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 und ihre Basen (1/3)

(a) 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 $n, m \geqslant N$.

(b) Die Elemente ϕ eines Hilbertraums mit $|\phi| = 1$ heißen **Zustände**.

- $\mathcal{B} \subseteq \mathcal{H}$ heißt ein **Orthonormalsystem**, wenn $\mathcal{B}$ nur aus Zuständen besteht 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.

  $\mathcal{V}$ ist ein dichter Unterraum von $\mathcal{H}$, wenn es zu jedem Element $x \in \mathcal{H}$ und zu jedem $\varepsilon > 0$ einen Vektor $y \in \mathcal{V}$ gibt, so dass $\|x - y\| \leqslant \varepsilon$.
- Eine Orthonormalsystem $\mathcal{B}$ heißt **Orthonormalbasis** von $\mathcal{H}$, wenn $\mathcal{B}$ den gesamten Raum $\mathcal{H}$ aufspannt.
  - ⋆ Die Koeffizienten α_i einer Linearkombination $\phi = \sum_{i \in I} \alpha_i \cdot \phi_i$ für eine Orthonormalbasis $\mathcal{B}$ von $\mathcal{H}$ heißen **Amplituden**.

Hilberträume und ihre Basen (2/3)

- 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
  $\Longrightarrow$ Hilberträume *endlicher* Dimension besitzen eine Orthonormalbasis.
- Übungsaufgabe: Hilberträume *unendlicher* Dimension besitzen keine Orthonormalbasis, wohl aber eine Hilbertbasis.

$\mathcal{H} = \mathbb{C}^N$: Der Hilbertraum der Quantenberechnungen

Sei $\phi_1, \ldots, \phi_N$ eine Orthonormalbasis von $\mathbb{C}^N$. Für Vektoren $\psi, \chi \in \mathcal{H}$ mit

$$\psi = \sum_{i=1}^{N} \alpha_i \cdot \phi_i \text{ und } \chi = \sum_{i=1}^{N} \beta_i \cdot \phi_i$$

definiere

$$\langle \psi, \chi \rangle := \sum_{i=1}^{N} \overline{\alpha_i} \cdot \beta_i.$$

- $\langle , \rangle$ 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.

$\mathbb{C}^N$ ist ein Hilbertraum und $\mathbb{C}^N$ ist der einzige Hilbertraum der Dimension N.

Hilberträume und ihre Basen (3/3)

Das abzählbar 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 die lineare Abbildung $\phi^* \circ L$ und
$\langle\phi\|L\|\psi\rangle$	für den 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.

Das Tensorprodukt

Tensorprodukt (1/2)

Seien $\mathcal{H}_1, \mathcal{H}_2$ Hilberträume mit inneren Produkten $\langle , \rangle_{\mathcal{H}_1}, \langle , \rangle_{\mathcal{H}_2}$ und 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

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

zusammen mit dem inneren Produkt

$$\langle \phi_1 \otimes \psi_1, \phi_2 \otimes \psi_2 \rangle_{\mathcal{H}_1 \odot \mathcal{H}_2} := \langle \phi_1, \phi_2 \rangle_{\mathcal{H}_1} \cdot \langle \psi_1, \psi_2 \rangle_{\mathcal{H}_2}$$

(b) Das **Tensorprodukt** $\mathcal{H}_1 \otimes \mathcal{H}_2$ ist die Vervollständigung des algebraischen Tensorprodukts. Aus Einteilchen-Systemen werden Mehrteilchensysteme gebaut.

- Es ist $\dim(\mathcal{H}_1 \otimes \mathcal{H}_2) = \dim(\mathcal{H}_1) \cdot \dim(\mathcal{H}_2)$.

Mit Tensorprodukten lassen sich neue aus alten Hilberträumen bauen!

Tensorprodukt (2/2)

$\mathcal{H}_1, \mathcal{H}_2$ seien zwei Hilberträume.

Für $|\phi\rangle \in \mathcal{H}_1$ und $|\psi\rangle \in \mathcal{H}_2$ gelte

$$|\phi\rangle = \sum_{h \in O_1} \alpha_h \cdot |h\rangle \text{ und } |\psi\rangle = \sum_{k \in O_2} \beta_k \cdot |k\rangle.$$

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 $|\psi\rangle$.

Es gelte $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ 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. Der entsprechende Zustand des Systems $\mathcal{H}$ ist nicht auf Zustände der Teilsysteme $\mathcal{H}_1, \mathcal{H}_2$ zurückführbar: Die Teilchen interagieren.
- Das Rechnen auf verschränkten Zuständen ist von großer Relevanz.

Qubits

(a) Ein **Qubit** ist ein 1-Teilchen-System mit den klassischen Zuständen 0 und 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.

(b) Werden die Hilberträume $\mathcal{H}_i$ von der Orthonormalbasis $|0\rangle, |1\rangle$ aufgespannt, dann ist

$$\mathcal{H} = \otimes_{i=1}^{k} \mathcal{H}_i = \mathbb{C}^{2^k}$$

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**.

Wie rechnet man mit Qubits? Wir müssen Operatoren und Messungen besprechen.

Operatoren und Messungen

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 ein 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 von Operatoren

Sei A die Matrix des Operators L und A^* die Matrix von L^*.

- A^* ist die Adjungierte von A, d.h. es gilt $A^*_{i,j} := \overline{A_{j,i}}$.
  - Es ist $\langle A\phi \,|\, \psi \rangle = \langle \phi \,|\, A^*\psi \rangle$
  - Für Matrizen A mit reellwertigen Einträgen stimmt die adjungierte Matrix mit der transponierten Matrix überein.
- A heißt genau dann unitär, wenn $A^* \cdot A = I$.
  - Eine unitäre Matrix mit reellwertigen Einträgen ist eine orthogonale Matrix.
- A heißt genau dann selbstadjungiert oder hermitesch, wenn $A^* = A$.
  - Eine hermitesche Matrix A ist unitär diagonalisierbar, d.h. es gibt eine unitäre Matrix U, so dass $U^{-1} \cdot A \cdot U$ eine Diagonalmatrix ist.
  - Hermitesche Matrizen besitzen nur reellwertige Eigenwerte.
  - Eine selbstadjungierte Matrix mit reellwertigen Einträgen ist symmetrisch.

Die Born-Regel

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

(a) Eine **Observable** (auf Hilbertraum $\mathcal{H}$) ist ein hermitescher Operator $L : \mathcal{H} \to \mathcal{H}$.
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 $\lambda_1, \ldots, \lambda_k$.

(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

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

- 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.

Das äußere Produkt

Für alle Zustände $\phi, \psi \in \mathcal{H}$ wird der Operator

$$|\phi\rangle\langle\psi| : \mathcal{H} \to \mathcal{H}$$

definiert durch

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

Man bezeichnet $|\phi\rangle\langle\psi|$ auch als **äußeres Produkt**. Wenn $\mathcal{H}$ endlich-dimensional ist, dann ist $|\phi\rangle\langle\psi|$ 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 $\mathcal{H}$.

- $|\phi_k\rangle\langle\phi_k|$ ist die Projektion von $\mathcal{H}$ auf den von $|\phi_k\rangle$ aufgespannten Unterraum:

$$\begin{aligned} |\phi_k\rangle\langle\phi_k|\Big(\sum_{i\in I}\alpha_i\phi_i\Big) &= \langle\phi_k|\sum_{i\in I}\alpha_i\phi_i\rangle\cdot|\phi_k\rangle \\ &= \alpha_k\cdot|\phi_k\rangle \end{aligned}$$

- Wenn der Unterraum $\mathcal{V} \subseteq \mathcal{H}$ von der Orthonormalbasis $|\phi_1\rangle, \ldots, |\phi_N\rangle$ aufgespannt wird, dann ist $\sum_{k=1}^{N} |\phi_k\rangle\langle\phi_k|$ die Projektion von $\mathcal{H}$ auf $\mathcal{V}$.
  Beachte, dass für $z' = e^{i\alpha}z$ stets $|z\rangle\langle z| = |z'\rangle\langle z'|$ gilt. Der **Dichteoperator** $|z\rangle\langle z|$ – ein hermitescher Operator – beschreibt den „physikalischen Zustand“ von z eineindeutig.

Quantenmechanische versus probabilistische Systeme

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.

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

Ein einzelnes Qubit

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

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

zu den orthogonalen Zuständen $|0\rangle$ und $|1\rangle$. Qubits entsprechen hier Zuständen im $\mathbb{C}^2$, d.h. es gilt

$$\langle\psi|\psi\rangle = |\alpha|^2 + |\beta|^2 = 1$$

und die Längen der quadrierten Amplitude definieren eine W-keitsverteilung:

- Gilt $|\psi\rangle = |0\rangle$, wird $|0\rangle$ mit absoluter Sicherheit beobachtet,
- gilt $|\psi\rangle = |1\rangle$, wird $|1\rangle$ mit absoluter Sicherheit beobachtet.

Die Eigenzustände $|0\rangle$, $|1\rangle$ sind deshalb unter allen Orthonormalbasen von $\mathbb{C}^2$ ausgezeichnet.

Wo kommen Qubits her? Wie wird die Born-Regel experimentell bestätigt?

Die Polarisierung von Photonen als Qubit

Ein Photon tritt in ein Kristall ein, sein Austrittspunkt hängt ab von seiner Polarisierung in Bezug auf die optischen Achse des Kristalls.

- $|0\rangle$ entspricht paralleler Polarisierung,
- $|1\rangle$ entspricht senkrechter Polarisierung.

- 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:
  - Alle Photonen mit „exakt“ paralleler (bzw. senkrechter) Polarisierung verlassen das Kristall mit Sicherheit an einer ersten (bzw. zweiten) Stelle des Kristalls.
  - Jedes Photon tritt an einer der beiden Stellen aus und zwar gesteuert von der W-keitsverteilung $|\alpha|^2 + |\beta|^2$.
- „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 bestätigen Definition einer Messung.

