Quantenalgorithmen

(Vorlesung vom 18.10.06) 11:40 - 13:10 C205

H. May	M. Hirvensalo, Quantum Computing
M. Vollmer	Chuang/Nielsen, Quantum Computation and Quantum Information
Maike Ritzenhofen	D. Aharonov, Quantum Computation

Übungsbetrieb: 2-wöchentlich, Start: 26.10.
Do. 9:50 - 11:30
Mo. 9:50 - 11:30 H102

Warum Quantenalgorithmen?

1) Notwendigkeit: Moore's Gesetz
   Bald Rechnerstruktur subatomarer Größe (Quantenphysik)
2) Potential: Quantencomputer können klassische Computer simulieren + event. mehr
   - Polyzeit-Alg. für Faktorisierung \ Dlog
   - Exp. Speed-up für relativierte Modelle
   - Quadratischer Speed-up für Datenbanksuche
   - Quantenkryptographie /-kodierung

Berechnungen:

	Eingabe	→ Berechnung	→ Ausgabe
Klassisch:	Bits	Boolsche Fkt./Schaltkreise prob. DTM, Kopierfunktion	Bits
Quanten:	Qubits	Reversible Fkt./Quantenschaltkreise QTM, lineare Funktionen Quantenparallelität, Interferenz, Verschränkung keine Kopiefunktion	Messung liefert Qubits

Probleme bei Implementierung: · Dekohärenz, Skalierbarkeit
· Quantenfehlerkorrektur

Klassische probabilistische Systeme: Seien $x_1, \dots, x_n$ Basiszustände.

Wahrscheinlichkeitsverteilung ~~eines~~ Zustandsraum:

$$p_1[x_1] + p_2[x_2] + \dots + p_n[x_n] \quad \text{mit } 0 \le p_i \le 1,\ \sum_{i=1}^n p_i = 1$$

Zustandsübergang $x_i \mapsto p_{1i}[x_1] + p_{2i}[x_2] + \dots + p_{ni}[x_n]$, $\sum_{j=1}^n p_{ji} = 1 \ \forall i$ (Markovkette)

Allgemein: $p_1[x_1] + p_2[x_2] + \dots + p_n[x_n]$

$$\mapsto p_1(p_{11}[x_1] + \dots + p_{n1}[x_n]) + \dots + p_n(p_{1n}[x_1] + \dots + p_{nn}[x_n])$$

$$= (\underbrace{p_1 p_{11} + p_2 p_{12} + \dots + p_n p_{1n}}_{p_1'})[x_1] + \dots + (\underbrace{p_1 p_{n1} + \dots + p_n p_{nn}}_{p_n'})[x_n]$$

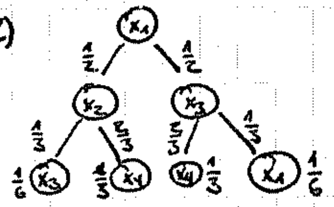
D.h. $$\begin{pmatrix}p_1'\\p_2'\\\vdots\\p_n'\end{pmatrix} = \overbrace{\begin{pmatrix}p_{11}&\cdots&p_{1n}\\&\ddots&\\p_{n1}&\cdots&p_{nn}\end{pmatrix}}^{\text{Markov-Matrix}}\cdot\begin{pmatrix}p_1\\\vdots\\\vdots\\p_n\end{pmatrix}$$

Übung: Zeigen Sie, dass $\sum_{i=1}^{n} p_i' = \sum_{i=1}^{n} p_i$.

Bsp.: (1) Münzwurf: Kopf $\mapsto \frac{1}{2}$ [Kopf] + $\frac{1}{2}$ [Zahl]

Zahl $\mapsto \frac{1}{2}$ [Kopf] + $\frac{1}{2}$ [Zahl]

(2)

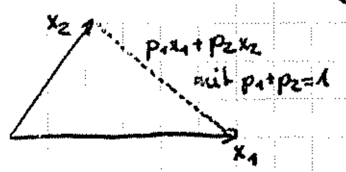


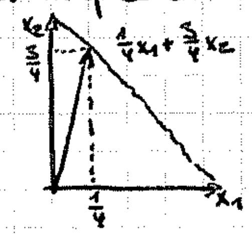
x_1, x_3 : Ws. $\frac{1}{6}$

x_4 : Ws $\frac{2}{3}$

Strategie: Maximiere Ws. des gewünschten Endzustands.

Vektorraum-Interpretation:
- $x_1, x_2, \dots, x_n$ Basisvektoren eines n-dim Vektorraums
- Wahrscheinlichkeitsverteilungen entsprechen konvexen Linearkombinationen





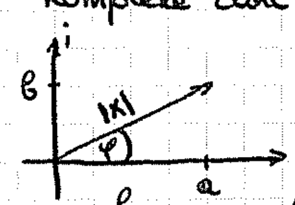
1-Qubit Systeme

Zustände eines Qubits: Einheitsvektoren im $\mathbb{C}^2$.

Exkurs über die komplexen Vektorräume $\mathbb{C}^n$:

$|x\rangle \in \mathbb{C}^n \Leftrightarrow |x\rangle = (x_1, \dots, x_n),\ x_i \in \mathbb{C}$ „ket"-Notation

Komplexe Zahl: $x = a + ib \quad a, b \in \mathbb{R},\ i = \sqrt{-1}$ d.h. $i^2 = -1$.



Konjugiert Komplexes $x^* = a - ib$

$|x| = \sqrt{x \cdot x^*} = \sqrt{a^2 + b^2}$

$\sin\varphi = \frac{b}{|x|},\ \cos\varphi = \frac{a}{|x|} \Rightarrow x = (\cos\varphi + i \sin\varphi) \cdot |x| = e^{i\varphi} \cdot |x|$ insb. $e^{2\pi i} = 1$

Sei $|x\rangle = (x_1, \dots, x_n)$ $\quad \langle x| = (x_1^*, \dots, x_n^*)$ und $\langle x|x\rangle = \sum_{i=1}^{n} x_i x_i^* = |x|^2$

$|y\rangle = (y_1, \dots, y_n)$ $\quad \langle x|y\rangle = \sum_{i=1}^{n} x_i^* y_i$ $\quad |x\rangle, |y\rangle$ orthogonal $\Leftrightarrow \langle x|y\rangle = 0$

Satz: Die Vektoren $|x_1\rangle, |x_2\rangle, \dots, |x_n\rangle \in \mathbb{C}^n$ bilden eine orthonormale Basis des $\mathbb{C}^n$ falls

1.) $\langle x_i|x_j\rangle = 0$ für alle i,j mit $i \neq j$

2.) $\left||x_i\rangle\right| = 1$ für $i = 1, \dots, n$

Orthonormale Basis für $\mathbb{C}^2$

Bsp.: • $|0\rangle = (1,0)$, $|1\rangle = (0,1)$

• $(e^{i\varphi},0)$, $(0,e^{i\varphi})$

• $\frac{1}{\sqrt{5}}(1,2)$, $\frac{1}{\sqrt{5}}(2,-1)$

Orthonormale Basen für $\mathbb{C}^4$:

• $|0\rangle = (1,0,0,0)$, $|1\rangle = (0,1,0,0)$, $|2\rangle = (0,0,1,0)$, $|3\rangle = (0,0,0,1)$

• $\frac{1}{5}(1,2,2,4)$, $\frac{1}{5}(2,-1,4,-2)$, $\frac{1}{5}(2,4,-1,-2)$, $\frac{1}{5}(4,-2,-2,1)$

<u>Zustand eines Qubits</u>: Seien $|0\rangle, |1\rangle$ eine orthonormale Basis des $\mathbb{C}^2$. Der Zustand eines Qubits ist ein Einheitsvektor der Form: $\alpha_0 \cdot |0\rangle + \alpha_1 \cdot |1\rangle$, $\alpha_0, \alpha_1 \in \mathbb{C}$

<u>Übung</u>: $|\alpha_0 \cdot |0\rangle + \alpha_1 \cdot |1\rangle| = 1 \Leftrightarrow |\alpha_0|^2 + |\alpha_1|^2 = 1$

<u>Allgemein</u>: Seien $|x_1\rangle, \dots, |x_n\rangle$ eine orthonormale Basis des $\mathbb{C}^n$ (auch H_n für Hilbertraum).

Zustand eines Quantensystems: $\alpha_1|x_1\rangle + \alpha_2|x_2\rangle + \dots + \alpha_n|x_n\rangle$ mit $|\alpha_1|^2 + \dots + |\alpha_n|^2 = 1$

Messung: x_i mit Ws. $|\alpha_i|^2$

<u>Bez.</u>: - Basisvektoren $|x_i\rangle$ werden <u>Basiszustände</u> genannt

• α_i heißen Amplituden.

• Allg. Zustand ist <u>Superposition</u> der Basiszustände (Überlagerung)

• $\psi(x_i) = \alpha_i$ heißt <u>Wellenfunktion</u>.

• $|x\rangle = e^{i\varphi}|y\rangle \Leftrightarrow$ Zustände $|x\rangle$ und $|y\rangle$ heißen äquivalent

<u>Vergleich</u>: Wahrscheinlichkeitsverteilung $p_1[x_1] + \dots + p_n[x_n]$ $\quad \sum_{i=1}^{n} p_i = 1$

Superposition $\alpha_1|x_1\rangle + \dots + \alpha_n|x_n\rangle$ $\quad \sum_{i=1}^{n} |\alpha_i|^2 = 1$, d.h. α_i Ws-Verteilung

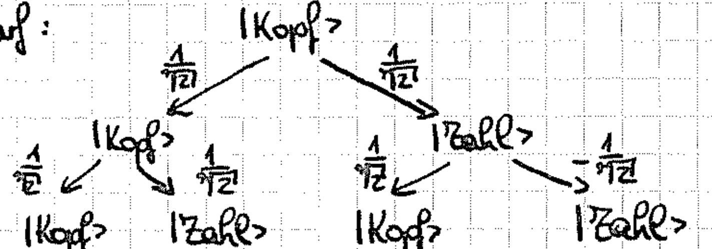
Trotzdem fundamental verschieden!

<u>Bsp.</u> Quanten-Münzwurf: $|Kopf\rangle \mapsto \frac{1}{\sqrt{2}}|Kopf\rangle + \frac{1}{\sqrt{2}}|Zahl\rangle$

$|Zahl\rangle \mapsto \frac{1}{\sqrt{2}}|Kopf\rangle - \frac{1}{\sqrt{2}}|Zahl\rangle$

Einfacher Münzwurf: Liefert Kopf oder Zahl mit Ws. jeweils $\frac{1}{2}$.

Zweifacher Münzwurf:



Amplituden: $\frac{1}{2}$ $\quad \frac{1}{2}$ $\quad \frac{1}{2}$ $\quad -\frac{1}{2}$

- Amplituden von $|Kopf\rangle$ summieren sich zu 1 → positive Interferenz
- Amplituden von $|Zahl\rangle$ summieren sich zu 0 → negative Interferenz (Auslöschung)
- Ebenen des Baums beschreiben Superpositionen → Quantenparallelität

Strategie: Statt die Ws. unerwünschter Konfigurationen klein zu halten, kann man auch deren Amplituden gegenseitig auslöschen.

25.10.06

Man beachte: Superposition $\alpha_1|x_1\rangle + \dots + \alpha_n|x_n\rangle$ liefert x_i mit Ws. $|\alpha_i|^2$

Wechsel zu anderer orthonormaler Basis $|x_1'\rangle, \dots, |x_n'\rangle$ mit $|x_1'\rangle = \alpha_1|x_1\rangle + \dots + \alpha_n|x_n\rangle$ liefert x_1' mit Ws. 1.

Zustandsübergänge

Da Quantenzustände stets Einheitsvektoren sind : längenerhaltende Abbildung

Aus den Gesetzen der Quantenphysik : lineare Abbildung, reversibel

Def. (unitäre Abb.): Eine lineare Abb. $U: \mathbb{C}^n \to \mathbb{C}^n$ heißt unitär, falls für alle $|x\rangle \in \mathbb{C}^n$ gilt: $\quad ||x\rangle| = \sqrt{\langle x|x\rangle} = \sqrt{\langle U|x\rangle | U|x\rangle\rangle} = |U|x\rangle|$

Eine Matrix heißt unitär falls $(U^*)^T = U^{-1}$.

Satz: Sei $U \in \mathbb{C}^{m \times m}$ eine unitäre Matrix. Dann gilt für alle $x \in \mathbb{C}^m$: $|U|x\rangle| = ||x\rangle|$

D.h. U beschreibt eine unitäre Abb.

