

Quantencomputer: Einführung

Martin Lange

Institut für Informatik

Ludwig-Maximilians-Universität München

Einleitung

Geschichte

Computer sind physikalische Geräte, unterliegen den Gesetzen der Physik

Geschichte

Computer sind physikalische Geräte, unterliegen den Gesetzen der Physik

was sind die Gesetze der Physik?

Geschichte

Computer sind physikalische Geräte, unterliegen den Gesetzen der Physik

was sind die Gesetze der Physik?

klassische Physik ist nicht widerspruchsfrei

Geschichte

Computer sind physikalische Geräte, unterliegen den Gesetzen der Physik

was sind die Gesetze der Physik?

klassische Physik ist **nicht widerspruchsfrei**

Anfang des 20. Jh.: Quantenmechanik

Geschichte

Computer sind physikalische Geräte, unterliegen den Gesetzen der Physik

was sind die Gesetze der Physik?

klassische Physik ist **nicht widerspruchsfrei**

Anfang des 20. Jh.: Quantenmechanik

Vorteil: beschreibt die Welt besser als klassische Physik

Geschichte

Computer sind physikalische Geräte, unterliegen den Gesetzen der Physik

was sind die Gesetze der Physik?

klassische Physik ist **nicht widerspruchsfrei**

Anfang des 20. Jh.: **Quantenmechanik**

Vorteil: beschreibt die Welt besser als klassische Physik

Nachteil: nicht sonderlich intuitiv

Die Church-Turing-These

allgemein akzeptiert in der Informatik:

Die Church-Turing-These

allgemein akzeptiert in der Informatik:

Jeder Algorithmus kann als (probabilistische)
Turing-Maschine dargestellt werden.

Die Church-Turing-These

allgemein akzeptiert in der Informatik:

Jeder Algorithmus kann als (probabilistische)
Turing-Maschine dargestellt werden.

wichtiger Aspekt des Modells Turing-Maschine:

Die Church-Turing-These

allgemein akzeptiert in der Informatik:

Jeder Algorithmus kann als (probabilistische)
Turing-Maschine dargestellt werden.

wichtiger Aspekt des Modells Turing-Maschine:

Satz: Es gibt eine universelle Turing-Maschine.

Die Church-Turing-These

allgemein akzeptiert in der Informatik:

Jeder Algorithmus kann als (probabilistische)
Turing-Maschine dargestellt werden.

wichtiger Aspekt des Modells Turing-Maschine:

Satz: Es gibt eine **universelle Turing-Maschine**.

Idee wird in jedem Computer benutzt, geht auf von Neumann zurück

Deutsche Idee

Problem mit Church-Turing-These: unbeweisbar wegen Begriff
Algorithmus

Deutschs Idee

Problem mit Church-Turing-These: unbeweisbar wegen Begriff
Algorithmus

Deutsch: evtl. stärkere These beweisbar

Deutschs Idee

Problem mit Church-Turing-These: unbeweisbar wegen Begriff *Algorithmus*

Deutsch: evtl. stärkere These beweisbar

Jeder physikalische Prozess läßt sich auf Maschine X simulieren.

Deutschs Idee

Problem mit Church-Turing-These: unbeweisbar wegen Begriff *Algorithmus*

Deutsch: evtl. stärkere These beweisbar

Jeder physikalische Prozess läßt sich auf Maschine X simulieren.

Aber was ist X ?

Deutschs Idee

Problem mit Church-Turing-These: unbeweisbar wegen Begriff *Algorithmus*

Deutsch: evtl. stärkere These beweisbar

Jeder physikalische Prozess läßt sich auf Maschine X simulieren.

Aber was ist X ?

Quantencomputer, da die Welt quantenmechanisch ist

Von Interesse für die Informatik

Quantencomputer ist Berechnungsmodell

Von Interesse für die Informatik

Quantencomputer ist Berechnungsmodell

Wie verhält er sich zu anderen (z.B. TM, Schaltkreisen, Prog.-sprachen, ...) bzgl. der Berechnungsstärke?