Elektronenspin als Qubit

Der Elektronenspin – also der Eigendrehimpuls eines Elektrons – definiert die Eigenzustände $|\uparrow\rangle$ (*Aufwärts-Spin*) und $|\downarrow\rangle$ (*Abwärts-Spin*).

- Elektronen – obwohl punktförmige Objekt – besitzen eine Drehachse.
- Das höchste Drehmoment wird bei paralleler Mess- und Drehachse gemessen.
  - Der gemessene Wert $w(\alpha)$ für das Drehmoment sinkt mit einem größer werdenden Winkel α zwischen Mess- und Drehachse.
    - Es ist $w(90) = 0$ und $w(180) = -w(0)$.
    - $|\uparrow\rangle$ entspricht einem Winkel von 0 Grad, $|\downarrow\rangle$ einem Winkel von 180 Grad.
    - Der Drehimpuls bleibt bei späteren Messungen konstant: Das entsprechende Qubit hat den Wert 1 bei positivem und 0 bei negativem Ergebnis.
  - Die Überlagerung $|\psi\rangle = \alpha \cdot |\uparrow\rangle + \beta \cdot |\downarrow\rangle$ eines Elektrons beschreibt die W-keit der Messung von $\uparrow$ bzw. $\downarrow$.

Vielteilchen-Systeme

Vielteilchen-Systeme haben wir 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**.

In einem Vielteilchensystem existieren verschränkte Teilchen nur in einem gemeinsamen Zustand, der auch über große Distanzen bestehen bleibt.

Verschränkung

Verschränkung: Ein Vielteilchensystem kann als Ganzes einen Zustand einnehmen, ohne dass Teilsysteme einen eigenen Zustand besitzen:

- Verschränkte Zustände entsprechen keinem Tensorprodukt von Zuständen der Teilsysteme.
- Ein nicht lokales Verhalten der Teilchen kann resultieren.

Ein verschränkter Zustand entsteht, wenn Teilsysteme in Wechselwirkung eintreten, z. B. miteinander kollidieren.

Eine experimentelle Beobachtung: Trifft ein Photon auf einen bestimmten Kristall, teilt es sich in zwei verschränkte Photonen.

- Durchlaufen die beiden Photonen auf unterschiedlichen Wegen ein Meßgerät, werden entweder beide durchgelassen oder beide nicht.
- Dieses Verhalten bleibt auch bei veränderten Meßgeräten erhalten.

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.

Einstein: ... Ich kann nicht an eine „spukhafte Fernwirkung“ glauben, mit der die Messung an einem Teilsystem das Ergebnis der Messung an einem anderen beeinflussen kann ...

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

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

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:

(a) Jede Quelle v besitzt genau eine ausgehende Kante, d.h. es ist $\text{fanout}(v) = 1$. Jeder Quelle wird genau ein Qubit zugewiesen.

(b) Jede Senke v besitzt genau eine eingehende Kante, d.h. es ist $\text{fanin}(v) = 1$.

(c) Jedem sonstigen Knoten v wird ein Quanten-Gatter mit $\text{fanin}(v) = \text{fanout}(v)$ zugewiesen. Eine ausgehende Kante denke man sich mit „ihrem“ Qubit markiert.

- 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.
- 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.

Quantengatter

Im Folgenden wird die aus den klassisischen Zuständen

$$|\, c_1 \cdots c_{n+m} \,\rangle \text{ (für } c_1, \ldots, c_{n+m} \in \{0,1\})$$

bestehende Orthonormalbasis zugrundegelegt. Jedes Quanten-Gatter $\mathcal{G}$ führt einen unitären Operator aus, der nur von wenigen – im Regelfall bis zu 3 – Qubits abhängt.

- Wenn $\mathcal{G}$ die unitäre Matrix U auf den ersten k Qubits ausführt, dann überführt $\mathcal{G}$ die 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

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

.

- In Diagrammen zu $\mathcal{G}$ entspricht die Reihenfolge der Qubits an den Ausgängen von $\mathcal{G}$ stets der Reihenfolge an den Eingängen.

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 auf einem Qubit

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 $|1\rangle \mapsto e^{i\cdot\alpha}|1\rangle$.

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

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 $|1\rangle \mapsto \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big)$.

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

  Das Hadamard-Gatter würfelt: In Nebeneinanderausführung wird auf Eingabe $|0^k\rangle$ in einem Schritt eine Gleichverteilung auf allen k Qubits berechnet.

$$\begin{aligned} \otimes_{i=1}^{k} H|0\rangle &= \otimes_{i=1}^{k} \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) = \frac{1}{2^{k/2}} \sum_{b_1,\ldots,b_k \in \{0,1\}} |b_1\rangle \otimes \cdots \otimes |b_k\rangle \\ &= \frac{1}{2^{k/2}} \sum_{b_1,\ldots,b_k \in \{0,1\}} |b_1 \cdots b_k\rangle \end{aligned}$$

Quanten-Gatter auf zwei Qubits

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.

Quanten-Gatter auf drei Qubits

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 Bitflip- bzw. Phasenflip-Gattern rekonstruieren, denn er kennt $b_1\,b_2$: **Quanten-Teleportation**.

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 mit der Startkonfiguration c_0 übereinstimmt und ansonsten $v_c^{(0)} = 0$.
- M befindet sich zum Zeitpunkt k in der Überlagerung

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

Insbesondere gibt es also eine Darstellung

$$|v^{(k)}\rangle = \sum_d v_d^{(k)} \cdot |d\rangle$$

von $|v^{(k)}\rangle$ mit den Amplituden $v_d^{(k)}$ der Konfigurationen d.

  - Beachte, dass $v_d^{(k)}$ die Amplitude aller Berechnungen von M ist, die in der Konfiguration c_0 beginnen und nach k Schritten in Konfiguration d enden.
  - Es gilt also $v_d^{(k)} = U_M^k[c_0, d]$.

Nur Konfigurationen polynomieller Länge seien von c_0 aus erreichbar und es gelte $\log k = \text{poly}(n) \Longrightarrow v_d^{(k)}$ ist für jede Konfiguration d deterministisch mit polynomiellem Speicherplatz berechenbar.

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

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

Es gilt

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

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?

Die Beziehungen

$$\mathtt{WeakBQP} = \mathtt{BQP} = \mathtt{StrongBQP}$$

können wie im Nachweis von Weak$\mathtt{BPP} = \mathtt{BPP} =$ Strong$\mathtt{BPP}$ gezeigt werden, nämlich mit einer Mehrheitsbildung nach entsprechend häufiger Wiederholung.

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

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

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

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. Zur Erinnerung, es ist

$$|b_1 b_2 b_3\rangle \overset{\text{Toffoli}}{\mapsto} |b_1 b_2 b_3\rangle, \text{ falls } b_1 b_2 \neq 11, \text{ und } |11b\rangle \overset{\text{Toffoli}}{\mapsto} |11\overline{b}\rangle.$$

Das Toffoli-Gatter ist ein universelles Gatter, denn

$$\begin{aligned} \text{Toffoli}(|b_1 b_2 0\rangle) &:= |b_1 b_2\ \text{AND}(b_1 b_2)\rangle \text{ und} \\ \text{Toffoli}(|11b\rangle) &:= |11\overline{b}\rangle \end{aligned}$$

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.

Zufallsbits können mit k nebeneinander gestellten Hadamard-Gattern, angewandt jeweils auf $|0\rangle$ „hergestellt“ werden:

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

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

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

$$\begin{aligned} U\Big(|x\rangle \otimes H^{\otimes k}(|0^k\rangle) \otimes |0^m\rangle\Big) &= \frac{1}{\sqrt{2^k}} \cdot \sum_{r_1,\ldots,r_k \in \{0,1\}} U|x, r, 0^m\rangle \\ &= \frac{1}{\sqrt{2^k}} \cdot \sum_{r_1,\ldots,r_k \in \{0,1\}} |x, r,\ \text{müll}(x, r), S_n(x, r)\rangle. \end{aligned}$$

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 von Zustand $U|x0^m\rangle$ 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 $2^{\text{poly}(|x|)}$ 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.

Das BQP-Subroutine-Theorem

Be tidy!

1. Wir rufen eine „Subroutine“ U während einer Berechnung auf, wobei $U|b\rangle = |b\rangle$ für $b \in \{0, 1\}$ gelte.
   - Betrachte den Operator HUH für den Hadamard-Operator H.
   - $UH|0\rangle = \frac{1}{\sqrt{2}} \cdot (|0\rangle + |1\rangle)$ und $HUH|0\rangle = |0\rangle$.
2. Eine zweite „Subroutine“ V kommt zum selben Ergebnis, macht sich aber Notizen, d.h. es ist $V|b0\rangle = |bb\rangle$ für $b \in \{0, 1\}$.
   - Der Hadamard-Operator wird jetzt auf das erste Qubit angewandt. Der „äquivalente“ Operator HVH verhält sich überhaupt nicht äquivalent, denn
   - $VH|0\rangle = \frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)$ und $HVH|0\rangle = \frac{1}{2} \cdot (|00\rangle + |10\rangle + |01\rangle - |11\rangle)$.
3. Während $|0\rangle$ mit Wahrscheinlichkeit 1 als das erste Qubit von $HUH|0\rangle$ beobachtet wird, wird für $HVH|0\rangle$ das Qubit $|0\rangle$ mit Wahrscheinlichkeit $\frac{1}{2}$ beobachtet.

Was ist passiert? Die beabsichtigte Interferenz, die zum Ausschalten von Qubit $|1\rangle$ führt, wird durch den Inhalt des „Arbeitsregisters“ von V blockiert.

