

## Heutige (klassische) Computer:

Quantentheorie als theoretisches Werkzeug beim Bau solcher Rechner:

- Z. B. benötigt, um Halbleiter zu verstehen.
- Zunehmend wichtig bei fortschreitender Miniaturisierung.

## Hier:

Benutze quantentheoretische Effekte, d. h. Effekte, die sich nicht (richtig) mit klassischer Physik beschreiben lassen, um neuartige Algorithmen zu entwerfen.

Modelle: [Feynman \(1981\)](#), [Deutsch \(1985\)](#).

## Wesentliche Motivation:

Zwei berühmte Algorithmen für Quantencomputer:

- **Shor (1994):**

Polynomialzeitalgorithmus für Faktorisierung von ganzen Zahlen.

Klassisch: ??? – Vermutung: expo. Zeit benötigt.

- **Grover (1994):**

Lösungen von Suchproblemen über  $\{0, 1\}^n$  in Zeit  $O(2^{n/2})$ .

Blackbox für  $f: \{0, 1\}^n \rightarrow \{0, 1\}$  gegeben,

finde  $x \in \{0, 1\}^n$  mit  $f(x) = 1$ .

Klassisch: Randomisierter Blackbox-Algorithmus braucht  $\Omega(2^n)$  Anfragen.

## Praktische Bedeutung:

Kann man denn Quantencomputer bauen?

- Keine grundsätzlichen theoretischen Hindernisse bekannt.
- Prototypen bereits experimentell realisiert.
- Skalierbarkeit extremes (ingenieurmäßiges) Problem.

## Wenn man hinreichend „großen“ Quantencomputer hat:

Faktorisierung → Brechen von RSA.

Aber auch viele „positive“ Anwendungen, z. B.  
quadratische Beschleunigung von Suchheuristiken.

## Quantenkryptographie:

Beweisbar sicherer Austausch von Schlüsseln.

## Übersicht:

- 1 Was ist ein Quantencomputer?
- 2 Der Deutsch-Jozsa-Algorithmus
- 3 Ideen zu Shors Algorithmus

# 1. Was ist ein Quantencomputer?

Bauteile analog zu klassischem Computer:

- Speicher, Inhalt Qubits statt Bits.
- Transformation des Speicherinhalts mit geeignetem Quantenschaltkreis.
- Quantenschaltkreis aufgebaut aus (elementaren) Quantenbausteinen („Gatter“).

Quantenschaltkreise einfacher als algorithmisches Modell zu beschreiben (und Standard in der Literatur).

## Qubits:

Zustände eines „klassischen“ Bits: 0, 1.

### Zustände eines Qubits:

- *Basiszustände*:  $e_0 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ ,  $e_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ .

- Allgemeiner Zustand:

$$s = \alpha_0 \cdot e_0 + \alpha_1 \cdot e_1 = \begin{bmatrix} \alpha_0 \\ \alpha_1 \end{bmatrix};$$

$$\alpha_0, \alpha_1 \in \mathbb{C} \text{ mit } |\alpha_0|^2 + |\alpha_1|^2 = 1.$$

### Jargon:

- $\alpha_0, \alpha_1$  *Amplituden*;
- $\alpha_0 \cdot e_0 + \alpha_1 \cdot e_1$  *Überlagerung, Superposition*.

## Messung eines Qubits im Zustand $s = \alpha_0 e_0 + \alpha_1 e_1$ :

Ergebnis „0“ mit Wahrscheinlichkeit  $|\alpha_0|^2$ ;

Ergebnis „1“ mit Wahrscheinlichkeit  $|\alpha_1|^2$ .

Danach Qubit im Zustand  $e_0$  bzw.  $e_1$ .

## Beispiele:

- $s = \frac{1}{\sqrt{2}}(e_0 + e_1) = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$ :

Wskt. für „0“ = Wskt. für „1“ =  $|1/\sqrt{2}|^2 = 1/2$ .

Wie klassisches Zufallsbit.

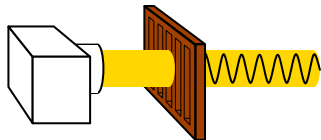
- $s = \frac{i}{\sqrt{3}}e_0 + \sqrt{\frac{2}{3}}e_1$ :

Wskt. für „0“ =  $|i/\sqrt{3}|^2 = 1/3$ ;

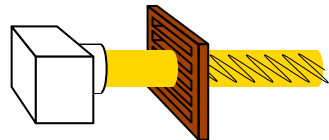
Wskt. für „1“ =  $|\sqrt{2/3}|^2 = 2/3$ .

