum logic gates

Das Präparieren von Quanten-Registern und andere Operationen auf den Registern werden durch *unitäre* Operationen realisiert.

**Definition:** Ein Quanten-Logik-Gatter (quantum logic gate) ist eine Vorrichtung, die eine bestimmte unitäre Operation auf bestimmten Qubits, in einer festen Zeitperiode, ausführt.

# Quantum networks

**Definition:** Ein Quanten-Netzwerk ist eine Vorrichtung, die aus Quanten-Logik-Gattern besteht, deren Verarbeitungsschritte zeitlich synchronisiert sind. Die Ausgänge einiger Gatter sind mit den Eingängen anderer Gatter verbunden.

# Quantum networks

**Definition:** Ein Quanten-Netzwerk ist eine Vorrichtung, die aus Quanten-Logik-Gattern besteht, deren Verarbeitungsschritte zeitlich synchronisiert sind. Die Ausgänge einiger Gatter sind mit den Eingängen anderer Gatter verbunden.

Die Größe des Netzwerks ist die Anzahl der Quanten-Logik-Gatter aus denen es besteht.

# Hadamard gate

## 2.1 Das Hadamard Gate

- geläufigstes Quanten-Logik-Gatter
- operiert auf einem einzelnen Qubit
- führt die Hadamard-Transformation aus
- stellt Superposition her

# H als unitäre Abbildung

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



# H als unitäre Abbildung

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

- $H = \overline{H}$

# H als unitäre Abbildung

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

- $H = \overline{H}$
- $H = H^t$

# H als unitäre Abbildung

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

- $H = \overline{H}$
- $H = H^t$
- $H = H^{-1}$

# H als unitäre Abbildung

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

- $H = \overline{H}$
- $H = H^t$
- $H = H^{-1}$
- $\Rightarrow H^{-1} = \overline{H}^t$ , also H ist eine unitäre Abbildung

# Verschiedene Darstellungen von H

- Wertetabelle von H:

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

# Verschiedene Darstellungen von H

- Wertetabelle von H:

$$|0\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \quad |1\rangle \mapsto \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

- Schematische Darstellung von H:

$$|x\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \frac{1}{\sqrt{2}}(-1)^x |x\rangle + |1-x\rangle$$

# H auf $|000_b\rangle$ angewandt ...

Wendet man H auf jedes Qubit eines Registers an, so erhält man eine Superposition aller möglichen Werte des Registers:

$$\left. \begin{array}{l} |0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \frac{|0\rangle + |1\rangle}{\sqrt{2}} \end{array} \right\}$$

# H auf $|000_b\rangle$ angewandt ...

Wendet man H auf jedes Qubit eines Registers an, so erhält man eine Superposition aller möglichen Werte des Registers:

$$\left. \begin{array}{l} |0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \frac{|0\rangle + |1\rangle}{\sqrt{2}} \\ |0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \frac{|0\rangle + |1\rangle}{\sqrt{2}} \end{array} \right\}$$

$$= \left( \frac{1}{\sqrt{2}} \right)^3 (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle)$$



# H auf $|000_b\rangle$ angewandt

$$\begin{aligned} &= \left(\frac{1}{\sqrt{2}}\right)^3 (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \otimes (|0\rangle + |1\rangle) \\ &= \left(\frac{1}{\sqrt{2}}\right)^3 (|000_b\rangle + |001_b\rangle + |010_b\rangle + |011_b\rangle + \\ &\quad |100_b\rangle + |101_b\rangle + |110_b\rangle + |111_b\rangle) \\ &= \left(\frac{1}{\sqrt{2}}\right)^3 (|0_d\rangle + |1_d\rangle + |2_d\rangle + |3_d\rangle + \\ &\quad |4_d\rangle + |5_d\rangle + |6_d\rangle + |7_d\rangle) \end{aligned}$$

$$\mathbf{H}(|y\rangle), y \neq 000_b$$

Auf den vorigen Folien wurde  $\mathbf{H}(|000_b\rangle)$  berechnet. Es ergab sich die Superposition, in der alle Koeffizienten ein positives Vorzeichen hatten.

