Quantenberechnungen

Mathematische Grundlagen: Hilberträume

Komplexe Zahlen

$\mathbb{C} = \mathbb{R} + i \cdot \mathbb{R}$ ist die Menge der komplexen Zahlen, wobei $i := \sqrt{-1}$.
Eine Zahl $z \in \mathbb{C}$ mit $z = a + i \cdot b$ besitzt Realteil $a \in \mathbb{R}$ und Imaginärteil $b \in \mathbb{R}$.

- Es gelten die Rechenregeln:

$$\begin{aligned} (a + i \cdot b) + (c + i \cdot d) &= (a + c) + i \cdot (b + d) \\ (a + i \cdot b) \cdot (c + i \cdot d) &= (a \cdot c - b \cdot d) + i \cdot (b \cdot c + a \cdot d) \end{aligned}$$

- Für $z \in \mathbb{C}$ mit $z = x + i \cdot y$ ist $\overline{z} = x - i \cdot y$ die (komplex) Konjugierte von z. Es gilt:

$$\overline{x + y} = \overline{x} + \overline{y} \quad \text{und} \quad \overline{x \cdot y} = \overline{x} \cdot \overline{y}$$

- Die Länge der komplexen Zahl z ist $|z| := \sqrt{z \cdot \overline{z}}$.

Für das Folgende betrachten wir Vektorräume über den komplexen Zahlen.

Das innere Produkt

Sei $\mathcal{V}$ ein Vektorraum über $\mathbb{C}$.

Ein **inneres Produkt** über $\mathcal{V}$ ist eine Abbildung $\langle , \rangle : \mathcal{V}^2 \to \mathbb{C}$ mit den folgenden Eigenschaften für alle Vektoren $\phi, \psi, \rho \in \mathcal{V}$.

(1) $\langle \phi, \phi \rangle \geqslant 0$ und $\langle \phi, \phi \rangle = 0$ genau dann, wenn $\phi = 0$.

(2) $\langle \alpha \cdot \phi + \beta \cdot \psi, \gamma\rho \rangle = \overline{\alpha}\gamma \cdot \langle \phi, \rho \rangle + \overline{\beta}\gamma \cdot \langle \psi, \rho \rangle$ für alle komplexen Zahlen α, β, γ.

(3) $\langle \phi, \psi \rangle = \overline{\langle \psi, \phi \rangle}$.

Die von dem inneren Produkt abgeleitete Norm $\| \cdots \|$ ist definiert durch

$$\|\phi\| := \sqrt{\langle \phi, \phi \rangle}.$$

Ein Vektorraum $\mathcal{V}$ über $\mathbb{C}$ mit einem inneren Produkt heißt ein **Prähilbertraum**.

Hilberträume

Ein Prähilbertraum $\mathcal{H}$ heißt ein **Hilbertraum** genau dann, wenn $\mathcal{H}$ **vollständig** ist, d.h. falls jede **Cauchy-Folge** gegen einen Vektor aus $\mathcal{H}$ konvergiert.

- Eine Folge $(\phi_n \mid n \in \mathbb{N})$ heißt Cauchy-Folge, falls es zu jedem $\varepsilon > 0$ eine natürliche Zahl N gibt, so dass $\|\phi_n - \phi_m\| \leqslant \varepsilon$ für alle $n, m \geqslant N$.

Elemente ϕ von $\mathcal{H}$ mit $\|\phi\| = 1$ heißen **Zustände**.

Beispiel $\mathcal{H} = \mathbb{C}^n$:

Für Zustände $\phi, \psi \in \mathcal{H}$ mit $\phi = (\phi_1, \ldots, \phi_n)$ und $\psi = (\psi_1, \ldots, \psi_n)$ definiere

$$\langle \phi, \psi \rangle := \sum_{i=1}^{n} \overline{\phi_i} \cdot \psi_i.$$

- $\langle , \rangle$ ist ein inneres Produkt.
- Eine Cauchy-Folge $f = (\phi_n \mid n \in \mathbb{N})$ induziert eine Cauchy-Folge auf Real- und Imaginärteilen der Folge. Die beiden induzierten Folgen konvergieren.
- $\Longrightarrow \mathbb{C}^n$ ist ein Hilbertraum!

Orthonormalsysteme und Hilbertbasen (1/2)

Sei $\mathcal{H}$ ein Hilbertraum.

(a) $\mathcal{B} \subseteq \mathcal{H}$ heißt ein **Orthonormalsystem**, wenn alle Elemente von $\mathcal{B}$ die Norm 1 besitzen und je zwei Zustände in $\mathcal{B}$ senkrecht aufeinander stehen.

- Eine **Hilbertbasis** ist ein Orthonormalsystem $\mathcal{B}$, so dass der von $\mathcal{B}$ aufgespannte Unterraum eine dichte Teilmenge von $\mathcal{H}$ ist.
- Eine **Orthonormalbasis** ist Orthonormalsystem, das Raum $\mathcal{H}$ aufspannt.

(b) Die Koeffizienten α_i einer Linearkombination $\phi = \sum_{i \in I} \alpha_i \cdot \phi_i$ für eine *endliche* Teilmenge $I \subseteq \mathcal{B}$ einer Orthonormalbasis $\mathcal{B}$ heißen **Amplituden**.

- $\mathcal{V}$ ist ein dichter Unterraum von $\mathcal{H}$, wenn zu jedem Element $x \in \mathcal{H}$ und zu jedem $\varepsilon > 0$ es einen Vektor $y \in \mathcal{V}$ gibt, so dass $\|x - y\| \leqslant \varepsilon$.
- Ein Hilbertraum $\mathcal{H}$ ist insbesondere ein Vektorraum und besitzt damit eine Basis:
  - Das Orthogonalisierungsverfahren von Gram-Schmidt: Die Basis eines Vektorraums *endlicher* Dimension wird in eine Orthonormalbasis überführt.
  - Hilberträume *endlicher* Dimension besitzen eine Orthonormalbasis.
- Übungsaufgabe: Hilberträume *unendlicher* Dimension besitzen keine Orthonormalbasis, wohl aber eine Hilbertbasis.

Orthonormalsysteme und Hilbertbasen (2/2)

Das unendlich große Orthonormalsystem $\mathcal{B}$ spanne den Vektorraum $\mathcal{V}$ aller endlichen Linearkombinationen auf.

- Vektoren $\phi, \psi \in \mathcal{V}$ sind durch endliche Mengen C_ϕ und C_ψ von Basisvektoren beschrieben: $\phi = \sum_{c \in C_\phi} \alpha_c \cdot c$ und $\psi = \sum_{c \in C_\psi} \beta_c \cdot c$
- Inneres Produkt von $\mathcal{V}$: $\langle \phi, \psi \rangle := \sum_{c \in C_u \cap C_v} \overline{\alpha_c} \cdot \beta_c$
- $\mathcal{V}$ ist ein nicht-vollständiger Prähilbertraum: Die Folge $f_n = \sum_{i=1}^{n} 2^{-i} \cdot \phi_i$ ist eine Cauchy-Folge, ihr Grenzwert $f = \sum_{i=1}^{\infty} 2^{-i} \cdot \phi_i$ liegt aber nicht in $\mathcal{V}$.
  - Wir fügen Grenzwerte aller Cauchy-Folgen zu $\mathcal{V}$ hinzu: $\mathcal{H}$ besteht aus allen Summen $\phi := \sum_{i=1}^{\infty} \alpha_i \phi_i$, so dass: $\| \sum_{i=1}^{\infty} \alpha_i \cdot \phi_i \|^2 = \sum_{i=1}^{\infty} |\alpha_i|^2 \overset{!}{<} \infty$
  - Inneres Produkt von $\mathcal{V}$ auf $\mathcal{H}$ fortgesetzt: $\langle \sum_{i=1}^{\infty} \alpha_i \cdot \phi_i, \sum_{i=1}^{\infty} \beta_i \cdot \phi_i \rangle := \sum_{i=1}^{\infty} \overline{\alpha_i} \cdot \beta_i$

$\mathcal{V}$ ist dichter Unterraum von $\mathcal{H} \Longrightarrow \mathcal{B}$ wird zu einer Hilbertbasis.

Vervollständigung von Prähilberträumen

Ein metrischer Raum (X, d) besteht aus einer Grundmenge X und einer Distanzfunktion $d : X \times X \to \mathbb{R}_{\geqslant 0}$. Für die Distanzfunktion gilt:

(1) $d(x, y) = 0$ genau dann, wenn $x = y$,

(2) $d(x, y) = d(y, x)$ für alle $x, y \in X$ (Symmetrie),

(3) $d(x, z) \leqslant d(x, y) + d(y, z)$ für alle $x, y, z \in X$ (Dreiecksungleichung).

- Jeder metrischer Raum (X, d) besitzt eine eindeutige kleinste Vervollständigung, also einen metrischen Raum (X^*, d^*), so dass
  - $d^*(x, y) = d(x, y)$ für alle $x, y \in X$,
  - X eine dichte Teilmenge von X^* ist und
  - alle Cauchy-Folgen gegen ein Element von X^* konvergieren.
- Man erhält X^* durch Hinzufügen aller Grenzwerte von Cauchy-Folgen.

Ein Prähilbertraum ist ein metrischer Raum $\Longrightarrow$

Jeder Prähilbertraum besitzt einen eindeutig bestimmten **kleinsten** Hilbertraum, der ihn enthält.

Dirac-Notation

Dirac-Notation: Dualräume

- Ein Zustand $\phi \in \mathcal{H}$ definiert die lineare Funktion

$$\phi^* : \mathcal{H} \to \mathbb{C}, \quad \text{mit } \phi^*(\psi) := \langle \phi, \psi \rangle.$$

- Der Raum

$$\mathcal{H}^* = \{\phi^* \mid \phi \in \mathcal{H}\}$$

ist abgeschlossen unter Linearkombinationen und somit ein Vektorraum.

  - Die bijektive Abbildung $L : \mathcal{H} \to \mathcal{H}^*$ mit $L(\phi) := \phi^*$ zeigt, dass $\mathcal{H}$ und $\mathcal{H}^*$ als Vektorräume *isomorph* sind.
    - Das innere Produkt von $\mathcal{H}$ kann deshalb für $\mathcal{H}^*$ übernommen werden durch:

$$\langle \phi^*, \psi^* \rangle := \langle \phi, \psi \rangle$$

    - Eine Folge $(f_n \mid n \in \mathbb{N})$ konvergiert genau dann gegen $f \in \mathcal{H}$, wenn $(f_n^* \mid n \in \mathbb{N})$ gegen $f^* \in \mathcal{H}^*$ konvergiert.
  - $\mathcal{H}^*$ ist ein Hilbertraum, der als der **Dualraum** von $\mathcal{H}$ bezeichnet wird.

Dirac-Notation: Bra und Ket

- Ket-Notationen $|\phi\rangle$ für Zustände $\phi \in \mathcal{H}$: $|\phi\rangle$ „ist“ Spaltenvektor
- Bra-Notation $\langle\phi|$ für Elemente ϕ^* des Dualraums $\mathcal{H}^*$: $\langle\phi|$ „ist“ Zeilenvektor
- Für eine lineare Abbildung $L : \mathcal{H} \to \mathcal{H}$ benutze die Abkürzungen

$L\|\phi\rangle$	für $L(\phi)$
$\langle\phi\|L$	für lineare Abbildung $\phi^* \circ L$ und
$\langle\phi\|L\|\psi\rangle$	für Wert des inneren Produktes $\langle\phi^*, L(\psi)\rangle = (\phi^* \circ L)(\psi)$.

- Wenn $I : \mathcal{H} \to \mathcal{H}$ die identische Transformation (bzw. die Einheitsmatrix) bezeichnet, dann erhält man das innere Produkt

$$\langle\phi|\psi\rangle := \langle\phi|I|\psi\rangle.$$

- Wir benutzen ϕ und $|\phi\rangle$ *bedeutungsgleich* um ein Element des Hilbertraums zu bezeichnen.
  - Beachte: Die Vektor-Darstellung $(\phi_1, \ldots, \phi_n)$ eines Zustands $|\phi\rangle$ ist nicht formal identisch mit $|\phi\rangle$, denn die Darstellung hängt von Wahl der Basis ab.

Anwendungen der Dirac-Notation: Qubits etc.

Ein Qubit ist ein 1-Teilchen-System mit den klassischen Zuständen 0 und 1.

1. Den klassischen Bits entsprechen die Basisvektoren $|0\rangle$ und $|1\rangle$, die den Hilbertaum $\mathbb{C}^2$ aller möglichen Linearkombinationen $\alpha|0\rangle + \beta|1\rangle$ aufspannen.
2. In einem System von n Teilchen entsprechen die Basisvektoren den Zuständen $|b_1 \cdots b_n\rangle$, die den Hilbertraum $\mathbb{C}^{2^n}$ aufspannen.

Gleich: Die Definition eines Tensorraums zeigt die Flexibilität der Dirac-Notation.

Das Tensorprodukt

Tensorprodukt

Seien $\mathcal{H}_1, \mathcal{H}_2$ Hilberträume mit Hilbertbasen O_1 bzw. O_2.