## Beispiel für Physikalische Realisierung:

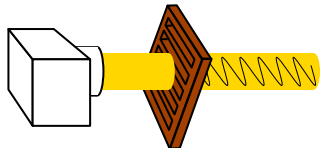
**Polarisation von Licht:**



vertikal



horizontal



45°

**Einzelnes Photon:**

Zustand  $e_0$

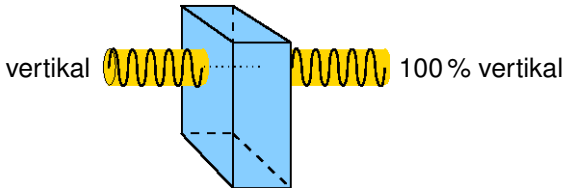
Zustand  $e_1$

Zustand  $\frac{1}{\sqrt{2}}(e_0 + e_1)$

## Physikalische Realisierung (Forts.):

### Messung der Polarisation von Licht:

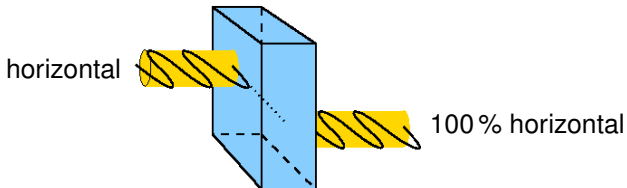
Kalkspalkristall lenkt Lichtstrahlen je nach ihrer Polarisation ab.



## Physikalische Realisierung (Forts.):

### Messung der Polarisation von Licht:

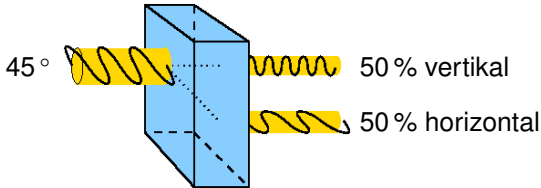
Kalkspalkristall lenkt Lichtstrahlen je nach ihrer Polarisation ab.



## Physikalische Realisierung (Forts.):

### Messung der Polarisation von Licht:

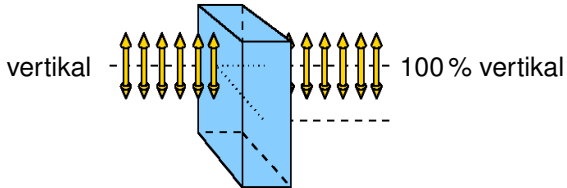
Kalkspalkristall lenkt Lichtstrahlen je nach ihrer Polarisation ab.



## Physikalische Realisierung (Forts.):

### Messung der Polarisation von Photonen:

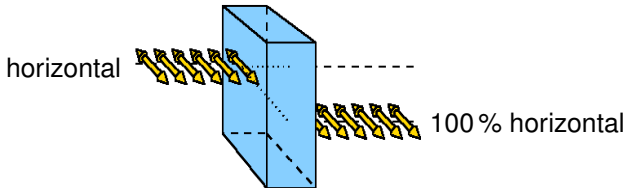
Intensität der Lichtstrahlen  $\rightarrow$  Wahrscheinlichkeiten



## Physikalische Realisierung (Forts.):

### Messung der Polarisation von Photonen:

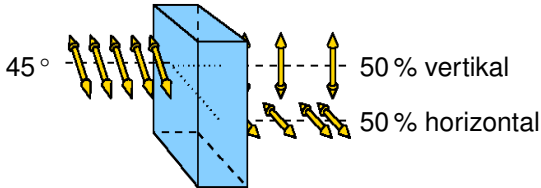
Intensität der Lichtstrahlen  $\rightarrow$  Wahrscheinlichkeiten



## Physikalische Realisierung (Forts.):

### Messung der Polarisation von Photonen:

Intensität der Lichtstrahlen  $\rightarrow$  Wahrscheinlichkeiten



## Qubit-Register mit $n$ Qubits:

Entsprechend Registern aus  $n$  Speicherzellen in klassischem Computer. Dort Zustände  $\{0, 1\}^n$ .