Wie können wir ungestraft Subroutinen aufräumen?

Compute-Uncompute

U sei ein unitärer Operator. Wir möchten eine Subroutine

$$U|b_1 \cdots b_n 0^k\rangle = |b_1 \cdots b_n, \text{Müll}, f(b_1 \cdots b_n)\rangle$$

z.B. für die boolesche Funktion $f : \{0,1\}^n \to \{0,1\}$ aufrufen.

- Probleme können störende Berechnungsspuren und mgl. – mit kleiner W-keit – fehlerhafte Ergebnisse sein.
- **Aber** unitäre Berechnungen lassen sich mit unitärer Berechnung umkehren!

Compute-Uncompute

1. **Amplify**: Berechne die Funktion f in `StrongBQP` mit dem neuen Operator V.
2. **Compute**: Führe $V|b_1 \cdots b_n 0^k\rangle$ aus.
3. **Save**: Speichere das Ergebnis in einem dafür reservierten Qubit.
   - Z. B. wende das Controlled-Not-Gatter auf die Qubits $|f(b_1 \cdots b_n)0\rangle$ an.
4. **Uncompute**: Führe V^{-1} aus.

Das BQP-Subroutine-Theorem

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

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

ohne akkumulierende Fehler und unerwünschte Berechnungsspuren

aufrufen darf.

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

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.

Grover's Algorithmus

Für eine boolesche Funktion $f : \{0,1\}^n \to \{0,1\}$ suchen wir eine „Lösung“, d.h. ein Wort $x \in \{0,1\}^n$ mit $f(x) = 1$. Setze

$$\text{Bad} := f^{-1}(0) \text{ und } |\text{Bad}\rangle := \frac{1}{\sqrt{|\text{Bad}|}} \cdot \sum_{x \in \{0,1\}^n, f(x)=0} |x\rangle,$$

$$\text{Good} := f^{-1}(1) \text{ und } |\text{Good}\rangle := \frac{1}{\sqrt{|\text{Good}|}} \cdot \sum_{x \in \{0,1\}^n, f(x)=1} |x\rangle.$$

Sei *GB* der durch $|\text{Good}\rangle$ und $|\text{Bad}\rangle$ aufgespannte Raum.

1. Setze $|z\rangle := H^{\otimes n}|0^n\rangle$.

   Es ist $|z\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle$.

2. Wiederhole genügend oft:

   - Setze $|z\rangle := U|z\rangle$.

U führt Raum *GB* eine Drehung mit Winkel 2θ aus, wobei $\theta := \arcsin(\frac{\sqrt{|\text{Good}|}}{2^{n/2}})$.

Was ist U?

Erste Beobachtungen (1/2)

- Wir kennen weder $|\text{Bad}|$, $|\text{Good}|$ noch $|\text{Bad}\rangle$, $|\text{Good}\rangle$, geschweige denn U.
- Wir wissen: U führt in GB eine Drehung mit Winkel $\theta := \arcsin(\frac{\sqrt{|\text{Good}|}}{2^{n/2}})$ aus.

Es ist $|\text{Bad}\rangle := \frac{1}{\sqrt{|\text{Bad}|}} \cdot \sum_{x \in \{0,1\}^n, f(x)=0} |x\rangle$ und $|\text{Good}\rangle := \frac{1}{\sqrt{|\text{Good}|}} \cdot \sum_{x \in \{0,1\}^n, f(x)=1} |x\rangle$.

Nach dem ersten Schritt von Grover's Algorithmus ist

$$\begin{aligned} |z\rangle &= H^{\otimes n}|0^n\rangle = \frac{1}{2^{n/2}} \sum_{x \in \{0,1\}^n} |x\rangle \\ &= \frac{\sqrt{|\text{Bad}|}}{2^{n/2}} \cdot |\text{Bad}\rangle + \frac{\sqrt{|\text{Good}|}}{2^{n/2}} \cdot |\text{Good}\rangle \\ &= \cos(\theta) \cdot |\text{Bad}\rangle + \sin(\theta) \cdot |\text{Good}\rangle \end{aligned}$$

Nach k Anwendungen von Operator U ist

$$|z\rangle = \cos((2k+1)\theta) \cdot |\text{Bad}\rangle + \sin((2k+1)\theta) \cdot |\text{Good}\rangle$$

Erste Beobachtungen (2/2)

Nach k Anwendungen von Operator U ist

$$|z\rangle = \cos((2k+1)\theta) \cdot |\text{Bad}\rangle + \sin((2k+1)\theta) \cdot |\text{Good}\rangle$$

Beobachte $|z\rangle$ und hoffe darauf, eine Lösung zu erhalten:

- Angenommen, wir kennen die Anzahl $\ell = |\text{Good}|$ aller Lösungen.
  - O.B.d.A. $\ell \leqslant 2^{n/2}$.
  - Es ist $\sin(x) = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!}$. In der Nähe des Nullpunkts ist $\sin(x) \approx x$
    $\implies \theta \approx \frac{\sqrt{|\text{Good}|}}{2^{n/2}}$.
  - Wähle $k := \lfloor \frac{\pi}{4} \cdot \frac{2^{n/2}}{\sqrt{|\text{Good}|}} \rfloor$.
- Und wenn ℓ nicht bekannt ist?
  - Achtung: Gefahr des Überschießens!
  - Nimm an, dass $|\text{Good}| = m$ für $m \in \{2^1, 2^2, \ldots, 2^{n/2}\}$ und führe mehrere Beobachtungen für jedes m durch.

Die Laufzeit ist durch $\mathcal{O}(n^2 \cdot 2^{n/2})$ beschränkt. Aber was ist U?

Der Operator U (1/3)

1. Wir definieren die beiden folgenden unitären Operatoren:

$$\mathcal{O}_f|x\rangle := (-1)^{f(x)}|x\rangle \text{ und } \mathcal{O}^*|x\rangle := \begin{cases} |0^n\rangle & x = 0^n \\ -|x\rangle & \text{sonst.} \end{cases}$$

   Aus dem BQP-Subroutine-Theorem folgt eine schnelle Quantenberechnung für beide Orakel, falls f schnell berechenbar ist.

2. Setze

$$U := H^{\otimes n} \circ \mathcal{O}^* \circ H^{\otimes n} \circ \mathcal{O}_f.$$

Was tut $H^{\otimes n} \circ \mathcal{O}^* \circ H^{\otimes n}$?

Der Operator U (2/3)

Beachte $|0^n\rangle\langle 0^n||x\rangle = \begin{cases} |0^n\rangle & x = 0^n \\ 0 & \text{sonst.} \end{cases}$

Da außerdem $HH = I$ gilt – denn H ist eine symmetrische Rotation –, folgt

$$\begin{aligned} H^{\otimes n} \circ \mathcal{O}^* \circ H^{\otimes n} &= H^{\otimes n} \circ \left(2 \cdot |0^n\rangle\langle 0^n| - I\right) \circ H^{\otimes n} \\ &= 2|W\rangle\langle W| - I. \end{aligned}$$

für den Zustand $|W\rangle := \frac{1}{2^{n/2}} \cdot \sum_{x \in \{0,1\}^n} |x\rangle$.

- $H^{\otimes n} \circ \mathcal{O}^* \circ H^{\otimes n}$ ist eine Spiegelung am durch $|W\rangle$ aufgespannten Teilraum:
  - $H^{\otimes n} \circ \mathcal{O}^* \circ H^{\otimes n}|V\rangle = -|V\rangle$, falls $|V\rangle, |W\rangle$ orthogonal sind,
  - während Elemente des Teilraums von $|W\rangle$ unverändert bleiben.
- $\mathcal{O}_f$ ist eine Spiegelung am durch $|\text{Bad}\rangle$ aufgespannten Teilraum von GB.
  - $\mathcal{O}_f|\text{Good}\rangle = -|\text{Good}\rangle$, $\mathcal{O}_f|\text{Bad}\rangle = |\text{Bad}\rangle$,

Der Operator U (3/3)

- Wir haben den Winkel θ so gewählt, dass gilt

$$|W\rangle = \cos(\theta) \cdot |\text{Bad}\rangle + \sin(\theta) \cdot |\text{Good}\rangle.$$

- Beachte, dass der Operator U
  - zuerst am durch $|\text{Bad}\rangle$ aufgespannten Teilraum von GB spiegelt
  - und danach am durch $|W\rangle$ aufgespannten Teilraum von GB.
- U, eingeschränkt auf GB, muss jedesmal um den Winkel 2θ drehen!

Grover's Algorithmus:
Optimalität im Orakel-Modell

Liegen NP-vollständige Probleme in BQP?

Mit Wahrscheinlichkeit 1 über alle dünnen Orakel $A \subseteq \{0,1\}^*$ gilt:
Ein Quantenalgorithmus kann die Sprache

$$L_A := \{\, 1^n \,:\, A \cap \{0,1\}^n \neq \emptyset \,\}$$

nur mit $\Omega(2^{n/2})$ Anfragen an das Orakel akzeptieren.

Das Orakel A ist dünn, wenn $|A \cap \{0,1\}^n| \leqslant 1$ für jede natürliche Zahl n gilt.

Grover's Algorithmus ist asymptotisch optimal!

+ 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. Warum?
! Wir zeigen: $\mathrm{NP}^A \not\subseteq \mathrm{BQP}^A$.
  - 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.
  - Grover's Algorithmus ist asymptotisch optimal $\Longrightarrow$ L_A gehört nicht zu BQP^A.