Berechnet man  $\mathbf{H}(|y\rangle)$  für ein  $y \neq 000_b$ , so haben die Hälfte der Summanden negatives Vorzeichen:

## $\mathbf{H}(|y\rangle), y \neq 000_b$ . **Beispiel**

$$\begin{aligned} |110_b\rangle &\mapsto \left(\frac{1}{\sqrt{2}}\right)^3 \left( (|0\rangle - |1\rangle) \otimes (|0\rangle - |1\rangle) \otimes (|0\rangle + |1\rangle) \right) \\ &= \left(\frac{1}{\sqrt{2}}\right)^3 \left( |000_b\rangle + |001_b\rangle - |010_b\rangle - |011_b\rangle \right. \\ &\quad \left. - |100_b\rangle - |101_b\rangle + |110_b\rangle + |111_b\rangle \right) \end{aligned}$$

Die Hälfte der Summanden hat positives, die andere Hälfte negatives Vorzeichen.

# $H(|y\rangle)$ , allgemeine Formel

Wendet man  $H$  auf jedes Qubit eines Quanten-Registers der Größe  $n$  an und ist  $|y\rangle$  der Wert, der sich in dem Register befindet, so gilt:

$$|y\rangle \mapsto \left(\frac{1}{\sqrt{2}}\right)^n \sum_{x \in \{0,1\}^n} (-1)^{y \cdot x} |x\rangle$$

Dabei ist für  $y = (y_{n-1}, \dots, y_0)$  und  $x = (x_{n-1}, \dots, x_0)$ :  $y \cdot x = \sum_{i=0}^{n-1} y_i \cdot x_i$ . Hier wird die Anzahl der Qubits gezählt, an der  $x$  und  $y$  beide eine 1 haben.

# Phase-Shift-Gate $\phi$

## 2.2 Das Phase-Shift Gate

ist ein weiteres Gatter, dass auf einem einzelnen Qubit operiert.

- $|0\rangle \mapsto |0\rangle, |1\rangle \mapsto e^{i\phi} |1\rangle$

- Schema:  $|x\rangle \xrightarrow{\phi} e^{ix\phi} |x\rangle$

- Matrixschreibweise:  $\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$

# $\phi$ als unitäre Abbildung

$$\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}, \quad \bar{\phi} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\phi} \end{pmatrix} = \phi^{-1}$$
$$\Rightarrow \phi^{-1} = \bar{\phi}^t$$

Also  $\phi$  ist eine unitäre Abbildung.

# Kombination von H und $\phi$

Mit Hilfe von H und  $\phi$  lassen sich alle reinen Zustände eines Qubits erzeugen (bis auf globale Phase), vermöge nachfolgendem Quanten-Netzwerk:

$$|0\rangle \xrightarrow{\quad 2\theta \quad} \boxed{\text{H}} \xrightarrow{\quad \frac{\pi}{2} + \phi \quad} \boxed{\text{H}} \xrightarrow{\quad} e^{i\phi} (\cos\theta |0\rangle + e^{i\phi} \sin\theta |1\rangle)$$

# H und $\phi$ reichen für ein Qubit

Mit dem Hadamard Gate und dem Phase-Shift Gate lassen sich alle unitären Operationen auf einem einzelnen Qubit zusammensetzen.

Nun kann man H und  $\phi$  auf jedem Qubit eines Quanten-Registers der Größe  $n$  operieren lassen, man erhält aus der Eingabe  $|00 \dots 0_b\rangle$  die Ausgabe  $|\Psi_1\rangle|\Psi_2\rangle \dots |\Psi_n\rangle$ , wobei  $\Psi_i$  eine beliebige Superposition von  $|0\rangle$  und  $|1\rangle$  ist.



# Bisher noch kein Entanglement!

Bisher lassen sich in einem Qubit beliebige Superpositionen bilden. Die Superpositionen der einzelnen Qubits in einem Register sind bisher voneinander unabhängig. Damit lassen sich nur Zustände erzeugen, die nicht entangled sind.

# Entangled states

Ein Quantenregisters der Größe  $n > 1$  läßt sich mit einem Zustand präparieren, der sich nicht als Tensorprodukt schreiben läßt, dessen Faktoren Zustände eines einzelnen Qubits sind.

# Entangled states

Ein Quantenregisters der Größe  $n > 1$  läßt sich mit einem Zustand präparieren, der sich nicht als Tensorprodukt schreiben läßt, dessen Faktoren Zustände eines einzelnen Qubits sind.