Antwort:

Von Interesse für die Informatik

Quantencomputer ist Berechnungsmodell

Wie verhält er sich zu anderen (z.B. TM, Schaltkreisen, Prog.-sprachen, ...) bzgl. der Berechnungsstärke?

Antwort:

- mindestens so stark:
kann per Definition TM simulieren

Von Interesse für die Informatik

Quantencomputer ist Berechnungsmodell

Wie verhält er sich zu anderen (z.B. TM, Schaltkreisen, Prog.-sprachen, ...) bzgl. der Berechnungsstärke?

Antwort:

- mindestens so stark:
kann per Definition TM simulieren
- höchstens so stark:
kann auf TM simuliert werden

Das ist aber noch nicht alles ...

Aber: Simulation auf TM vermutlich **exponentiell**!

Das ist aber noch nicht alles ...

Aber: Simulation auf TM vermutlich **exponentiell**!

Quantencomputer interessant für **Komplexitätstheorie**, denn:

Das ist aber noch nicht alles ...

Aber: Simulation auf TM vermutlich **exponentiell**!

Quantencomputer interessant für Komplexitätstheorie, denn:

bekannte Komplexitätsklassen (P, NP, PSPACE, EXPTIME)
robust weil unabhängig von Maschinenmodell

Das ist aber noch nicht alles ...

Aber: Simulation auf TM vermutlich **exponentiell!**

Quantencomputer interessant für Komplexitätstheorie, denn:

bekannte Komplexitätsklassen (P, NP, PSPACE, EXPTIME)
robust weil unabhängig von Maschinenmodell

gilt das auch für Quantencomputer?

Überblick über das Seminar

- Begriffsbildung

Überblick über das Seminar

- Begriffsbildung
- der Quantencomputer als Berechnungsmodell
(Quanten-TM, -Schaltkreise, -Automaten, . . .)

Überblick über das Seminar

- Begriffsbildung
- der Quantencomputer als Berechnungsmodell
(Quanten-TM, -Schaltkreise, -Automaten, ...)
- Quanten-Komplexitätsklassen

Überblick über das Seminar

- Begriffsbildung
- der Quantencomputer als Berechnungsmodell (Quanten-TM, -Schaltkreise, -Automaten, ...)
- Quanten-Komplexitätsklassen
- Algorithmen für Quantencomputer

Überblick über das Seminar

- Begriffsbildung
- der Quantencomputer als Berechnungsmodell (Quanten-TM, -Schaltkreise, -Automaten, ...)
- Quanten-Komplexitätsklassen
- Algorithmen für Quantencomputer
- Anwendung: Kryptographie

Überblick über das Seminar

- Begriffsbildung
- der Quantencomputer als Berechnungsmodell (Quanten-TM, -Schaltkreise, -Automaten, . . .)
- Quanten-Komplexitätsklassen
- Algorithmen für Quantencomputer
- Anwendung: Kryptographie
- Programmiersprachen für Quantencomputer

Begriffsbildung

Quanten-Bits

QuBit is fundamentale Informationseinheit für Qu.-Computer

	Bit	QuBit
Zustand		
Messung liefert		
Zustand danach		

Quanten-Bits

QuBit is fundamentale Informationseinheit für Qu.-Computer

	Bit	QuBit
Zustand	$\psi \in \{0, 1\}$	
Messung liefert		
Zustand danach		

Quanten-Bits

QuBit is fundamentale Informationseinheit für Qu.-Computer

	Bit	QuBit
Zustand	$\psi \in \{0, 1\}$	$ \psi\rangle = \alpha \cdot 0\rangle + \beta \cdot 1\rangle$ mit $ \alpha ^2 + \beta ^2 = 1$
Messung liefert		
Zustand danach		