(a) Das **algebraische Tensorprodukt** $\mathcal{H}_1 \odot \mathcal{H}_2$ ist der von der Orthonormalbasis $\{ |hk\rangle : h \in O_1, k \in O_2 \}$ aufgespannte Prähilbertraum:

$$\mathcal{H}_1 \odot \mathcal{H}_2 := \left\{ \sum_{(h,k)\in I} \alpha_{h,k} \cdot |hk\rangle \; : \; I \subseteq O_1 \times O_2, I \text{ ist endlich} \right\}.$$

(b) Das **Tensorprodukt** $\mathcal{H}_1 \otimes \mathcal{H}_2$ ist die Vervollständigung des algebraischen Tensorprodukts.

(c) Für $|\phi\rangle \in \mathcal{H}_1$ und $|\psi\rangle \in \mathcal{H}_2$ gelte $|\phi\rangle = \sum_{h\in O_1} \alpha_h \cdot |h\rangle$ und $|\psi\rangle = \sum_{k\in O_2} \beta_k \cdot |k\rangle$

Dann ist

$$|\phi\rangle \otimes |\psi\rangle := \sum_{h\in O_1, k\in O_2} \alpha_h \cdot \beta_k \cdot |hk\rangle$$

das Tensorprodukt von $|\phi\rangle$ und $|\psi\rangle$.

Mit Tensorprodukten lassen sich neue aus alten Hilberträumen bauen!

Verschränkung (engl. Entanglement)

- Angenommen, $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ gilt und $\mathcal{H}$ ist somit das Tensorprodukt der Räume $\mathcal{H}_1, \mathcal{H}_2$.
- Jeder Zustand von $\mathcal{H}$, der selbst kein Tensorprodukt von Zuständen in $\mathcal{H}_1$ und $\mathcal{H}_2$ ist, wird als verschränkt (engl. entangled) bezeichnet.

Nicht-verschränkte Zustände entsprechen „gewissermaßen“ unabhängigen Zufallsvariablen.

Das äußere Produkt

Definiere das **äußere Produkt** $|\phi\rangle\langle\psi|$ für Zustände $|\phi\rangle \in \mathcal{H}$ und $\langle\psi| \in \mathcal{H}^*$ durch

$$|\phi\rangle\langle\psi| := |\phi\rangle \otimes \langle\psi|.$$

Wenn $\mathcal{H}$ endlich-dimensional ist, dann ist $|\phi\rangle \otimes \langle\psi|$ das Produkt des Spaltenvektors $|\phi\rangle$ mit dem Zeilenvektor $\langle\psi|$, also die Matrix $(\phi_i \cdot \psi_j)_{i,j}$.

Sei $\{\phi_i : i \in I\}$ eine Hilbertbasis von $\mathcal{H}$.

- $|\phi_j\rangle\langle\phi_j|$ ist die Projektion von $\mathcal{H}$ auf den von $|\phi_j\rangle$ aufgespannten Unterraum, denn

$$\begin{aligned}\left(|\phi_j\rangle\langle\phi_j|\right)\left|\sum_{i\in I}\alpha_i\phi_i\right\rangle &= \left(|\phi_j\rangle \otimes \langle\phi_j|\right)\left|\sum_{i\in I}\alpha_i\phi_i\right\rangle \\ &= |\phi_j\rangle \otimes \left(\left\langle\phi_j\middle|\sum_{i\in I}\alpha_i\phi_i\right\rangle\right) = \alpha_j \cdot |\phi_j\rangle\end{aligned}$$

- Wenn der Unterraum $\mathcal{V} \subseteq \mathcal{H}$ von der Orthonormalbasis $|\phi_1\rangle, \ldots, |\phi_N\rangle$ aufgespannt wird, dann ist $\sum_{i=1}^{N} |\phi_i\rangle\langle\phi_i|$ die Projektion von $\mathcal{H}$ auf $\mathcal{V}$.

Operatoren und Messungen

Unitäre Operatoren

Sei $\mathcal{H}$ ein Vektorraum über $\mathbb{C}$.

Eine lineare Abbildung $L : \mathcal{H} \to \mathcal{H}$ heißt ein **Operator** auf $\mathcal{H}$.

Wie rechnet ein quantenmechanisches System? Mit Hilfe von **unitären Operatoren!**

Sei $L : \mathcal{H} \to \mathcal{H}$ ein Operator.

(a) $L^* : \mathcal{H} \to \mathcal{H}$ heißt die **Adjungierte** von L, falls für alle $\phi, \psi \in \mathcal{H}$ gilt:

$$\langle L(\psi) \,|\, \phi \rangle = \langle \psi \,|\, L^*(\phi) \rangle$$

- L heißt **selbstadjungiert** oder **hermitesch**, falls $L = L^*$, d.h. falls gilt

$$\langle L(\psi) \,|\, \phi \rangle = \langle \psi \,|\, L(\phi) \rangle.$$

- L heißt **unitär**, falls $L \circ L^* = L^* \circ L = I$.

(b) Die Norm von L definieren wir als

$$\|L\| := \sup_{\| \,|\phi\rangle\| = 1} \| \,|L(\phi)\rangle\|.$$

Eigenschaften unitärer Operatoren

Unitäre Operatoren verändern die *Länge der Zustände* nicht!

Die Operatoren $U_1, U_2 : \mathcal{H} \to \mathcal{H}$ seien unitär.

(a) Es gilt $\|U_1(\phi)\| = \|\phi\|$.

(b) $U_1 \circ U_2$ ist unitär.

- Beweis (a): Da U_1 unitärer Operator ist, folgt $U_1^* \circ U_1 = I$. Weiterhin ergibt sich $\langle U_1(\psi) \mid \phi \rangle = \langle \psi \mid U_1^*(\phi) \rangle$ aus Definition des adjungierten Operators. Deshalb ist

$$\| \ |U_1(\phi)\rangle\| = \sqrt{\langle U_1(\phi) \mid U_1(\phi)\rangle} = \sqrt{\langle \phi \mid U_1^* \circ U_1(\phi)\rangle} = \| \ |\phi\rangle\|.$$

- (b) Für unitäre Operatoren U_1 und U_2 (mit Adjungierten U_1^* und U_2^*) folgt

$$\langle U_2^* \circ U_1^*(\psi) \mid \phi \rangle = \langle U_1^*(\psi) \mid U_2(\phi) \rangle = \langle \psi \mid U_1 \circ U_2(\phi) \rangle$$

und $U_2^* \circ U_1^*$ ist die Adjungierte von $U_1 \circ U_2$.

Da $U_2^* \circ U_1^* \cdot U_1 \circ U_2 = U_2^* \circ U_2 = I$, ist $U_1 \circ U_2$ unitär. □

Matrixdarstellung unitärer Operatoren

- Sei A die Matrix des Operators L und A^* die Matrix von L^*.
  - A^* bezeichnet die Adjungierte von A.
  - A heißt genau dann unitär bzw. selbstadjungiert, wenn L unitär bzw. selbstadjungiert ist.
- Angenommen die Matrix A des Operators L hat nur reellwertige Einträge.
  - Die adjungierte Matrix stimmt überein mit der transponierten Matrix.
  - Eine selbstadjungierte Matrix ist symmetrisch.
  - Eine unitäre Matrix mit reellwertigen Einträgen ist eine orthogonale Matrix.

Projektive Messungen

Sei $\mathcal{H}$ ein Hilbertraum.

- $\mathcal{H}$ zerfalle in orthogonale Teilräume $\mathcal{H}_i$ mit $\mathcal{H} = \mathcal{H}_1 \oplus \cdots \oplus \mathcal{H}_k$,
  d.h. für alle $i \neq j$, $|\phi_i\rangle \in \mathcal{H}_i$, $|\phi_j\rangle \in \mathcal{H}_j$ gilt $\langle \phi_i \mid \phi_j \rangle = 0$.
- Für $|\phi\rangle = |\phi_1\rangle + \cdots |\phi_k\rangle$ mit $|\phi_i\rangle \in \mathcal{H}_i$ definiere die Projektion $P_i : \mathcal{H} \to \mathcal{H}_i$ durch

$$P_i|\phi\rangle := |\phi_i\rangle.$$

- Dann ist $P_i \circ P_j = 0$ für $i \neq j$. Jeder Zustand $|\phi\rangle \in \mathcal{H}$ besitzt die Darstellung

$$|\phi\rangle = P_1|\phi\rangle + \cdots + P_k|\phi\rangle.$$

Wir möchten das **Messergebnis $\lambda_i \in \mathbb{R}$** erhalten, wenn sich der Zustand $|\phi\rangle$ nach der Messung im Raum $\mathcal{H}_i$ befindet. Definiere den Operator $L : \mathcal{H} \to \mathcal{H}$ mit

$$L|\phi\rangle := \sum_{i=1}^{k} \lambda_i \cdot P_i|\phi\rangle.$$

Observable und Born-Regel

Warum hermitsche Operatoren? Der Hilbertraum $\mathcal{H}$ sei endlich dimensional $\Longrightarrow$
Jeder hermitesche Operator L (d.h. $L = L^*$) ist diagonalisierbar, d.h. es gilt

$$L|\phi\rangle = \sum_{i=1}^{k} \lambda_i \cdot P_i|\phi\rangle$$

mit paarweise verschiedenen reellen Zahlen $\lambda_1, \ldots, \lambda_k$.

(a) Eine **Observable** (auf Hilbertraum $\mathcal{H}$) ist ein hermitescher Operator $L : \mathcal{H} \to \mathcal{H}$.

(b) Die **Born-Regel**:

- Wenn der hermitesche Operator $L(|\phi\rangle) := \sum_{i=1}^{k} \lambda_i \cdot P_i|\phi\rangle$ im Zustand $|\phi\rangle$ gemessen wird, dann definiere

$$\text{prob}[\text{ Die Messung von } L(|\phi\rangle) \text{ hat Ergebnis } \lambda_i\,] := \|P_i|\phi\rangle\|^2.$$

- Nach Messung befindet sich das quantenmechanische System im Zustand

$$\frac{P_i|\phi\rangle}{\|P_i|\phi\rangle\|}.$$

Man sagt, dass Zustand $|\phi\rangle$ nach Messung in den Zustand $\frac{P_i|\phi\rangle}{\|P_i|\phi\rangle\|}$ kollabiert.

Quantenmechanische Systeme

- Ein quantenmechanisches System ist im Allgemeinen nicht statisch, sondern evolviert.
  - Evolution erfolgt durch einen unitären Operator oder durch Messung.
  - Unitäre Operatoren sind *umkehrbar*: Das System rechnet auf reversible Art.
  - Eine Messung verliert Information und ist nicht umkehrbar.
- Born-Regel: Für hermitesche Operatoren

$$L(|\phi\rangle) := \sum_{i=1}^{k} \lambda_i \cdot P_i|\phi\rangle$$

stimmt die W-keit p_i des Messwerts λ_i überein mit der W-keit in den Eigenraum $P_i\mathcal{H}$ von λ_i zu projizieren.

  - Dann ist $p_i = \|P_i|\phi\rangle\|^2$ und p_i stimmt überein mit der *quadrierten* Norm der Projektion in den Eigenraum.
  - Die Amplituden haben quadratischen Einfluß auf die W-keit des Resultats.

Quantenmechanische versus probabilistische Systeme

Quantenmechanische vs. probabilistische Systeme

- Probabilistisches System mit zwei Zufallsvariablen X_1, X_2, die jeweils N verschiedene Werte annehmen können.
  - Variablen unabhängig: (X_1, X_2) mit $2N$ Parametern beschreibbar.
  - Variablen korreliert: bis zu N^2 Parameter erforderlich.
- Quantenmechanisches System über zwei Hilberträumen $\mathcal{H}_1, \mathcal{H}_2$ jeweils der Dimension N
  - N Parameter genügen, um einen Zustand in $\mathcal{H}_i$ für $i = 1, 2$ zu beschreiben.
  - Nicht-verschränkte Zustände $|\phi_1\rangle \otimes |\phi_2\rangle$ mit $\phi_i \in \mathcal{H}_i$ erfordern nicht mehr als $2N$ Parameter.
  - Anzahl der Parameter explodiert auf bis zu N^2, wenn verschränkte Zustände $|\phi\rangle$ im Tensorraum $\mathcal{H}_1 \otimes \mathcal{H}_2$ zu beschreiben sind.

Hier enden die Ähnlichkeiten: Quantenmechanische Systeme rechnen durch Ausführung von **unitären Operatoren**.

Interferenz (engl. Interference)

Betrachte beispielhaft die unitäre **Hadamard-Matrix** $H := \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix}$

- Klassischer Zustand $|0\rangle$ wird in Überlagerung $H|0\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle + |1\rangle)$ überführt:

  Das System würfelt: Mit W-keit $\frac{1}{2}$ befindet es sich im Zustand $|0\rangle$ bzw. $|1\rangle$.
- Wir würfeln ein zweites Mal (H nochmal angewandt): Das System befindet sich mit W-keit 1 wieder im klassischen Zustand $|0\rangle$!?
  - Fall 1: Zustand $|0\rangle$ wird über Zwischenzustände $|0\rangle$ *und* $|1\rangle$ jeweils mit Amplitude $\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}}$ erreicht.
    - ⋆ *konstruktive* Interferenz: Beide Amplituden verstärken sich!
  - Fall 2: Zustand $|1\rangle$ wird über $|0\rangle$ mit Amplitude $\frac{1}{\sqrt{2}} \cdot \frac{1}{\sqrt{2}}$ und über $|1\rangle$ mit Amplitude $\frac{1}{\sqrt{2}} \cdot (-\frac{1}{\sqrt{2}})$ erreicht.
    - ⋆ *destruktive* Interferenz: Die beiden Amplituden heben sich auf!