Beweis: Lineare Algebra: Für jedes $A \in \mathbb{C}^{m \times m}$, $|x\rangle, |y\rangle \in \mathbb{C}^m$ gilt: $\langle x | A|y\rangle\rangle = \langle (A^*)^T|x\rangle | y\rangle\rangle$

$$\Rightarrow |U|x\rangle| = \sqrt{\langle U|x\rangle | U|x\rangle\rangle} = \sqrt{\langle \underbrace{(U^*)^T}_{U^{-1}} U|x\rangle | |x\rangle\rangle} = \sqrt{\langle x|x\rangle} = ||x\rangle|$$

Bsp. Hadamard-Walsh matrix $\quad W_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$

Übung: $W_2 \cdot (W_2^*)^T = I$

Anmerkung: W_2 beschreibt „Quanten-Münzwurf" (s. Bsp. 3, S. 5)

Entwicklung eines Quantenbits: Sei $|0\rangle = (1,0)$, $|1\rangle = (0,1)$, $U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = a\begin{pmatrix} 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{d.h. } |0\rangle \xmapsto{U} a|0\rangle + b|1\rangle$$

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} = c\begin{pmatrix} 1 \\ 0 \end{pmatrix} + d\begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad \text{d.h. } |1\rangle \xmapsto{U} c|0\rangle + d|1\rangle$$

Beispiele unitärer Abbildungen

Bsp. 1 (Quanten Not): $M_7 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ M_7 ist unitär, $(M_7^*)^T = M_7$

$(1,0) \mapsto (0,1)$ d.h. $|0\rangle \mapsto |1\rangle$ und $M_7^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

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

Bsp. 2 (Wurzel des Not): $\sqrt{M_7} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$

$$|0\rangle \xmapsto{\sqrt{M_7}} \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \xmapsto{\sqrt{M_7}} \frac{1+i}{2}\left(\frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle\right) + \frac{1-i}{2}\left(\frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle\right)$$

$$= \left(\left(\frac{1+i}{2}\right)^2 + \left(\frac{1-i}{2}\right)^2\right) \cdot |0\rangle + 2 \cdot \frac{1-i^2}{4}|1\rangle$$

$$= \frac{1+2i+i^2+1-2i+i^2}{4} \cdot |0\rangle + \frac{4}{4}|1\rangle = |1\rangle$$

Äquivalent $|1\rangle \xmapsto{\sqrt{M_7}} \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \xmapsto{\sqrt{M_7}} |0\rangle$

Wegen $\left|\frac{1+i}{2}\right|^2 = \left|\frac{1-i}{2}\right|^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$:

Nach einmaliger Anwendung von $\sqrt{M_7}$ auf $|0\rangle, |1\rangle$: Messung von $|0\rangle, |1\rangle$ mit Ws. $\frac{1}{2}$

Übung: $\sqrt{M_7}$ ist unitär, $(\sqrt{M_7})^2 = M_7$

Bsp. 3 (Hadamard-Walsh matrix): $W_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$|0\rangle \xmapsto{W_2} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \xmapsto{W_2} \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right)$$

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

Übung: W_2 ist unitär, $W_2^2 = I$

Bsp. 4 (Flip): $F = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

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

$|1\rangle \mapsto -|1\rangle$

allgemein: $F_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}$

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

$|1\rangle \mapsto e^{i\theta}|1\rangle$ Man beachte $F_\pi = F$

Def. (Äquivalenz von Zuständen): Zwei Zustände $|x\rangle, |y\rangle \in \mathbb{C}^n$ heißen genau dann äquivalent, wenn gilt: $|x\rangle = e^{i\theta}|y\rangle$

Flip transformiert $|1\rangle$ in einen äquivalenten Zustand. Messung von $|1\rangle$ mit selber Ws.

Übung: $U = \begin{pmatrix} i\cos\Theta & -i\sin\Theta \\ i\sin\Theta & i\cos\Theta \end{pmatrix}$ ist unitär.

Der Zustand eines 2-Qubit Systems ist ein Einheitsvektor im $\mathbb{C}^4$.

Exkurs über Tensorprodukte

Def. (Tensorprodukt): Seien $|x\rangle = (x_1, \dots, x_n) \in \mathbb{C}^n$, $|y\rangle = (y_1, \dots, y_m) \in \mathbb{C}^m$. Das Tensorprodukt von x und y ist definiert als

$$|x\rangle \otimes |y\rangle = (x_1 y_1, x_1 y_2, \dots, x_1 y_m, x_2 y_1, \dots, x_2 y_m, \dots, x_n y_1, \dots, x_n y_m) \in \mathbb{C}^{nm}$$

Bsp.:
- $|0\rangle = (1,0)$, $|1\rangle = (0,1)$

  $|0\rangle \otimes |1\rangle = (0,1,0,0)$
- $|x\rangle = \frac{1}{\sqrt{2}}(1,-1)$, $|y\rangle = \frac{1}{\sqrt{2}}(1,1)$

  $|x\rangle \otimes |y\rangle = \frac{1}{2}(1,1,-1,-1)$

Man beachte: $|x\rangle \otimes |y\rangle \neq |y\rangle \otimes |x\rangle$

Rechenregeln für das Tensorprodukt
- Distributivität:

  $\forall\, |x\rangle \in \mathbb{C}^n, |y\rangle, |z\rangle \in \mathbb{C}^m: \quad |x\rangle \otimes (|y\rangle + |z\rangle) = |x\rangle \otimes |y\rangle + |x\rangle \otimes |z\rangle$

  $\forall\, |x\rangle, |y\rangle \in \mathbb{C}^n, |z\rangle \in \mathbb{C}^m: \quad (|x\rangle + |y\rangle) \otimes |z\rangle = |x\rangle \otimes |z\rangle + |y\rangle \otimes |z\rangle$
- Skalare Multiplikation:

  $\forall\, |x\rangle \in \mathbb{C}^n, |y\rangle \in \mathbb{C}^m, c \in \mathbb{C}: \quad (c|x\rangle) \otimes y = c \cdot (|x\rangle \otimes |y\rangle) = |x\rangle \otimes (c|y)$
- Skalarprodukt

  $\forall\, |v\rangle, |x\rangle \in \mathbb{C}^n, |y\rangle, |z\rangle \in \mathbb{C}^m: \langle |v\rangle \otimes |y\rangle \,|\, |x\rangle \otimes |z\rangle \rangle = \langle v|x\rangle \cdot \langle y|z\rangle$
- Norm des Tensorprodukts

  $\forall\, |x\rangle \in \mathbb{C}^n, |y\rangle \in \mathbb{C}^m \quad : \big||x\rangle \otimes |y\rangle\big|^2 = ||x\rangle|^2 \cdot ||y\rangle|^2$

Lemma: Sei $|x_1\rangle, \dots, |x_n\rangle \in \mathbb{C}^n$ eine orthonormale Basis des $\mathbb{C}^n$ und $|y_1\rangle, \dots, |y_m\rangle \in \mathbb{C}^m$ eine orthonormale Basis des $\mathbb{C}^m$. Dann ist

$$|x_1\rangle \otimes |y_1\rangle, |x_1\rangle \otimes |y_2\rangle, \dots, |x_1\rangle \otimes |y_m\rangle, |x_2\rangle \otimes |y_1\rangle, \dots\dots, |x_n\rangle \otimes |y_m\rangle \in \mathbb{C}^{nm}$$

eine orthonormale Basis des $\mathbb{C}^{n \cdot m}$.

Beweis: Für $|x_i\rangle, |y_j\rangle$ gilt:

$$\big||x_i\rangle \otimes |y_j\rangle\big| = ||x_i\rangle| \cdot ||y_j\rangle| = 1 \cdot 1 = 1$$

Weiterhin sind die Vektoren paarweise orthogonal:

$\langle |x_i\rangle \otimes |y_j\rangle \,|\, |x_k\rangle \otimes |y_l\rangle\rangle = \langle x_i|x_k\rangle \cdot \langle y_j|y_l\rangle = 0$ für $i \neq k$ oder $j \neq l$. ∎

Bsp.:
- $|0\rangle = (1,0)$, $|1\rangle = (0,1)$

$|0\rangle \otimes |0\rangle = (1,0,0,0)$

$|0\rangle \otimes |1\rangle = (0,1,0,0)$

$|1\rangle \otimes |0\rangle = (0,0,1,0)$

$|1\rangle \otimes |1\rangle = (0,0,0,1)$

- $|x\rangle = \frac{1}{\sqrt{2}}(1,-1)$, $|y\rangle = \frac{1}{\sqrt{2}}(1,1)$

$|x\rangle \otimes |x\rangle = \frac{1}{2}(1,-1,-1,1)$

$|x\rangle \otimes |y\rangle = \frac{1}{2}(1,1,-1,-1)$

$|y\rangle \otimes |x\rangle = \frac{1}{2}(1,-1,1,-1)$

$|y\rangle \otimes |y\rangle = \frac{1}{2}(1,1,1,1)$

Notation: Seien $|x\rangle \in \mathbb{C}^n$, $|y\rangle \in \mathbb{C}^m$. Wir bezeichnen $|x\rangle \otimes |y\rangle$ abkürzend als $|xy\rangle$.

Insbesondere gilt $|0\rangle \otimes |0\rangle = |00\rangle$, $|0\rangle \otimes |1\rangle = |01\rangle$, usw.

2-Quanten Register

Bezeichne $|00\rangle = (1,0,0,0)$, $|01\rangle = (0,1,0,0)$, $|10\rangle = (0,0,1,0)$, $|11\rangle = (0,0,0,1)$ eine orthonormale Basis des $\mathbb{C}^4$.

Zustand eines 2-Qubit Systems: Ein Zustand eines 2-Qubit Systems ist ein Einheitsvektor

$$|v\rangle = c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle \in \mathbb{C}^4 \text{ mit } c_0, c_1, c_2, c_3 \in \mathbb{C}$$

Es gilt: $|v\rangle$ ist ein Einheitsvektor $\Leftrightarrow |c_0|^2 + |c_1|^2 + |c_2|^2 + |c_3|^2 = 1$

D.h. die Amplitudenquadrate liefern eine Ws-Verteilung.

Messung eines 2-Qubit Systems: Messung von $|v\rangle$ liefert
- Basiszustand $|00\rangle$ mit Ws. $|c_0|^2$
- — " — $|01\rangle$ mit Ws. $|c_1|^2$
- — " — $|10\rangle$ mit Ws. $|c_2|^2$
- — " — $|11\rangle$ mit Ws $|c_3|^2$

Nach der Messung befindet sich das 2-Qubit System im gemessenen Basiszustand. (Kollaps der Wellenfunktion, irreversibel)

01.11.

Messung eines einzelnen Qubits eines 2-Qubit Systems

Messung des 1. Qubits von $|v\rangle$ liefert:
- $|0\rangle$ mit Ws. $|c_0|^2 + |c_1|^2$
- $|1\rangle$ mit Ws. $|c_2|^2 + |c_3|^2$

Nach der Messung befindet sich das System im Zustand

$$\frac{c_0|00\rangle + c_1|01\rangle}{\sqrt{|c_0|^2+|c_1|^2}} \quad \text{falls } |0\rangle \text{ im 1. Qubit gemessen wurde}$$

$$\frac{c_2|10\rangle + c_3|11\rangle}{\sqrt{|c_2|^2+|c_3|^2}} \quad \text{falls } |1\rangle \text{ im 1. Qubit gemessen wurde}$$

Man beachte: $\left|\frac{c_0|00\rangle + c_1|01\rangle}{\sqrt{|c_0|^2+|c_1|^2}}\right| = \frac{1}{\sqrt{|c_0|^2+|c_1|^2}} \cdot |c_0|00\rangle + c_1|01\rangle| = \frac{1}{\sqrt{|c_0|^2+|c_1|^2}} \cdot \sqrt{|c_0|^2+|c_1|^2} = 1$

D.h. der neue Zustand ist wieder ein Einheitsvektor im $\mathbb{C}^4$.

<u>Def. (separabel/verschränkt)</u>: Wir nennen den Zustand $|z\rangle \in \mathbb{C}^4$ eines 2-Qubit Systems <u>separabel</u>, falls $|z\rangle = |x\rangle \otimes |y\rangle$ für $|x\rangle, |y\rangle \in \mathbb{C}^2$.
Ein Zustand, der nicht separabel ist, heißt <u>verschränkt</u>.