Quanten-Bits

QuBit is fundamentale Informationseinheit für Qu.-Computer

	Bit	QuBit
Zustand	$\psi \in \{0, 1\}$	$ \psi\rangle = \alpha \cdot 0\rangle + \beta \cdot 1\rangle$ mit $ \alpha ^2 + \beta ^2 = 1$
Messung liefert	ψ mit $P = 1$	
Zustand danach		

Quanten-Bits

QuBit is fundamentale Informationseinheit für Qu.-Computer

	Bit	QuBit
Zustand	$\psi \in \{0, 1\}$	$ \psi\rangle = \alpha \cdot 0\rangle + \beta \cdot 1\rangle$ mit $ \alpha ^2 + \beta ^2 = 1$
Messung liefert	ψ mit $P = 1$	$ \varphi\rangle = \begin{cases} 0\rangle & \text{mit } P = \alpha ^2 \\ 1\rangle & \text{mit } P = \beta ^2 \end{cases}$
Zustand danach		

Quanten-Bits

QuBit is fundamentale Informationseinheit für Qu.-Computer

	Bit	QuBit
Zustand	$\psi \in \{0, 1\}$	$ \psi\rangle = \alpha \cdot 0\rangle + \beta \cdot 1\rangle$ mit $ \alpha ^2 + \beta ^2 = 1$
Messung liefert	ψ mit $P = 1$	$ \varphi\rangle = \begin{cases} 0\rangle & \text{mit } P = \alpha ^2 \\ 1\rangle & \text{mit } P = \beta ^2 \end{cases}$
Zustand danach	ψ	

Quanten-Bits

QuBit is fundamentale Informationseinheit für Qu.-Computer

	Bit	QuBit
Zustand	$\psi \in \{0, 1\}$	$ \psi\rangle = \alpha \cdot 0\rangle + \beta \cdot 1\rangle$ mit $ \alpha ^2 + \beta ^2 = 1$
Messung liefert	ψ mit $P = 1$	$ \varphi\rangle = \begin{cases} 0\rangle & \text{mit } P = \alpha ^2 \\ 1\rangle & \text{mit } P = \beta ^2 \end{cases}$
Zustand danach	ψ	$ \varphi\rangle$

Operationen auf QuBits ...

... sind immer linear,

Operationen auf QuBits ...

... sind immer linear, d.h. beschrieben durch Matrix

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}$$

Operationen auf QuBits ...

... sind immer linear, d.h. beschrieben durch Matrix

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}$$

Sei $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$:

$$A|\psi\rangle =$$

Operationen auf QuBits ...

... sind immer linear, d.h. beschrieben durch Matrix

$$A = \begin{bmatrix} a_{00} & a_{01} \\ a_{10} & a_{11} \end{bmatrix}$$

Sei $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$:

$$A|\psi\rangle = (a_{00} \cdot \alpha + a_{01} \cdot \beta) \cdot |0\rangle + (a_{10} \cdot \alpha + a_{11} \cdot \beta) \cdot |1\rangle$$

Welche Operationen sind zugelassen?

nur *unitäre*,

Welche Operationen sind zugelassen?

nur *unitäre*, d.h. beschrieben durch Matrix A , wobei

$$A^\dagger A = I$$

mit

Welche Operationen sind zugelassen?

nur *unitäre*, d.h. beschrieben durch Matrix A , wobei

$$A^\dagger A = I$$

mit

- I ist 2×2 -Einheitsmatrix

Welche Operationen sind zugelassen?

nur *unitäre*, d.h. beschrieben durch Matrix A , wobei

$$A^\dagger A = I$$

mit

- I ist 2×2 -Einheitsmatrix
- $A^\dagger = (A^*)^T$

Welche Operationen sind zugelassen?

nur *unitäre*, d.h. beschrieben durch Matrix A , wobei

$$A^\dagger A = I$$

mit

- I ist 2×2 -Einheitsmatrix
- $A^\dagger = (A^*)^T$
- A^* ist A mit Einträgen komplex-konjugiert