Mit Interferenzen spielt ein Quantenrechner seine Kraft aus: Quantenmechanische Systeme arbeiten mit unkonventionellen (negativen / komplexwertigen) „W-keiten“.

Qubits

Qubits

Sei $|0\rangle$ (gesprochen „Ket 0“) und $|1\rangle$ (gesprochen „Ket 1“) eine Orthonormalbasis des Hilbertraums $\mathcal{H} := \mathbb{C}^2$.

Ein Qubit $|\psi\rangle \in \mathbb{C}^2$ entsteht durch eine **Überlagerung** (engl. **Superposition**)

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

der „klassischen“ Zustände $|0\rangle$ und $|1\rangle$.

- $|0\rangle$ entspricht dem Spaltenvektor $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$.
- $|1\rangle$ entspricht dem Spaltenvektor $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$.
- Wir nehmen stets an, dass $1 = \langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2$ gilt.

Beispiele (1-Teilchen-Systeme)

Der Hilbertraum $\mathbb{C}^2$ kann verwendet werden für die Beschreibung von:

- Polarisierung von Lichtteilchen: Photon tritt in ein Kristall ein, Austrittspunkt hängt ab von Polarisierung (*parallel* oder *senkrecht* zur optischen Achse des Kristalls) des Photons .
  - Für Zustand $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ wird $1 = \langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2$ gefordert $\Longrightarrow$ $(|\alpha|^2, |\beta|^2)$ lässt sich als Wahrscheinlichkeitsverteilung auffassen.
  - Experimentelle Beobachtung: Beide Polarisierungen treten mit Wahrscheinlichkeit $|\alpha|^2$ bzw. $|\beta|^2$ auf.
  - „Nachschaltung“ eines zweiten Kristalls:
    - Nach *Beobachtung* des Quantenzustands $|\psi\rangle$ ist der dem beobachtetem Ausgang entsprechende Basiszustand $|0\rangle$ bzw. $|1\rangle$ „festgefroren“.
    - Experimentelle Beobachtungen sind konform mit Definition einer Messung.
- Elektronenspin (Eigendrehimpuls eines Elektrons): *Aufwärts-Spin* $|\uparrow\rangle$ und *Abwärts-Spin* $|\downarrow\rangle$
  - Zustand $|\psi\rangle = \alpha \cdot |\uparrow\rangle + \beta \cdot |\downarrow\rangle$ eines Elektrons auffassbar als Überlagerung der klassischen Zustände $|\uparrow\rangle$ und $|\downarrow\rangle$.

Vielteilchen-Systeme

Vielteilchen-Systeme werden mit Hilfe des Tensorprodukts definiert.

1. Wenn die Hilberträume $\mathcal{H}_i$ die Dimension d_i besitzen, dann ist $\mathcal{H} := \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_k$ ein Hilbertraum der Dimension $d_1 \cdots d_k$.
2. Werden die Hilberträume $\mathcal{H}_i$ von der Orthonormalbasis $|0\rangle, |1\rangle$ aufgespannt, dann ist $\mathcal{H} = \mathbb{C}^{2^k}$ ein Hilbertraum der Dimension 2^k mit der Orthonormalbasis

$$|b_1 \cdots b_k\rangle := |b_1\rangle \otimes \cdots \otimes |b_k\rangle$$

für $b_1, \ldots, b_k \in \{0, 1\}$. In diesem Fall ist $\mathcal{H}$ der **Hilbertraum der k Qubits**.

Messungen in Vielteilchen-Systemen

- Die W-keit $p_{b_1,\ldots,b_k}$ der Beobachtung von $|b_1 \cdots b_k\rangle$ im Zustand

$$|\psi\rangle = \sum_{b_1,\ldots,b_k \in \{0,1\}^k} \alpha_{b_1,\ldots,b_k} \cdot |b_1 \cdots b_k\rangle.$$

  ist $p_{b_1,\ldots,b_k} = |\alpha_{b_1,\ldots,b_k}|^2$.

- Die Messung des *ersten* Qubits entspricht der Zerlegung von $\mathbb{C}^{2^k}$ in die von

$$\{|0 b_2 \cdots b_k\rangle \,:\, b_2,\ldots,b_k \in \{0,1\}\} \text{ bzw. } \{|1 b_2 \cdots b_k\rangle \,:\, b_2,\ldots,b_k \in \{0,1\}\}$$

  aufgespannten Räume.

  - Für Zustand $\phi = \sum_{b_1,\ldots,b_k \in \{0,1\}^k} \beta_{b_1,\ldots b_k} \cdot |b_1,\ldots,b_k\rangle$ hat Ergebnis b

$$\text{die Wahrscheinlichkeit } p_b = \sum_{b_2,\ldots,b_k \in \{0,1\}^{k-1}} |\beta_{b,b_2,\ldots b_k}|^2.$$

  - Ist b das Ergebnis der Beobachtung, dann kollabiert Zustand $|\,\phi\,\rangle$ zu $\frac{|\,\mu\,\rangle}{\|\mu\|}$ mit

$$\mu := \sum_{b_2,\ldots,b_k \in \{0,1\}^{k-1}} \beta_{b,b_2,\ldots b_k} \cdot |b, b_2,\ldots,b_k\rangle.$$

Beispiel: Einstein-Podolsky-Rosen (EPR) Paare

- Wir betrachten den *verschränkten* Zustand

$$|\,\phi\,\rangle := \frac{1}{\sqrt{2}} \cdot |\,00\,\rangle + \frac{1}{\sqrt{2}} \cdot |\,11\,\rangle.$$

  - Wird das erste Qubit mit Ergebnis 0 gemessen, dann kollabiert $|\,\phi\,\rangle$ in den Zustand $|\,\phi_0\,\rangle := |\,00\,\rangle$.
  - Analoges gilt für das Ergebnis 1.

- Die Beobachtung des ersten Qubits von ϕ fixiert das zweite Qubit,

  obwohl sich beide Qubits nicht in räumlicher Nähe befinden müssen.

Quantenmechanische Systeme können nicht-lokales Verhalten zeigen.

Quantenrechner

Rechnungen auf Qubits

1. Ein quantenmechanisches System rechnet durch aufeinander folgende bzw. parallele **Anwendungen unitärer Operatoren**.
   - Parallel ausgeführte Operatoren sind auf unterschiedliche Qubits anzuwenden.
   - Die ausgeführten Operatoren sollten „einfach“ sein, d.h. nur von wenigen Qubits abhängen.
2. Startzustand: $|b_1 \cdots b_n\rangle |0^m\rangle$ mit Bits $b_1, \ldots, b_n \in \{0, 1\}$
   - Mit Zustand $|0^m\rangle$ wird genügend „Platz“ für den bei Berechnungen anfallenden Datenmüll geschaffen.
   - Warum ist zusätzlicher Platz i.A. notwendig? Unitäre Berechnungen sind umkehrbar und Datenmüll kann deshalb nicht entsorgt werden.
3. Das Ergebnis des Systems wird durch eine **Messung** ermittelt.

Wir betrachten mit *Quanten-Schaltkreisen* und *Quanten-Turingmaschinen* zwei Implementierungen eines rechnenden „Qubit-Systems“.

Quanten-Schaltkreise

Quanten-Schaltkreise

Ein Quanten-Schaltkreis wird durch einen kreisfreien gerichteten Graphen $G = (V, E)$ beschrieben.

- Die Eingabe $|b_1 \cdots b_n\rangle|0^m\rangle$ für $b_1, \ldots, b_n \in \{0, 1\}$ wird an $n + m$ Quellen von G angelegt.
- Den Knoten von G werden Quanten-Gatter zugewiesen.
  - Jedes Quanten-Gatter führt einen unitären Operator aus, der nur von wenigen Qubits abhängt.
  - Quanten-Gatter $\mathcal{G}$ führe die unitäre Matrix U auf den ersten k Qubits aus. $\mathcal{G}$ überführt Überlagerung $|\phi\rangle = \sum_{b_1,\ldots,b_{n+m}\in\{0,1\}} \alpha_{b_1\cdots b_{n+m}}|b_1 \cdots b_{n+m}\rangle$ in

$$\mathcal{G}|\phi\rangle := \sum_{b_1,\ldots,b_{n+m}\in\{0,1\}} \alpha_{b_1\cdots b_{n+m}} \Big(U|b_1 \cdots b_k\rangle \otimes |b_{k+1} \cdots b_{n+m}\rangle \Big)$$

  .
- Jede Kante transportiert genau ein Qubit und alle Kanten, die dasselbe Qubit transportieren, bilden einen Weg von einer Quelle zu einer Senke.
- Das Ergebnis wird am Ende der Berechnung an den Senken von G durch eine Messung ermittelt.

No-Cloning-Theorem

- Quanten-Gatter berechnen umkehrbare Operatoren, denn unitäre Operatoren sind umkehrbar.
- Für jeden inneren Knoten stimmen Ein- und Aus-Grad überein, denn Quanten-Schaltkreise können nicht kopieren!

Für jedes Qubit $|\phi\rangle$ ist die Abbildung L mit

$$|\phi\rangle \otimes |0\rangle \overset{L}{\mapsto} |\phi\rangle \otimes |\phi\rangle$$

nicht-linear.

Beweis: Für Qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ ist L die nicht-lineare Transformation

$$\begin{aligned} |\phi\rangle \otimes |0\rangle = \alpha|00\rangle + \beta|10\rangle\rangle \quad &\overset{L}{\mapsto} \quad \Big(\alpha|0\rangle + \beta|1\rangle\Big) \otimes \Big(\alpha|0\rangle + \beta|1\rangle\Big) \\ &= \quad \alpha^2|00\rangle + \alpha\beta\big(|01\rangle + |10\rangle\big) + \beta^2|11\rangle \end{aligned}$$

□

Quanten-Gatter

Zuerst die Gatter, die auf einem einzigen Qubit arbeiten. Zeilen und Spalten der unitären Matrizen sind gemäß der Reihenfolge $|0\rangle, |1\rangle$ angeordnet.

- Das **Bitflip-Gatter** vertauscht die klassischen Basiszustände $|0\rangle$ und $|1\rangle$, d.h. es ist $|0\rangle \mapsto |1\rangle$ und $|1\rangle \mapsto |0\rangle$.

$$B := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

- Für das **Phasenflip-Gatter** gilt $|0\rangle \mapsto |0\rangle$ und $|1\rangle \mapsto -|1\rangle$.

$$P := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

- Das **Phasen-Gatter** rotiert die Phase des klassischen Zustands $|1\rangle$ um α Grad, d.h. es ist $|0\rangle \mapsto |0\rangle$ und $|1\rangle \mapsto \exp^{i\cdot\alpha} |1\rangle$.

$$P_\alpha := \begin{pmatrix} 1 & 0 \\ 0 & \exp^{i\cdot\alpha} \end{pmatrix} \quad \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

Für $z \in \mathbb{C}$ ist $z = |z| \cdot e^{i\phi}$ die **Polarkoordinaten-Darstellung** von z.

Hadamard-Gatter

- Mit dem **Hadamard-Gatter** kann gewürfelt werden:
  Es gilt $|0\rangle \mapsto \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big)$ und $|1\rangle \mapsto \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$.

$$H := \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{-1}{\sqrt{2}} \end{pmatrix} \quad \begin{matrix} |0\rangle \\ |1\rangle \end{matrix}$$

- Sowohl von $|0\rangle$ wie auch von $|1\rangle$ ausgehend werden die klassischen Zustände mit W-keit $\frac{1}{2}$ beobachtet.

Controlled-U-Gatter

- Die Matrix U sei unitär. Das **Controlled-U-Gatter** arbeitet auf zwei Qubits.

$$C_U := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & U_{1,1} & U_{1,2} \\ 0 & 0 & U_{2,1} & U_{2,2} \end{pmatrix} \quad \begin{matrix} |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{matrix}$$

  - Ist das erste Qubit 0, dann bleibt das erste und zweite Qubit unverändert:

$$|00\rangle \overset{C_U}{\mapsto} |00\rangle, |01\rangle \overset{C_U}{\mapsto} |01\rangle.$$

  - Ist das erste Qubit 1, dann wird U ausgeführt:

$$|10\rangle \overset{C_U}{\mapsto} U_{1,1}|10\rangle + U_{2,1}|11\rangle \text{ sowie } |11\rangle \overset{C_U}{\mapsto} U_{1,2}|10\rangle + U_{2,2}|11\rangle.$$

- Beschreibt U das Bitflip-Gatter, erhält man das **Controlled-Not-Gatter**:

  Das zweite Bit wird genau dann „geflippt“, wenn das erste Bit 1 ist: Das erste Bit *kontrolliert* das zweite.

Toffoli-Gatter

- Das **Toffoli-Gatter** wird auf drei Qubits angewandt.

$$T := \left(\begin{array}{cccccc|cc} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{array}\right) \begin{array}{l} |000\rangle \\ |001\rangle \\ |010\rangle \\ |011\rangle \\ |100\rangle \\ |101\rangle \\ |110\rangle \\ |111\rangle \end{array}$$

- Für $b_1 b_2 \neq 11$ ist $|b_1 b_2 b_3\rangle \mapsto |b_1 b_2 b_3\rangle$.
- Andererseits ist $|110\rangle \mapsto |111\rangle$ und $|111\rangle \mapsto |110\rangle$:
  Die beiden ersten Qubits kontrollieren das dritte Qubit.