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.
- Q rechnet für T Schritte. In Iteration t ruft Q zuerst den unitären Operator U_t und dann den Orakel-Operator $\mathcal{O}$ auf.
  - Basiszustände von Q nach Ausführung von U_t und vor Anfrage an $\mathcal{O}$ sind $|x, w, t\rangle$ für den Arbeitsspeicher $w \in \{0,1\}^m$ und die Anfrage $x \in \{0,1\}^n$.
  - Der „Systemzustand" vor der Anfrage ist $\sum_{x \in \{0,1\}^n, w \in \{0,1\}^m} \alpha_{x,w,t} |x, w, t\rangle$.
  - Die „Amplitude von Anfrage x zur Zeit t" wird definiert als die reelle Zahl

$$\alpha_{x,t} := \sqrt{\sum_w |\alpha_{x,w,t}|^2}.$$

    Die Wahrscheinlichkeit, x im Schritt t zu beobachten, ist $\alpha_{x,t}^2$.
- Q wendet also den Operator $U_T \circ (\mathcal{O} \circ U_{T-1}) \circ \cdots \circ (\mathcal{O} \circ U_1)$ an und beoachtet das „Anfrageregister" in Iteration T.

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

ist die W-keit, x *irgendwann* zu beobachten. Dann ist

$$\sum_{x \in \{0,1\}^n} q_x = \sum_{t=1}^{T} \Big(\underbrace{\sum_{x \in \{0,1\}^n} \sum_{w} |\alpha_{x,w,t}|^2}_{\text{der Systemzustand hat Länge 1}} \Big) = \sum_{t=1}^{T} 1 = T.$$

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 Analyse benutzen wir ein „**Hybrid-Argument**“:

1. Wir nehmen zuerst an, dass **alle** Anfragen negativ beantwortet werden.
2. Dann nehmen wir an, dass im Schritt $T-1$ – und nur in diesem Schritt – Anfragen nach x_0 positiv beantwortet werden.
3. Und fragen uns dann, wie Q reagiert, wenn schon ab Schritt $T-2$ Anfragen nach x_0 positiv beantwortet werden.
4. Am Ende können wir die unterschiedliche Reaktion von Q im Bezug auf nur negative Antworten bzw. auf positive Antworten für x_0 in allen Schritten beurteilen.

Das Hybrid-Argument (1/3)

Positive Antworten auf Anfragen nach x_0 mögen ab – und inklusive – Schritt $T - i$ gegeben werden. Dann sei

$$z_t^{(i)} = \sum_w \alpha_{x,w,t}^{(i)} \cdot |x, w, t\rangle$$

der Systemzustand in Iteration t vor Anwendung des Orakeloperators.

Insbesondere ist also $\alpha_{x,z,t}^{(0)} = \alpha_{x,z,t}$.

Für $t \leqslant T - 1$ ist $\alpha_{x,w,t}^{(0)} = \alpha_{x,w,t}^{(1)}$. Das Orakel antwortet in Iteration $T - 1$ für $x \neq x_0$ mit $\mathcal{O}(|x, w, T-1\rangle) = |x, w, T-1\rangle$, bzw. mit $\mathcal{O}(|x_0, w, T-1\rangle) = -|x_0, w, T-1\rangle \Longrightarrow$

$$\begin{aligned}
\|z_T^{(0)} - z_T^{(1)}\| &\overset{U_T \text{ ist linear}}{=} \|U_T\Big(\sum_w \big(\alpha_{x_0,w,T-1}^{(0)} - (-\alpha_{x_0,w,T-1}^{(0)})\big) \cdot |x_0, w, T-1\rangle\Big)\| \\
&= \|2 \cdot U_T\Big(\sum_w \alpha_{x_0,w,T-1}^{(0)} \cdot |x_0, w, T-1\rangle\Big)\| \\
&\overset{U_T \text{ erhält Längen}}{=} 2 \cdot \sqrt{\sum_w |\alpha_{x_0,w,T}^{(0)}|^2} = 2 \cdot \alpha_{x_0,T-1}
\end{aligned}$$

Das Hybrid-Argument (2/3)

- Für $t \leqslant T-2$ ist $\alpha^{(1)}_{x,w,t} = \alpha^{(2)}_{x,w,t}$. Das Orakel antwortet in Iteration $T-2$ für $x \neq x_0$ mit $\mathcal{O}(|x, w, T-2\rangle) = |x, w, T-2\rangle$, bzw. mit $\mathcal{O}(|x_0, w, T-2\rangle) = -|x_0, w, T-2\rangle$.

$$\begin{aligned}
\|z^{(1)}_{T-1} - z^{(2)}_{T-1}\| &\overset{U_{T-1}\text{ ist linear}}{=} \|U_{T-1}\Big(\sum_w \big(\alpha^{(1)}_{x_0,w,T-2} - (-\alpha^{(2)}_{x_0,w,T-2})\big)|x_0, w, T-2\rangle\Big)\| \\
&= \|2 \cdot U_{T-1}\Big(\sum_w \alpha^{(0)}_{x_0,w,T-2} \cdot |x_0, w, T-2\rangle\Big)\| \\
&\overset{U_{T-1}\text{ erhält Längen}}{=} 2 \cdot \sqrt{\sum_w |\alpha^{(0)}_{x_0,w,T-1}|^2} = 2 \cdot \alpha_{x_0,T-1}.
\end{aligned}$$

- Wie groß ist der Abstand zwischen $z^{(0)}_T$ und $z^{(2)}_T$?

  Ab Iteration $t \geqslant T-1$ werden in $z^{(1)}_t$ bzw. $z^{(2)}_t$ dieselben unitären – also längenerhaltenden – Operatoren eingesetzt: Es ist $z^{(1)}_T - z^{(2)}_T = U_T \circ \mathcal{O}\big(z^{(1)}_{T-1} - z^{(2)}_{T-1}\big)$.

$$\begin{aligned}
\|z^{(0)}_T - z^{(2)}_T\| &= \|z^{(0)}_T - z^{(1)}_T + z^{(1)}_T - z^{(2)}_T\| \\
&\leqslant \|z^{(0)}_T - z^{(1)}_T\| + \|z^{(1)}_T - z^{(2)}_T\| \\
&\leqslant 2 \cdot \alpha_{x_0,T} + 2 \cdot \alpha_{x_0,T-1}.
\end{aligned}$$

Das Hybrid-Argument (3/3)

Und wenn Anfragen nach x_0 erst ab Iteration $T-3$ positiv beantwortet werden? Dann gilt mit analogem Argument

$$\|z_{T-2}^{(2)} - z_{T-2}^{(3)}\| \leqslant 2\alpha_{x_0,T-2}$$

und da die unitären Operatoren ab Iteration $T-2$ übereinstimmen:

$$\|z_T^{(2)} - z_T^{(3)}\| \leqslant 2\alpha_{x_0,T-2}.$$

Also erhalten wir

$$\|z_T^{(0)} - z_T^{(3)}\| = \|z_T^{(0)} - z_T^{(2)} + z_T^{(2)} - z_T^{(3)}\| \leqslant 2\big(\alpha_{x_0,T-2} + \alpha_{x_0,T-1} + \alpha_{x_0,T}\big).$$

Grover's Algorithmus ist asymptotisch optimal, denn

$$\|z_T^{(0)} - z_T^{(T-1)}\| \leqslant 2 \cdot \sum_{t=1}^{T} \alpha_{x_0,t} \leqslant 2 \cdot \frac{T}{2^{n/2}}.$$

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

Trennung von NP^A und BQP^A

Mit W-keit 1 über die dünnen Orakel A gilt $\mathrm{NP}^A \not\subseteq \mathrm{BQP}^A$.

- Es ist stets $L_A \in \mathrm{NP}^A$. Zeige: $L_A \notin \mathrm{BQP}^A$.
- Das bisherige Argument zeigt bei $o(2^{n/2})$ Anwendungen von $\mathcal{O}$:
  - Vernachlässigbarer Unterschied in Beobachtungs-W-keiten zwischen NEIN-Szenario und allgemeinem Szenario.
- Für jeden Quanten-Algorithmus Q mit $o(2^{n/2})$ Anwendungen von $\mathcal{O}$, genügend großen Eingabelängen 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 $|A \cap \{0,1\}^n| = 1$.

Ein (sehr vereinfachendes) Fazit

Wenn wir in einem Haufen von n Grashalmen nach einer Stecknadel suchen:

- Ein randomisierter Ansatz zieht zufällig und findet die Nadel in einem Versuch mit Wahrscheinlichkeit $\frac{1}{N}$ und allgemein, nach t Versuchen mit Wahrscheinlichkeit $\frac{t}{N}$.
  - Es werden $\Theta(N)$ Versuche benötigt.
- Ein Quantenansatz hat eine „Erfolgsamplitude“ von $\frac{1}{\sqrt{N}}$ nach einem Versuch und allgemein, nach t Versuchen eine „Erfolgsamplitude“ von $\frac{t}{\sqrt{N}}$.
  - $\frac{t}{\sqrt{N}} \approx 1$ ist hinreichend: Grover's Algorithmus
  - und notwendig: Unser Orakel-Argument hat die Linearität und die Längenerhaltung unitärer Operatoren ausgenutzt.

$\Theta(\sqrt{N})$ Iterationen sind hinreichend und notwendig.

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

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

   - Wende den Hadamard-Operator $H^{\otimes n}$ auf die ersten n Qubits an und beobachte das Ergebnis. (Die zweiten n Qubits werden nicht mehr beachtet.)

2. Wiederhole dieses Vorgehen $\mathcal{O}(n)$-Mal.

3. Bestimme s mit einem linearen Gleichungssystem aus den Beobachtungen.
   - Das gelingt mit einem klassischen Algorithmus, also nur mit Toffoli-Gattern.

Lineares Gleichungssystem für Geheimnis s

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

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 $1 - 2^{-n}$ nach $\mathcal{O}(n)$ Anfragen an das Orakel.