Welche Operationen sind zugelassen?

nur *unitäre*, d.h. beschrieben durch Matrix A , wobei

$$A^\dagger A = I$$

mit

- I ist 2×2 -Einheitsmatrix
- $A^\dagger = (A^*)^T$
- A^* ist A mit Einträgen komplex-konjugiert
- A^T ist A transponiert

Welche Operationen sind zugelassen?

nur *unitäre*, d.h. beschrieben durch Matrix A , wobei

$$A^\dagger A = I$$

mit

- I ist 2×2 -Einheitsmatrix
- $A^\dagger = (A^*)^T$
- A^* ist A mit Einträgen komplex-konjugiert
- A^T ist A transponiert

Aber auch: jede unitäre Operation ist zulässig!

Lineare Algebra

Vektorraum der Dimension n

$|\psi\rangle$ $n \times 1$ -Vektor

Lineare Algebra

Vektorraum der Dimension n

$|\psi\rangle$ $n \times 1$ -Vektor

$\langle\psi|$ $1 \times n$ -Vektor mit komplex-konjugierten Einträgen

Lineare Algebra

Vektorraum der Dimension n

$|\psi\rangle$ $n \times 1$ -Vektor

$\langle\psi|$ $1 \times n$ -Vektor mit komplex-konjugierten Einträgen

$\langle\varphi|\psi\rangle$ inneres Produkt = Skalarprodukt $\langle\varphi| \cdot |\psi\rangle$

Lineare Algebra

Vektorraum der Dimension n

$|\psi\rangle$ $n \times 1$ -Vektor

$\langle\psi|$ $1 \times n$ -Vektor mit komplex-konjugierten Einträgen

$\langle\varphi|\psi\rangle$ inneres Produkt = Skalarprodukt $\langle\varphi| \cdot |\psi\rangle$

$|\varphi\rangle\langle\psi|$ äußeres Produkt, $n \times n$ -Matrix

Lineare Algebra

Vektorraum der Dimension n

$|\psi\rangle$ $n \times 1$ -Vektor

$\langle\psi|$ $1 \times n$ -Vektor mit komplex-konjugierten Einträgen

$\langle\varphi|\psi\rangle$ inneres Produkt = Skalarprodukt $\langle\varphi| \cdot |\psi\rangle$

$|\varphi\rangle\langle\psi|$ äußeres Produkt, $n \times n$ -Matrix

$A \otimes B$ Tensorprodukt

Tensorprodukt

$$A = \begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nm} \end{bmatrix} \quad B = \begin{bmatrix} b_{11} & \dots & b_{1p} \\ \vdots & & \vdots \\ b_{k1} & \dots & b_{kp} \end{bmatrix}$$

Tensorprodukt

$$A = \begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nm} \end{bmatrix}$$

$$B = \begin{bmatrix} b_{11} & \dots & b_{1p} \\ \vdots & & \vdots \\ b_{k1} & \dots & b_{kp} \end{bmatrix}$$

$$aB = \begin{bmatrix} ab_{11} & \dots & ab_{1p} \\ \vdots & & \vdots \\ ab_{k1} & \dots & ab_{kp} \end{bmatrix}$$

Tensorprodukt

$$A = \begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{nm} \end{bmatrix} \quad B = \begin{bmatrix} b_{11} & \dots & b_{1p} \\ \vdots & & \vdots \\ b_{k1} & \dots & b_{kp} \end{bmatrix}$$

$$aB = \begin{bmatrix} ab_{11} & \dots & ab_{1p} \\ \vdots & & \vdots \\ ab_{k1} & \dots & ab_{kp} \end{bmatrix} \quad A \otimes B = \begin{bmatrix} a_{11}B & \dots & a_{1m}B \\ \vdots & & \vdots \\ a_{n1}B & \dots & a_{nm}B \end{bmatrix}$$