Universelle Quanten-Gatter

Eine Menge $\mathcal{G}$ von Quanten-Gattern ist **universell**, wenn jeder von einem Quanten-Schaltkreis polynomieller Größe berechenbare unitäre Operator sich effizient von einem Quanten-Schaltkreis mit Gattern aus $\mathcal{G}$ *approximieren* lässt.

- Bitflip-Gatter, Toffoli-Gatter und Controlled-Not-Gatter permutieren klassische Zustände.
  - Effiziente Simulation durch konventionelle Schaltkreise auch nach Hinzufügen des Phasenflip-Gatters möglich.
- Alle Quanten-Gatter, die ein einzelnes Qubit modifizieren, zusammen mit dem Controlled-Not-Gatter erzeugen eine **universelle Menge** von Gattern.
- Hadamard- und Controlled-Not-Gatter: Effiziente „klassische“ Simulation gelingt.
  - Aber: Hadamard-Gatter zusammen mit Controlled-Not- und Phasen-Gatter (für $\alpha = \frac{\pi}{4}$) bilden eine **universelle Menge**.
- Hadamard-Gatter zusammen mit Toffoli-Gatter bilden **universelle Menge** für unitäre Operatoren mit reellwertigen Einträgen.

Zwischenmessungen

In Quanten-Schaltkreisen wird nur an den Senken gemessen.

Können zwischenzeitliche Messungen die Berechnungskraft erhöhen?

Wende den Operator $L = \begin{pmatrix} L_{1,1} & L_{1,2} \\ L_{2,1} & L_{2,2} \end{pmatrix}$ auf Qubit $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ (mit $\|\phi\| = 1$) an.

- Messen $\rightarrow$ Rechnen $\rightarrow$ Messen:
  - Messe ϕ: $|0\rangle$ mit W-keit $|\alpha|^2$ sowie $|1\rangle$ mit W-keit $|\beta|^2$,
  - wende L auf Ergebnis der Messung an:
    Mit W-keit $|\alpha|^2$ erhalte $L_{1,1}|0\rangle + L_{2,1}|1\rangle$, mit W-keit $|\beta|^2$ erhalte $L_{1,2}|0\rangle + L_{2,2}|1\rangle$.
  - Messe danach: W-keit von $|0\rangle$ ist $|\alpha L_{1,1}|^2 + |\beta L_{1,2}|^2$.
- Rechnen $\rightarrow$ Messen:
  - Zuerst wende Controlled-Not-Gatter auf $|\phi 0\rangle$ an und dann wende L an $\Longrightarrow$
  - $$L\Big(\underbrace{\alpha|00\rangle + \beta|11\rangle}_{\text{Controlled-Not-Gatter}}\Big) = \alpha\Big(L_{1,1}\cdot|00\rangle + L_{2,1}\cdot|10\rangle\Big) + \beta\Big(L_{1,2}\cdot|01\rangle + L_{2,2}\cdot|11\rangle\Big)$$
  - W-keit einer finalen Beobachtung von $|0*\rangle$ ist $|\alpha L_{1,1}|^2 + |\beta L_{1,2}|^2 \Longrightarrow$
    Die zwischenzeitliche Messung von $|\phi\rangle$ ist im neuen Schaltkreis unnötig!

Versand von Qubits über klassischen Kanal (1/2)

Alice möchte ihr Qubit $\phi := \alpha|0\rangle + \beta|1\rangle$ über einen klassischen Kanal an Bob schicken.

(a) Alice besitzt das erste Qubit des EPR-Paars $\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)$, während Bob auf das zweite Qubit zugreifen kann.

(b) Der gemeinsame Zustand ist

$$|\psi\rangle := \Big(\alpha|0\rangle + \beta|1\rangle\Big) \otimes \left(\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)\right).$$

1. Alice wendet das Controlled-Not-Gatter auf ihre beiden ersten Qubits an:

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

2. und danach den Hadamard-Operator auf ihr erstes Qubit:

$$\frac{\alpha}{\sqrt{2}} \cdot \Big(|0\rangle + |1\rangle\Big) \otimes \left(\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)\right) + \frac{\beta}{\sqrt{2}} \cdot \Big(|0\rangle - |1\rangle\Big) \otimes \left(\frac{1}{\sqrt{2}} \cdot (|10\rangle + |01\rangle)\right)$$

$$= \frac{1}{2} \cdot \Big(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle) + |10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\Big)$$

Versand von Qubits über klassischen Kanal (2/2)

3. Der gemeinsame Zustand nach Schritt 1 ist:

$$|\psi\rangle := \frac{1}{2} \cdot \Big(|00\rangle\big(\alpha|0\rangle + \beta|1\rangle\big) + |01\rangle\big(\alpha|1\rangle + \beta|0\rangle\big) + |10\rangle\big(\alpha|0\rangle - \beta|1\rangle\big) + |11\rangle\big(\alpha|1\rangle - \beta|0\rangle\big) \Big)$$

4. In Schritt 2 misst Alice ihre beiden ersten Qubits und schickt das Ergebnis $b_1\,b_2$ über den klassischen Kanal an Bob.

Alice hat ihr Qubit $\alpha|0\rangle + \beta|1\rangle$ verloren. Aber Bob kann das Qubit mit Hilfe von Bitflip- bzw. Phasenflip-Gattern rekonstruieren, denn er kennt $b_1\,b_2$.

Quanten-Turingmaschinen

Quanten-Turingmaschinen (1/5)

Eine Quanten-Turingmaschine (QTM) M wird durch das Tupel

$$M = (\Sigma, Q, q_0, q_F, \delta)$$

beschrieben.

- Σ ist das endliche Eingabe- und Arbeitsalphabet. Wir nehmen an, dass Σ das Blank-Symbol B enthält.
- Q ist die endliche Zustandsmenge, $q_0 \in Q$ ist der Anfangszustand und $q_F \in Q$ ist der (einzige) Haltezustand.
- Die Überführungsfunktion δ hat die Form $\delta : Q \times \Sigma \to \hat{\mathbb{C}}^{\Sigma \times Q \times \{L,R\}}$.
  - $\hat{\mathbb{C}}$ ist Menge aller komplexen Zahlen z, so dass det. TM Approximation Real- und Imaginärteil von z mit Fehler höchstens 2^{-n} in Zeit poly(n) bestimmt.
  - Für Zustand $q \in Q$ und Buchstaben $a \in \Sigma$ weist $\delta(q, a)$ jedem Tripel $(a', q', \beta) \in \Sigma \times Q \times \{L, R\}$ die komplexe Zahl $\alpha^{q,a}_{a',q',\beta} \in \hat{C}$ zu,

    nämlich die **„Amplitude“** des Übergangs $(q, a) \to (a', q', \beta)$.

- Die **Architektur** von M besteht aus:
  - einem beidseitig unendlichem Band, dessen Zellen mit ganzen Zahlen adressiert sind,
  - einem Lese/Schreibkopf, der in einem Schritt die gelesene Zelle überdrucken und zur linken oder rechten Nachbarzelle wandern kann.
- Eine **Konfiguration** von M besteht aus einer vollständigen Beschreibung des Bandinhaltes, der Kopfposition und des gegenwärtigen Zustands q.
  - Die Startkonfiguration besteht aus der in den Zellen $0, \ldots, n-1$ abgelegten Eingabe, der Kopfposition 0 und dem Anfangszustand q_0.
  - Eine Konfiguration heißt Haltekonfiguration, falls q_F der aktuelle Zustand der Konfiguration ist.
  - Die Ausgabe der Haltekonfiguration ist der Bandinhalt vom linkesten Nicht-Blank bis zum rechtesten Nicht-Blank.

- Wir fassen die Konfigurationen von M als Elemente einer Orthonormalbasis $\mathcal{C}$ auf. $\mathcal{V}_M$ ist die Menge aller Überlagerungen, also als die Menge aller endlichen komplexwertigen Linearkombinationen der Orthonormalbasis.
- Für endliche Teilmengen $C_u, C_v \subseteq \mathcal{C}$ und Zustände $|u\rangle = \sum_{c \in C_u} \beta_c \cdot |c\rangle$ und $|v\rangle = \sum_{c \in C_v} \gamma_c \cdot |c\rangle$ wird das innere Produkt definiert durch

$$\langle u|v\rangle := \sum_{c \in C_u \cap C_v} \overline{\beta_c} \cdot \gamma_c.$$

- Dann ist $\mathcal{V}_M$ ein Prähilbertraum und

$$\mathcal{H}_M := \left\{ \sum_c \alpha_c |c\rangle \ : \ \sum_c |\alpha_c|^2 < \infty \right\}$$

ist sein Hilbertraum.

- Die **Zeit-Evolution** U_M von M wird durch eine lineare Transformation von $\mathcal{H}_M$ beschrieben.
  - Die Matrix U_M besteht aus abzählbar unendlich vielen Zeilen und Spalten, die jeweils durch Konfigurationen von M indiziert sind.
  - In Zeile c und Spalte d wird die Amplitude für einen Ein-Schritt Übergang von c nach d eingetragen.
- Beachte, dass die Amplitude $U_M[c, d]$ nur abhängig ist von:
  - dem aktuellen Zustand q von c, dem gelesenen Buchstaben a von c,
  - dem neuen Zustand, dem zu druckenden Buchstaben und der gewählten Kopfbewegung von d.
- Wir fordern, dass U_M **unitär** ist.

Quanten-Turingmaschinen (5/5)

- Sei $|v^{(0)}\rangle \in \mathcal{V}_M$ der Zustand der Startkonfiguration, d.h. es gilt $v_c^{(0)} = 1$ genau dann, wenn c die Startkonfiguration ist und ansonsten $v_c^{(0)} = 0$.
- Wir sagen: M befindet sich zum Zeitpunkt k in der Überlagerung

$$\langle v^{(k)}| = \langle v^{(0)}| U_M^k .$$

  - Beachte, dass

$$\left(\langle v^{(0)}| U_M^k\right)[c, c_k] = \sum_{c_1,\ldots,c_k} U_M[c, c_1] \cdot \prod_{i=1}^{k-1} U_M[c_i, c_{i+1}].$$

  - Wir sagen, dass $U_M[c, c_1] \cdot \prod_{i=1}^{k-1} U_M[c_i, c_{i+1}]$ die Amplitude des Weges $(c, c_1, \ldots, c_k)$ ist und dass $v_d^{(k)}$ die Amplitude der Konfiguration d ist.
  - $v_d^{(k)}$ ist die Summe der Amplituden aller Wege der Länge k von c nach d.

Jede Amplitude von $\langle v^{(k)}|$ kann deterministisch auf polynomiellem Speicherplatz berechnet werden, solange $\log k = \text{poly}(n)$ gilt.

Berechnungen einer QTM (1/5)

Wir sagen, dass eine Überlagerung $|v\rangle \in \mathcal{V}_M$ eine Konfiguration c^* *enthält* bzw. dass c^* eine Konfiguration von $|v\rangle$ ist, wenn $|v\rangle = \sum_{c \in C} \alpha_c \cdot |c\rangle$ mit $\alpha_{c^*} \neq 0$ gilt.

Eine QTM M **hält** auf Eingabe x **nach T Schritten**, falls

(1) x der Inhalt des Bandes der Startkonfiguration c ist (also $v_c^{(0)} = 1$),

(2) $|v^{(t)}\rangle$ für $t < T$ keine Haltekonfiguration enthält,

(3) alle in $|v^{(T)}\rangle$ auftretenden Konfigurationen Haltekonfigurationen sind.

- Wenn M auf allen Eingaben hält, dann nennen wir M **wohl-definiert**.
- Die **Laufzeit** einer wohldefinierten QTM M auf Eingaben der Länge n ist das Maximum der Laufzeiten von M über alle Eingaben der Länge n.

Berechnungen einer QTM (2/5)

Eine QTM M **rechnet** auf Eingabe x **mit Speicherplatz höchstens S**, falls

(1) es Zeitpunkt T gibt, so dass M auf Eingabe x nach T Schritten hält und

(2) $|v^{(t)}\rangle$ zu jedem Zeitpunkt $t \leqslant T$ nur Konfigurationen mit höchstens S Zellen des Bands enthält.

Der **Speicherplatz** einer wohldefinierten QTM M auf Eingaben der Länge n ist der maximale Speicherplatz über alle Eingaben der Länge n.

Berechnungen einer QTM (3/5)

- Angenommen, die Zellen mit Positionen in der Menge P werden zum Zeitpunkt k beobachtet, und es ist $|v^{(k)}\rangle = \sum_c \alpha_c \cdot |c\rangle$.
- C_a ist Menge der Konfigurationen, deren Zellen in P den Wert a besitzen.

(a) Dann ist a **das Ergebnis der Beobachtung** mit Wahrscheinlichkeit

$$p_a = \sum_{c \in C_a} |\alpha_c|^2.$$

(b) Nach der Beobachtung der Zellen in P ist

$$\sqrt{\frac{1}{p_a}} \cdot \sum_{c \in C_a} \alpha_c \cdot |c\rangle$$

die aktuelle Überlagerung. Damit sind alle Konfigurationen verloren gegangen, deren Wert in den Positionen von P von a verschieden ist.

Berechnungen einer QTM (4/5)

(a) Wird die Zelle mit Adresse 0 zum Zeitpunkt T beobachtet und ist p_α die W-keit der Beobachtung 1, dann ist p_α die W-keit, dass M die Eingabe x **akzeptiert**.