Der Algorithmus arbeitet auf einem Quanten-Schaltkreis mit polynomiell vielen Hadamard- und Toffoli-Gattern.

(b) Zeige: 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.

Aber mindestens $\Omega(2^{n/2})$ Anfragen werden auch benötigt.

(c) Zeige: $\mathtt{BPP}^A \subset \mathtt{BQP}^A$ mit W-keit 1 über die Wahl eines Orakels 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 $\frac{2}{3}$. □

Trennung von $\mathtt{BPP}^A$ und $\mathtt{BQP}^A$ (3/5)

Beweis (b,c)

- Das „**Zufallsorakel**“ A würfelt für jedes n mit W-keit $\frac{1}{2}$ entweder eine zufällig bijektive Funktion oder eine zufällige 2-bijektive Funktion (mit Geheimnis) aus.
- 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 – nach Fixierung der Zufallsbits – als Folge

    $$(D_w \,:\, w \in \{0,1\}^*)$$

    deterministischer Algorithmen angesehen werden: Wenn $R(f)$ bzw. $D_w(f)$ die Ausgabe von D_w für Orakel f ist, dann ist

    $$\mathrm{pr}[\, R(f) = \text{bijektive}\,] = \sum_w p_w \cdot \mathrm{pr}[\, D_w(f) = \text{bijektive}\,]$$

    wobei p_w die Wahrscheinlichkeit für die Zufallsbits w ist.
  - 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 (b,c): 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 (b,c)

$$
\begin{aligned}
& \text{pr}[\,\text{bei } N \text{ Anfragen taucht kein Funktionswert 2-mal auf }\,] \\
= \quad & \prod_{k=1}^{N-1} \text{pr}[\,k+1 \text{ Anfragen sind ohne Kollision} \mid k \text{ Anfragen sind ohne Kollision}\,] \\
\geqslant \quad & \prod_{k=1}^{N-1} \left(1 - \frac{k}{2^n - \binom{k}{2}}\right) \qquad \overset{(1-a)(1-b)\geqslant 1-(a+b)}{\geqslant} \quad 1 - \sum_{k=1}^{N-1} \frac{k}{2^n - \binom{k}{2}} \\
= \quad & 1 - \Theta\left(\frac{N^2}{2^n}\right) \qquad \text{falls } N \leqslant 2^{n/2}.
\end{aligned}
$$

Behauptung (b) folgt. Für Teil (c): Mit W-keit 1 gilt $\mathtt{BPP}^A \subset \mathtt{BQP}^A$. □

Zusammenfassung

Zusammenfassung (1/2)

- Zustände eines Quantensystems sind Überlagerungen in einem **Hilbertraum** $\mathcal{H}$.
  - Ein Quanten-System rechnet durch Anwendung von **unitären Operatoren** $U : \mathcal{H} \to \mathcal{H}$ auf Überlagerungen.
  - Quantenalgorithmen nutzen Quantenparallelität mit Hilfe verschränkter Zustände aus.
- Eine Beobachtung schließt die Berechnung ab
  - Nach der **Born-Regel** kann ein **hermitescher Operator** gemessen werden.
  - Das Ergebnis der Messung von H ist ein Eigenwert λ von H. Der aktuelle Zustand kollabiert in die Projektion auf den Eigenraum von λ.
- Quantenberechnungen erlauben eine quadratische Beschleunigung für unstrukturierte Suche (**Grover's Algorithmus**).
  - Grover's Algorithmus ist im Orakelmodell asymptotisch optimal.
  - Die Optimalität von Grover's Algorithmus liefert ein – allerdings schwaches – Indiz dafür, dass NP-harte Probleme *nicht* in BQP liegen.

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.

  Simon's Algorithmus: Mit W-keit 1 über die Wahl von A gilt $\mathtt{BPP}^A \subset \mathtt{BQP}^A$.
- Es ist $\mathtt{BPP} \subseteq \mathtt{BQP} \subseteq \mathtt{PP} \subseteq \mathtt{PSPACE}$.

Die Quanten-Fourier-Transformation

Einheitswurzeln

- Die n Potenzen $e^{2\pi i \cdot j/n}$ für $j = 0, \ldots, n-1$ sind die $n$ten Einheitswurzeln, also Wurzeln des Polynoms $x^n - 1$.
  - Es ist $e^{i \cdot x} = \cos x + i \sin x$.
  - Also folgt $\left(e^{2\pi i \cdot j/n}\right)^n = 1 \implies$ die n.ten Einheitswurzeln sind die Wurzeln von $x_n - 1$.
- Die Einheitswurzeln bilden eine multiplikative Gruppe, denn

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

  - $w_n = e^{2\pi i/n}$ ist eine primitive $n$te Einheitswurzel, d.h. alle anderen Einheitswurzeln sind Potenzen von w_n.
    w_n^j ist eine primitive $n$te Einheitswurzel $\iff$ j und n sind teilerfremd.
- Für alle $j, n \in \mathbb{N}$ gilt

$$\sum_{k=0}^{n-1} e^{2\pi i \cdot jk/n} = \sum_{k=0}^{n-1} w_n^{jk} = 0.$$

Für eine primitive n.te Einheitswurzel $e^{2\pi ij/n}$ gilt $\prod_{k=0}^{n-1}(x - e^{2\pi i \cdot jk/n}) = x^n - 1$.

Die diskrete Fourier-Transformation (DFT)

Die **diskrete Fourier-Transformation (DFT)**

$$x \mapsto F_n \cdot x$$

wird durch die Matrix

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

mit der primitiven n.ten Einheitswurzel w_n beschrieben. Eine Komponente

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

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

Die Matrix F_n

Die Matrix F_n ist **unitär**. Warum?

- Spalte k hat Länge Eins, denn $\sum_{j=0}^{n-1} \left(\frac{1}{\sqrt{n}}\right)^2 \cdot w_n^{-j\cdot k} w_n^{j\cdot k} = 1.$
- Zur Erinnerung: $\sum_{j=0}^{n-1} w_n^{jk} = 0$ für alle $k \in \mathbb{N} \Longrightarrow$
  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, d.h.

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

gilt. Insbesondere ist F_n unitär.

DFT: Die Sichtweise der Interpolation

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

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

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

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

Schnelle Multiplikation von Polynomen p_x, p_y jeweils vom Grad $n-1$:

1. Werte p_x und p_y an allen $2n$.ten Einheitswurzeln aus.
2. Für $\ell = 0, \ldots, 2n-1$ multipliziere

$$q(w_{2n}^\ell) := p_x(w_{2n}^\ell) \cdot p_y(w_{2n}^\ell).$$

3. Wende die inverse Fouriertransformation auf die Werte $q(w_{2n}^\ell)$ an, um die Koeffizienten des Produktpolynoms zu bestimmen.

Die Quanten-Fourier-Transformation (QFT)

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 $c = c_1 \cdots c_n \in \{0,1\}^n$ ist

$$\text{zahl}(c) := c_1 2^{n-1} + c_2 2^{n-2} + \cdots c_{n-1} 2^1 + c_n 2^0 = \sum_{\ell=1}^{n} c_\ell 2^{n-\ell}.$$

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

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

– auf n Qubits – wird für $z = \sum_{b_1,\ldots,b_n \in \{0,1\}} \alpha_{b_1 \cdots b_n} \cdot |b_1 \cdots b_n\rangle$ definiert durch

$$F_N|z\rangle = \frac{1}{\sqrt{N}} \sum_{b_1,\ldots b_n \in \{0,1\}} \alpha_{b_1 \cdots b_n} \cdot \sum_{a \in \{0,1\}^n} e^{2\pi i \cdot \text{zahl}(a) \cdot \text{zahl}(b)/N} |a\rangle.$$

Das Ergebnis der QFT bei vollständiger Beobachtung ist der **Fourier-Koeffizient**

$$\frac{1}{\sqrt{N}} \sum_{b_1,\ldots b_n \in \{0,1\}} \alpha_{b_1 \cdots b_n} \cdot e^{2\pi i \cdot \text{zahl}(a) \cdot \text{zahl}(b)/N}.$$

Beachte

$$F_N|b_1 \cdots b_n\rangle = \frac{1}{\sqrt{N}} \cdot \sum_{a \in \{0,1\}^n} e^{2\pi i \cdot \text{zahl}(a) \cdot \text{zahl}(b)/N} |a\rangle.$$

Quanten-Fourier-Transformation (3/7)

Sei $N = 2^n$.

Die Quanten-Fourier-Transformation F_N für n Qubits wird durch Quanten-Schaltkreise

- mit $\mathcal{O}(n \log n)$ Gattern scharf approximiert und
- mit $\mathcal{O}(n^2)$ Gattern exakt berechnet.

Die klassische Fouriertransformation F_N benötigt klassische Schaltkreise mit $\mathcal{O}(N \log_2 N)$ Gattern unter „Beobachtung“ **aller** Fourier-Koeffizienten.

Die Quanten-Fourier-Transformation besitzt **logarithmische** Laufzeit, aber nur „Mutter Natur“ kennt das Ergebnis: Wir beobachten nur einen Fourier-Koeffizienten.

Da $N = 2^n$ ist

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

denn $e^{2\pi i \cdot m} = 1$ 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 $\ell = 1, \ldots, n$.

- Bestimme $|z_1\rangle$: Es ist

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

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

  Achtung: Die Berechnung von $|z_1\rangle$ verändert das n.te Qubit.