<u>Bsp.</u> (separabler Zustand): $|z\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$ ist separabel

Gesucht $\alpha_0, \alpha_1, \beta_0, \beta_1 \in \mathbb{C}$ mit $|z\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$

$$= \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

Gleichungssystem $\left| \begin{array}{l} \alpha_0\beta_0 = \frac{1}{2} \\ \alpha_0\beta_1 = \frac{1}{2} \\ \alpha_1\beta_0 = \frac{1}{2} \\ \alpha_1\beta_1 = \frac{1}{2} \end{array} \right|$ erfüllt für $\alpha_0 = \beta_0 = \alpha_1 = \beta_1 = \frac{1}{\sqrt{2}}$ (ebenso z.B. für $-\frac{1}{\sqrt{2}}$)

Sei $|z\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$ ein separabler Zustand.

<u>Frage</u>: Wie groß ist die Ws., $|0\rangle$ im 1. Qubit zu messen?

$$|z\rangle = \alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle + \alpha_1\beta_0|10\rangle + \alpha_1\beta_1|11\rangle$$

Messung von $|0\rangle$ im 1. Qubit mit Ws.:

$$|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2 = |\alpha_0|^2 \cdot \underbrace{(|\beta_0|^2 + |\beta_1|^2)}_{=1} = |\alpha_0|^2$$

Nach Messung von $|0\rangle$ befindet sich das 2-Qubit System im Zustand

$$\frac{\alpha_0\beta_0|00\rangle + \alpha_0\beta_1|01\rangle}{\sqrt{|\alpha_0\beta_0|^2 + |\alpha_0\beta_1|^2}} = \frac{\alpha_0|0\rangle \otimes (\beta_0|0\rangle + \beta_1|1\rangle)}{\sqrt{|\alpha_0|^2 \underbrace{(|\beta_0|^2+|\beta_1|^2)}_{=1}}} = \underbrace{\frac{\alpha_0}{\sqrt{|\alpha_0|^2}}|0\rangle}_{\text{äquivalent zu } |0\rangle} \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$$

Analog:

- Mit Ws. $|\alpha_1|^2$ Messung $|1\rangle$ im 1. Qubit. Nach Messung: $|1\rangle \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$
- Mit Ws $|\beta_0|^2$ Messung $|0\rangle$ im 2. Qubit. Nach Messung: $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |0\rangle$
- Mit Ws $|\beta_1|^2$ Messung $|1\rangle$ im 2. Qubit. Nach Messung: $(\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes |1\rangle$

Man beachte: Bei separablen 2-Qubit Systemen können die einzelnen Qubits unabhängig voneinander betrachtet werden.

Bsp. (verschränkter Zustand): $|z\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

Schreibe $|z\rangle = (\alpha_0|0\rangle + \alpha_1|1\rangle) \otimes (\beta_0|0\rangle + \beta_1|1\rangle)$

$$\Rightarrow \text{Gleichungssystem} \begin{vmatrix} \alpha_0\beta_0 = \frac{1}{\sqrt{2}} \\ \alpha_0\beta_1 = 0 \\ \alpha_1\beta_0 = 0 \\ \alpha_1\beta_1 = \frac{1}{\sqrt{2}} \end{vmatrix} \begin{matrix} \Rightarrow \alpha_0 \neq 0 \wedge \beta_0 \neq 0 \\ \Rightarrow \alpha_0 = 0 \vee \beta_1 = 0 \\ \Rightarrow \alpha_1 = 0 \vee \beta_0 = 0 \\ \Rightarrow \alpha_1 \neq 0 \wedge \beta_1 \neq 0 \end{matrix} \quad ↯ \text{ nicht erfüllbar}$$

Bezeichnung (EPR Paar): Ein 2-Qubit System im Zustand $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ wird als EPR-Paar (Einstein, Podolsky, Rosen) bezeichnet.

Messung des 1. Qubits eines EPR-Paars liefert

$|0\rangle$ mit Ws. $\frac{1}{2}$, nachher in Zustand $\frac{\frac{1}{\sqrt{2}}|00\rangle}{\frac{1}{\sqrt{2}}} = |00\rangle$

D.h. aber: Messung des 2. Qubits liefert ebenfalls Null! (Qubits sind abhängig)

Fakt: 2-Qubit Systeme entwickeln sich gemäß unitärer Abb. $M \in \mathbb{C}^{4\times4}$.

Bsp. (CNOT)

$$M_{cnot} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad \begin{matrix} |00\rangle \mapsto |00\rangle \\ |01\rangle \mapsto |01\rangle \\ |10\rangle \mapsto |11\rangle \\ |11\rangle \mapsto |10\rangle \end{matrix}$$

Controlled-NOT: Das 2. Bit wird genau dann invertiert, wenn das 1. Bit (Kontroll-Bit) gesetzt ist.

Man überprüfe, dass $M_{cnot} \cdot (M_{cnot}^*)^T = I_2$

Def.: $M \in \mathbb{C}^{m\times m}$ heißt Permutationsmatrix gdw. M in jeder Zeile und Spalte genau eine Eins und sonst Nullen enthält.

Bsp.: M_{cnot} ist Permutationsmatrix.

Übung: Permutationsmatrizen sind unitär.

Bez.: Eine unitäre Abbildung, die nur auf einem Teil der Qubits agiert, heißt lokal unitär.

Sei $|z\rangle = (c_0|00\rangle + c_1|01\rangle + c_2|10\rangle + c_3|11\rangle)$ ein 2-Qubit und $A, B \in \mathbb{C}^{2\times2}$ unitär.

$c_0(A|0\rangle \otimes B|0\rangle) + c_1(A|0\rangle + B|1\rangle) + c_2(A|1\rangle + B|0\rangle) + c_3(A|1\rangle + B|1\rangle)$ heißt

Anwendung von A auf das 1. Qubit und Anwendung von B auf das 2. Qubit.

Spezialfälle: $B = I_2$ liefert eine lokal unitäre Abb. auf dem 1. Qubit.
$A = I_2$ liefert ——— " ——— 2. Qubit.

Def. (Tensorprodukt bzw. Kronecker-Produkt von Matrizen): Seien

$$A = \begin{pmatrix} a_{11} & \cdots & a_{m1} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \in \mathbb{C}^{m \times m}, \quad B = \begin{pmatrix} b_{11} & \cdots & b_{n1} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \in \mathbb{C}^{n \times n}.$$

Dann ist das Tensorprodukt von A und B definiert als

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{m1}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix} \in \mathbb{C}^{mn \times mn}.$$

Bsp: $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$, $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$

$$A \otimes B = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

Satz: Seien $A, B \in \mathbb{C}^{2\times 2}$ unitär. Ferner sei $|z\rangle \in \mathbb{C}^4$ ein 2-Qubit System. Die Anwendung von A auf das 1. Qubit und B auf das 2. Qubit wird beschrieben durch

$$(A \otimes B)\,|z\rangle.$$

Bew: Für $|00\rangle$, andere Basiszustände folgen analog:

$$\begin{aligned}(A \otimes B)|00\rangle &= a_{11}b_{11}|00\rangle + a_{11}b_{21}|01\rangle + a_{21}b_{11}|10\rangle + a_{21}b_{21}|11\rangle \\ &= a_{11}|0\rangle \otimes (b_{11}|0\rangle + b_{21}|1\rangle) + a_{21}|1\rangle \otimes (b_{11}|0\rangle + b_{21}|1\rangle) \\ &= (a_{11}|0\rangle + a_{21}|1\rangle) \otimes (b_{11}|0\rangle + b_{21}|1\rangle) \\ &= A|0\rangle \otimes B|0\rangle\end{aligned}$$

Aus der Linearität von $A \otimes B$ folgt: Gilt obige Identität für alle Basiszustände, so gilt sie auch für alle Linearkombinationen von Basiszuständen.

$\Rightarrow$ Identität gilt für beliebiges $|z\rangle \in \mathbb{C}^4$. ∎

Man beachte: Lokal unitäre Abb. auf separablen Zuständen $|z\rangle = |x\rangle \otimes |y\rangle$ liefert stets einen separablen Zustand: $|z\rangle \xmapsto{A \otimes B} A|x\rangle \otimes B|y\rangle$.

D.h. lokal unitäre Operationen allein können keine Verschränkung erzeugen.

<u>Bsp.1</u>: Anwendung von W_2 auf das 1. Qubit: $W_2 \otimes I_2$

$$W_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\1&-1\end{pmatrix} \qquad I_2 = \begin{pmatrix}1&0\\0&1\end{pmatrix}$$

$$W_2 \otimes I_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1&0&1&0\\0&1&0&1\\1&0&-1&0\\0&1&0&-1\end{pmatrix} \qquad |00\rangle \longmapsto \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) = \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)}_{W_2} \otimes |0\rangle$$

<u>Bsp.2</u>: $W_4 = W_2 \otimes W_2$

$$W_4 = \frac{1}{2}\begin{pmatrix}1&1&1&1\\1&-1&1&-1\\1&1&-1&-1\\1&-1&-1&1\end{pmatrix}$$

Zustandsübergang für Basiszustand $|x_0x_1\rangle$, $x_0, x_1 \in \{0,1\}$:

$$W_4|x_0x_1\rangle = \frac{1}{2}\left(|00\rangle + (-1)^{x_1}|01\rangle + (-1)^{x_0}|10\rangle + (-1)^{x_0+x_1}|11\rangle\right)$$
$$= \underbrace{\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_0}|1\rangle\right)}_{W_1|x_0\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^{x_1}|1\rangle\right)}_{W_2|x_1\rangle}$$

Wissen bereits: Nicht jeder 2-Qubit Zustand ist Tensorprodukt zweier 1-Qubit Zustände.

Analog gilt:

<u>Satz</u>: Nicht jede unitäre Abb. $U \in \mathbb{C}^{4\times 4}$ ist Tensorprodukt unitärer Matrizen $A, B \in \mathbb{C}^{2\times 2}$.

<u>Bew.</u>:
$$M_{cnot} = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix} \text{ ist unitär.}$$

<u>Ann.</u>: M_{cnot} sei Tensorprodukt zweier unitärer Abb., d.h. $M_{cnot} = A \otimes B$

Betrachte: $|00\rangle \xmapsto{W_2 \otimes I_2} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \xmapsto{A \otimes B} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

D.h. wir erhalten ein <u>verschränktes</u> EPR-Paar durch lokal unitäre Abbildungen auf dem separablen Zustand $|00\rangle$. $\lightning$ (Widerspruch, s. Seite 10 unten)

<u>Def.</u> (Quanten-Kopiermaschine): Sei $|x\rangle \in \mathbb{C}^2$ ein Qubit. Eine Quanten-Kopiermaschine ist eine unitäre Abb. U mit: $\quad U(|z\rangle \otimes |x\rangle) = |z\rangle \otimes |z\rangle$ für alle Qubits $|z\rangle \in \mathbb{C}^2$.

<u>Satz</u> (No-Cloning Theorem): Es gibt keine Quantenkopiermaschine.

<u>Bew.</u>: Ann.: Es gibt Quanten-Kopiermaschine U.

Seien $|0\rangle, |1\rangle$ Basiszustände. Aufgrund der Kopiereigenschaft gilt:

$U(W_2|0\rangle \otimes |1\rangle) = W_2|0\rangle \otimes W_2|0\rangle$ ist separabel.

Aufgrund der Linearität von U gilt aber ebenfalls

$$U(W_2|0\rangle \otimes |1\rangle) = U\left(\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{1}{\sqrt{2}}\left(U|01\rangle + U|11\rangle\right) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

ist verschränkt (EPR-Paar). $\lightning$

<u>Man beachte:</u>

$$H_{cnot} = \begin{pmatrix} 1&0&0&0 \\ 0&1&0&0 \\ 0&0&0&1 \\ 0&0&1&0 \end{pmatrix}$$ ist Kopiermaschine für <u>Basiszustände</u> $|0\rangle, |1\rangle$, denn

$$|00\rangle \mapsto |00\rangle$$
$$|10\rangle \mapsto |11\rangle$$

Allerdings gilt $(\alpha_0|0\rangle + \alpha_1|1\rangle)|0\rangle \xmapsto{H_{cnot}} \alpha_0|00\rangle + \alpha_1|11\rangle \neq (\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0|0\rangle + \alpha_1|1\rangle)$

für $\alpha_0, \alpha_1 \neq 0$

<u>n-Qubit Zustandssysteme (Register)</u>

Sei $|0\rangle, |1\rangle$ eine orthonormale Basis des $\mathbb{C}^2$.

Gemäß Basis-Lemma (S.6): $|0\rangle\otimes|0\rangle, |0\rangle\otimes|1\rangle, |1\rangle\otimes|0\rangle, |1\rangle\otimes|1\rangle$ ist orthonormale Basis des $\mathbb{C}^4$.