Beispiel:

- Kein Entanglement:

$$\alpha |00\rangle + \beta |01\rangle = |0\rangle \otimes (\alpha |0\rangle + \beta |1\rangle)$$

# Entangled states

Ein Quantenregisters der Größe  $n > 1$  läßt sich mit einem Zustand präparieren, der sich nicht als Tensorprodukt schreiben läßt, dessen Faktoren Zustände eines einzelnen Qubits sind.

Beispiel:

- Kein Entanglement:

$$\alpha |00\rangle + \beta |01\rangle = |0\rangle \otimes (\alpha |0\rangle + \beta |1\rangle)$$

- Entanglement:

$$\alpha |00\rangle + \beta |11\rangle \neq (\lambda_1 |0\rangle + \lambda_2 |1\rangle) \otimes (\lambda_3 |0\rangle + \lambda_4 |1\rangle) = \lambda_1 \lambda_3 |00\rangle + \lambda_1 \lambda_4 |01\rangle + \lambda_2 \lambda_3 |10\rangle + \lambda_2 \lambda_4 |11\rangle$$

# Entanglement durch 2-Qubit-Gatter

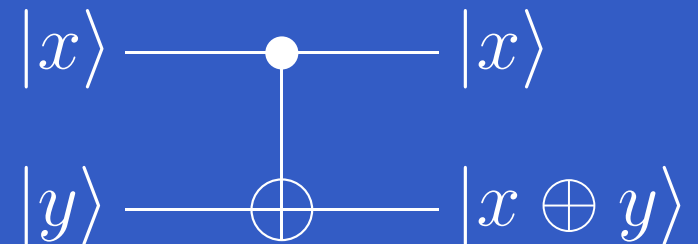
Um zwei Qubits zu verschränken, benötigen wir ein Gatter, das zwei Qubits als Eingabe hat:

## 2.3 Das Controlled-NOT Gate

(C-NOT) ist das verbreitetste 2-Qubit-Gatter. Es negiert das zweite Qubit (target), wenn das erste Qubit (control) gleich  $|1\rangle$  ist. Ist das erste Qubit gleich  $|0\rangle$ , so wird das zweite Qubit nicht verändert.

# C-NOT als unitäre Abbildung

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



Wieder ist  $C = \overline{C} = C^t = C^{-1} \Rightarrow C^{-1} = \overline{C}^t$ , also  $C$  ist unitär.

# C-NOT im Detail

Wertetabelle:  $(control, target)$

- $(|0\rangle, |0\rangle) \mapsto (|0\rangle, |0\rangle)$
- $(|0\rangle, |1\rangle) \mapsto (|0\rangle, |1\rangle)$
- $(|1\rangle, |0\rangle) \mapsto (|1\rangle, |1\rangle)$
- $(|1\rangle, |1\rangle) \mapsto (|1\rangle, |0\rangle)$

# C-NOT im Detail

Wertetabelle:  $(control, target)$

- $(|0\rangle, |0\rangle) \mapsto (|0\rangle, |0\rangle)$
- $(|0\rangle, |1\rangle) \mapsto (|0\rangle, |1\rangle)$
- $(|1\rangle, |0\rangle) \mapsto (|1\rangle, |1\rangle)$
- $(|1\rangle, |1\rangle) \mapsto (|1\rangle, |0\rangle)$

Ist das target =  $|0\rangle$ :

$$|x\rangle |0\rangle \mapsto |x\rangle |x\rangle, x \in \{0, 1\}$$

so wird es durch eine Kopie von control ersetzt.



# C-NOT kopiert keine Superpositionen

Ist  $|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$  eine Superposition, so ist

$$C(|\Psi\rangle |0\rangle) \neq (|\Psi\rangle |\Psi\rangle):$$

Mit  $|\Psi\rangle = \alpha |0\rangle + \beta |1\rangle$  und  $\alpha \cdot \beta \neq 0$ :

$$(\alpha |0\rangle + \beta |1\rangle) \otimes |0\rangle \longmapsto \alpha |00\rangle + \beta |11\rangle$$

$$C \cdot \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} \alpha \\ 0 \\ \beta \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \\ 0 \\ \beta \end{pmatrix}$$

# No-cloning Theorem

Eine unitäre Abbildung  $U$ , die auf einem Quanten-Register der Größe 2 arbeitet heißt Quanten-Kopiermaschine, falls für jeden Zustand  $|x\rangle$  des ersten Qubits gilt:

$$U(|x\rangle |0\rangle) = |x\rangle |x\rangle$$

Satz: Es gibt keine Quanten-Kopiermaschine.