(b) Werden alle Eingaben entweder mit W-keit mindestens $\frac{2}{3}$ oder höchstens $\frac{1}{3}$ akzeptiert, dann sagt man, dass M einen beschränkten Fehler hat und definiert

$$L(M) := \left\{ x \in \Sigma^* \;:\; M \text{ akzeptiert } x \text{ mit Wahrscheinlichkeit mindestens } \tfrac{2}{3} \right\}$$

als die von M akzeptierte Sprache.

(c) **„Quanten-**$\mathtt{PSPACE}$**“** wird definiert durch

$$\mathtt{QPSPACE} := \left\{ L(M) \;:\; \begin{array}{l} \text{die QTM } M \text{ rechnet mit Fehler höchstens } \frac{1}{3} \\ \text{auf polynomiellem Speicherplatz} \end{array} \right\}.$$

Man kann zeigen, dass

$$\mathtt{QPSPACE} = \mathtt{PSPACE}$$

gilt.

Berechnungen einer QTM (5/5)

Die Berechnungskraft von QTMs und uniformen Quanten-Schaltkreisen ist bis auf polynomielle Faktoren identisch.

(a) Die Quanten-Turingmaschine M rechne in Zeit $t(n)$.
Dann gibt es eine uniforme Familie $(S_n \mid n \in \mathbb{N})$ von Quanten-Schaltkreisen mit $\text{poly}(n + t(n))$ Gattern, so dass M und S_n auf Eingaben der Länge n Beobachtungen mit identischer Wahrscheinlichkeit besitzen.

(b) Die uniforme Familie $(S_n \mid n \in \mathbb{N})$ von Quanten-Schaltkreisen habe $t(n)$ Gatter.
Dann gibt es eine Quanten-Turingmaschine M mit Laufzeit $\text{poly}(n + t(n))$, so dass M und S_n auf Eingaben der Länge n Beobachtungen mit identischer W-keit haben.

Beweis: Siehe A. Yao, Quantum cicuit complexity, Proc. of the Symposium on Foundations of Computer Science, pp. 352-361, 1993.

BQP

Bounded-Error Quantum Polynomial Time

Familien von Quanten-Schaltkreisen

- Wir nehmen an, dass ein Quanten-Schaltkreis ein einziges Ausgabegatter g besitzt: Ist $|0\rangle$ das Ergebnis einer Messung von g, dann wird verworfen und ansonsten akzeptiert.
- Beachte: Messungen der Quellen verlaufen zufällig, ein Quanten-Schaltkreis berechnet also eine Zufallsvariable.

Eine Familie $(Q_n : n \in \mathbb{N})$ von Quanten-Schaltkreisen akzeptiert Sprache $L \subseteq \{0,1\}^*$ mit Fehlerwahrscheinlichkeit höchstens ε genau dann, wenn es zu jeder Eingabelänge n eine natürliche Zahl $m \in \mathbb{N}$ gibt, so dass

- Eingabe $|w\rangle \otimes |0^m\rangle$ genau dann mit Wahrscheinlichkeit mindestens $1 - \varepsilon$ von Q_n akzeptiert wird, wenn $w \in L$.
- Wenn $w \notin L$, dann wird $|w\rangle \otimes |0^m\rangle$ mit Wahrscheinlichkeit höchstens ε akzeptiert.

Komplexitätsklasse $\mathtt{BQP}_f$

Sei $f : \mathbb{N} \to [0, \frac{1}{2}]$ gegeben.

Die Komplexitätsklasse

$\mathtt{BQP}_f$ (Bounded-Error- Quantum-Polynomial-Time mit Fehler f)

besteht aus allen Sprachen, die von uniformen Familien $(S_n : n \in \mathbb{N})$ von Quanten-Schaltkreisen mit polynomieller Größe in n und Fehler höchstens $f(n)$ akzeptiert werden können.

- Für $f(n) = \frac{1}{3}$ ist $\mathtt{BQP} := \mathtt{BQP}_f$,
- $\mathtt{WeakBQP} := \bigcup_{k \in \mathbb{N}} \mathtt{BQP}_{\frac{1}{2} - n^{-k}}$ und
- $\mathtt{StrongBQP} := \bigcap_{k \in \mathbb{N}} \mathtt{BQP}_{2^{-n^k}}$.

Wie mächtig ist BQP?

$$\mathtt{P} \subseteq \mathtt{BPP} \subseteq \mathtt{WeakBQP} = \mathtt{BQP} = \mathtt{StrongBQP} \subseteq \mathtt{PP} \subseteq \mathtt{PSPACE} = \mathtt{QPSPACE}.$$

Beweis: Die Inklusionen $\mathtt{BPP} \subseteq \mathtt{BQP} \subseteq \mathtt{PP}$ werden gleich gezeigt.

Zur Vorbereitung der Nachweis $\mathtt{P} \subseteq \mathtt{BQP}$.

$\mathrm{P} \subseteq \mathrm{BQP}$

Simuliere eine Familie $\mathcal{S} = (S_n : n \in \mathbb{N})$ klassischer Schaltkreise durch Quanten-Schaltkreis Q_n vergleichbarer Größe.

Q_N besteht ausschließlich aus Toffoli-Gattern. Beachte:

- AND zusammen mit NOT ist universell für klassische Schaltkreise.
- $$\begin{aligned} \text{Toffoli}(|b_1 b_2 0\rangle) &:= |b_1 b_2\ \text{AND}(b_1 b_2)\rangle \text{ und} \\ \text{Toffoli}(|11 b\rangle) &:= |11\ \text{NOT}(b)\rangle \end{aligned}$$

Insbesondere: Jeder klassische Schaltkreis ist durch einen reversiblen klassischen Schaltkreis vergleichbarer Größe simulierbar.

Alle Sprachen in BPP können durch klassische, uniforme Schaltkreis- Familien polynomieller Größe akzeptiert werden,

wenn diese Schaltkreise auf Zufallsbits zugreifen dürfen.

Wie können k Zufallsbits „hergestellt“ werden?

Mit k parallel geschalteten Hadamard-Gattern, angewandt auf $|0^k\rangle$:

$$H^{\otimes k}|0^k\rangle := H|0\rangle \otimes \cdots \otimes H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \cdots \otimes \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$
$$= \frac{1}{\sqrt{2^k}} \cdot \sum_{r_1,\ldots,r_k \in \{0,1\}} |r_1 \cdots r_k\rangle.$$

Sei $S_n(x, r)$ ein konventioneller deterministischer Schaltkreis, der mit den Zufallsbits $r \in \{0,1\}^k$ rechnet.

- S_n kann mit Toffoli-Gattern und damit durch einen unitären Operator U simuliert werden.
- Es ist also $U|x, r, 0^m\rangle = |x, r,\ \text{müll}(x, r), S(x, r)\rangle$ und damit

$$U\Big(|x\rangle \otimes H^{\otimes k}(|0^k\rangle) \otimes |0^m\rangle\Big) = \frac{1}{\sqrt{2^k}} \cdot \sum_{r_1,\ldots,r_k \in \{0,1\}} U|x, r, 0^m\rangle$$

$$= \frac{1}{\sqrt{2^k}} \cdot \sum_{r_1,\ldots,r_k \in \{0,1\}} |x, r,\ \text{müll}(x, r), S(x, r)\rangle.$$

Die Messung des letzten Qubits beendet die Simulation $\Longrightarrow$

$$\text{BPP} \subseteq \text{BQP}.$$

Sei U die von einem Quanten-Schaltkreis Q_n polyn. Größe berechnete unitäre Matrix.

- O.B.d.A. bestehe Q_n nur aus Hadamard- und Toffoli-Gattern. Für Eingabe $x \in \{0,1\}^n$ ist das letzte Qubit in der Darstellung von $U|x0^m\rangle$ zu beobachten.
  - Die Wahrscheinlichkeit, dass Eingabe x akzeptiert wird, stimmt überein mit der Summe $|\alpha_z|^2$ über alle Basiszustände $z = |b_1 \cdots b_{m+n-1}1\rangle$.
    - ⋆ Jede Amplitude α_z ist eine Summe von (höchstens $2^{\text{poly}(n)}$ vielen) Amplituden $\alpha_{z,p}$, wobei jedes $\alpha_{z,p}$ determ. in Zeit poly(n) für $n = |x|$ berechenbar ist.
  - Berechne die folgende Summe in PP

$$-\frac{1}{2} + \sum_z |\alpha_z|^2 = -\frac{1}{2} + \sum_{z,p,q} \overline{\alpha_{z,p}} \cdot \alpha_{z,q}.$$

  - Übungsaufgabe: Ist jede der Zahlen $y_1, \ldots, y_{2^{\text{poly}(n)}}$ effizient deterministisch berechenbar, dann ist die Frage $-\frac{1}{2} + \sum_{i=1}^{2^{\text{poly}(n)}} y_i \stackrel{?}{>} 0$ in PP beantwortbar.
- BQP ⊆ PP folgt.

Quantenparallelität

Quantenparallelität (1/4)

Ein Quantenrechner kann in einem Schritt viele potenzielle Lösungen r erzeugen.

Für die unitäre Matrix U gelte

$$U|r, 0^m\rangle = |r, f(r)\rangle.$$

Dann ist

$$U \cdot H^{\otimes n}(|0^n\rangle) \otimes |0^m\rangle = \frac{1}{\sqrt{2^n}} \cdot \sum_{r \in \{0,1\}^n} |r, f(r)\rangle.$$

Aber wie findet man eine tatsächliche Lösung unter den potenziellen Lösungen?

Nutze Interferenzen auf nicht-triviale Weise aus!

Häufiges Problem: Berechne $|x, 0^m\rangle \mapsto |x, g(x)\rangle$ und nicht $|x, 0^m\rangle \overset{U}{\mapsto} |x, f(x)\rangle$, wobei

$$g(x) \neq f(x)$$

mit kleiner Wahrscheinlichkeit.

- Was ist das Problem?
  Die Berechnung ist randomisiert und damit möglicherweise fehlerhaft!
- $\texttt{BQP} = \texttt{StrongBQP} \Longrightarrow$ Mache Fehler negativ-exponentiell klein ✓

Quantenparallelität (3/4)

Angenommen, der komplizierte Operator U wird in mehreren Schritten durch die unitäre Berechnung V implementiert, also $|x0^n0^m\rangle \overset{V}{\mapsto} |x \text{ müll } f(x)\rangle$.

- Unitäre Berechnungen können Berechnungsspuren, also den Datenmüll, nicht einfach löschen.
- **Aber** unitäre Berechnungen lassen sich mit unitärer Berechnung umkehren:

Compute-Uncompute

1. **Amplify**: Berechne die Funktion f in `StrongBQP`.
2. **Compute**: Führe die zugehörige unitäre Berechnung V aus.
3. **Save**: Speichere das Ergebnis in einem dafür reservierten Qubit.
   - Wende zum Beispiel das Controlled-Not-Gatter auf die Qubits $|f(x)0\rangle$ an.
4. **Uncompute**: Berechne V^{-1}.

Orakel-Berechnungen (4/4)

Als Konsequenz erhalten wir das $\mathtt{BQP}$**-Subroutine-Theorem**:

$$\mathtt{BQP}^{\mathtt{BQP}} = \mathtt{BQP}.$$

$\mathtt{BQP}$-Berechnungen mit einem $\mathtt{BQP}$-Orakel sind $\mathtt{BQP}$-Berechnungen.

Wir können also davon ausgehen, dass ein effizienter Quanten-Algorithmus andere effiziente Quanten-Algorithmus komplikationsfrei, also

ohne akkumulierende Fehler und unerwünschte Berechnungsspuren

aufrufen kann.

Grover's Algorithmus

Das Suchproblem

- Sei $f : \{0,1\}^n \to \{0,1\}$ eine boolesche Funktion.
- Wir nehmen an, dass es ein Orakel für f gibt, das auf Anfrage $x \in \{0,1\}^n$ den Wert $f(x)$ ausgibt.
- Insbesondere nehmen wir an, dass es einen unitären Operator O gibt mit

$$|x\rangle \overset{O}{\mapsto} (-1)^{f(x)} \cdot |x\rangle.$$

Im **Suchproblem zu f** möchten wir eine **Lösung** x, also ein Wort x mit $f(x) = 1$ bestimmen und dürfen dazu das Orakel für f verwenden.

Anwendungen für das Suchproblem

Klassische Algorithmen benötigen im Worst-Case 2^n Anfragen an das Orakel.

(1) Suche in einer **Datenbank** mit N Schlüsseln $x_1, \ldots, x_N$ nach Schlüssel y.

- Durch Hinzunahme geeignet vieler Kopien des Schlüssels 0 kann angenommen werden, dass $N = 2^n$ gilt.
- Definiere die „boolesche“ Funktion f durch $f(i) = \begin{cases} 1 & y = x_i \\ 0 & \text{sonst.} \end{cases}$
- Eine Lösung des Suchproblems zu f löst das Suchproblem für Datenbanken.

(2) Für eine KNF α mit den aussagenlogischen Variablen $X_1, \ldots, X_n$ frage nach einer **erfüllenden Belegung**

$$f(x) = \begin{cases} 1 & \alpha(x) = 1 \\ 0 & \text{sonst.} \end{cases}$$

Quanten-Algorithmen lösen das Suchproblem mit $\mathcal{O}(2^{n/2})$ Anfragen an das Orakel.