### Zustände für $n$ Qubits:

- Basiszustände:  $e_x, x \in \{0, 1\}^n$ .
- Allgemeiner Zustand:

$$\sum_{x \in \{0, 1\}^n} \alpha_x e_x, \quad \sum_{x \in \{0, 1\}^n} |\alpha_x|^2 = 1.$$

**Beachte:** Vektorraum ist  $\mathbb{C}^{2^n}$ , nicht  $\mathbb{C}^{2n}$ !

Messungen analog zu einzelner Qubit.

## Zustandstransformationen:

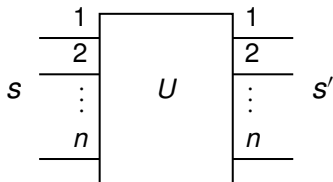
Wie können wir Inhalt eines  $n$ -Qubit-Registers verändern?

- Quantentheorie erlaubt nur *lineare* Abbildungen, hier  $U: \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$ .
- Zusätzlich: Summe der Quadrate der Amplitudenbeträge der Bildvektoren muss wieder 1 sein.

Entsprechende Abbildung heißen *unitäre Abbildungen* ( $\rightarrow$  lineare Algebra).

Identifiziere unitäre Abbildung  $U: \mathbb{C}^{2^n} \rightarrow \mathbb{C}^{2^n}$   
hier auch mit  *$n$ -Qubit-Baustein*.

## Symbolische Darstellung für $n$ -Qubit-Baustein:



Analog zu klassischen Schaltkreisbausteinen:

An linke „Eingangsleitungen“ Zustand  $s$  anlegen,  
dann kommt auf „Ausgangsleitungen“ rechts  $s'$  heraus.

(Vorstellung hat Tücken, denn evtl. Zustand nicht in  
Zustände für einzelne Leitungen zerlegbar!)

## Beispiel: Der Hadamard-Baustein

$$\text{---} \boxed{H} \text{---} \quad H := \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

Auf Basisvektoren angewendet:

$$He_0 = \frac{1}{\sqrt{2}}(e_0 + e_1), \quad He_1 = \frac{1}{\sqrt{2}}(e_0 - e_1).$$

Messung liefert beides Mal 0/1 je mit Wskt. 1/2.  
Nachbildung von klassischem fairem Münzwurf.

Zwei  $H$ -Bausteine hintereinanderschalten, auf  $e_0$  anwenden:

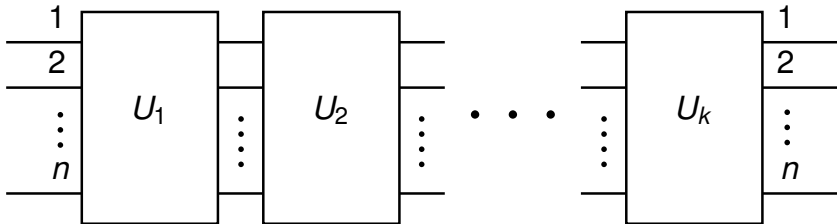
$$H(He_0) = e_0.$$

Exakte Rückgewinnung des Ursprungszustandes  
aus Zufallsbit („unscrambling eggs“)!

Allgemein gilt:  $\boxed{H^{-1} = H}$ .

## Quantenschaltkreise:

Allgemein folgendes Aussehen:



Dabei müssen  $U_1, \dots, U_k$  unitäre Abbildungen bzw. legale  $n$ -Qubit-Bausteine sein.

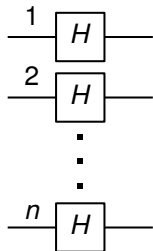
**Semantik:**  $U = U_k \cdot \dots \cdot U_1$  (unitär).

**Rechenzeit:**

Anzahl der auszuwertenden Bausteine, also hier  $k$ .

## Quantenparallelismus:

Will  $n$  Münzwürfe mit Hadamard-Bausteinen durchführen.  
Kann das parallel machen, so:



Was berechnet der Schaltkreis auf klassischem  
Startzustand  $00 \dots 0$ , d. h. eigentlich  $e_{00\dots 0}$ ?

Was Schaltkreis auf  $e_{00\dots 0}$  berechnet:

- $He_0 = \frac{1}{\sqrt{2}}(e_0 + e_1)$ .
- Auf jeder Ausgangsleitung *unabhängig* klassische Zustände 0, 1 jeweils mit Amplitude  $1/\sqrt{2}$ .