2 QuBits

geg. 2 QuBits in Zuständen

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \quad \text{und} \quad |\varphi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

2 QuBits

geg. 2 QuBits in Zuständen

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \quad \text{und} \quad |\varphi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

Tensorprodukt zum Zusammenbauen größerer Systeme

2 QuBits

geg. 2 QuBits in Zuständen

$$|\psi\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle \quad \text{und} \quad |\varphi\rangle = \beta_0|0\rangle + \beta_1|1\rangle$$

Tensorprodukt zum Zusammenbauen größerer Systeme

Zustand eines 2-QuBit-System beschrieben durch

$$|\psi\rangle \otimes |\varphi\rangle = \sum_{i,j \in \{0,1\}} \alpha_i \beta_j \cdot |ij\rangle$$

Operationen auf 2-QuBit-Systemen

unitäre Matrizen der Form

$$A = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$$

Operationen auf 2-QuBit-Systemen

unitäre Matrizen der Form

$$A = \begin{bmatrix} a_{00} & a_{01} & a_{02} & a_{03} \\ a_{10} & a_{11} & a_{12} & a_{13} \\ a_{20} & a_{21} & a_{22} & a_{23} \\ a_{30} & a_{31} & a_{32} & a_{33} \end{bmatrix}$$

usw. für n -QuBit-Systeme

Quantenmechanik ist nicht intuitiv

Bsp.: beliebiges 2-Bit-System, Zustand $\psi = (b_0, b_1)$

Quantenmechanik ist nicht intuitiv

Bsp.: beliebiges 2-Bit-System, Zustand $\psi = (b_0, b_1)$

messe b_0 , dann b_1 ; Ergebnisse unabhängig voneinander

Quantenmechanik ist nicht intuitiv

Bsp.: beliebiges 2-Bit-System, Zustand $\psi = (b_0, b_1)$

messe b_0 , dann b_1 ; Ergebnisse unabhängig voneinander

aber: 2-QuBit-System in *Bell*-Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Quantenmechanik ist nicht intuitiv

Bsp.: beliebiges 2-Bit-System, Zustand $\psi = (b_0, b_1)$

messe b_0 , dann b_1 ; Ergebnisse unabhängig voneinander

aber: 2-QuBit-System in *Bell*-Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Messung von 1. QuBit liefert mit Wahrscheinlichkeit $\frac{1}{2}$ jeweils

Quantenmechanik ist nicht intuitiv

Bsp.: beliebiges 2-Bit-System, Zustand $\psi = (b_0, b_1)$

messe b_0 , dann b_1 ; Ergebnisse unabhängig voneinander

aber: 2-QuBit-System in *Bell*-Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Messung von 1. QuBit liefert mit Wahrscheinlichkeit $\frac{1}{2}$ jeweils

- $|0\rangle$ und Folgezustand $|\psi'\rangle = |00\rangle$

Quantenmechanik ist nicht intuitiv

Bsp.: beliebiges 2-Bit-System, Zustand $\psi = (b_0, b_1)$

messe b_0 , dann b_1 ; Ergebnisse unabhängig voneinander

aber: 2-QuBit-System in *Bell*-Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Messung von 1. QuBit liefert mit Wahrscheinlichkeit $\frac{1}{2}$ jeweils

- $|0\rangle$ und Folgezustand $|\psi'\rangle = |00\rangle$
- $|1\rangle$ und Folgezustand $|\psi'\rangle = |11\rangle$

Quantenmechanik ist nicht intuitiv

Bsp.: beliebiges 2-Bit-System, Zustand $\psi = (b_0, b_1)$

messe b_0 , dann b_1 ; Ergebnisse unabhängig voneinander

aber: 2-QuBit-System in *Bell*-Zustand

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

Messung von 1. QuBit liefert mit Wahrscheinlichkeit $\frac{1}{2}$ jeweils

- $|0\rangle$ und Folgezustand $|\psi'\rangle = |00\rangle$
- $|1\rangle$ und Folgezustand $|\psi'\rangle = |11\rangle$

Messung von 2. QuBit liefert danach Wert des 1.!