Diffusionsoperator

Sei $f : \{0,1\}^n \to \{0,1\}$ eine durch effiziente Quanten-Algorithmen berechenbare Funktion.

Grover's Algorithmus löst das Suchproblem zu f mit Wahrscheinlichkeit mindestens $\frac{2}{3}$ und wendet den Orakeloperator O höchstens $\mathcal{O}(2^{n/2})$ Mal an.

- Der Worst-Case: Es gibt genau eine Lösung x^* des Suchproblems zu f.
- Der **Diffusionsoperator** D überführt alte Amplituden α_x in neue Amplituden $2\mu - \alpha_x$, wobei μ die durchschnittliche Amplitude ist:

$$\sum_{x \in \{0,1\}^n} \alpha_x \cdot |x\rangle \overset{D}{\mapsto} \sum_{x \in \{0,1\}^n} (2\mu - \alpha_x) \cdot |x\rangle.$$

  - D ist unitär, denn D ist linear und D bewahrt Längen. Details: Übungsaufgabe
  - D bewahrt die durchschnittliche Amplitude. Details: Übungsaufgabe

Was ist die Wirkung von D auf eine negative Amplitude α, wenn μ positiv ist?

α wird ersetzt durch die überdurchschnittlich große Amplitude $2\mu - \alpha$.

Grover's Algorithmus

1. Wende das Tensorprodukt $H^{\otimes n}$ auf den Zustand $|0^n\rangle$ an. Der neue Zustand ist

$$z := H^{\otimes n}|0^n\rangle = \frac{1}{2^{n/2}} \cdot \sum_{x \in \{0,1\}^n} |x\rangle.$$

2. Setze $t = 0$. Wiederhole die folgenden Schritte $c \cdot 2^{n/2}$-mal:

   (a) Führe eine Anfrage x an das Orakel aus: Wenn $z = \sum_{x \in \{0,1\}^n} \gamma_x |x\rangle$ der alte Zustand ist, dann ist $z' = \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \cdot \gamma_x |x\rangle$ der neue Zustand.

   - ⋆ Der „Orakel-Operator"

$$|x\rangle \overset{O}{\mapsto} (-1)^{f(x)} \cdot |x\rangle$$

   ist unitär, denn O ist linear und bewahrt Längen.

   (b) Wende den Diffusionsoperator auf Zustand z' an. Der neue Zustand ist

$$z := D|z'\rangle = \alpha^{(t)}|x^*\rangle + \sum_{x \in \{0,1\}^n, x \neq x^*} \beta^{(t)} \cdot |x\rangle,$$

   wobei $\alpha^{(t)}$ und $\beta^{(t)}$ die Amplituden von x^* bzw x (für $x \neq x^*$) nach der t.ten Anwendung von D sind.

3. Beobachte $|z\rangle$.

Analyse: Grover's Algorithmus (1/3)

$\alpha^{(t)}$ und $\beta^{(t)}$ sind die Amplituden von x^* bzw. x ($x \neq x^*$) nach der t.ten Anwendung von D, $\mu^{(t)}$ ist die durchschnittliche Amplitude nach der t.ten Anfrage an das Orakel.

- $\alpha^{(0)} = \beta^{(0)} = \mu^{(0)} = 2^{-n/2}$.
- Nach der ersten Anfrage an das Orakel für f ist der aktuelle Zustand

$$\frac{-1}{2^{n/2}} \cdot |x^*\rangle + \frac{1}{2^{n/2}} \cdot \sum_{x \in \{0,1\}^n, x \neq x^*} |x\rangle$$

und die durchschnittliche Amplitude ist

$$\mu^{(1)} := \frac{1}{2^n} \cdot \left(-\frac{1}{2^{n/2}} + \frac{2^n - 1}{2^{n/2}} \right) = \frac{2^n - 2}{2^{3n/2}} < \frac{1}{2^{n/2}}.$$

- Nach Anwendung des Diffusionsoperators erhält $|x^*\rangle$ die Amplitude

$$\alpha^{(1)} = 2\mu^{(1)} + 2^{-n/2} \approx \frac{3}{2^{n/2}}.$$

Die Amplituden aller anderen Basiszustände fallen leicht.

Analyse: Grover's Algorithmus (2/3)

Es ist $\alpha^{(t)} = 2\mu^{(t-1)} + \alpha^{(t-1)}$ und $\beta^{(t)} = 2\mu^{(t-1)} - \beta^{(t-1)} \leqslant \beta^{(t-1)}$.

Steigt $\alpha^{(t)}$ „lange genug“ um $\theta(2^{-n/2})$ an?

Achtung: Die durchschnittliche Amplitude, und damit auch der Anstieg von $\alpha^{(t)}$ gegenüber $\alpha^{(t-1)}$, sinkt leicht!

Wenn $\mu^{(t)} = \Omega(2^{-n/2})$ für $t \leqslant$ Konstante $\cdot\, 2^{n/2}$, dann folgt die Behauptung, denn

$$\alpha^{(t+1)} = 2\mu^{(t)} + \alpha^{(t)} \stackrel{!}{=} \Omega(\frac{1}{2^{n/2}}) + \alpha^{(t)}$$

und nach Konstante $\cdot\, 2^{n/2}$ Schritten wird x^* mit nicht-vernachlässigbarer W-keit beobachtet.

Das vollständige Argument wird im Skript beschrieben.

Analyse: Grover's Algorithmus (3/3)

Um den Fehler von Grover's Algorithmus auf höchstens $\frac{1}{3}$ zu beschränken, muss der Algorithmus mit geeigneter Häufigkeit wiederholt werden.

Weitere Bemerkungen zur Analyse:

(a) Der Diffusionsoperator kann mit $\mathcal{O}(n)$ Hadamard- und Toffoli-Gattern implementiert werden. Grover's Algorithmus benötigt somit höchstens $\mathcal{O}(n \cdot 2^{n/2})$ Gatter.

(b) Die folgende Verallgemeinerung kann gezeigt werden:

> *Wenn es einen Quanten-Algorithmus A gibt, der mit Wahrscheinlichkeit p eine Lösung für $f : \{0,1\}^n \to \{0,1\}$ findet, dann findet eine Variante von Grover's Algorithmus eine Lösung nach höchstens $\mathcal{O}(1/\sqrt{p})$ Anwendungen von A. (Achtung: Beachte Laufzeit von A.)*

Grover's Algorithmus ist im Orakel-Modell optimal

Liegen NP-vollständige Probleme in BQP?

+ Die Kraft der Quanten-Parallelität hat sich in Grover's Algorithmus gezeigt.
- Aber Restriktionen von Quantenrechnungen haben sich bisher für eine Lösung NP-vollständiger Probleme als viel zu einschneidend erwiesen.
! Wir zeigen: Es gibt ein „dünnes" Orakel $A \subseteq \{0,1\}^*$ mit $\mathrm{NP}^A \not\subseteq \mathrm{BQP}^A$.

  Das Orakel A ist dünn, wenn A für jede natürliche Zahl n höchstens ein Wort der Länge n besitzt.

  - Die Sprache $L_A := \{\, 1^n : A \cap \{0,1\}^n \neq \emptyset \,\}$ gehört offensichtlich zu NP^A:
    - Rate $x \in A \cap \{0,1\}^n$ und stelle x als Anfrage.
  - Wir zeigen, dass L_A nicht zu BQP^A gehört.

Neben einer Trennung von NP^A und BQP^A zeigen wir auch, dass Grover's Algorithmus mit einer asymptotisch minimalen Anzahl von Anfragen arbeitet.

Optimalität von Grover's Algorithmus (1/3)

Mit W-keit 1 (über alle dünnen Orakel A) beobachtet ein Quantenalgorithmus Q eine Lösung $x \in A \cap \{0,1\}^n$ nur nach mindestens $\Omega(2^{n/2})$ Anfragen an das Orakel.

Die Ausgangslage für Eingabelänge n:

- Das Orakel antwortet stets mit NEIN!?
- In Iteration t führt Q den unitären Operator U_t aus und stellt dann eine Anfrage F_t.
  - Die Basiszustände von Q nach Ausführung von U_t und vor Anfrage F_t sind

    $|x, z, t\rangle$ für den Arbeitsspeicher z und die Anfrage x.
  - Der „Systemzustand" vor der Anfrage ist $\sum_{x \in \{0,1\}^n, z} \alpha_{x,z,t} |x, z, t\rangle$.
  - Die „Amplitude" der Anfrage x zur Zeit t wird definiert als die reelle Zahl

$$\alpha_{x,t} := \sqrt{\sum_z |\alpha_{x,z,t}|^2}.$$

- Q führt bis zu T Iterationen durch. Allerdings führt Q in der letzten Iteration eine Beobachtung anstelle der Anfrage F_T durch.

Optimalität von Grover's Algorithmus (2/3)

$$q_x := \sum_{t=1}^{T} \sum_{z} |\alpha_{x,z,t}|^2 = \sum_{t=1}^{T} \alpha_{x,t}^2$$

ist eine obere Schranke für die W-keit, dass *irgendwann* nach x gefragt wird. Also ist

$$\sum_{x \in \{0,1\}^n} q_x = \sum_{t=1}^{T} \Big(\underbrace{\sum_{x \in \{0,1\}^n} \sum_{z} |\alpha_{x,z,t}|^2}_{\text{zur Zeit } t \text{ wird irgendeine Anfrage gestellt}} \Big) = \sum_{t=1}^{T} 1 = T.$$

Also gibt es x_0 mit $q_{x_0} \leqslant T/2^n$ und deshalb folgt $q_{x_0} = \sum_{t=1}^{T} \alpha_{x_0,t}^2 \leqslant T/2^n$.

Aus der Ungleichung $\langle u|v\rangle \leqslant \|u\| \cdot \|v\|$ von Cauchy-Schwartz folgt

$$\sum_{t=1}^{T} \alpha_{x_0,t} \leqslant \sqrt{\sum_{t=1}^{T} \alpha_{x_0,t}^2} \cdot \sqrt{T} \leqslant \frac{T}{\sqrt{2^n}}.$$

Optimalität von Grover's Algorithmus (3/3)

Wie sollte ein schwieriges Orakel A für Q aussehen?

- x_0 ist eine potenzielle Lösung, die von Q im „NEIN-Szenario“ mit Wahrscheinlichkeit höchstens q_{x_0} nachgefragt wird.
- Ab jetzt nehmen wir an, dass A alle Anfragen verneint bis auf die Anfrage nach x_0.

Wie verändern sich die Amplituden $\alpha_{x_0,T}$ im Unterschied zum NEIN-Szenario?

(*) Für die erste Iteration ($t = 1$) ist $\alpha_{x_0,z,1}$ durch $\alpha'_{x_0,z,1} := -\alpha_{x_0,z,1}$ zu ersetzen.

- Es ist $(\alpha'_{x_0,1})^2 = \alpha^2_{x_0,1}$ zur Zeit 1.
- Der *unitäre* Operator U_2 verändert $(\alpha'_{x_0,1})^2$ ebenfalls nicht.

(*) Auch in den nachfolgenden Iterationen t gilt $(\alpha'_{x_0,t})^2 = \alpha^2_{x_0,t}$.

$$\Longrightarrow \quad (\alpha'_{x_0,T})^2 = \alpha^2_{x_0,T} \leqslant \Big(\sum_{t=1}^{T} \alpha_{x_0,t}\Big)^2 \leqslant \frac{T^2}{2^n}$$

Um x_0 (mit W-keit mindestens $\frac{2}{3}$) zu beobachten, muss $T = \Omega(2^{n/2})$ gelten $\Longrightarrow$

Grover's Algorithmus ist optimal!

Trennung von NP^A und BQP^A

Es gibt ein Orakel A mit $\mathrm{NP}^A \not\subseteq \mathrm{BQP}^A$.

- Es ist stets $L_A \in \mathrm{NP}^A$. Zeige: $L_A \notin \mathrm{BQP}^A$.
- Das bisherige Argument zeigt: Unterschied in Beobachtungs-W-keiten zwischen NEIN-Szenario und allgemeinem Szenario ist vernachlässigbar!
- Für jeden Quanten-Algorithmus Q, jede Eingabelänge n und mindestens 50% aller dünnen Orakel $A_n \subseteq \{0,1\}^n$:

  Q unterscheidet nicht zwischen L_{A_n} und der leeren Menge.
- Baue alle möglichen „Zufalls-Orakel“ A:

  Für jedes n wähle $A \cap \{0,1\}^n = \emptyset$ oder $|A \cap \{0,1\}^n| = 1$.

Simon's Algorithmus

Ist BQP mächtiger als BPP?

- Viele Anzeichen (z.B. Shor's Algorithmus) deuten auf $\mathtt{BPP} \subset \mathtt{BQP}$ hin.
- Hier zeigen wir: Es gibt ein Orakel A, so dass $\mathtt{BPP}^A \subset \mathtt{BQP}^A$.
- Das Orakel A verbirgt eine Funktion $f_n : \{0,1\}^n \to \{0,1\}^n$ für jedes n :
  - Für eine Anfrage $x \in \{0,1\}^n$ wird A mit dem Funktionswert $f_n(x)$ antworten.
  - f_n ist „2-bijektiv“ mit „Geheimnis“ $s \in \{0,1\}^n$, d.h.: x und y *kollidieren* genau dann (d.h. es ist $f_n(x) = f_n(y)$ für $x \neq y$), wenn $x = y \oplus s$ gilt.