Alle klassischen Zustände aus  $\{0, 1\}^n$  kommen vor, jeder mit *Produkt* der Einzelamplituden:

$$\underbrace{\frac{1}{\sqrt{2}} \cdots \frac{1}{\sqrt{2}}}_{n\text{-mal}} = \frac{1}{2^{n/2}}.$$

Damit:

$$e_{00\dots 0} \mapsto \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} e_x.$$

## Parallele Funktionsauswertung:

Funktion  $f: \{0, 1\}^n \rightarrow \{0, 1\}$ , dafür

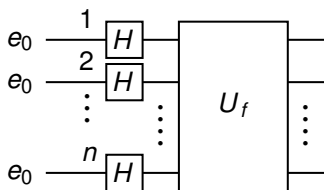
*Quanten-Blackbox-Baustein* gegeben:

Dieser berechnet (unitäre) Abbildung  $U_f$ : Für  $x \in \{0, 1\}^n$ :

$$e_x \mapsto U_f e_x = (-1)^{f(x)} e_x.$$

## Parallele Funktionsauswertung (Forts.):

Schaltkreis:



Was macht der Schaltkreis:

$$e_{00\dots 0} \mapsto \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} e_x$$

$$\mapsto \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} e_x.$$

Nutze aus, dass Bausteine lineare Abbildungen berechnen.

## Parallele Funktionsauswertung (Forts.):

Endergebnis ist Zustand

$$s = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} e_x.$$

- Enthält alle  $2^n$  Funktionswerte  $f(x)$ ,  $x \in \{0, 1\}^n$ .
- Nur *eine* Auswertung der Blackbox, 1 Schritt.

## Parallele Funktionsauswertung (Forts.):

Endergebnis ist Zustand

$$s = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} e_x.$$

- Enthält alle  $2^n$  Funktionswerte  $f(x)$ ,  $x \in \{0, 1\}^n$ .
- Nur *eine* Auswertung der Blackbox, 1 Schritt.

## Problem für praktische Nutzung:

Messung von  $s$  liefert zufällig gleichverteilten Bitvektor!

## 2. Der Deutsch-Jozsa-Algorithmus

### Problem:

$f: \{0, 1\}^n \rightarrow \{0, 1\}$  durch Blackbox gegeben. „Versprechen“:

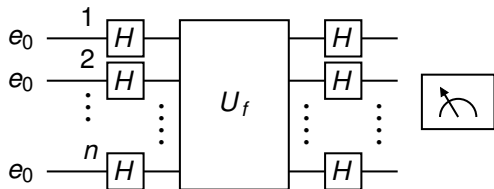
- Entweder  $f$  konstant oder
- $f$  balanciert, d. h.  $|f^{-1}(0)| = |f^{-1}(1)|$ .

**Frage:** Welcher der beiden Fälle liegt vor?

Falls Versprechen nicht erfüllt: Beliebige Ausgabe erlaubt.

Bekomme Quanten-Blackbox-Baustein für  
Berechnung von  $f$ .

Quantenschaltkreis für das Deutsch-Jozsa-Problem:



Funktionsweise hier nur für Spezialfall  $n = 1$ :

## Auswertung des DJ-Schaltkreises für $n = 1$ :

$$e_0 \xrightarrow{H} \frac{1}{\sqrt{2}}(e_0 + e_1) \xrightarrow{U_f} \frac{1}{\sqrt{2}}((-1)^{f(0)}e_0 + (-1)^{f(1)}e_1).$$

$$f \text{ konstant, } f(0) = f(1): \quad = \pm \frac{1}{\sqrt{2}}(e_0 + e_1) = \pm He_0.$$

$$f \text{ balanciert, } f(0) \neq f(1): \quad = \pm \frac{1}{\sqrt{2}}(e_0 - e_1) = \pm He_1.$$

## Anwendung von $H$ + Messung:

$f$  konstant,  $f(0) = f(1)$ : Ergebnis „0“ mit Wskt. 1;

$f$  balanciert,  $f(0) \neq f(1)$ : Ergebnis „1“ mit Wskt. 1.

## Analyse DJ-Algorithmus:

- Für  $n = 2$ :  
Nur eine Funktionsauswertung statt zwei klassisch.
- Für beliebiges  $n$ :  
Immer noch eine Funktionsauswertung,  
klassisch mindestens  $2^{n-1} + 1$  notwendig.