Schaltelemente

Lemma: Sei A unitär. Dann ist $A^\dagger$ unitär.

Schaltelemente

Lemma: Sei A unitär. Dann ist $A^\dagger$ unitär.

Folgerung:

- Operationen auf QuBits sind reversible
- Schaltelemente haben gleiche Anzahl von Ein- und Ausgängen

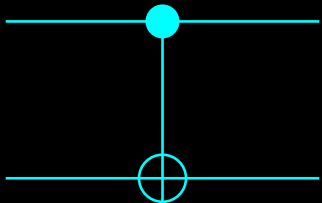
Schaltelemente

Lemma: Sei A unitär. Dann ist $A^\dagger$ unitär.

Folgerung:

- Operationen auf QuBits sind reversible
- Schaltelemente haben gleiche Anzahl von Ein- und Ausgängen

z.B. CONTROLLED-NOT



oder

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

Schaltkreise ...

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

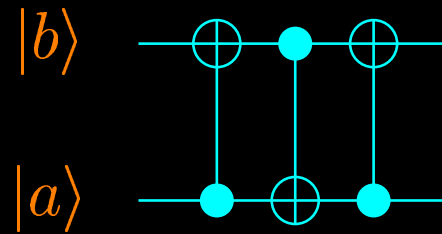
Schaltelemente können aber sequentiell verbunden werden

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:

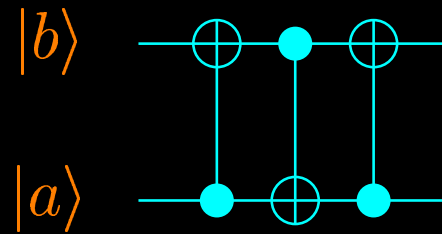


Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

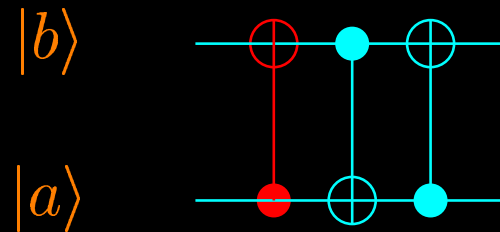
$|a\rangle, |b\rangle$

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

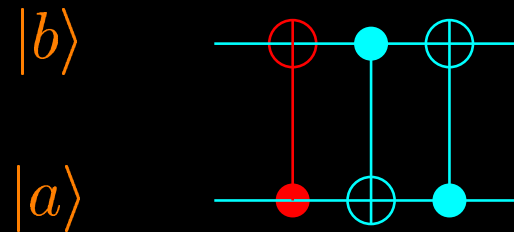
$|a\rangle, |b\rangle$

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

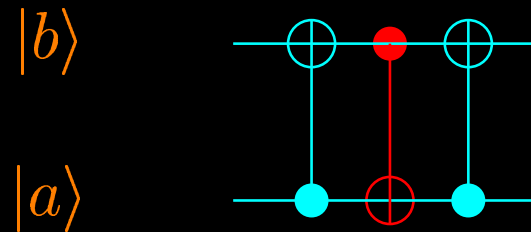
$$|a\rangle, |b\rangle \rightarrow |a\rangle, |a \oplus b\rangle$$

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

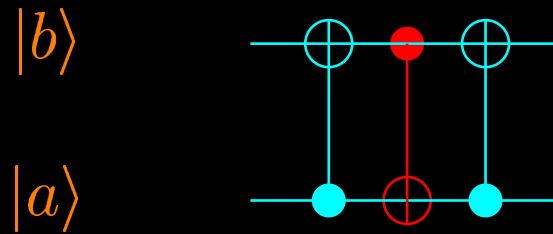
$$|a\rangle, |b\rangle \rightarrow |a\rangle, |a \oplus b\rangle$$