# No-cloning Theorem

Beweis: Angenommen es gäbe eine solche Quanten-Kopiermaschine. Dann würde gelten:

$$U\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

# No-cloning Theorem

U ist aber eine lineare Abbildung:

$$\begin{aligned} U\left(\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle\right) &= \frac{1}{\sqrt{2}}U(|00\rangle + |10\rangle) = \\ &= \frac{1}{\sqrt{2}}U(|00\rangle) + \frac{1}{\sqrt{2}}U(|10\rangle) = \\ &= \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle, \text{ da } U(|00\rangle) = |00\rangle, U(|10\rangle) = |11\rangle \end{aligned}$$

Widerspruch zur vorigen Folie!

$$B(\phi)$$

## 2.4 Das Controlled-Phase-Shift Gate

ist ein weiteres 2-Qubit-Gatter. Es ist definiert als

$$B(\phi) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{i\phi} \end{pmatrix}$$

# $B(\phi)$ ist unitär

Es gilt:

$$B(\phi)^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & e^{-i\phi} \end{pmatrix} = \overline{B(\phi)}$$

$$B(\phi) = B(\phi)^t \Rightarrow B(\phi)^{-1} = \overline{B(\phi)}^t$$

Also  $B(\phi)$  ist eine unitäre Abbildung.

# $B(\phi)$ im Detail

- Schema:



- Wertetabelle:

$$|00_b\rangle \mapsto |00_b\rangle$$

$$|01_b\rangle \mapsto |01_b\rangle$$

$$|10_b\rangle \mapsto |10_b\rangle$$

$$|11_b\rangle \mapsto e^{i\phi} |11_b\rangle$$

# Controlled-U Gate

## 2.5 Controlled-U-Gate

Controlled-Not und Controlled-Phase-Shift ( $B(\phi)$ ) sind alle von der Form:

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{11} & u_{12} \\ 0 & 0 & u_{21} & u_{22} \end{pmatrix}, U = \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \text{ unitär}$$

Man bezeichnet solche Gatter als Controlled-U Gatter.

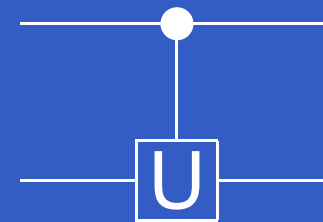


# Controlled-U

$U$  ist eine unitäre Matrix, die auf einem einzelnen Qubit operiert. Ist das erste Qubit (control) gesetzt ( $=|1\rangle$ ), so wird  $U$  auf das zweite Qubit angewandt. Andernfalls wird das zweite Qubit übernommen:

$$|0\rangle |x\rangle \mapsto |0\rangle |x\rangle$$

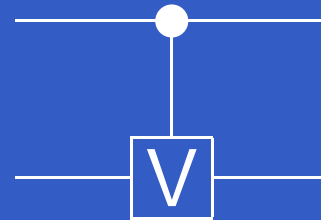
$$|1\rangle |x\rangle \mapsto |1\rangle U(|x\rangle)$$



# Controlled-V

Controlled-V ist ein spezielles Controlled-U-Gate:

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



$$V(|00\rangle) = |00\rangle$$

$$V(|01\rangle) = |01\rangle$$

$$V(|10\rangle) = |10\rangle$$

$$V(|11\rangle) = i |11\rangle$$

- 
- 
- 

# Zusammenfassung

# Zusammenfassung

- 1-Qubit Gates: H und  $\phi$

# Zusammenfassung

- 1-Qubit Gates: H und  $\phi$
- 2-Qubit Gates: Controlled-Not

# Zusammenfassung

- 1-Qubit Gates: H und  $\phi$
- 2-Qubit Gates: Controlled-Not
- H erstellt Superposition