(Untere Schranken für Blackbox-Algorithmen.)

## Allerdings:

Zufall hilft. Zwei Auswertungen an zufälligen Stellen → Fehlerwskt. höchstens  $1/2$ .

Ähnliches, komplizierteres Problem auch für randomisierten Fall schwierig.

### **Wichtigste Grundidee:**

Fouriertransformationen  $\rightarrow$  Periode von Funktionen.

Für reelle Funktion  $\rightarrow$  Frequenzspektren,  
viele technische Anwendungen.

Für diskrete Funktionen:

Diskrete Fouriertransformation, DFT.

## Erinnerung:

DFT für Polynom  $f = a_{N-1}x^{N-1} + \dots + a_1x^1 + a_0$ :

$$\begin{aligned} \text{DFT}_N(f) &= [f(w^0), f(w^1), \dots, f(w^{N-1})] \\ &= \left[ \sum_{j=0}^{N-1} a_j w^{0 \cdot j}, \dots, \sum_{j=0}^{N-1} a_j w^{(N-1) \cdot j} \right]. \end{aligned}$$

Hier  $w$   $N$ -te Einheitswurzel in  $\mathbb{C}$ ,  $w = e^{2\pi i/N}$ .

## Finden von Perioden:

### Problem:

Funktion  $f: \mathbb{Z}_N \rightarrow \mathbb{Z}$  gegeben, es gibt ein  $r \in \mathbb{Z}_N$  mit  $f(x) = f(x + r)$  für alle  $x \in \mathbb{Z}_N$ .

**Aufgabe:** Finde  $r$ .

Hier der Einfachheit halber  $N = rd$ .

Ziel: Lösung mit DFT.

Funktion  $f \rightarrow [a_0, \dots, a_{N-1}]$ ,  $a_i := f(i)$  für  $i \in \mathbb{Z}_N$ .

Dann DFT wie bei Polynomen:

$$\text{DFT}_N(f)_k = \sum_{j=0}^{N-1} a_j w^{jk}, \quad k = 0, \dots, N-1.$$

Für festes  $k \in \{0, \dots, N-1\}$ :

$$\begin{aligned} \text{DFT}_N(f)_k &= \sum_{j=0}^{N-1} a_j w^{jk} \\ &= \sum_{j=0}^{N-1} a_{j+r} w^{(j+r-r)k} \quad (\text{Periodizität}) \\ &= w^{-kr} \sum_{j=0}^{N-1} a_{j+r} w^{(j+r)k} \\ &= w^{-kr} \text{DFT}_N(f)_k. \end{aligned}$$

Dann gilt  $\text{DFT}_N(f)_k \neq 0$  nur dann, wenn  $w^{-rk} = 1$ .

Ergebnisvektor ungleich 0 für solche  $k$ , wo

$$w^{-rk} = 1 \Leftrightarrow rk \equiv 0 \pmod{N} \Leftrightarrow k \equiv 0 \pmod{N/r}.$$

Anders ausgedrückt:

$k$  ist Vielfaches von  $N/r$ ,  $k = c(N/r)$  und

$$\frac{k}{N} = \frac{c}{r}.$$

Shors Algorithmus realisiert diese DFT-Berechnung und liefert (Messung am Ende) zufälliges  $k \rightarrow$  zufälliges  $c \in \{0, \dots, r-1\}$ .

Daraus mit hoher Wskt.  $r$  bestimmbar.

## Anwendung:

Bestimmung der Ordnung eines Elements  $a \in \mathbb{Z}_N^*$ ,  
d. h. des kleinsten  $r \in \mathbb{N}$  mit  $a^r \equiv 1 \pmod{N}$ .

## Bekannt:

Klassischer randomisierter Algorithmus, der Faktorisierung mit Teilmodul zur Ordnungsbestimmung effizient löst.

- Ordnungsbestimmung selbst klassisch vermutlich nur mit Exponentialzeit-Algorithmus lösbar.
- Quantenschaltkreis, basierend auf DFT, benötigt nur  $\text{poly}(\log N)$  viele Bausteine/Schritte.

Wesentlich: Effizienter Quantenschaltkreis für  $\text{DFT}_N$ :  
Klassisch  $\Theta(N \log N) \rightarrow$  QSK mit  $O(\log^2 N)$  Bausteinen.