- Wir arbeiten mit dem „kontrollierten“ Phasengatter C_P^s, das auf dem Qubit $|b\rangle$ – kontrolliert durch das Qubit $|a\rangle$ – arbeitet.
  - Für $a = 0$ wird die Einheitsmatrix auf $|b\rangle$ angewandt
  - und nur für $a = 1$ erfolgt eine mögliche Änderung – nämlich eine Phasenverschiebung um $2\pi/2^s$ – durch die Anwendung von C_P^s, wobei

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

- Bestimme $|z_2\rangle$: Wende C_P^2 auf Qubit $|b_{n-1}\rangle$ an, kontrolliert von Qubit $|b_n\rangle$:

$$\begin{aligned} C_P^2\Big(|b_n\rangle \otimes H|b_{n-1}\rangle\Big) &= C_P^2\Big(|b_n\rangle \otimes \frac{1}{\sqrt{2}} \cdot \big(|0\rangle + e^{2\pi i \cdot 0.b_{n-1}}|1\rangle\big)\Big) \\ &= |b_n\rangle \otimes \frac{1}{\sqrt{2}} \cdot \big(|0\rangle + e^{2\pi i \cdot 0.b_{n-1}b_n}|1\rangle\big) = |b_n\rangle \otimes |z_2\rangle. \end{aligned}$$

Achtung: Die Berechnung von $|z_2\rangle$ verändert das $n-1$.te Qubit!

- Bestimme $|z_3\rangle$:

$$\begin{aligned} & C_P^3\Big(|b_n\rangle \otimes C_P^2\Big(|b_{n-1}\rangle \otimes H|b_{n-2}\rangle\Big)\Big) \\ \overset{|b_{n-1}\rangle \text{ kontrolliert}}{=} \; & C_P^3\Big(|b_n\rangle \otimes C_P^2\Big(|b_{n-1}\rangle \otimes \frac{1}{\sqrt{2}} \cdot \Big(|0\rangle + e^{2\pi i \cdot 0.b_{n-2}}|1\rangle\Big)\Big)\Big) \\ \overset{|b_n\rangle \text{ kontrolliert}}{=} \; & |b_{n-1}\rangle \otimes C_P^3\Big(|b_n\rangle \otimes \frac{1}{\sqrt{2}} \cdot \Big(|0\rangle + e^{2\pi i \cdot 0.b_{n-2}b_{n-1}}|1\rangle\Big)\Big) \\ = \; & |b_{n-1}\rangle \otimes |b_n\rangle \otimes \frac{1}{\sqrt{2}} \cdot \big(|0\rangle + e^{2\pi i \cdot 0.b_{n-2}b_{n-1}b_n}|1\rangle\big) \\ = \; & |b_{n-1}\rangle \otimes |b_n\rangle \otimes |z_3\rangle. \end{aligned}$$

Kehre die Reihenfolge der Berechnungen um.

- Berechne $|z_n\rangle$ zuerst: Wende zuerst H auf $|b_1\rangle$ an, danach C_P^2 kontrolliert durch $|b_2\rangle$, C_P^3 kontrolliert durch $|b_3\rangle$, bis schließlich C_P^n kontrolliert durch $|b_n\rangle$ angewandt wird.
  - n Gatter werden benötigt.
- Führe die Berechnung weiter mit der Berechnung von $|z_{n-1}\rangle$ bis schließlich auch $|z_1\rangle$ berechnet ist.
  - Insgesamt genügen $n + (n-1) + \cdots + 1 = \binom{n}{2}$ Gatter.
  - Die Operatoren C_P^s für $s = \Omega(\log_2 n)$ unterscheiden sich kaum vom Einheitsoperator $\Longrightarrow \mathcal{O}(n \log_2 n)$ Gatter reichen für eine approximative Berechnung.

Schnelle Faktorisierung

Schnelle Faktorisierung

Bestimme die Primfaktorzerlegung für eine natürliche Zahl N.

- Effiziente deterministische Algorithmen, also Algorithmen mit Laufzeit $\text{poly}(\log_2 N)$, sind nicht bekannt.
- Die schnellsten deterministischen Algorithmen benötigen mindestens asymptotische Laufzeit $2^{\Omega(\log_2^b N)}$ für $b \geqslant 1/3$:
  - Das quadratische Sieb hat vermutlich Laufzeit $2^{\mathcal{O}(\sqrt{\log N \cdot \log\log N})}$,
  - für das Zahlkörpersieb scheinen $2^{\mathcal{O}((\log N)^{1/3} \cdot (\log\log N)^{2/3})}$ Operationen zu genügen.
- 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.

Faktorisierung und Periodenbestimmung

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
- $x^{r/2} + 1$ kein Vielfaches von N ist.

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 besitzen $x^{r/2} + 1$ wie auch $x^{r/2} - 1$ gemeinsame Faktoren mit N: $x^{r/2} + 1$ ist nach Wahl von x kein Vielfaches von N und auch $x^{r/2} - 1$ ist kein Vielfaches, da r die Ordnung von x ist.

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

N ist effizient faktorisierbar, wenn die Periode einer Restklasse x modulo N effizient bestimmt werden kann.

Shor's Algorithmus für die Periodenbestimmung

Shor's Algorithmus (1/4)

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

1. Sei x eine Restklasse modulo N mit gerader – aber unbekannter – Periode r und N sei kein Teiler von $x^{r/2} + 1$.
2. Wende den Hadamard-Operator

$$|0^\ell\rangle \otimes |0^n\rangle \overset{H^{\otimes \ell}}{\mapsto} \frac{1}{\sqrt{2^l}} \cdot \sum_{a=0}^{2^\ell - 1} |a\rangle \otimes |0^n\rangle$$

   auf die ersten ℓ Qubits an.
3. Eine Quanten-Subroutine führt den Operator $|a\rangle|0^n\rangle \mapsto |a\rangle|x^a \mod N\rangle$ aus:
   - Simuliere ein effizientes deterministisches Programm, das $x^a \mod N$ durch wiederholtes Quadrieren bestimmt.

   Der Zustand

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

   wird erreicht: Quantenparallelität wird ausgenutzt.

Shor's Algorithmus (2/4)

4. Beobachte die letzten n Qubits mit dem Ergebnis $x^a \mod N$.
   - Dann gilt $x^a \equiv x^b \mod N \iff a \equiv b \mod r$ für die Periode r von x.
   - Vernachlässige die letzten n Qubits: Das Ergebnis $x^a \mod N$ ist uninteressant.

Für m mit $(m-1) \cdot r + a < 2^\ell \leqslant m \cdot r + a$ ist der Zustand kollabiert zu

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

Wenn r ein Teiler von 2^ℓ ist, dann ist $m \cdot r = 2^\ell$.

- Es ist $|z\rangle = \frac{1}{\sqrt{m}} \Big(|a\rangle + |r+a\rangle + |2r+a\rangle + |3r+a\rangle + \cdots \Big)$.
- Wenn wir $|z\rangle$ mehrfach beobachten könnten, dann hätten wir leichtes Spiel?! Leider beobachten wir dann $x^c \mod N$ (für $a \neq c$) statt $x^a \mod N$.

Scott Aaronson:

In science and engineering, any time you have a periodic signal and you're trying to extract its period, there's a single tool that gets called upon: The Fourier Transform!

5. Wende die Quanten-Fourier-Transformation F_{2^ℓ} auf

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

an. Es ist

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

Beobachte $F_{2^\ell}|z\rangle$: Basiszustand $|b\rangle$ ist hochwahrscheinlich falls $|\alpha_b|^2$ groß ist.

Shor's Algorithmus (4/4)

Es ist $F_{2^\ell}|z\rangle = \frac{1}{\sqrt{m2^\ell}} \cdot \sum_{b=0}^{2^\ell-1} e^{2\pi i \cdot \frac{ab}{2^\ell}} \underbrace{\left(\sum_{j=0}^{m-1} e^{2\pi i \cdot \frac{jrb}{2^\ell}} \right)}_{\alpha_b} |b\rangle$.

6. Beobachte $F_{2^\ell}|z\rangle$ mehrfach:
   - Führe jedes Mal die Schritte 2-5 durch und beobachte dann b.
   - Zentrale Fragen:
     - ⋆ Welche b's werden wir beobachten, d.h. wann ist die quadrierte Amplitude $|\alpha_b|^2$ groß?
     - ⋆ Wie sind die Beobachtungen auszuwerten?
7. Bestimme die Ordnung von x aus diesen Beobachtungen.

Analyse: r ist ein Teiler von 2^ℓ

$$F_{2^\ell}|z\rangle = \frac{1}{\sqrt{m2^\ell}} \cdot \sum_{b=0}^{2^\ell-1} e^{2\pi i \cdot \frac{ab}{2^\ell}} \underbrace{\left(\sum_{j=0}^{m-1} e^{2\pi i \cdot \frac{jrb}{2^\ell}} \right)}_{\alpha_b} |b\rangle$$

- r teilt 2^ℓ. Also ist $(m-1)r + a < 2^\ell \leqslant mr + a$ und $m = \frac{2^\ell}{r}$ folgt.
  - Es ist $\alpha_b = \sum_{j=0}^{m-1} \omega^{jb}$ für die primitive $m$te Einheitswurzel $\omega = e^{2\pi i/m}$.
- Ist b kein Vielfaches von m, dann ist verschwindet α_b als Summe aller Potenzen einer nicht-trivialen m.ten Einheitswurzel: Destruktive Interferenz!
- Wenn b ein Vielfaches von m ist: Konstruktive Interferenz!
  - $|\frac{\alpha_b}{\sqrt{m2^\ell}}|^2 = (\frac{m}{\sqrt{m2^\ell}})^2 = \frac{m}{2^\ell} \Longrightarrow$ alle m-Vielfachen b sind gleichwahrscheinlich.
  - Beobachte ein m-Vielfaches b, d.h. $b = m \cdot s$, bzw. $\frac{b}{2^\ell} = \frac{s}{r}$ für $s < r$.
- Beobachte genügend viele b's bis s und r teilerfremd sind $\Longrightarrow$ r ist der Nenner in $\frac{b}{2^\ell}$ nach Kürzung.