Erneute Anwendung des Lemmas liefert eine orthonormale Basis $|b_0 b_1 b_2\rangle$, $b_i \in \{0,1\}$ des $\mathbb{C}^{2^3}$.

Induktiv: $|b_0 \dots b_{n-1}\rangle$, $b_i \in \{0,1\}$ ist orthonormale Basis des $\mathbb{C}^{2^n}$.

<u>Def.</u>: Ein n-Qubit System ist ein Einheitsvektor im $\mathbb{C}^{2^n}$ der Form

$$|z\rangle = \sum_{x\in\{0,1\}^n} c_x |x\rangle \quad \text{mit } c_x \in \mathbb{C}, \sum_{x\in\{0,1\}^n} |c_x|^2 = 1$$

<u>Notation</u>: Wir interpretieren $x = x_0 \dots x_{n-1}$ als Binärdarstellung der natürlichen Zahl $\sum_{i=0}^{n-1} x_i \cdot 2^{n-1-i}$. Damit schreiben wir auch $|z\rangle = \sum_{i=0}^{2^n-1} c_i |i\rangle$

<u>Zustandsübergang</u>: • n-Qubit Systeme entwickeln sich gemäß unitärer Abb. $U: \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$

• Lokal unitäre Abbildungen operieren auf einzelnen Qubits des Systems.

<u>Beobachtung</u>: • n Qubits werden durch 2^n Amplituden beschrieben.

• Unitäre Matrizen $U \in \mathbb{C}^{2^n \times 2^n}$ haben Beschreibungsgröße 2^{2n}.

D.h. die Beschreibungsgröße ist exponentiell in der physikalischen Größe n.

Feynman: „Quantenrechner sollten nicht effizient auf klassischen Rechnern simulierbar sein"

<u>Def. (Separabilität)</u>: Ein n-Qubit $|z\rangle \in \mathbb{C}^{2^n}$ heißt separabel gdw.

$$|z\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle \text{ für } |x_i\rangle \in \mathbb{C}^2.$$

Nicht separable Zustände heißen verschränkt.

<u>Bsp.</u>: $|z\rangle = \frac{1}{\sqrt{3}}(|000\rangle - |001\rangle - |111\rangle)$ ist verschränkt.

Messung des 1. Qubits: $|0\rangle$ mit Ws $\frac{2}{3}$

$|1\rangle$ mit Ws $\frac{1}{3}$

Falls $|0\rangle$ gemessen: Zustand $\frac{\frac{1}{\sqrt{3}}(|000\rangle - |001\rangle)}{\sqrt{\frac{2}{3}}} = \frac{1}{\sqrt{2}}(|000\rangle - |001\rangle)$

$|1\rangle$ gemessen: Zustand $\frac{\frac{1}{\sqrt{3}}|111\rangle}{\sqrt{\frac{1}{3}}} = |111\rangle$

Quanten Teleportation

Szenario: • Alice besitzt Qubit $|z\rangle = c_0|0\rangle + c_1|1\rangle$. Amplituden c_0, c_1 sind Alice unbekannt.

- Alice kann über klassischen Kanal mit Bob kommunizieren (d.h. Bits, keine Qubits)
- Alice und Bob teilen sich EPR-Paar $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; 1. Bit ist Alice, 2. Bit gehört Bob

<u>Ziel</u>: Alice sendet $|z\rangle$ an Bob.

Probleme:
- Alice kennt Amplituden nicht.
- Messung zerstört Wellenfunktion.
- Alice kann keine Kopien von $|z\rangle$ erzeugen, um Amplituden durch hinreichend viele Messungen zu approximieren. Würde auch nur $|c_0|^2, |c_1|^2$ liefern, nicht c_0, c_1.
- Gibt es einen Algorithmus zur Rekonstruktion von Quantenbits aus klassischer Information, so existiert ein Quanten-Kopierer. ↯ (No cloning-Theorem)

Lösung: Nutze Verschränkung zur Übertragung.

Zusammengesetzter Zustand von $|z\rangle$ und $|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$|z\rangle \otimes |e\rangle = (c_0|0\rangle + c_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$= \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|100\rangle + c_1|111\rangle)$$

Man beachte: Alice hat Zugriff auf die ersten beiden Qubits, Bob auf das 3. Qubit.

<u>Protokoll für die Teleportation von $|z\rangle$</u>

1. Alice wendet CNOT auf das 2. Qubit mit dem 1. Qubit als Kontrollbit an:

$$|ze\rangle \xrightarrow{CNOT} \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|110\rangle + c_1|101\rangle)$$

2. Alice wendet nun auf das 1. Qubit die Hadamard-Walsh Transformation W_2 an:

$$\frac{1}{\sqrt{2}}\left(\frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle + \frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|11\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|10\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|01\rangle\right)$$

$$= \frac{1}{2}\left(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle\right)$$

$$= \frac{1}{2}\left(|00\rangle(c_0|0\rangle + c_1|1\rangle) + |01\rangle(c_0|1\rangle + c_1|0\rangle) + |10\rangle(c_0|0\rangle - c_1|1\rangle) + |11\rangle(c_0|1\rangle - c_1|0\rangle)\right)$$

3. Alice misst die ersten beiden Qubits. Sie erhält jeweils mit Ws. $\frac{1}{4}$

Qubit	Zustand nach Messung
$\|00\rangle$	$\|00\rangle(c_0\|0\rangle + c_1\|1\rangle)$
$\|01\rangle$	$\|01\rangle(c_0\|1\rangle + c_1\|0\rangle)$
$\|10\rangle$	$\|10\rangle(c_0\|0\rangle - c_1\|1\rangle)$
$\|11\rangle$	$\|11\rangle(c_0\|1\rangle - c_1\|0\rangle)$

Alice sendet Messergebnis 00, 01, 10 oder 11 zu Bob.

4. Abhängig vom Messergebnis führt Bob folgende Operation aus.

Für $|00\rangle$: Bobs Qubit ist bereits im gewünschten Zustand.

$|01\rangle$: NOT Operation $c_0|1\rangle + c_1|0\rangle \xmapsto{NOT} c_0|0\rangle + c_1|1\rangle$

$|10\rangle$: Flip Operation $c_0|0\rangle - c_1|1\rangle \xmapsto{Flip} c_0|0\rangle + c_1|1\rangle$

$|11\rangle$: Flip ∘ NOT $c_0|1\rangle - c_1|0\rangle \xmapsto{Flip \circ NOT} c_0|0\rangle + c_1|1\rangle$

<u>Beobachtung</u>:
- Alices Zustand $|z\rangle$ wird <u>übertragen</u>, nicht kopiert.
- Es wird nur der Zustand übertragen, kein physikalisches Qubit.
- Bob benötigt Alices Messung, um $|z\rangle$ zu erhalten.

<u>Superdense Coding (Bennett, Wiesner 1992)</u>

Szenario:
- Alice und Bob teilen sich ein EPR $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
- Alice & Bob besitzen einen Quantenkanal zum Übertragen von Qubits.

<u>Ziel</u>: Übertrage zwei klassische Bits b_0, b_1 mit Hilfe eines <u>einzelnen</u> Qubits.

<u>Protokoll Superdense Coding</u>

1. Abhängig von b_0, b_1 berechnet Alice:

Falls $b_0 = 1$: Flip auf 1. Qubit

Falls $b_1 = 1$: NOT auf 1. Qubit

b_0	b_1	Zustand
0	0	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$
0	1	$\frac{1}{\sqrt{2}}(\|10\rangle + \|01\rangle)$
1	0	$\frac{1}{\sqrt{2}}(\|00\rangle - \|11\rangle)$
1	1	$\frac{1}{\sqrt{2}}(\|10\rangle - \|01\rangle)$

Alice sendet $|z\rangle$ an Bob.

2. Bob wendet die folgende unitäre Matrix U auf $|z\rangle$ an.

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & -1 & 1 & 0 \end{pmatrix}$$

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \xmapsto{U} \frac{1}{2}(|00\rangle + |10\rangle + |00\rangle - |10\rangle) = |00\rangle$ Interpretation: $(b_0, b_1) = (0,0)$

$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \xmapsto{U} \frac{1}{2}(|01\rangle - |11\rangle + |01\rangle + |11\rangle) = |01\rangle$ Interpretation: $(b_0, b_1) = (0,1)$

$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \xmapsto{U} \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle + |10\rangle) = |10\rangle$ Interpretation: $(b_0, b_1) = (1,0)$

$\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \xmapsto{U} \frac{1}{2}(-|01\rangle + |11\rangle + |01\rangle + |11\rangle) = |11\rangle$ Interpretation: $(b_0, b_1) = (1,1)$

Quanten Schlüsselaustausch

One-Time Pad für n-Bit Nachricht $m = m_1 m_2 \dots m_n \in \{0,1\}^n$

Alice		Bob
Alice $SK = k_1 \dots k_n \in \{0,1\}^n$	$\xrightarrow{E_{SK}(m)\ =\ m \oplus SK}$	Bob $SK = k_1 \dots k_n \in \{0,1\}^n$

$$D_{SK}(E_{SK}(m)) = E_{SK}(m) \oplus SK = m \oplus SK \oplus SK = m$$

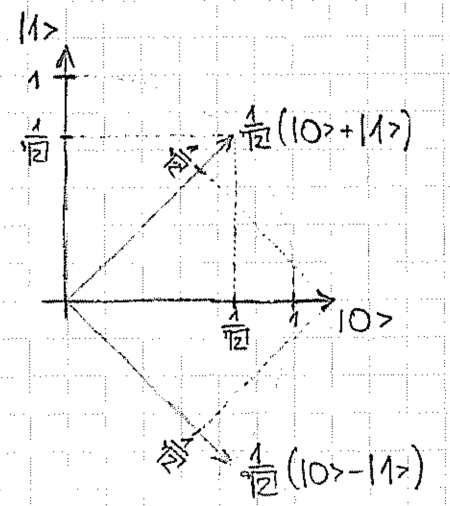
Szenario:
- Alice und Bob besitzen Quantenkanal
- ——— " ——— authentisierten klassischen Kanal
- Kanäle werden belauscht und manipuliert durch Eve.

Ziel: Austausch von n klassischen Bits, so dass
- Eve durch Belauschen keine Information erhält
- Manipulation von Eve entdeckt wird

Einfache Lösung, falls Alice & Bob n EPR-Paare $\frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)$ teilen:
Messen in derselben Basis $|0\rangle, |1\rangle$ liefert n identische Zufallsbits.

Def (Z- und X-Basis): Wir nennen $|0\rangle, |1\rangle$ die Z-Basis des $\mathbb{C}^2$.
Die Basis $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, die durch Anwendung von W_2 auf die Basisvektoren der Z-Basis entsteht, bezeichnen wir als X-Basis.

Beobachtung:
- Messung von $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ in Z-Basis liefert $|0\rangle, |1\rangle$ jeweils mit Ws. $\frac{1}{2}$.
- Messung von $|0\rangle$ oder $|1\rangle$ in X-Basis " $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ ——— " ———.



Idee: Kodiere Bit $a \in \{0,1\}$ entweder in der X-Basis oder der Z-Basis.

Kodierungstabelle:

Bit a	Basis b		Zustand $\|z_{ab}\rangle$
0	0	Z-Basis	$\|z_{00}\rangle = \|0\rangle$
1	0		$\|z_{10}\rangle = \|1\rangle$
0	1	X-Basis	$\|z_{01}\rangle = \frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$
1	1		$\|z_{11}\rangle = \frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$

<u>BB84-Protokoll (Bennett-Brassard)</u>

1. Alice wählt zufällige 4n-Bit Strings $a = a_1 \dots a_{4n}, b = b_1 \dots b_{4n} \in \{0,1\}^{4n}$.
   Alice sendet 4n Qubits $|z_{a_i b_i}\rangle$, $i = 1 \dots 4n$, an Bob.
2. Bob wählt einen zufälligen Bitstring $b' = b'_1 \dots b'_{4n} \in \{0,1\}^{4n}$.
   Falls $b'_i = 0$: Messe $|z_{a_i b_i}\rangle$ zur Z-Basis. Falls $|0\rangle$, setze $a'_i = 0$. Sonst $a'_i = 1$.
   $b'_i = 1$: Messe $|z_{a_i b_i}\rangle$ zur X-Basis. Falls $\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$, setze $a'_i = 0$. Sonst $a'_i = 1$.
   Bob erklärt, dass er gemessen hat.
3. Alice gibt die Basen $b_1, \dots, b_{4n}$ bekannt. Für $b_i \neq b'_i$ wird das i-te Bit a_i verworfen.
   Im Erwartungswert bleiben 2n Bits übrig.
4. Alice und Bob vergleichen von den 2n übrigen Bits n zufällig gewählte Testbits.
   Stimmen nicht alle Testbits überein, Abbruch (Manipulationsversuch von Eve).
   Sonst bilden die restlichen n Bits den geheimen Schlüssel SK.