# Zusammenfassung

- 1-Qubit Gates: H und  $\phi$
- 2-Qubit Gates: Controlled-Not
- H erstellt Superposition
- Controlled-Not erstellt Entanglement

### 3 Reversible Gatter und Univ. Gatter



# Reversible Gatter

Quanten-Gatter führen unitäre (und damit invertierbare) Operationen aus. Damit sind sie eine Verallgemeinerung der reversiblen Gatter aus der klassischen Informatik:

**Definition:** Reversible Gatter auf  $n$  Bits üben eine Permutation des  $\mathbb{F}_2^n$  aus.

Die Darstellungsmatrix ist eine Permutationsmatrix. Es gibt  $(2^n)!$  verschiedene reversible Gatter auf  $n$  Bits.

# Universelle Menge rev. Gatter

**Definition:** Eine Schaltung heißt reversibel, wenn sie eine Permutation des  $\mathbb{F}_2^n$  ist, die aus reversiblen Gattern aufgebaut ist.

# Universelle Menge rev. Gatter

**Definition:** Eine Schaltung heißt reversibel, wenn sie eine Permutation des  $\mathbb{F}_2^n$  ist, die aus reversiblen Gattern aufgebaut ist.

**Definition:** Ein Menge R von reversiblen Gattern heißt universell, wenn jede reversible Schaltung mit Gattern aus R und Konstanten, konstruiert werden kann.

# Bsp. für ein univ. rev. Gatter

Das Toffoli Gatter ist ein universelles reversibles Gatter:

$$T : \mathbb{F}_2^3 \rightarrow \mathbb{F}_2^3, T(x_1, x_2, x_3) \mapsto (x_1, x_2, x_1x_2 - x_3)$$

T ist die Not-Operation, falls  $x_1 = x_2 = 1$ .

# Bsp. für ein univ. rev. Gatter

Das Toffoli Gatter ist ein universelles reversibles Gatter:

$$T : \mathbb{F}_2^3 \rightarrow \mathbb{F}_2^3, T(x_1, x_2, x_3) \mapsto (x_1, x_2, x_1x_2 - x_3)$$

T ist die Not-Operation, falls  $x_1 = x_2 = 1$ .

$$(0, 0, 0) \mapsto (0, 0, 0) \qquad (0, 0, 1) \mapsto (0, 0, 1)$$

$$(0, 1, 0) \mapsto (0, 1, 0) \qquad (0, 1, 1) \mapsto (0, 1, 1)$$

$$(1, 0, 0) \mapsto (1, 0, 0) \qquad (1, 0, 1) \mapsto (1, 0, 1)$$

$$(1, 1, 0) \mapsto (1, 1, 1) \qquad (1, 1, 1) \mapsto (1, 1, 0)$$

# Bsp. für ein univ. rev. Gatter

- Not:  $T(1, 1, x_1) = (1, 1, \text{not } x_1)$
- And:  $T(x_1, x_2, 0) = (x_1, x_2, x_1 \text{ and } x_2)$
- Or:  $x_1 \text{ or } x_2 = \text{not} (\text{not } x_1 \text{ and } \text{not } x_2)$
- CNot:  $T(1, x_1, x_2) = (1, x_1, x_1 - x_2)$

# Bsp. für ein univ. rev. Gatter

- Not:  $T(1, 1, x_1) = (1, 1, \text{not } x_1)$
- And:  $T(x_1, x_2, 0) = (x_1, x_2, x_1 \text{ and } x_2)$
- Or:  $x_1 \text{ or } x_2 = \text{not} (\text{not } x_1 \text{ and } \text{not } x_2)$
- CNot:  $T(1, x_1, x_2) = (1, x_1, x_1 - x_2)$

Schon mit and, or, not lassen sich alle (i.A. irreversiblen) Funktionen  $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$  berechnen. Dann lassen sich mit dem Toffoli Gatter alle reversiblen Funktionen  $\mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  berechnen. Das Toffoli Gatter ist ein universelles reversibles Gatter.

# Zusang rev. Schaltungen und QC

Da reversible Operationen unitär sind und durch reversible Operationen alle booleschen-Funktionen berechnet werden können, lassen sich mit Quantencomputern ebenfalls alle booleschen Funktionen berechnen.