Bestimme das Geheimnis nach möglichst wenigen Anfragen an Orakel A.

Simon's Algorithmus

1. Starte in Zustand $|0^n\rangle|0^n\rangle$, wende den Hadamard-Operator $H^{\otimes n}$ auf die ersten n Qubits und danach den Anfrageoperator A auf die zweiten n Qubits an.

$$|0^n\rangle|0^n\rangle \overset{H^{\otimes n}}{\mapsto} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|0^n\rangle \overset{A}{\mapsto} \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle|f(x)\rangle.$$

   - Beobachte die zweiten n Qubits. Als Konsequenz kollabiert der Zustand zu

$$|z\rangle := \frac{1}{\sqrt{2}}\Big(|x\rangle + |x \oplus s\rangle\Big) \otimes |f(x)\rangle$$

   - Ab jetzt werden die zweiten n Qubits nicht mehr beachtet.

2. Wiederhole $\mathcal{O}(n)$-Mal: Führe den Hadamard-Operator $H^{\otimes n}$ auf den ersten n Quibts aus und beobachte das Ergebnis.

3. Bestimme s mit einem linearen Gleichungssystem aus den Beobachtungen.

Lineares Gleichungssystem für Geheimnis s

$$
\begin{aligned}
H^{\otimes n}|z\rangle &= \frac{1}{\sqrt{2^n}}\Big(\sum_{y\in\{0,1\}^n}(-1)^{\langle x,y\rangle_2}|y\rangle + \sum_{y\in\{0,1\}^n}(-1)^{\langle x\oplus s,y\rangle_2}|y\rangle\Big) \\
&= \frac{1}{\sqrt{2^n}}\Big(\sum_{y\in\{0,1\}^n}(-1)^{\langle x,y\rangle_2}\big(1+(-1)^{\langle s,y\rangle_2}\big)|y\rangle\Big),
\end{aligned}
$$

denn in $\mathbb{Z}_2$ gilt $\langle x\oplus s,y\rangle_2 = \langle x,y\rangle_2 \oplus \langle s,y\rangle_2$.

- Die Amplitude von y ist genau dann von Null verschieden, wenn $\langle s,y\rangle_2 = 0$. Bei erneuter Beobachtung ist das Ergebnis also ein zufälliges Wort

$$y^{(1)} \in \{\, y\in\{0,1\}^n \,:\, \langle s,y\rangle_2 = 0 \,\}.$$

- Wiederhole bis $n-1$ lin. unabh. Zustände $y^{(1)},\ldots,y^{(n-1)}$ beobachtet wurden.
- Bestimme Geheimnis s aus dem linearen Gleichungssystem $Y\cdot s = 0$ für

$$Y = \begin{pmatrix} y^{(1)} \\ \cdots \\ y^{(n-1)} \end{pmatrix}.$$

Trennung von $\mathtt{BPP}^A$ und $\mathtt{BQP}^A$ (1/5)

(a) Simon's Algorithmus findet das Geheimnis $s \in \{0,1\}^n$ mit W-keit mindestens $\frac{2}{3}$, ein Quanten-Schaltkreis mit $\mathcal{O}(n)$ Hadamard- und Toffoli-Gattern ist ausreichend.

(b) Ein klassischer randomisierter Algorithmus findet das Geheimnis nach einer erwarteten Anzahl von $\mathcal{O}(2^{n/2})$ Anfragen an das Orakel.

- Benutze das Geburtstags-Paradox.

(c) Jeder randomisierte Algorithmus benötigt aber mindestens $\Omega(2^{n/2})$ Anfragen.

(d) Es gibt ein Orakel A mit $\mathtt{BPP}^A \not\subseteq \mathtt{BQP}^A$.

Warum benötigen randomisierte Algorithmen so viele Anfragen?

Beweis (b)

- Ziehe zufällig N Worte $x_1, \ldots, x_N \in \{0,1\}^n$.
- *Kollidieren* Worte x_i, x_j mit $i \neq j$, dann ist $s = x_i \oplus x_j$ und das Geheimnis ist gelüftet.
- Die gezogenen Worte bilden $\binom{N}{2}$ Paare, wobei die beiden Worte eines Paars mit Wahrscheinlichkeit $\frac{1}{2^n-1}$ kollidieren.
  - Für die erwartete Anzahl K_N an Kollisionen gilt deshalb

$$K_n = \binom{N}{2} \cdot \frac{1}{2^n - 1} \approx \frac{N^2}{2^{n+1}}.$$

  - Für eine Konstante c und $N := c \cdot 2^{n/2}$ ist also $K_N = \Theta(c^2)$.
- Für eine geeignet große Konstante c gibt es eine Kollision mit Wahrscheinlichkeit mindestens $\frac{2}{3}$. □

Beweis (c,d)

- Betrachte das „**Zufallsorakel**“ A, das für jedes n mit W-keit $\frac{1}{2}$ entweder eine zufällig bijektive Funktion oder eine zufällige 2-bijektive Funktion (mit Geheimnis) auswürfelt.
- Sei R ein randomisierter Algorithmus, der N Anfragen an das Zufallsorakel stellt: R muss entscheiden, ob die Funktion des Orakels bijektiv oder 2-bijektiv ist.
  - R fällt Zufallsentscheidungen und kann deshalb als Folge $(D_w : w \in \{0,1\}^*)$ deterministischer Algorithmen angesehen werden.
  - Zeige: Jeder deterministische Algorithmus D muss mindestens $\Omega(2^{n/2})$ Anfragen stellen, um einen Fehler von höchstens $\frac{1}{3}$ zu erreichen!
  - $\Longrightarrow$ R muss mindestens $\Omega(2^{n/2})$ Anfragen stellen.

Beweis (c,d): Eine untere Schranke für deterministische Algorithmen

- **Fall 1**: Die Funktion des Orakels ist bijektiv.
  - Jede Folge von N Funktionswerten ist gleichwahrscheinlich.
- **Fall 2**: Die Funktion des Orakels ist 2-bijektiv.
  - Taucht kein Funktionswert 2-mal auf:

    Alle Antwort-Folgen auch diesmal gleichwahrscheinlich!
  - Jeder Versuch, bijektive und 2-bijektive Funktionen zu unterscheiden, führt zu vernachlässigbaren Erfolgswahrscheinlichkeiten.

Zeige: Bei $N = o(2^{n/2})$ Anfragen treten Funktionswerte nur mit W-keit $o(1)$ 2-mal auf.

Fortsetzung Beweis (c,d)

- Also folgt

$$\begin{aligned} & \text{prob}[\,\text{bei } N \text{ Anfragen taucht kein Funktionswert 2-mal auf }\,] \\ = & \prod_{k=2}^{N-1} \text{prob}[\,k+1 \text{ Anfragen sind ohne Kollision} \mid k \text{ Anfragen sind ohne Kollision}\,] \\ = & \prod_{k=2}^{N-1} \left(1 - \frac{k}{2^n - \binom{k}{2} - 1}\right) \geqslant 1 - \sum_{k=2}^{N-1} \frac{k}{2^n - \binom{k}{2} - 1}. \end{aligned}$$

- Die Wahrscheinlichkeit, dass $N = o(2^{n/2})$ Anfragen keine Kollisionen besitzen, ist mindestens $1 - o(1)$. Warum? (Aufgabe)

Behauptung (c) folgt.

Für Teil (d) baue ein „deterministisches“ Orakel aus dem Zufallsorakel. □

Zusammenfassung

Zusammenfassung (1/2)

- Die Zustände eines Quantensystems sind Vektoren (Überlagerungen) in einem Hilbertraum $\mathcal{H}$.
  - Ein Quanten-System rechnet durch Anwendung von **unitären Operatoren** $U : \mathcal{H} \to \mathcal{H}$ auf Überlagerungen.
  - Eine Beobachtung schließt die Berechnung ab: Die Born-Regel legt die Wahrscheinlichkeit eines Beobachtungsergebnisses fest.
- Die **Born-Regel**: Sei H ein hermitescher Operator.
  - Das Ergebnis der Messung von H ist ein Eigenvektor λ von H.
  - Der aktuelle Zustand kollabiert in die Projektion auf den Eigenraum von λ.
- Quantenberechnungen erlauben quadratische Beschleunigung für unstrukturierte Suche (**Grover's Algorithmus**).
  - Eine effiziente Lösung NP-vollständiger Probleme ist nicht zu erwarten.
  - Die Optimalität von Grover's Algorithmus liefert ein (allerdings schwaches) Indiz dafür, dass NP-harte Probleme *nicht* in BQP liegen.
- Quantenberechnungen sind randomisierten Berechnungen überlegen, wenn nach Mustern in Eingabe zu suchen ist (**Simon's Algorithmus**).

Zusammenfassung (2/2)

- Die Komplexitätsklasse $\mathtt{BQP}$ besteht aus allen Sprachen, die sich durch
  - Quanten-Schaltkreise polynomieller Größe oder
  - Quanten-Turingmaschinen polynomieller Laufzeit

  mit Fehlerwahrscheinlichkeit höchstens $\frac{1}{3}$ akzeptieren lassen.
- Es gibt ein Orakel A mit $\mathtt{NP}^A \not\subset \mathtt{BQP}^A$:
  - Effiziente Quantenberechnungen haben also vermutlich nicht die Berechnungskraft effizienter nichtdeterministischer Berechnungen.
- Es ist $\mathtt{BPP} \subseteq \mathtt{BQP}$, denn
  - zum Einen gelingt eine effiziente Simulation deterministischer Berechnungen mit Hilfe von Toffoli-Gattern und
  - zum Anderen genügen Hadamard-Gatter für die Erzeugung des Zufalls.

  Als Konsequenz von Simon's Algorithmus kann die Existenz eines Orakels A mit $\mathtt{BPP}^A \subset \mathtt{BQP}^A$ gezeigt werden.
- Eine „Simulation" von $\mathtt{BQP}$ gelingt in der Klasse $\mathtt{PP}$, die ihrerseits in der Klasse $\mathtt{PSPACE}$ enthalten ist.

Die Quanten-Fourier-Transformation

Einheitswurzeln

- Die n Potenzen $\exp^{2\pi i \cdot k/n}$ für $k = 0, \ldots, n-1$ sind die $n$ten Einheitswurzeln, also Wurzeln des Polynoms $x^n - 1$.
- $w_n = \exp^{2\pi i/n}$ ist eine primitive $n$te Einheitswurzel.
- Die Einheitswurzeln bilden eine multiplikative Gruppe, denn

$$\exp^{2\pi i \cdot j/n} \cdot \exp^{2\pi i \cdot k/n} = \exp^{2\pi i \cdot (j+k \mod n)/n}.$$

Fourier-Transformation

Die diskrete Fourier-Transformation

$$x \mapsto F_n \cdot x$$

wird durch die Matrix

$$F_n := \frac{1}{\sqrt{n}} \cdot \left(w_n^{j \cdot k}\right)_{0 \leqslant j,k \leqslant n-1}$$

beschrieben, wobei $w_n := \exp^{2\pi i/n}$ der Einheitsvektor mit Winkel $2\pi/n$ ist.

Die Komponenten

$$\hat{x}_\ell := (F_n \cdot x)_\ell = \frac{1}{\sqrt{n}} \cdot \sum_{k=0}^{n-1} w_n^{\ell \cdot k} x_k$$

(für $\ell = 0, \ldots, n-1$) heißen **Fourier-Koeffizienten** von x.

Interpolation

Für einen Vektor $x \in \mathbb{C}^n$ betrachte das Polynom

$$p(z) := \frac{1}{\sqrt{n}} \cdot \sum_{k=0}^{n-1} x_k \cdot z^k$$

mit Koeffizientenvektor x. Die diskrete Fourier-Transformation lässt sich als Auswertung von p an allen $n$ten Einheitswurzeln auffassen, denn

$$F_n \cdot x = \hat{x} = (p(w_n^\ell) \ : \ 0 \leqslant \ell \leqslant n-1).$$

Die Matrix F_n

Die Matrix F_n ist **unitär**. Warum?

- Spalte k hat Länge Eins, denn $\sum_{j=0}^{n-1} \left(\frac{1}{\sqrt{n}}\right)^2 \cdot w_n^{-j\cdot k} w_n^{j\cdot k} = 1.$
- Da die Einheitswurzeln die Wurzeln von $x^n - 1$ sind, entspricht ihre Differenz dem Koeffizienten von x^{n-1}.
- Dieser Koeffizient verschwindet $\Longrightarrow$ die Summe der Einheitswurzeln verschwindet und die Spalten k_1, k_2 für $k_1 \neq k_2$ stehen senkrecht aufeinander:

$$\sum_{j=0}^{n-1} \left(\frac{1}{\sqrt{n}} w_n^{-j\cdot k_1}\right) \cdot \left(\frac{1}{\sqrt{n}} w_n^{j\cdot k_2}\right) = \frac{1}{n} \cdot \sum_{j=0}^{n-1} w_n^{-j\cdot(k_1-k_2)} = 0.$$

Das Inverse von F_n stimmt mit ihrer Adjungierten überein und F_n ist unitär.

Quanten-Fourier-Transformation (1/6)

Sei $N = 2^n$. Die **Quanten-Fourier-Transformation (QFT)**

$$F_N : \mathbb{C}^N \to \mathbb{C}^N$$

besitzt einen Quanten-Schaltkreis mit $\mathcal{O}(n \log n)$ Gattern.