<u>Korrektheit</u>: Falls keine Manipulation der Qubits vorliegt, gilt

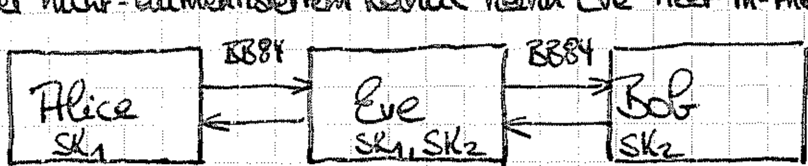
$$Ws(a_i = a'_i \mid b_i = b'_i) = 1,$$ denn Bob misst Basiszustände in der korrekt gewählten Basis.

Eve erhält nur dann das i-te Bit, falls sie $|z_{a_i b_i}\rangle$ misst.

1. Fall: Eve misst zur korrekten Basis mit Ws $\frac{1}{2}$.
   In diesem Fall sendet sie $|z_{a_i b_i}\rangle$ an Bob und kennt a_i.
2. Fall: Eve misst zur inkorrekten Basis $\bar{b}_i$ mit Ws $\frac{1}{2}$.
   Sie sendet $|z_{\tilde{a}_i \bar{b}_i}\rangle$ an Bob, wobei $\tilde{a}_i \in_R \{0,1\}$. Misst Bob in Basis b_i, so erhält er a_i' mit $Pr(a_i' = a_i) = \frac{1}{2}$.
   D.h. wird das i-te Bit für die Menge der Testbits ausgewählt, erfolgt Abbruch mit Ws $\frac{1}{2}$.

Damit ist nicht schwer zu zeigen, dass Eves Erfolgsws., unbemerkt k Bits zu ermitteln, exponentiell klein in k ist.

Beobachtungen:
- Eve kann Denial-of-Service Angriff durchführen, d.h. Abbruch erzwingen.
- Bei nicht-authentisierten Kanal kann Eve Meet-in-the-Middle Angriff durchführe



B92 Protokoll (Bennett)

Führe die folgenden Schritte durch, bis n Bits ausgetauscht wurden:

1. Alice wählt ein Zufallsbit $a \in_R \{0,1\}$ und sendet
$$|z\rangle = \begin{cases} |0\rangle & \text{falls } a=0 \\ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) & \text{falls } a=1 \end{cases}$$
2. Bob wählt $a' \in_R \{0,1\}$. Bob misst $|z\rangle$ in der
   - Z-Basis für $a'=0$: Falls Ergebnis $|0\rangle$, setze $b=0$. Sonst setze $b=1$.
   - X-Basis für $a'=1$: Falls $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, ——— " ———.

   Sende b an Alice.
3. Falls $b=0$: Zurück zu Schritt 1.
   Falls $b=1$: Schlüsselbit ist a für Alice
   $1-a'$ für Bob

In jedem Durchlauf wird ein Schlüsselbit generiert gdw. $b=1$ gilt.

Satz: $Ws(b=1) = \frac{1}{4}$

Beweis: Es gilt

$$\begin{aligned} Ws(b=1) &= Ws(b=1 \mid a=a') \cdot Ws(a=a') + Ws(b=1 \mid a \neq a') \cdot Ws(a \neq a') \\ &= \quad 0 \quad \cdot \quad \tfrac{1}{2} \quad + \quad \tfrac{1}{2} \quad \cdot \quad \tfrac{1}{2} \quad = \tfrac{1}{4}, \end{aligned}$$

denn im Fall $a = a'$ misst Bob stets den von Alice gesendeten Basiszustand ($b=0$), im Fall $a \neq a'$ misst Bob einen anderen Zustand mit Ws. $\frac{1}{2}$.

D.h. also, dass wir im Erwartungswert $4n$ Protokolldurchläufe benötigen, bis n Schlüsselbits generiert sind. Es bleibt zu zeigen, dass die erzeugten Schlüsselbits korrekt sind, d.h. $a = 1-a'$.

<u>Satz</u>: $Ws(a = 1-a' \mid b=1) = 1$

Beweis: Es gilt $Ws(a=1-a' \mid b=1) \cdot Ws(b=1) = Ws(b=1 \mid a=1-a') \cdot Ws(a=1-a')$

$$\Rightarrow Ws(a=1-a' \mid b=1) = \frac{Ws(b=1 \mid a=1-a') \cdot Ws(a=1-a')}{Ws(b=1)} = \frac{\frac{1}{2} \cdot \frac{1}{2}}{\frac{1}{4}} = 1$$

D.h. falls $b=1$, so müssen a und a' verschiedene Bits sein.

Damit erhalten Alice und Bob dasselbe Bit $a = 1-a'$.

<u>Boolesche Schaltkreise</u>

Ziel: Berechne Boolesche Funktionen $f_n : \mathbb{F}_2^n \to \mathbb{F}_2^m$, $n \in \mathbb{N}$

Bsp.: Und $\wedge : \mathbb{F}_2^2 \to \mathbb{F}_2$, $(x_1, x_2) \xmapsto{\wedge} x_1 \wedge x_2 = x_1 x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$, $(x_1, \dots, x_n) \mapsto ((x_1 \wedge x_2) \wedge x_3) \dots x_n)$

Oder $\vee : \mathbb{F}_2^2 \to \mathbb{F}_2$, $(x_1, x_2) \xmapsto{\vee} x_1 \vee x_2 = x_1 + x_2 + x_1 x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$, $(x_1, \dots, x_n) \mapsto ((x_1 \vee x_2) \vee x_3) \dots x_n)$

Nicht $\neg : \mathbb{F}_2 \to \mathbb{F}_2$, $x \xmapsto{\neg} 1-x$ Schreibweise auch: $\bar{x}$

Kopierfunktion $c : \mathbb{F}_2 \to \mathbb{F}_2^2$, $x \xmapsto{c} (x, x)$

Entscheiden von Sprachen L: $\chi_L : \mathbb{F}_2^n \to \mathbb{F}_2$, $\chi_L(w) = \begin{cases} 1 & \text{falls } w \in L \\ 0 & \text{sonst} \end{cases}$

z.B. $SAT = \{ \langle \phi \rangle \mid \phi$ ist erfüllbare Boolesche Formel$\}$, mit $\langle \phi \rangle$ n-Bit Kodierung von ϕ

<u>Def.</u> (Boolescher Schaltkreis): Sei S eine Menge von Booleschen Funktionen, die eine konstante Anzahl von Eingabebits auf eine konstante Anzahl von Ausgabebits abbildet (z.B. $S = \{\wedge, \vee, \neg\}$).

Ein Boolescher Schaltkreis über S ist ein azyklisches, gerichteter Graph $G = (V, E)$ mit:

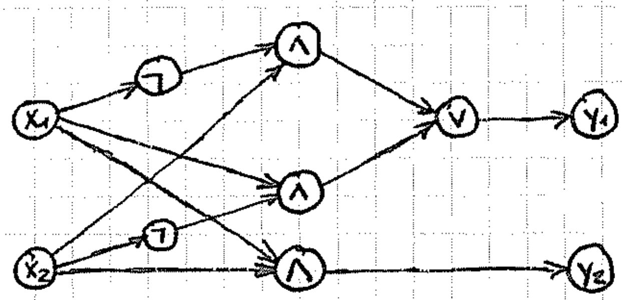
- Die Knoten V sind gelabelt mit Eingabe-/Ausgabevariablen oder Elementen aus S.

- Eingabeknoten haben Eingrad 0. Ausgabeknoten haben Eingrad 1, Ausgrad 0.
- Knoten mit Label $s \in S$, $s: \mathbb{F}_2^n \to \mathbb{F}_2^m$ haben Eingrad n und Ausgrad m.

Die Komplexität des Booleschen Schaltkreises ist definiert als $|V|+|E|$ (bezüglich S).

Bsp: Addierer $f(x_1,x_2)=(y_1,y_2)$ mit $y_1 = x_1 \oplus x_2$, y_2 Übertrag

x_1	x_2	y_1	y_2
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1



$y_1 = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})$

$y_2 = x_1 \wedge x_2$

Komplexität bezüglich $\{\wedge, \vee, \neg\}$: $|V|+|E| = 10 + 12 = 22$

Def (universell). Sei S eine Menge von Booleschen Fkt., die eine konstante Anzahl von Bits auf eine konstante Anzahl von Bits abbilden. S ist universell, falls jede Boolesche Funktion $\mathbb{F}_2^n \to \mathbb{F}_2$ durch Verknüpfung von Elementen aus S realisiert werden kann.

Übung: Sei S universell. Dann kann jede Fkt. $f: \mathbb{F}_2^n \to \mathbb{F}_2^m$ mittels S realisiert werden.

Satz: $S_u = \{\wedge, \neg, c\}$ ist eine universelle Menge.

Beweis: Wir definieren die Fkt. M_a, $a=(a_1,\dots,a_n) \in \mathbb{F}_2^n$ vermöge

$$M_a(x_1,\dots,x_n) = \phi_1(x_1) \wedge \phi_2(x_2) \wedge \dots \phi_n(x_n) \quad \text{für } \phi_i(x_i) = \begin{cases} x_i & \text{für } a_i = 1 \\ \overline{x_i} & \text{für } a_i = 0 \end{cases}$$

D.h. M_a ist die charakteristische Fkt. $M_a(x_1,\dots,x_n) = \begin{cases} 1 & \text{falls } x = a \\ 0 & \text{sonst} \end{cases}$.

Sei $T = \{ a \in \mathbb{F}_2^n \mid f(a) = 1 \}$. Dann gilt

$$f = \bigvee_{a \in T} M_a(x_1,\dots,x_n) = \neg\Big(\bigwedge_{a\in T} \neg M_a(x_1,\dots,x_n)\Big).$$

D.h. wir können f als $\neg, \wedge$-Verknüpfung von Kopien von $(x_1,\dots,x_n)$ darstellen. ■

Bsp.: (obiger Addierer) Für Ausgabebit y_1 gilt:

$$T = \{(0,1),(1,0)\} \Rightarrow y_1 = \bigvee_{a \in T} M_a(x_1,x_2) = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})$$

$$= \neg(\neg((\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2}))) = \neg\left(\overline{(\overline{x_1} \wedge x_2)} \wedge \overline{(x_1 \wedge \overline{x_2})}\right)$$

Beobachtung: Seien S_1, S_2 Mengen von booleschen Funktionen und S_1 universell. Falls jedes $s \in S_1$ durch eine Verknüpfung aus S_2 darstellbar ist, dann ist S_2 universell.

Sei $\text{nand}(x_1, x_2) = \overline{x_1 \wedge x_2}$.

<u>Satz</u>: $S = \{\text{nand}, c\}$ ist universell.

Beweis: Wir stellen $\neg$ und $\wedge$ als Verknüpfung durch nand-Funktionen dar.

$\neg$: $\text{nand}(x, x) = \overline{x \wedge x} = \overline{x}$ (Anwendung von c, um x zu duplizieren)

$\wedge$: $\text{nand}(\text{nand}(x_1, x_2), \text{nand}(x_1, x_2)) = \text{nand}(\overline{x_1 \wedge x_2}, \overline{x_1 \wedge x_2}) = x_1 \wedge x_2$

Bezeichnung: Wir bezeichnen mit C_n Schaltkreise mit n Eingabeknoten.

Wir nennen $C = \{C_n\}_{n \in \mathbb{N}}$ eine Schaltkreisfamilie.

<u>Def.</u>: Eine boolesche Fkt. f_n, $n \in \mathbb{N}$, hat <u>nicht-uniforme</u> Schaltkreiskomplexität $O(g(n))$ bzgl. einer universellen Menge S, falls es eine Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ über S mit Komplexität $O(g(n))$ gibt, die f_n berechnet.

Beobachtung: Nach Satz S. 19 können alle Fkt. $\mathbb{F}_2^n \to \mathbb{F}_2$ mittels einer nicht-uniformen Schaltkreisfamilie $C = \{C_n\}_{n \in \mathbb{N}}$ berechnet werden. Insbesondere existiert C mit:

$$C_n = \begin{cases} 1 & \text{falls DTM } M_n \text{ auf Eingabe } M_n \text{ hält} \\ 0 & \text{sonst} \end{cases}$$

D.h. C_n entscheidet das im Turingmaschinen-Modell nicht entscheidbare Halteproblem.