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

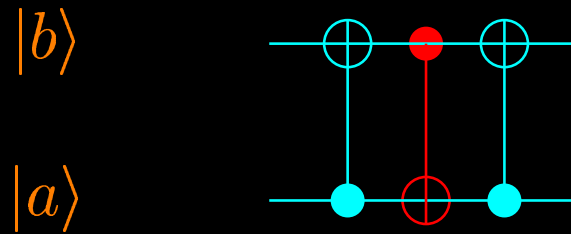
$$|a\rangle, |b\rangle \rightarrow |a\rangle, |a \oplus b\rangle \rightarrow |a \oplus (a \oplus b)\rangle, |a \oplus b\rangle$$

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

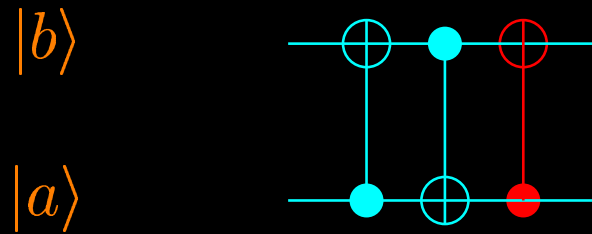
$$|a\rangle, |b\rangle \rightarrow |a\rangle, |a \oplus b\rangle \rightarrow |a \oplus (a \oplus b)\rangle, |a \oplus b\rangle = |b\rangle, |a \oplus b\rangle$$

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

$$|a\rangle, |b\rangle \rightarrow |a\rangle, |a \oplus b\rangle \rightarrow |a \oplus (a \oplus b)\rangle, |a \oplus b\rangle = |b\rangle, |a \oplus b\rangle$$

Schaltkreise ...

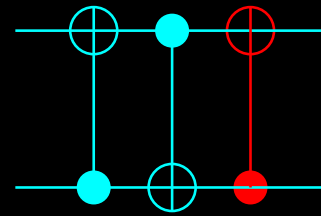
... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:

$|b\rangle$

$|a\rangle$



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

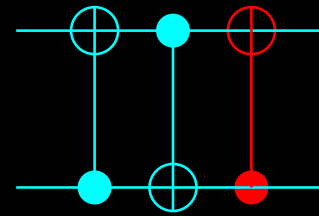
$$\begin{aligned} |a\rangle, |b\rangle &\rightarrow |a\rangle, |a \oplus b\rangle \rightarrow |a \oplus (a \oplus b)\rangle, |a \oplus b\rangle = |b\rangle, |a \oplus b\rangle \\ &\rightarrow |b\rangle, |b \oplus (a \oplus b)\rangle \end{aligned}$$

Schaltkreise ...

... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:

 $|b\rangle$ $|a\rangle$ 

betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

$$\begin{aligned} |a\rangle, |b\rangle &\rightarrow |a\rangle, |a \oplus b\rangle \rightarrow |a \oplus (a \oplus b)\rangle, |a \oplus b\rangle = |b\rangle, |a \oplus b\rangle \\ &\rightarrow |b\rangle, |b \oplus (a \oplus b)\rangle = |b\rangle, |a\rangle \end{aligned}$$

Schaltkreise ...

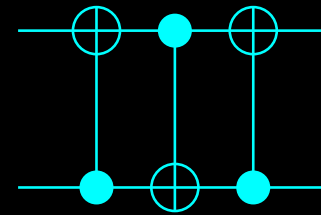
... gibt es nicht, denn Rückwärtskanten sind verboten
ebenfalls kein FAN-IN oder FAN-OUT

Schaltelemente können aber sequentiell verbunden werden

z.B. QuBit-Vertauscher:

$|b\rangle$

$|a\rangle$



betrachte Aktion auf $|0\rangle$ und $|1\rangle$:

$$\begin{aligned} |a\rangle, |b\rangle &\rightarrow |a\rangle, |a \oplus b\rangle \rightarrow |a \oplus (a \oplus b)\rangle, |a \oplus b\rangle = |b\rangle, |a \oplus b\rangle \\ &\rightarrow |b\rangle, |b \oplus (a \oplus b)\rangle = |b\rangle, |a\rangle \end{aligned}$$

Messen

Ergebnisse nicht einfach an beliebiger Stelle auslesen

Messen beeinflusst Zustand des Systems

Messen

Ergebnisse nicht einfach an beliebiger Stelle auslesen

Messen beeinflusst Zustand des Systems

Messapparat ist ebenfalls physikalisches System

Messen

Ergebnisse nicht einfach an beliebiger Stelle auslesen

Messen beeinflusst Zustand des Systems

Messapparat ist ebenfalls physikalisches System

Sei m mögliches Resultat einer Messung

Messen

Ergebnisse nicht einfach an beliebiger Stelle auslesen

Messen beeinflusst Zustand des Systems

Messapparat ist ebenfalls physikalisches System

Sei m mögliches Resultat einer Messung

Messung geg. durch unitären Operator M_m , d.h.

Messung ist $M_m|\psi\rangle$

Quantencomputer arbeiten anders

die Gesetze des Quantumcomputing lassen sich als **Postulate** formulieren

Quantencomputer arbeiten anders

die Gesetze des Quantumcomputing lassen sich als **Postulate** formulieren

1. Postulat: (Zustandsraum)

Zu jedem isolierten, physikalischen System gehört ein Hilbertraum (= komplexer Vektorraum mit innerem Produkt). Der Zustand des Systems wird beschrieben durch einen Vektor der Einheitslänge in diesem Raum.

2. Postulat: (Evolution)

Die Evolution eines isolierten Systems vom Zeitpunkt t zu t' wird durch einen unitären Operator U in dem zug. Hilbertraum beschrieben.

$$|\psi_{t'}\rangle = U|\psi_t\rangle$$

3. Postulat: (Messung)

Messungen sind gegeben durch eine Reihe $\{M_m\}$ von unitären Messoperatoren. Für diese gilt:

3. Postulat: (Messung)

Messungen sind gegeben durch eine Reihe $\{M_m\}$ von unitären Messoperatoren. Für diese gilt:

- m wird in $|\psi\rangle$ gemessen mit Wahrscheinlichkeit

$$P(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

3. Postulat: (Messung)

Messungen sind gegeben durch eine Reihe $\{M_m\}$ von unitären Messoperatoren. Für diese gilt:

- m wird in $|\psi\rangle$ gemessen mit Wahrscheinlichkeit

$$P(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

- der Zustand nach dieser Messung ist

$$|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$$

3. Postulat: (Messung)

Messungen sind gegeben durch eine Reihe $\{M_m\}$ von unitären Messoperatoren. Für diese gilt:

- m wird in $|\psi\rangle$ gemessen mit Wahrscheinlichkeit

$$P(m) = \langle \psi | M_m^\dagger M_m | \psi \rangle$$

- der Zustand nach dieser Messung ist

$$|\psi'\rangle = \frac{M_m |\psi\rangle}{\sqrt{\langle \psi | M_m^\dagger M_m | \psi \rangle}}$$

- die Wahrscheinlichkeiten addieren sich zu 1

$$\sum_m M_m^\dagger M_m = I$$

4. Postulat: (Zusammengesetzte Systems)

Der Zustandsraum eines zusammengesetzten Systems ist das Tensorprodukt der Zustandsräume seiner Komponenten. D.h. sind Komponenten in Zuständen $|\psi_0\rangle, \dots, |\psi_n\rangle$, dann ist das Gesamtsystem im Zustand

$$|\psi_0\rangle \otimes \dots \otimes |\psi_n\rangle$$

The End