# Universelle Quanten-Gatter-Menge

Ganz ähnlich möchte man unitäre Operationen auf Qubits mit wenigen Quanten-Gattern konstruieren:

**Definition:** Eine Menge von Quanten-Logik-Gattern wird als Universelle Gatter-Menge bezeichnet (universal set of gates), wenn sich mit ihr alle unitären  $n$ -Qubit Operationen, mit endlich vielen Gattern aus der Menge, simulieren lassen.

# Unendliche universelle Gatter-Menge

Eine unendliche universelle Gatter-Menge (infinite universal set of gates) besteht aus:

- Hadamard Gatter  $H$
- allen Phase-Shift Gattern  $\phi$  mit  $\phi \in [0, 2\pi]$
- C-Not Gatter

Jede  $n$ -Qubit unitäre Operation lässt sich dann mit  $O(4^n n)$  solchen Gattern simulieren.

# Endliche universelle Gatter-Mengen

Jedes Gatter, welches ein Qubit-Paar entanglen kann lässt sich verwenden:

- Hadamard
- Controlled-V

Diese beiden Gatter bilden eine endliche universelle Gatter-Menge (finite universal set of gates).

# Endliche universelle Gatter-Mengen

Quanten-Netzwerke, die nur aus einer endlichen Anzahl von Hadamard (H) und controlled-V (c-V) Gattern bestehen, können jede unitäre Transformation von Qubits approximieren:

# Endliche universelle Gatter-Mengen

Quanten-Netzwerke, die nur aus einer endlichen Anzahl von Hadamard (H) und controlled-V (c-V) Gattern bestehen, können jede unitäre Transformation von Qubits approximieren:

Ist  $U$  ein 2-Qubit Gatter und  $\epsilon > 0$ , dann gibt es ein Quanten-Netzwerk der Größe  $O(\log^d(\frac{1}{\epsilon}))$  ( $d$  eine Konstante), welches nur aus H und c-V Gattern besteht und eine unitäre Transformation  $U'$  berechnet, die nur  $\epsilon$  von  $U$  abweicht.

# Abstand von $U$ und $U'$

$U$  hat den Abstand  $\epsilon$  von  $U'$ , wenn es ein  $\lambda \in \mathbb{C}$ ,  $\|\lambda\| = 1$  gibt, so dass  $\|U - \lambda U'\| \leq \epsilon$ .

# Abstand von $U$ und $U'$

$U$  hat den Abstand  $\epsilon$  von  $U'$ , wenn es ein  $\lambda \in \mathbb{C}$ ,  $\|\lambda\| = 1$  gibt, so dass  $\|U - \lambda U'\| \leq \epsilon$ .

Wird nun  $U'$  statt  $U$  berechnet, dann approximiert der Endzustand  $\sum_x a'_x |x\rangle$  den Endzustand  $\sum_x a_x |x\rangle$  des ursprünglichen Netzwerks:

$$\sqrt{\sum_{x \in \{0,1\}^n} |\lambda a'_x - a_x|^2} \leq \epsilon$$

Die Wahrscheinlichkeit eines Ergebnisses ändert sich höchstens um  $\epsilon$ .

# Schlussbemerkungen

- ein Quanten-Computer ist ein Quanten-Netzwerk oder eine Familie von Quanten-Netzwerken
- eine Quanten-Berechnung (quantum computation) ist eine unitäre Entwicklung (unitary evolution) des Netzwerkes, die einen Eingabe-Zustand in einen Ausgabe-Zustand überführt



- 
- 
- 

# Zusammenfassung

# Zusammenfassung

- Reversible Operationen

# Zusammenfassung

- Reversible Operationen
- universelle Mengen von reversiblen Gattern

# Zusammenfassung

- Reversible Operationen
- universelle Mengen von reversiblen Gattern
- Quanten-Computer können mind. alle mgl. booleschen Funktionen berechnen

# Zusammenfassung

- Reversible Operationen
- universelle Mengen von reversiblen Gattern
- Quanten-Computer können mind. alle mgl. booleschen Funktionen berechnen
- es gibt eine endliche universelle Menge von Quanten-Gattern, die alle unitären Operationen approximieren kann

# Quellen

- Eckert, Hayden, Inamori: Basic concepts in quantum computation
- Hirvensalo: Quantum Computing