Problem: Konstruktion von C_n erfordert die Kenntnis der Funktionswerte der f_n.

<u>Def.</u> (uniformes Modell): Eine Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ heißt uniform, falls es eine DTM gibt, die für alle $n \in \mathbb{N}$ bei Eingabe 1^n in Zeit und Platz $\text{poly}(n)$ C_n ausgibt.

Eine boolesche Fkt. f_n, $n \in \mathbb{N}$, hat <u>uniforme</u> Schaltkreiskomplexität $O(g(n))$, falls es eine uniforme Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ mit Größe $O(g(n))$ gibt, die f_n berechnet.

Bezeichnung: $\text{poly}(n) = O(n^c)$ für konstantes c.

<u>Def.</u> (P): Die Klasse P besteht aus allen booleschen Fkt. f_n, $n \in \mathbb{N}$, mit uniformer Schaltkreiskomplexität $\text{poly}(n)$.

Bsp.: $f_n = \bigwedge_{i=1}^{n} x_i$ hat uniforme Schaltkreiskomplexität $O(n)$ bezüglich $S_u = \{\wedge, \neg, c\}$.

$f_n = \bigvee_{i=1}^{n} x_i$ ——————— " ———————

Sei $nand(x_1,x_2) = \overline{x_1 \wedge x_2}$.

Satz: $S = \{nand, c\}$ ist universell.

Beweis: Wir stellen $\neg$ und $\wedge$ als Verknüpfung durch nand-Funktionen dar.

$\neg$: $nand(x,x) = \overline{x \wedge x} = \overline{x}$ (Anwendung von c, um x zu duplizieren)

$\wedge$: $nand(nand(x_1,x_2), nand(x_1,x_2)) = nand(\overline{x_1 \wedge x_2}, \overline{x_1 \wedge x_2}) = x_1 \wedge x_2$

Bezeichnung: Wir bezeichnen mit C_n Schaltkreise mit n Eingabeknoten.

Wir nennen $C = \{C_n\}_{n \in \mathbb{N}}$ eine Schaltkreisfamilie.

Def.: Eine boolesche Fkt. $f_n, n \in \mathbb{N}$, hat nicht-uniforme Schaltkreiskomplexität $O(g(n))$ bzgl. einer universellen Menge S, falls es eine Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ über S mit Komplexität $O(g(n))$ gibt, die f_n berechnet.

Beobachtung: Nach Satz S. 19 können alle Fkt. $\mathbb{F}_2^n \to \mathbb{F}_2$ mittels einer nicht-uniformen Schaltkreisfamilie $C = \{C_n\}_{n \in \mathbb{N}}$ berechnet werden. Insbesondere existiert C mit:

$$C_n = \begin{cases} 1 & \text{falls DTM } M_n \text{ auf Eingabe } M_n \text{ hält} \\ 0 & \text{sonst} \end{cases}$$

D.h. C_n entscheidet das im Turingmaschinen-Modell nicht entscheidbare Halteproblem.

Problem: Konstruktion von C_n erfordert die Kenntnis der Funktionswerte der f_n.

Def. (uniformes Modell): Eine Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ heißt uniform, falls es eine DTM gibt, die für alle $n \in \mathbb{N}$ bei Eingabe 1^n in Zeit und Platz poly(n) C_n ausgibt.

Eine boolesche Fkt. $f_n, n \in \mathbb{N}$, hat uniforme Schaltkreiskomplexität $O(g(n))$, falls es eine uniforme Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ mit Größe $O(g(n))$ gibt, die f_n berechnet.

Bezeichnung: $poly(n) = O(n^c)$ für konstantes c.

Def. (P): Die Klasse P besteht aus allen booleschen Fkt. $f_n, n \in \mathbb{N}$, mit uniformer Schaltkreiskomplexität poly(n).

Bsp.: $f_n = \bigwedge_{i=1}^{n} x_i$ hat uniforme Schaltkreiskomplexität $O(n)$ bezüglich $S_u = \{\wedge, \neg, c\}$.

$f_n = \bigvee_{i=1}^{n} x_i$ ——————— " ———————

<u>Def.</u>: Die Klasse <u>BPP</u> besteht aus allen booleschen Funktionen $f_n, n\in\mathbb{N}$, für die es eine uniforme Schaltkreisfamilie $\{C_n\}_{n\in\mathbb{N}}$ gibt mit:

- C_n hat Größe $\mathrm{poly}(n)$
- $\exists m=\mathrm{poly}(n): y\in_R \mathbb{F}_2^m\ \forall x\in\mathbb{F}_2^n:\ Ws_y\big(C(x,y)=f_n(x)\big)\geq\frac{2}{3}$

<u>Bsp.</u>: Sei x eine n-Bit Zahl, $f_n(x)=\begin{cases}1 & \text{falls } x \text{ prim}\\ 0 & \text{sonst}\end{cases}$

Miller-Rabin Test liefert uniforme Schaltkreisfamilie mit $Ws\big(C(x,y)=f_n(x)\big)\geq\frac{3}{4}$.

<u>Def.</u> (NP): Die Klasse NP besteht aus allen booleschen Fkt. f_n ($\mathbb{F}_2^n\to\mathbb{F}_2$), $n\in\mathbb{N}$, für die es eine uniforme Schaltkreisfamilie $\{C_n\}_{n\in\mathbb{N}}$ gibt mit:

- C_n hat Größe $\mathrm{poly}(n)$
- $\exists\, m=\mathrm{poly}(n)\ \forall x\in\mathbb{F}_2^n:\ f_n(x)=1 \Leftrightarrow \exists\, y\in\mathbb{F}_2^m: C(x,y)=1$.

<u>Bsp.</u>: $f_n=\chi_{SAT}(\langle\phi\rangle)=\begin{cases}1 & \text{falls } \langle\phi\rangle\in SAT\\ 0 & \text{sonst}\end{cases}$

$\chi_{SAT}\in NP$, denn für jedes $\langle\phi\rangle\in SAT$ mit m Variablen gibt es eine erfüllbare Belegung $y\in\mathbb{F}_2^m$.
Der Schaltkreis C_n wertet ϕ mit Belegung y aus.

<u>Reversible Schaltkreise</u>

<u>Def.</u> (reversibel): Sei $f:\mathbb{F}_2^n\to\mathbb{F}_2^m$ eine beliebige boolesche Funktion.

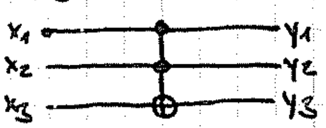
Die reversible Einbettung U_f von f ist definiert als $U_f:\mathbb{F}_2^{n+m}\to\mathbb{F}_2^{n+m},\ (x,y)\mapsto(x,f(x)+y)$

Beachte: $U_f(U_f(x,y))=U_f(x,f(x)+y)=(x,f(x)+f(x)+y)=(x,y)$, d.h. U_f ist Permutation.

Wir bezeichnen Permutationen auch als reversible Fkt. Sie werden durch Perm.-Matrizen beschrieben.

<u>Bsp.</u>: $\wedge:\mathbb{F}_2^2\to\mathbb{F}_2,\ (x_1,x_2)\mapsto x_1x_2$

$T=U_\wedge:\mathbb{F}_2^3\to\mathbb{F}_2^3,\ (x_1,x_2,x_3)\longmapsto(x_1,x_2,x_1x_2+x_3)=(x_1,x_2,x_1\wedge x_2\oplus x_3)$

Toffoli-Funktion T 

NOT auf x_3 gdw. $x_1=x_2=1$

$I:\mathbb{F}_2\to\mathbb{F}_2,\ x_1\longmapsto x_1$

$CNOT=U_I:\mathbb{F}_2^2\to\mathbb{F}_2^2,\ (x_1,x_2)\longmapsto(x_1,x_1+x_2)$

Man beachte: $CNOT(x_1,0)\longmapsto(x_1,x_1)$ liefert Kopierfkt. c für $x_1\in\mathbb{F}_2$

Def (r-universell): Sei R eine Menge von reversiblen Booleschen Fkt, die auf einer konstanten Anzahl von Bits operieren. R heißt <u>r-universell</u>, falls jede reversible Fkt. als Verknüpfung von Elementen aus R, Hilfsvariablen und Konstanten 0,1 dargestellt werden kann.

<u>Satz</u>: $\{T\}$ ist r-universell.

Beweis: Da $S_u = \{\wedge, \neg, c\}$ universell ist, kann insbesondere jede reversible Fkt. mittels S_u dargestellt werden. Es genügt daher, jedes Element als Verknüpfung von T, Hilfsvar. und 0/1 zu schreiben.
Rest: Übungsaufgabe.

Die Klassen QP und BQP

Def: Seien $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ und $U_f:\mathbb{F}_2^{n+\ell} \to \mathbb{F}_2^{m+k}$ boolesche Funktionen. Wir nennen f *einbettbar* in U_f, falls es ein $h \in \mathbb{F}_2^\ell$ gibt mit

$$U_f(x,h) = (h', f(x)) \quad \text{für ein } h' \in \mathbb{F}_2^k.$$

Satz: Jede boolesche Funktion $f:\mathbb{F}_2^n \to \mathbb{F}_2^m$ ist in eine reversible Funktion $U_f:\mathbb{F}_2^{n+m} \to \mathbb{F}_2^{n+m}$ einbettbar.

Beweis: Verwende reversible Einbettung von S. 21: $U_f:(x,y) \mapsto (x, f(x)+y)$

Damit ist f in U_f eingebettet, denn $U_f(x,0^m) = (x, f(x))$, d.h. $h = 0^m$ und $h' = x$. ■

Reversible boolesche Schaltkreise bestehen ausschließlich aus Gattern, die reversible boolesche Funktionen realisieren. Wir betten nun boolesche Schaltkreise in reversible Schaltkreise ein.

Satz: Sei $C = \{C_n\}_{n\in\mathbb{N}}$ eine uniforme Schaltkreisfamilie über $S = \{\wedge, \neg\}$ der Größe $O(g(n))$, die f_n, $n \in \mathbb{N}$, berechnet. Dann gibt es eine uniforme reversible Schaltkreisfamilie C_r über $\{T, 0, 1\}$ der Größe $O(g(n))$, die

$$f_n^r:\mathbb{F}_2^{n+m+\ell} \to \mathbb{F}_2^{n+m+\ell} \text{ mit } (x,y,z) \mapsto (x, f_n(x)+y, z') \text{ berechnet.}$$

D.h. f_n und U_{f_n} sind in f_n^r eingebettet.

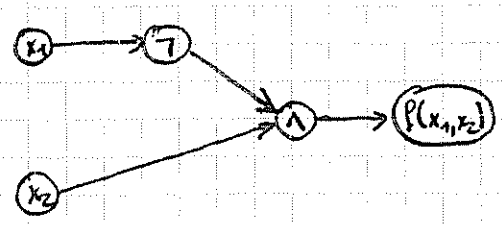
Beweis: Da C uniform ist, können wir für jedes n den Schaltkreis C_n auf einer DTM konstruieren. Wir ersetzen in C_n die $\wedge$-Gatter mit $T(x_1,x_2,0) = (x_1, x_2, x_1x_2)$

$\neg$-Gatter mit $T(x,1,1) = (x, 1, 1-x)$

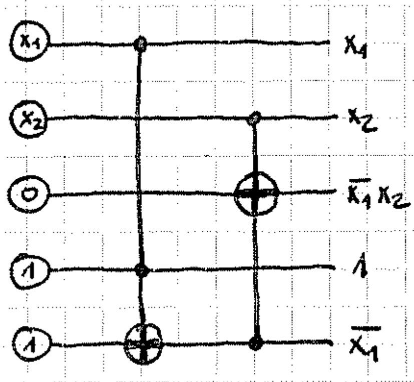
Dazu verwenden wir höchstens dreimal soviele Eingabeknoten/Ausgabeknoten wie in C_n. D.h. die Größe von C_r ist höchstens dreimal die Größe von C, d.h. die Größe von C_r ist $O(g(n))$.

Bsp.: $f(x_1,x_2) = \overline{x_1} \cdot x_2$

$U_f(x_1,x_2,0) = (x_1, x_2, \overline{x_1}x_2)$



$f^r(x_1,x_2,0,1,1) = (x_1,x_2,\overline{x_1}x_2,1,\overline{x_1})$ ist Einbettung von f und U_f



Def.: Eine QC-Familie $Q = \{Q_n\}_{n\in\mathbb{N}}$ heißt uniform, falls es eine DTM gibt, die für jedes $n \in \mathbb{N}$ bei Eingabe 1^n in Zeit und Platz $poly(n)$ Q_n ausgibt.
Eine boolsche Funktion $f_n, n \in \mathbb{N}$, hat uniforme Quanten-Schaltkreiskomplexität $O(g(n))$ bzgl. S, falls es eine uniforme QC-Familie über S gibt, die f_n berechnet.