Analyse: r ist kein Teiler von 2^ℓ (1/3)

$$F_{2^\ell}|z\rangle = \frac{1}{\sqrt{m2^\ell}} \cdot \sum_{b=0}^{2^\ell-1} e^{2\pi i \cdot \frac{ab}{2^\ell}} \underbrace{\left(\sum_{j=0}^{m-1} e^{2\pi i \cdot \frac{jrb}{2^\ell}} \right)}_{\alpha_b} |b\rangle$$

Fall 1: $b = \lfloor s \cdot \frac{2^\ell}{r} \rceil$ ist eine nächstliegende Zahl zu einem Vielfachen von $\frac{2^\ell}{r}$.

Es gelte $b = s \cdot \frac{2^\ell}{r} + \varepsilon$. Dann ist

$$\alpha_b = \sum_{j=0}^{m-1} e^{2\pi i \cdot \frac{jr(s \cdot \frac{2^\ell}{r} + \varepsilon)}{2^\ell}} = \sum_{j=0}^{m-1} e^{2\pi i \cdot \left(js + \frac{jr \cdot \varepsilon}{2^\ell}\right)} = \sum_{j=0}^{m-1} e^{2\pi i \cdot \frac{jr \cdot \varepsilon}{2^\ell}}$$

Für die primitive 2^ℓ.te Einheitswurzel ω werden $m \approx \frac{2^\ell}{r}$ aufeinanderfolgende Potenzen von $\omega^{r\varepsilon}$ addiert $\Longrightarrow$ „zumeist“ konstruktive Interferenz $\Longrightarrow$ b hat relativ große W-keit.

Analyse: r ist kein Teiler von 2^ℓ (2/3)

$$F_{2^\ell}|z\rangle = \frac{1}{\sqrt{m2^\ell}} \cdot \sum_{b=0}^{2^\ell-1} e^{2\pi i \cdot \frac{ab}{2^\ell}} \underbrace{\left(\sum_{j=0}^{m-1} e^{2\pi i \cdot \frac{jrb}{2^\ell}} \right)}_{\alpha_b} |b\rangle$$

Fall 2: $b \neq \lfloor s \cdot \frac{2^\ell}{r} \rceil$ für alle $s \in \mathbb{N}$.

Es gelte $b = s \cdot \frac{2^\ell}{r} + t + \varepsilon$ für eine ganze Zahl t. Dann ist

$$\alpha_b = \sum_{j=0}^{m-1} e^{2\pi i \cdot \frac{jr(s \cdot \frac{2^\ell}{r} + t + \varepsilon)}{2^\ell}} = \sum_{j=0}^{m-1} e^{2\pi i \cdot \left(js + \frac{jr \cdot (t+\varepsilon)}{2^\ell} \right)} = \sum_{j=0}^{m-1} e^{2\pi i \cdot \frac{jr \cdot (t+\varepsilon)}{2^\ell}}$$

Für die primitive 2^ℓ.te Einheitswurzel ω werden $m \approx \frac{2^\ell}{r}$ aufeinanderfolgende Potenzen von $\omega^{r(t+\varepsilon)}$ addiert $\Longrightarrow$ der Einheitskreis wird mehrfach durchlaufen $\Longrightarrow$ meist destruktive Interferenz bis auf (partiellen) letzten Durchlauf $\Longrightarrow$ b hat relativ kleine W-keit.

Analyse: r ist kein Teiler von 2^ℓ (3/3)

Die meisten Beobachtungen b weichen nur wenig von einem Vielfachen von $\frac{2^\ell}{r}$ ab, d.h. es ist häufig $b = \lfloor s \cdot \frac{2^\ell}{r} \rceil$.

- Es ist $b = s \cdot \frac{2^\ell}{r} + \varepsilon$ und deshalb
- $|\frac{b}{2^\ell} - \frac{s}{r}| \leqslant \frac{\varepsilon}{2^\ell}$: $\frac{s}{r}$ ist als naheliegender Bruch mit kleinem Nenner sichtbar, denn $2^\ell \approx N^2 > r^2$.
- Was ist zu tun?
  - b und $2^\ell \approx N^2$ sind bekannt, r ist eine (kleine) Zahl zwischen 1 und N.
  - Überprüfe, ob $\frac{b}{2^\ell}$ durch einen Bruch mit einem sehr kleinen Nenner, nämlich der Größe höchstens N approximierbar ist.
    - ⋆ Bestimme r aus einer Kettenbruchentwicklung von $\frac{b}{2^\ell}$.
    - ⋆ Und wenn s und r nicht teilerfremd sind? Wiederhole die Beobachtung.

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

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

Der Hamiltonoperator

Physikalische Systeme und Informatik

1. Kann „Physik“ von einem klassischen Rechner simuliert werden?
2. Kann „Physik“ von einem Quantenrechner simuliert werden?
   - Diskrete versus kontinuierliche Zeit
   - Der Hamilton-Operator steuert die Anwendung unitärer Operatoren.
3. Gibt es eine universelle Quanten-Simulation?
   - Quanten-Schaltkreise, Quanten-Turingmaschine
   - „Effiziente“ physikalische Systeme
   - Rechnet die Natur effizienter als es Rechner vermögen?

Richard Feynman: *Nature isn’t classical, dammit, and if you want to make a simulation of Nature, you’d better make it quantum mechanical, and by golly it’s a wonderful problem, because it doesn’t look so easy.*

Matrizen exponentieren

Sei A eine quadratische Matrix mit komplexwertigen Einträgen. Dann setze

$$e^A := \sum_{k=0}^{\infty} \frac{A^k}{k!}.$$

Z.B.: Sei $D(\lambda_1, \ldots, \lambda_N)$ die Diagonalmatrix mit den Einträgen $\lambda_1, \ldots, \lambda_N$. Dann ist

$$e^{D(\lambda_1,\ldots,\lambda_N)} = D(e^{\lambda_1}, \ldots, e^{\lambda_N}).$$

Wir sind vor allem an hermiteschen Matrizen A interessiert: Es gibt also eine unitäre Matrix U und eine reellwertige Diagonalmatrix D mit $A = UDU^{-1}$, und wir erhalten

$$e^A = \sum_{k=0}^{\infty} \frac{(UDU^{-1})^k}{k!} = \sum_{k=0}^{\infty} U \frac{D^k}{k!} U^{-1} = U \cdot e^D \cdot U^{-1}.$$

Beachte, dass U^{-1} mit der Adjungierten U^* von U übereinstimmt.

Evolution in kontinuierlicher Zeit

Ein quantenmechanisches System evolviert nicht in diskreten, sondern in kontinuierlicher Zeit. Hier machen wir die folgenden Annahmen:

- Die zeitabhängigen Zustände $|\psi(t)\rangle$ gehören einem Hilbertraum $\mathcal{H}$ endlicher Dimension an.
- Die Zeitevolution wird durch die **Schrödingergleichung**

$$i \cdot \hbar \cdot \frac{d\,|\psi(t)\rangle}{dt} = H|\psi(t)\rangle$$

beschrieben: $\hbar$ ist die reduzierte Plancksche Konstante und H ein hermitescher Operator.

Wir werden im Folgenden die Plancksche Konstante unterschlagen und vereinfachend annehmen, dass H zeitunabhängig ist. In diesem Fall ist

$$|\psi(t)\rangle = e^{-i \cdot H \cdot t}|\psi(0)\rangle$$

die Lösung der Schrödingergleichung, denn für $H = UD(\lambda_1, \ldots, \lambda_N)U^*$ ist

$$e^{-iHt} = Ue^{-iD(\lambda_1,\ldots,\lambda_N)t}U^* = U \cdot D(e^{-it\cdot\lambda_1}, \ldots, e^{-it\cdot\lambda_N})U^*.$$

Der Operator e^{-iHt}

1. Die Lösung e^{-iHt} der Schrödingergleichung ist für jede hermitesche Matrix $H = UD(\lambda_1, \ldots, \lambda_N)U^*$ eine unitäre Matrix, denn

$$e^{-iHt} \quad = \quad UD(e^{-it\lambda_1}, \ldots, e^{-it\lambda_N})U^*$$

   ist ein Produkt von unitären Matrizen: Auch die Diagonalmatrix ist unitär, da die Eigenwerte $\lambda_1, \ldots, \lambda_N$ reellwertig sind.

2. Zu jeder unitären Matrix U gibt es eine hermitesche Matrix H mit $U = e^{-iHt}$:
   - Zuerst diagonalisiere U, d.h. bestimme eine unitäre Matrix V mit

$$U = V \cdot D(\lambda_1, \ldots, \lambda_N) \cdot V^*.$$

   - Dann logarithmiere, d.h. bestimme μ_i mit $\lambda_i = e^{-it \cdot \mu_i}$.
   - Setze $H = V \cdot D(\mu_1, \ldots, \mu_N) \cdot V^*$

Bis auf den Startzustand $|\psi(0)\rangle$ steuert der Hamiltonoperator die zeitliche Evolution des physikalischen Systems. In diskreter Sichtweise stimmt e^{-iHt} mit t aufeinanderfolgenden Anwendungen des Operators e^{-iH} überein.

e^{-iHt} und sein Hamiltonoperator H

- Für $H = UD(\lambda_1, \ldots, \lambda_N)U^*$ ist $e^{-iHt} = UD(e^{-it\lambda_1}, \ldots, e^{-it\lambda_N})U^*$:
  - Sowohl H wie auch e^{-iHt} besitzen die Spalten $|v_k\rangle$ von U als Eigenvektoren.
  - Den Eigenwerten λ_k von H entsprechen die Eigenwerte $e^{-it\lambda_k}$ von e^{-iHt}.
- Für einen Eigenwert λ_k mit Eigenzustand $|v_k\rangle$ gilt

$$e^{-iHt}|v_k\rangle = e^{-it\lambda_k}|v_k\rangle.$$

  - Der Eigenzustand hat sich eine neue Phase „eingefangen“, die aber für sich genommen keinen Effekt hat.
- Ist $|z\rangle = \sum_{k=1}^{N} \alpha_k |v_k\rangle$, dann ist $e^{-iHt}|z\rangle = \sum_{k=1}^{N} \alpha_k e^{-it\lambda_k}|v_k\rangle$
  - Von $\alpha_k = \|\alpha_k\| e^{i\phi}$ nach $\alpha_k e^{-it\lambda_k} = \|\alpha_k\| e^{i(\phi - t\lambda_k)}$.
  - Die Eigenvektoren wandern mit ihren Phasen um den Einheitskreis mit einer Geschwindigkeit, die proportional zu ihrer „Energie“ λ_k ist.
  - Aaronson: This presents a terrifyingly boring picture of the history of the universe.