Was ist der Unterschied zur klassischen Fourier-Transformation $x \mapsto F_n \cdot x$?

- Die klassische Fouriertransformation F_N hat nur Implementierungen durch klassische Schaltkreise mit $\mathcal{O}(N \log_2 N)$ Gattern:

  Eine exponentiell kleinere Anzahl von Gattern im Vergleich zur klassischen Fourier-Transformation!

- Aber, das Ergebnis der QFT bei vollständiger Beobachtung ist nur ein Fourier-Koeffizient!

Wir bauen einen Quanten-Schaltkreis Q, der die Transformation

$$|b_1 \cdots b_n\rangle \mapsto F_N |b_1 \cdots b_n\rangle$$

für jeden n-Qubit-Zustand $|b_1 \cdots b_n\rangle$ berechnet.

- Da Q einen unitären (und damit insbesondere einen linearen) Operator berechnet, wird Q wie gewünscht die QFT berechnen.
- Für $c = c_1 \cdots c_n \in \{0,1\}^n$ identifiziere die Zustände $|c_1 \cdots c_n\rangle$ und $|\text{zahl}(c)\rangle$ wobei $\text{zahl}(c) := \sum_{\ell=1}^{n} c_\ell 2^{n-\ell}$.

Da $N = 2^n$ ist

$$\begin{aligned}
F_N|b_1 \cdots b_n\rangle &= \frac{1}{\sqrt{N}} \cdot \sum_{a\in\{0,1\}^n} \exp^{2\pi i \cdot \text{zahl}(a)\cdot\text{zahl}(b)/N} |a\rangle \\
&= \frac{1}{\sqrt{N}} \cdot \sum_{a\in\{0,1\}^n} \exp^{2\pi i \cdot (\sum_{\ell=1}^{n} a_\ell 2^{n-\ell})\cdot\text{zahl}(b)/2^n} |a\rangle \\
&= \frac{1}{\sqrt{N}} \cdot \sum_{a\in\{0,1\}^n} \prod_{\ell=1}^{n} \exp^{2\pi i \cdot a_\ell \cdot \text{zahl}(b)/2^\ell} |a\rangle \\
&= \bigotimes_{\ell=1}^{n} \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + \exp^{2\pi i \cdot \text{zahl}(b)/2^\ell} |1\rangle\right) \\
&= \bigotimes_{\ell=1}^{n} \frac{1}{\sqrt{2}} \cdot \Big(\underbrace{|0\rangle + \exp^{2\pi i \cdot 0.b_{n-\ell+1}\cdots b_n} |1\rangle}_{=:|z_\ell\rangle}\Big),
\end{aligned}$$

denn $\exp^{2\pi i \cdot m} = 1$ für $m \in \mathbb{Z}$ und nur die niedrigsten ℓ Bits von b sind relevant.

Das Ergebnis ist also ein Produkt-Zustand!

Berechne $|z_\ell\rangle$.

- Für $\ell = 1$ ist

$$|z_1\rangle := \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + \exp^{2\pi i \cdot 0.b_n} |1\rangle\right) = \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + (-1)^{b_n}|1\rangle\right) = H|b_n\rangle.$$

  Eine Anwendung des Hadamard-Gatters auf das $n$te Qubit genügt.

- Für Qubits $|b_n\rangle, \ldots, |b_1\rangle$ wird mit dem Controlled-$P_{2\pi/2^s}$-Gatter C_P^s gearbeitet. Hier ist seine unitäre Matrix:

$$C_P^s := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & \exp^{2\pi i/2^s} \end{pmatrix}.$$

  Beachte, dass C_P^s die Qubits $|00\rangle, |01\rangle, |10\rangle$ nicht verändert, aber $|11\rangle$ mit $\exp^{2\pi i/2^s}$ multipliziert: Das erste Qubit kontrolliert das zweite.

Es ist

$$C_P^2\left(|b_n\rangle \otimes H|b_{n-1}\rangle\right) = C_P^2\left(|b_n\rangle \otimes \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + \exp^{2\pi i \cdot 0.b_{n-1}} |1\rangle\right)\right)$$
$$= |b_n\rangle \otimes \frac{1}{\sqrt{2}} \cdot \left(|0\rangle + \exp^{2\pi i \cdot 0.b_{n-1}b_n} |1\rangle\right) = |b_n\rangle \otimes |z_2\rangle.$$

Beachte: Die Berechnung von $|z_1\rangle$ muss *nach* der Berechnung von $|z_2\rangle$ erfolgen, denn die Berechnung von $|z_1\rangle$ verändert das $n$te Qubit.

- Wie bestimmt man $|z_3\rangle$?
  - Wende das Hadamard-Gatter auf das $(n-2)$.te Qubit an, danach C_P^2 – kontrolliert durch das $(n-1)$.te Qubit – und letztlich C_P^3 – kontrolliert durch das $n$te Qubit.
  - Auch hier ist die Reihenfolge der Berechnungen umzukehren: Zuerst bestimme $|z_3\rangle$, danach $|z_2\rangle$ und schließlich $|z_1\rangle$.
- Allgemein: In der Berechnung von $|z_{k+1}\rangle$,
  - wende das Hadamard-Gatter auf das $(n-k)$.te Qubit an,
  - danach C_P^2 – kontrolliert durch das $(n-k+1)$.te Qubit – . . .
  - bis letztlich C_P^{k+1} – kontrolliert durch das n.te Qubit – angewandt wird.

Quanten-Fourier-Transformation (6/6)

Die Quanten-Fourier-Transformation

$$|x\rangle \mapsto F_{2^n}|x\rangle$$

kann durch einen Quanten-Schaltkreis mit $\mathcal{O}(n^2)$ Gattern berechnet werden.

Für eine approximative Bestimmung genügen Quanten-Schaltkreis mit $\mathcal{O}(n \log_2 n)$ Gattern, denn

$$\exp^{2\pi i/2^s} \approx 1$$

gilt für große Werte von s.

Schnelle Faktorisierung

Schnelle Faktorisierung

Bestimme die Primfaktorzerlegung für eine natürliche Zahl N.

- Effiziente deterministische Algorithmen sind nicht bekannt.
- Die schnellsten deterministischen Algorithmen benötigen mindestens die asymptotische Laufzeit $2^{\Omega(\log_2^b N)}$ für $b \geqslant 1/3$.
- Auch ist nicht bekannt, ob die Entscheidungsversion

  „Hat N einen Primfaktor p mit $p \leqslant m$?“

  NP-vollständig ist.
  - Die Entscheidungsversion der Faktorisierung gehört zu $\mathtt{NP} \cap \mathtt{coNP}$.
  - NP-Vollständigkeit erscheint eher unwahrscheinlich.

Periodenbestimmung (1/2)

Shor's Quanten-Algorithmus bestimmt eine Faktorisierung in Zeit polynomiell in $\log_2 N$.
Dazu betrachte das Problem der **Periodenbestimmung**:

Für eine Zahl N und eine prime Restklasse x modulo N

bestimme die Periode von x modulo N,

also die kleinste Potenz $r \geqslant 1$ mit $x^r \equiv 1 \mod N$.

Ohne Beweis verwenden wir das folgende Ergebnis:

Die Zahl N sei ungerade und keine Primzahlpotenz. Wird eine Restklasse $x \in \{2, \ldots, N\}$ zufällig ausgewürfelt, dann gilt mit W-keit mindestens $1/2$, dass

- x eine gerade Periode r besitzt und
- $x^{r/2} + 1$ und $x^{r/2} - 1$ keine Vielfachen von N sind.

Periodenbestimmung (2/2)

- Die Periode r einer Restklasse $x \in \{2, \ldots, N\}$ sei gerade und weder $x^{r/2} + 1$ noch $x^{r/2} - 1$ seien Vielfache von N. Dann gilt

$$\begin{aligned} x^r \equiv 1 \mod N &\iff (x^{r/2} + 1) \cdot (x^{r/2} - 1) \equiv 0 \mod N \\ &\iff (x^{r/2} + 1) \cdot (x^{r/2} - 1) = k \cdot N. \end{aligned}$$

  Zudem müssen $x^{r/2} + 1$ wie auch $x^{r/2} - 1$ gemeinsame Faktoren mit N besitzen, denn keiner von beiden ist ein Vielfaches von N.

- Also sind $\mathrm{ggT}(x^{r/2} + 1, N)$ und $\mathrm{ggT}(x^{r/2} - 1, N)$ nicht-triviale Teiler von N.

- *Wenn* die Periode von x modulo N bekannt ist, dann kann ein nicht-trivialer Faktor von N mit Wahrscheinlichkeit mindestens $\frac{1}{2}$ bestimmt werden:

Es genügt, wenn die Periode einer zufälligen Restklasse x modulo N bestimmt wird.

Shor's Algorithmus

Shor's Algorithmus (1/2)

Sei $n := \lceil \log_2 N \rceil$. Bestimme ℓ mit $N^2 < 2^\ell < 2N^2$.

1. Wende den Hadamard-Operator $|0^\ell\rangle \otimes |0^n\rangle \overset{H^{\otimes \ell}}{\mapsto} \frac{1}{\sqrt{2^l}} \cdot \sum_{a=0}^{2^\ell - 1} |a\rangle \otimes |0^n\rangle$ an.
2. Ein Orakel führe den Operator $|a\rangle|0^n\rangle \mapsto |a\rangle|x^a \mod N\rangle$ aus. Der Zustand

$$\frac{1}{\sqrt{2^l}} \cdot \sum_{a=0}^{2^\ell - 1} |a\rangle \otimes |x^a \mod N\rangle$$

wird erreicht. Beobachte die letzten n Qubits mit dem Ergebnis $x^a \mod N$.

- Sei r die Periode von x. Dann gilt $x^a \equiv x^b \mod N \iff a \equiv b \mod r$.
- Vernachlässige ab jetzt die letzten n Qubits. Der Zustand ist kollabiert zu

$$|z\rangle := \frac{1}{\sqrt{m}} \cdot \sum_{j=0}^{m-1} |j \cdot r + a\rangle,$$

falls $(m-1) \cdot r + a < 2^\ell \leqslant m \cdot r + a$.

3. Wende die Quanten-Fourier-Transformation F_{2^ℓ} auf $|z\rangle$ an. Es ist

$$\begin{aligned} F_{2^\ell}|z\rangle &= \frac{1}{\sqrt{m}} \cdot \sum_{j=0}^{m-1} \frac{1}{\sqrt{2^l}} \cdot \sum_{b=0}^{2^\ell-1} \exp^{2\pi i \cdot \frac{(jr+a)\cdot b}{2^\ell}} |b\rangle \\ &= \frac{1}{\sqrt{m2^\ell}} \cdot \sum_{b=0}^{2^\ell-1} \exp^{2\pi i \cdot \frac{ab}{2^\ell}} \underbrace{\left(\sum_{j=0}^{m-1} \exp^{2\pi i \cdot \frac{jrb}{2^\ell}} \right)}_{=:\alpha_b} |b\rangle. \end{aligned}$$

Beobachte $F_{2^\ell}|z\rangle$: Diejenigen Basis-Zustände $|b\rangle$ sind hochwahrscheinlich für die $|\alpha_b|^2$ groß ist.

Analyse Shor's Algorithmus (1/2)

„O.B.d.A" ist r *kein* Teiler von 2^ℓ. Zeige: $|\alpha_b| = \frac{\left|\sin(\pi mrb/2^\ell)\right|}{\left|\sin(\pi rb/2^\ell)\right|}$.

- Wenn b nahe an einem ganzzahligen Vielfachen von $\frac{2^\ell}{r}$ liegt, dann liegt der Nenner $\sin(\pi rb/2^\ell)$ nahe bei 0.
- Der Abstand zu einem ganzzahligen Vielfachen wächst nach Multiplikation mit m:
  - Der Nenner ist im Allgemeinen beträchtlich kleiner als der Zähler und b wird hochwahrscheinlich, wenn b fast ein ganzzahliges Vielfaches von $\frac{2^\ell}{r}$ ist.
- Diese Argumentation kann exakt gemacht werden und führt auf:

Mit großer Wahrscheinlichkeit wird eine Zahl b beobachtet mit

$$\left|\frac{b}{2^\ell} - \frac{c}{r}\right| \leqslant \frac{1}{2^{\ell+1}},$$

wobei c eine natürliche Zahl kleiner als r ist.

Analyse Shor's Algorithmus (2/2)

- Mit der Kettenbruchentwicklung, angewandt auf $\frac{b}{2^\ell}$, lässt sich $\frac{c}{r}$ effizient bestimmen.
- Wenn c und r teilerfremd sind, dann bestimme r mit dem Wissen von $\frac{c}{r}$.
  - Übungsaufgabe: $\frac{c}{r}$ ist die einzige rationale Zahl mit Nenner höchstens N und Abstand höchstens $\frac{1}{2^{\ell+1}}$ von $\frac{b}{2^\ell}$.
  - Mehrere Messungen von $F_{2^\ell}|z\rangle$ sind durchzuführen, um ein teilerfremdes c zu erwischen.

Insgesamt kann gezeigt werden:

Shor's Algorithmus bestimmt die Primfaktorzerlegung einer natürlichen Zahl N mit W-keit mindestens $\frac{2}{3}$ in Zeit

$$\mathcal{O}((\log^2 N)^2 (\log\log N)^2 \log\log\log N).$$