Def.: Die Klasse QP ist die Klasse aller boolschen Fkt. $f_n, n \in \mathbb{N}$, für die es ein $g(n) = poly(n)$ und eine uniforme QC-Familie $Q_{g(n)}$ bzgl. $S_2 = \{H, CNOT, T\}$ gibt mit:
- $Q_{g(n)}$ hat Größe $poly(n)$.
- $Q_{g(n)}$ berechnet $f_n^r : \mathbb{F}_2^{g(n)} \to \mathbb{F}_2^{g(n)}$, wobei f_n in f_n^r eingebettet ist für alle $n \in \mathbb{N}$.

Satz: $P \subseteq QP$

Beweis: Sei $f_n \in P$. Dann gibt es eine uniforme Schaltkreisfamilie C mit Größe $poly(n)$, die f_n berechnet.
$\overset{\text{Satz S.28}}{\Longrightarrow}$ $\exists$ uniforme reversible Schaltkreisfamilie C_r der Größe $poly(n)$, die f_n^r berechnet, so dass f_n in f_n^r eingebettet ist. C_r ist über $\{T, 0, 1\}$ definiert.
Ersetzung der boolschen Gatter T durch unitäre Gatter, die T beschreiben, transformiert C_r in einen Quantenschaltkreis. Damit ist die Funktion $f_n \in QP$.

Def.: Die Klasse BQP ist die Klasse aller boolschen Fkt. $f_n, n \in \mathbb{N}$, für die es ein $g(n) = poly(n)$ und eine uniforme QC-Familie $Q_{g(n)}$ bzgl. $\{H, CNOT, T\}$ gibt mit:
- $Q_{g(n)}$ hat Größe $poly(n)$.
- $\exists\, k = poly(n) : y \in_R \mathbb{F}_2^k \;\forall x \in \mathbb{F}_2^n : Ws_y(Q_{g(n)}(x,y) = f_n^r(x)) \geq \frac{2}{3}$, wobei f_n^r eine Einbettung von f_n ist.

Problem: Erzeugung zufälliger Eingaben $y \in \mathbb{F}_2^k$ mit QC.

Def. (H_k): Sei $x = |x_0 x_1 \ldots x_{k-1}\rangle$. Dann ist $H_k|x\rangle = H_k|x_0 \ldots x_{k-1}\rangle = H|x_0\rangle \otimes H|x_1\rangle \otimes \ldots \otimes H|x_{k-1}\rangle$ die Hadamard-Abbildung auf einem k-Qubit.

Satz: $H_k|x\rangle = \frac{1}{2^{k/2}} \sum_{y \in \{0,1\}^k} (-1)^{x \cdot y} |y\rangle$, wobei $x \cdot y$ das innere Produkt von x, y ist.

Bew.: $k = 1, 2$: s. Vorlesung $k = 3$: s. Übung
beliebiges k: induktiv

Korollar: $H_k|0^k\rangle = \frac{1}{2^{k/2}} \sum_{y\in\{0,1\}^k} |y\rangle$ liefert gleichmäßige Überlagerung der Basiszustände.

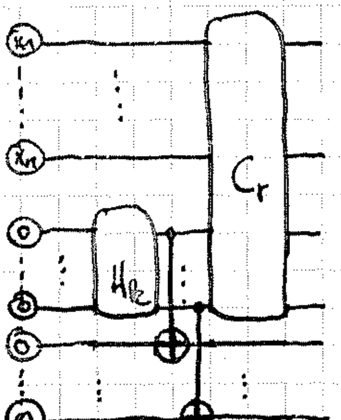
Satz: $BPP \subseteq BQP$

Beweis: Sei $f \in BPP$ und C die Schaltkreisfamilie polyn. Größe mit $Ws_y(C(x,y)=f_n) \geq \frac{2}{3}$.

Analog zum Beweis $P \subseteq QP$:

- Transformiere C in reversible Familie C_r über $\{T,0,1\}$ polyn. Größe, die $\hat{f}_n$ berechnet.
- Transformiere C_r in QC-Familie Q durch Ersetzung von T durch seine unitäre Variante.

Wir verwenden $H_k|0^k\rangle$ zur Erzeugung von y:



$|x0^{2k}\rangle \xrightarrow{H_k} \frac{1}{2^{k/2}} \sum_{y\in\{0,1\}^k} |xyy\rangle \xrightarrow{C_r} \frac{1}{2^{k/2}} \sum_{y\in\{0,1\}^k} C_r|xy\rangle \otimes |y\rangle$

Aber $C_r|xy\rangle = f(x)$ für alle x und mind. $2/3$ aller y.

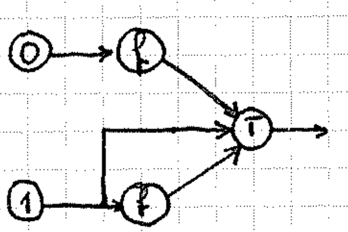
Messung der letzten k Qubits liefert $C_r|xy\rangle \otimes |y\rangle$ für jedes $y\in\{0,1\}^k$ mit $Ws \frac{1}{2^k}$. Messung der restlichen Qubits liefert $f(x)$ mit $Ws \geq \frac{2}{3}$.

Deutsch-Josza Problem

Gegeben: Gatter $f: \mathbb{Z}_2 \to \mathbb{Z}_2$

Gesucht: Schaltkreis, der entscheidet ob $f(0)=f(1)$ mit minimaler Anzahl von f-Gattern

Boolescher Schaltkreis C:

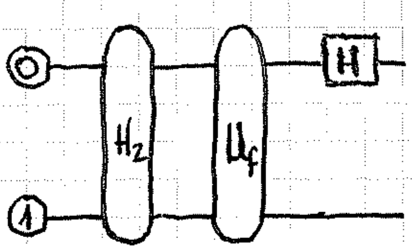


$C(0,1) = T(f(0),1,f(1)) = f(0)+f(1)$

$\Rightarrow C(0,1)=0 \Leftrightarrow f(0)=f(1)$

Minimale Anzahl von f-Gattern für Boolesche Schaltkreise, da $f(0)$ keine Information über $f(1)$ liefert.

Quantenschaltkreis Q:



$U_f|xy\rangle = |x\rangle \otimes |f(x)+y\rangle$ ist die reversible Einbettung von f.

Beachte: Q verwendet nur ein f-Gatter!

Satz: Q entscheidet das Deutsch-Josza Problem.

Beweis: $|01\rangle \xrightarrow{H_2 = H\otimes H} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$

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

$$\xrightarrow{U_f} \frac{1}{2}\left(|0\rangle \otimes (|0+f(0)\rangle - |1+f(0)\rangle) + |1\rangle(|0+f(1)\rangle - |1+f(1)\rangle)\right)$$

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

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

$$\xrightarrow{H\otimes I} \frac{1}{2^{3/2}}\left(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle\right) \otimes (|0\rangle - |1\rangle)$$

Für $f(0) = f(1)$: $(-1)^{f(0)} \cdot \frac{1}{\sqrt{2}} |0\rangle \otimes (|0\rangle - |1\rangle)$

$\Rightarrow$ Messung liefert 0 im 1. Qubit.

Für $f(0) \neq f(1)$: $(-1)^{f(0)} \cdot \frac{1}{\sqrt{2}} |1\rangle \otimes (|0\rangle - |1\rangle)$

$\Rightarrow$ Messung liefert 1 im 1. Qubit

D.h. die Messung des 1. Qubits entscheidet das Deutsch-Josza Problem.

Orakel-Modell: Information über $f: \mathbb{F}^n \to \mathbb{F}^m$ durch Auswerten von f.

<u>Verallgemeinertes Deutsch-Josza Problem</u>

Gegeben: $f: \mathbb{F}_2^n \to \mathbb{F}_2$ im Orakel-Modell

Promise-Problem: f ist entweder

- konstant, d.h. $f(x) = c$ für ein festes $c \in \mathbb{F}_2$ und alle x oder
- balanciert, d.h. $f(x) = 0$ für genau die Hälfte aller $x \in \mathbb{F}_2^n$.

Ziel: Entscheide, ob f konstant oder balanciert ist mit minimaler Zahl von f-Aufrufen.

- Klassischer deterministischer Algorithmus:
  - Setze $c = f(0^n)$
  - FOR $i = 1$ TO 2^{n-1}
    - Falls $f(i) \neq c$, Ausgabe „balanciert" und EXIT.
  - Ausgabe „konstant"

Anzahl f-Aufrufe $\leq 2^{n-1}+1$ (genau $2^{n-1}+1$ für konstante f)

Erfolgswahrscheinlichkeit: 1.

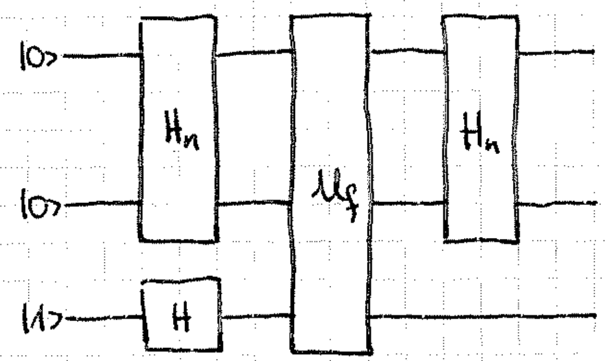
- Probabilistischer Algorithmus
  - Setze $c = f(0^n)$.
  - Für i-1 zufällige Werte $x_j \in \{1,2,\dots,2^n-1\}$
    - Falls $f(x_j) \neq c$, Ausgabe „balanciert" und EXIT.
  - Ausgabe „konstant"

Fehlerwahrscheinlichkeit: $\underbrace{Ws(\text{Ausgabe „balanciert"} \mid f \text{ konstant})}_{=0} + Ws(\text{Ausgabe „konst"} \mid f \text{ bal.})$

$$= Ws(x_1 = x_2 = \dots = x_{i-1} = f(0) \mid f \text{ balanciert}) = \prod_{j=1}^{i-1} \frac{2^{n-1}-j}{2^n} \le \left(\frac{1}{2}\right)^{i-1}$$

D.h. für i=3 f-Aufrufe ist die Ausgabe korrekt mit Ws. $\geq \frac{3}{4}$.

- Quantenschaltkreis Q_{DJ}



U_f ist reversible Einbettung von f:

$\mathbb{F}_2^{n+1} \to \mathbb{F}_2^{n+1}$

$|xy\rangle \mapsto |x\rangle \otimes |f(x)+y\rangle$ für $x \in \mathbb{F}_2^n, y \in \mathbb{F}_2$

Q_{DJ} besitzt nur ein U_f-Gatter, und damit nur ein f-Gatter!

Satz: Q_{DJ} entscheidet das verallgemeinerte Deutsch-Jozsa Problem.

Beweis:

$$|0^n 1\rangle \xrightarrow{H_n \otimes H} \frac{1}{2^{\frac{n}{2}}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\xrightarrow{U_f} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \left(|0+f(x)\rangle - |1+f(x)\rangle\right)$$

$$= \frac{1}{2^{\frac{n+1}{2}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes \left(|0\rangle - |1\rangle\right)$$

$$\xrightarrow{H_n} \frac{1}{2^{\frac{2n+1}{2}}} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+xy} |y\rangle \otimes \left(|0\rangle - |1\rangle\right) = |z\rangle$$

Lemma: $\sum_{x\in\{0,1\}^n} (-1)^{xy} = \begin{cases} 2^n & \text{für } y = 0^n \\ 0 & \text{sonst} \end{cases}$ Beweis: Übungsaufgabe

1. Fall: f konstant: Für die ersten n Qubits von $|z\rangle$ gilt

$$\frac{1}{2^{\frac{2n+1}{2}}} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} \cdot (-1)^{xy} |y\rangle = \frac{1}{2^{\frac{2n+1}{2}}} (-1)^{f(0)} \Big(2^n |0^n\rangle + \sum_{\substack{y\in\{0,1\}^n \\ y \neq 0^n}} \underbrace{\sum_{x\in\{0,1\}^n} (-1)^{xy}}_{0} |y\rangle \Big)$$

$$\Rightarrow |z\rangle = \frac{1}{\sqrt{2}} (-1)^{f(0^n)} |0^n\rangle \otimes (|0\rangle - |1\rangle)$$

D.h. für konstantes f liefert die Messung der ersten n Qubits 0^n.