Energieerhaltung: Die erwartete Energie $\sum_{k=1}^{N} |\alpha_k|^2 \lambda_k$ von Zustand $|z\rangle$ ist konstant.

Energieniveaus

Energieniveaus und Energieeigenzustände

Für eine hermitesche Matrix H und eine unitäre Matrix U gelte

$$H = UD(\lambda_1, \ldots, \lambda_N)U^* \quad \text{für } \lambda_1 \leqslant \lambda_2 \leqslant \cdots \leqslant \lambda_N.$$

Die zugehörigen Eigenzustände seien $|v_1\rangle, \ldots, |v_N\rangle$.

- Die Eigenwerte λ_k von H heißen **Energieniveaus**, ihre Eigenvektoren $|v_k\rangle$ heißen **Energieeigenzustände**. Beachte, dass Energieniveaus stets reellwertig sind.
- $|v_1\rangle$ heißt **Grundzustand** und λ_1 heißt Energie des Grundzustands.

  $|v_2\rangle$, bzw. $|v_3\rangle$ ist der erste bzw. zweite angeregte Zustand.
  - Um Energie zu minimieren, tendiert ein physikalisches System dazu, Energieeigenzustände mit geringem Energieniveau aufzusuchen.
  - Der Grundzustand bzw. niedrige angeregte Zustände sind „attraktiv“:
    - ★ Wandert ein Elektron in eine weiter innen liegende Schale unter Emission eines Photons, wird Energie abgegeben.
    - ★ Wird ein Elektron von einem Photon getroffen, wandert es in eine weiter aussen liegende Schale unter Aufnahme von Energie: Ein eher unwahrscheinliches Ereignis.
    - ★ Beachte Umkehrbarkeit trotz der Attraktivität niedriger Energieeigenzustände.

Summe von Hamiltonoperatoren

Wie modelliert man den *gleichzeitigen* Einfluß verschiedener Kräfte auf ein gegebenes System? Über die Summe von Hamiltonoperatoren.

- Wenn A, B hermitesch sind, dann ist auch $A + B$ hermitesch. Aber im Allgemeinen ist
$$e^{A+B} \neq e^A \cdot e^B.$$
Gleichheit folgt, falls A, B kommutieren, d.h. wenn $AB = BA$ gilt.
- Wie soll man dann einen unitären Operator $e^{i(H_1+\cdots+H_k)t}$ für großes k effizient anwenden, wenn man nur Zugriff auf die einzelnen Operatoren hat?
  - Wende die Methode der *Trotterisierung* an: Die Lie-Produkt-Formel besagt
$$\lim_{\varepsilon \to 0} \left(e^{\varepsilon A} \cdot e^{\varepsilon B} \right)^{1/\varepsilon} = e^{A+B}.$$
Dann approximiere e^{A+B} durch $\left(e^{A/r} e^{B/r}\right)^r$ für ein genügend großes r.

Das Problem der k-lokalen Hamiltonians

Grundzustände für k-lokale Hamiltonians

Ist die Bestimmung eines Grundzustands algorithmisch schwierig?

Es gelte $\mathcal{H} = \mathbb{C}^{2^n}$.

(a) Ein Hamiltonoperator $H : \mathcal{H} \to \mathcal{H}$ ist genau dann **k-lokal**, wenn H nur auf höchstens k der n Qubits agiert.

(b) Das Problem der k-lokalen Hamiltonians:

- $H_1, \ldots, H_m$ seien k-lokal mit Eigenwerten in $[0, 1]$. Für

$$H = H_1 + \cdots + H_m$$

ist die Energie eines Grundzustands von H approximativ zu bestimmen.

- Das Problem der 1-lokalen Hamiltonians kann effizient mit deterministischen Algorithmen gelöst werden. Aber schon für $k \geqslant 2$ ist „der Ofen aus“.
- Wir zeigen, dass das Problem der 3-lokalen Hamiltonians NP-hart ist.

Max-3SAT und 3-lokale-Hamiltonians

Selbst bei bekannten Grundzuständen von 3-lokalen Hamiltonians H_k ist die Bestimmung eines Grundzustands von $H = H_1 + \ldots + H_m$ NP-hart:

1. Sei $\phi = \bigwedge_{j=1}^{m} k_j$ eine 3-KNF mit Klauseln $k_j := \ell_{j_1} \vee \ell_{j_2} \vee \ell_{j_3}$ zu den aussagenlogischen Variablen $x_1, \ldots, x_n$. (Das Literal ℓ_{j_r} stimmt entweder mit x_{j_r} oder $\neg x_{j_r}$ überein.)
2. Wähle $\mathcal{H} = \mathbb{C}^{2^n}$ als Hilbertraum.
   - Für Klausel $k_j := \ell_{j_1} \vee \ell_{j_2} \vee \ell_{j_3}$ ist der Hamiltonoperator H_j eine $2^n \times 2^n$ Matrix, die nur auf den Qubits $x_{j_1}, x_{j_2}, x_{j_3}$ nicht-trivial agiert:
     - ⋆ Es ist genau dann $H_j|b_{j_1} b_{j_2} b_{j_3}\rangle = 1$, wenn die drei Wahrheitswerte Klausel k_j falsifizieren und sonst ist $H_j|b_{j_1} b_{j_2} b_{j_3}\rangle = 0$.
     - ⋆ Das Energieniveau des Grundzustands von $H = \sum_{j=1}^{m} H_j$ ist Null, wenn ϕ erfüllbar ist, und ansonsten positiv: Erfüllende Belegungen definieren Grundzustände.

- Die Sprachenversion des Problems der k-Hamiltonians wird vermutlich für $k \geqslant 2$ nicht zu NP gehören.
- Um die Komplexität des Problems der k-lokalen Hamiltonians bestimmen zu können, benötigen wir eine Quanten-Version von NP.

QMA: Quantum-Merlin-Arthur

QMA: Quantum-Merlin-Arthur (1/2)

In einer Quantenversion von NP wird man mit einem Zustand als Zeugen für die Zugehörigkeit einer Eingabe x zu einer Sprache L arbeiten wollen:

Dieser Zustand darf in einem hoch-dimensionalen Hilbertraum liegen!

Eine Sprache L gehört genau dann zu QMA, wenn einen effizienten Quantenalgorithmus Q und ein Polynom p mit den beiden folgenden Eigenschaften gibt:

- Wenn $x \in \Sigma^n$ ein Wort der Sprache L ist, dann gibt es einen Zustand $|z\rangle \in \mathbb{C}^{2^{p(n)}}$, so dass Q die Eingaben x und $|z\rangle$ mit W-keit mindestens $\frac{2}{3}$ akzeptiert.

  Der mächtige Zauberer Merlin hat seinen König Arthur überzeugt.

- Wenn $x \in \Sigma^n$ nicht zur Sprache L gehört, dann akzeptiert Q für jeden Zustand $|z\rangle \in \mathbb{C}^{2^{p(n)}}$ die Eingaben x und $|z\rangle$ mit W-keit höchstens $\frac{1}{3}$.

  König Arthur ist zwar ressourcen-beschränkt, aber klug genug, um nicht auf irgendeinen „faulen Zauber“ von Merlin hereinzufallen.

QMA: Quantum-Merlin-Arthur (2/2)

BQP $\subseteq$ QMA $\subseteq$ PP $\subseteq$ PSPACE sowie NP $\subseteq$ QMA.

Die folgenden *Promise-Probleme* sind vollständig für QMA (unter effizienten determ. Reduktionen): Um das Versprechen zu formulieren, werden reelle Zahlen α, β mit $\alpha - \beta \geqslant \frac{1}{\text{poly}(n)}$ benötigt.

- Die Sprachenversion des Problem der k-lokalen Hamiltonians:
  - Sei $H = H_1 + \cdots + H_m$ für k-lokale Hamiltonians H_i mit Energieniveaus in $[0, 1]$. Akzeptiere Eingabe $(H_1, \ldots, H_m)$, falls $\lambda_1 \leqslant \beta$ bzw. verwerfe, falls $\lambda_1 \geqslant \alpha$ gilt. λ_1 ist die Energie des Grundzustands von H.
- Quantum-Circuit-Sat: Für einen Quanten-Schaltkreis S (auf $n + m$ Qubits),
  - akzeptiere S, falls es einen Zustand $|z\rangle \in \mathbb{C}^{2^n}$ gibt, so dass S die Eingabe $|z0^m\rangle$ mit W-keit mindestens α akzeptiert.
  - Verwerfe S, wenn die Akzeptanz-W-keit für alle Zustände $|z\rangle \in \mathbb{C}^{2^n}$ höchstens β beträgt.
- Weitere QMA-vollständige Probleme finden sich in QMA-complete problems von Adam Bookatz.

QMA-vollständige Probleme erscheinen signifikant härter und weniger reich an Variationen als NP-vollständige Probleme.