2. Fall: f balanciert:

$$\sum_{y\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+xy}|y\rangle = \underbrace{\sum_{x\in\{0,1\}^n}(-1)^{f(x)}}_{0}|0^n\rangle + \sum_{\substack{y\in\{0,1\}^n\\ y\neq 0^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)+xy}|y\rangle$$

$\Rightarrow$ Messung des ersten n Qubits von z liefert 0^n mit Ws 0.

Entscheiden des DJ-Problems durch Messung der ersten n Qubits von $|z\rangle$:

Falls 0^n, Ausgabe „f konstant"

Sonst Ausgabe „f balanciert". ■

Vergleich:

	f-Aufrufe	Ws
· Deterministisch	$2^{n-1}+1$	1
· Probabilistisch	3	$\geq \frac{3}{4}$
· Quanten	1	1

Das Bernstein-Vazirani Problem (1983)

Gegeben: Funktion $f_a: \mathbb{F}_2^n \to \mathbb{F}_2$ mit $a\in\{0,1\}^n$ im Orakel-Modell

$$x \mapsto ax = \sum_{i=1}^{n} a_i x_i \mod 2$$

Gesucht: $a\in\{0,1\}^n$ mit minimaler Anzahl von f-Aufrufen.

• Klassisch:

Untere Schranke: Jeder Aufruf von f liefert 1 Bit an Information.

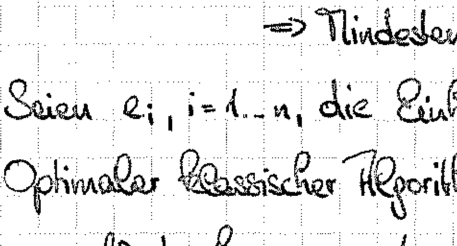
$\Rightarrow$ Mindestens n Aufrufe von f zur Bestimmung von a notwendig.

Seien e_i, $i=1..n$, die Einheitsvektoren.

Optimaler klassischer Algorithmus:

• Werte f_a an e_i, $1..n$, aus und gib die entsprechenden a_i aus.

• Quantenschaltkreis $Q_{BV} = Q_{DJ}$:



U_f ist reversible Einbettung von f_a.

Satz: Q_{BV} berechnet a mit einem Aufruf von f.

Beweis: $|0^n 1\rangle \xrightarrow{H_n \otimes H} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes (|0\rangle - |1\rangle)$

$\xrightarrow{U_{f_a}} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} |x\rangle \otimes (|0\rangle - |1\rangle)$

$\xrightarrow{H_n \otimes I_2} \frac{1}{2^{n+\frac{1}{2}}} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{xa} \cdot (-1)^{xy} |y\rangle \otimes (|0\rangle - |1\rangle) = |\varphi\rangle$

Beobachtung: $\sum_{x\in\{0,1\}^n} (-1)^{x(y+a)} = \begin{cases} 2^n & \text{für } y+a=0^n \text{, d.h. } y=a \\ 0 & \text{sonst} \end{cases}$

D.h. $|\varphi\rangle = \frac{1}{\sqrt{2}} |a\rangle \otimes (|0\rangle - |1\rangle)$

Messung der ersten n Qubits liefert a mit Wahrscheinlichkeit 1. ∎

Für das Bernstein-Vazirani Problem liefern Quantenschaltkreise einen Speedup von n, d.h. einen polynomiellen Faktor.

Das Problem von Simon (1994)

Gegeben: Funktion $f: \mathbb{F}_2^n \to \mathbb{F}_2^m$, $m \geq n$, im Orakel-Modell

Promise-Problem:

$\exists\, s \in \mathbb{F}_2^n : f(x) = f(y) \Leftrightarrow x = y + s$

D.h. insbesondere die Funktion f ist eine 2:1-Abbildung:

Je zwei Urbilder x und $x+s$ werden auf dasselbe Bild abgebildet.

Gesucht: $s \in \mathbb{F}_2^n$

- Klassischer Algorithmus:
  - Werte verschiedene $x_1, \dots, x_k$ aus bis Kollision $f(x_i) = f(x_j)$ gefunden. Ausgabe: $x_i + x_j$.

Deterministisch: $k \leq 2^{n-1} + 1$ Auswertungen notwendig

Probabilistisch: Wie groß muss k gewählt werden, damit Kollision erwartet wird?

Definiere $X_{i,j} = \begin{cases} 1 & \text{falls } f(x_i) = f(x_j) \\ 0 & \text{sonst} \end{cases}$ $\quad Pr(X_{i,j} = 1) = \frac{1}{2^n - 1}$

$E(\#\text{Kollisionen}) = \sum_{1\leq i<j\leq n} Pr(X_{i,j} = 1) = \binom{k}{2} \frac{1}{2^n-1} \approx \frac{k^2}{2^n-1}$

Der Erwartungswert ist konstant für $k = \Omega(2^{\frac{n}{2}})$, d.h. k ist exponentiell in n.

Quantenalgorithmen
(ab Vorlesung 09)

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Wintersemester 2011/12

Problem von Simon (1994)

Problem von Simon

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ mit $f(x) = f(y) \Leftrightarrow y = x + s$
Gesucht: $s \in \mathbb{F}_2^n$

Anmerkungen:

- Je zwei Urbilder x und $x + s$ werden auf dasselbe Bild abgebildet.
- Damit ist f eine (2:1)-Abbildung.

Klassischer Algorithmus:

- Werte paarweise verschiedene $x_1, \ldots, x_k$ aus, bis eine Kollision $f(x_i) = f(x_j)$ gefunden wird.
- Nach Schubfachprinzip genügen $k \leq 2^{n-1} + 1$ Auswertung von f.
- Probabilistisch genügen $k = \Theta(2^{\frac{n}{2}})$ mit hoher Ws.
- Definiere eine Indikatorvariable mit $X_{i,j} = 1$ gdw $f(x_i) = f(x_j)$.
- Die erwartete Anzahl von Kollisionen ist damit
$$E(Kollisionen) = \sum_{1 \leq i < j \leq k} \mathrm{Ws}[X_{i,j} = 1] = \frac{k^2}{2^n - 1}.$$
- Das heißt, wir benötigen $k = \Theta(2^{\frac{n}{2}})$, um Kollisionen zu erhalten.

Ermittle Vektor orthogonal zu s.

Quantenschaltkreis Q_S**:**

- Sei U_f die reversible Einbettung der Funktion f.
- Anwendung von $H_n \otimes I_n$ und U_f auf $0^n 0^n$ liefert
$$\frac{1}{2^n} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |f(x)\rangle.$$
- Messung der letzten n Register liefert für ein festes $f(x_0)$
$$\frac{1}{\sqrt{2}}(|x_0\rangle + |x_0 + s\rangle) \otimes f(x_0).$$
- Anwendung von $H_n \otimes I_n$ führt zu
$$\begin{aligned} & \frac{1}{\sqrt{2}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y \in \{0,1\}^n} ((-1)^{x_0 y} + (-1)^{(x_0+s)\cdot y})|y\rangle \right) \otimes f(x_0) \\ = \quad & \frac{1}{\sqrt{2}} \frac{1}{2^{\frac{n}{2}}} \left(\sum_{y \in \{0,1\}^n} (-1)^{x_0 y}(1 + (-1)^{sy})|y\rangle \right) \otimes f(x_0) \\ = \quad & \frac{1}{2^{\frac{n-1}{2}}} \left(\sum_{y \in \{0,1\}^n, ys=0} (-1)^{x_0 y} |y\rangle \right) \otimes f(x_0). \end{aligned}$$
- Messung der ersten n Register liefert gleichverteiltes y mit $ys = 0$.

Quantenalgorithmus für Simons Problem

Algorithmus Simon

EINGABE: Quantenschaltkreis Q_S

1. Konstruiere leere $(n \times n)$-Matrix Y.
2. Wiederhole bis $\mathrm{rang}(Y) = n$:
   1. Konstruiere mittels Q_S gleichverteiltes $y \in \{0,1\}^n$ mit $ys = 0$.
   2. Falls y linear unabhängig zu Vektoren aus Y, füge y zu Y hinzu.
3. Löse das Gleichungssystem $Y \cdot s = \mathbf{0}$ über $\mathbb{F}_2$.

AUSGABE: $s \in \mathbb{F}_2^n$ mit $f(x) = f(x+s)$ für alle $x \in \mathbb{F}_2^n$

- Korrektheit: Für $\mathrm{rang}(Y) = n$ ist s eindeutig bestimmt.
- Laufzeit: $\mathcal{O}(n)$ Gatteranwendungen ($+\mathcal{O}(n^3)$ für lineare Algebra).
- Exponentieller Speedup gegenüber der klassischen Lösung.

Verallgemeinertes Problem von Simon

Verallgemeinertes Problem von Simon

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ mit $f(x) = f(y) \Leftrightarrow x \oplus y \in S$ für einen Untervektorraum $S \subset \mathbb{F}_2^n$.

Gesucht: Basis für S

- Verwenden gleichen Quantenschaltkreis wie bei Simon's Problem.
- D.h. wir führen $H_n \otimes I_n$, U_f und wieder $H_n \otimes I_n$ durch.
- Durchführung von Hadamard und U_f auf $|0^n\rangle|0^n\rangle$ führt zu
$$\frac{1}{2^{\frac{n}{2}}} \sum_{x \in \{0,1\}^n} |x\rangle|f(x)\rangle.$$
- Messung der letzten n Register liefert ein $f(x_0)$, d.h.
$$\frac{1}{|S|^{\frac{1}{2}}} \sum_{s \in S} |x_0 + s\rangle \otimes |f(x_0)\rangle.$$
- Anwendung von Hadamard liefert
$$\frac{1}{(2^n|S|)^{\frac{1}{2}}} \sum_{y \in \{0,1\}^n} \sum_{s \in S} (-1)^{(x_0+s)y} |y\rangle$$
$$= \frac{1}{(2^n|S|)^{\frac{1}{2}}} \sum_{y \in \{0,1\}^n} (-1)^{x_0 y} \sum_{s \in S} (-1)^{sy} |y\rangle.$$

Messung für Simons Schaltkreis

- **Fall 1:** Sei $y \in S^\perp$, d.h. $sy = 0$. Für jedes y ist die Amplitude $\frac{\pm|S|}{(2^n|S|)^{\frac{1}{2}}}$, d.h. wir messen jedes y mit Ws $\frac{|S|}{2^n}$.
- Wegen $\dim(S) + \dim(S^\perp) = n$, gilt $|S| \cdot |S^\perp| = 2^n$.
- Damit wird jedes $y \in S^\perp$ mit Ws $\frac{1}{|S^\perp|}$ gemessen.
- D.h. die Ws für alle $y \notin S^\perp$ müssen 0 sein. Wir rechnen kurz nach.
- **Fall 2:** Sei $y \notin S^\perp$. Damit existiert ein $s' \in S$ mit $s'y = 1$. Es gilt

$$\begin{aligned}\sum_{s\in S}(-1)^{sy} &= -(-1)^{s'y}\sum_{s\in S}(-1)^{sy} = -\sum_{s\in S}(-1)^{(s+s')y}\\ &= -\sum_{s\in S}(-1)^{sy}.\end{aligned}$$

- Damit verschwindet die Summe und alle Amplituden für $y \notin S^\perp$.

Bestimmung von S

- Messung liefert gleichverteilte $y_i \in S^\perp$.
- Da $\dim(S^\perp)$ unbekannt ist, berechnen wir solange y_i bis die Anzahl der linear unabhängigen y_i stabil bleibt.
- Dazu genügen $\dim(S^\perp) + 4$ Werte mit hoher Ws.
- Wir berechnen aus den y_i eine Basis $B^\perp$ von $S^\perp$.
- Wir lösen das lineare Gleichungssystem $B^\perp s^T = \mathbf{0}$.
- Sei $B = \{s_1, \ldots, s_m\}$ eine Generatorenmenge des Lösungsraums.
- B ist die gesuchte Basis von S.

Speedup und Interpretation von Simons Problem

Speedup gegenüber klassischen Algorithmen:

- Jeder klassische Algorithmus für Simons Problem muss Kollisionen $f(x) = f(y)$ finden.
- Für zufällige x, y ist die Wahrscheinlichkeit einer Kollision $2^{\dim(S)-n}$.
- Geburtstagsparadoxon: Erwarten Kollision nach $2^{\frac{n-\dim(S)}{2}}$ Schritten.
- Quantenalgorithmus liefert Basis für ca. $\dim(S^\perp) = n - \dim(S)$ Auswertungen.
- Damit erhalten wir einen exponentiellen Speedup (Orakel-Modell).

Interpretation

- Simons Algorithmus findet versteckte Untergruppe S in $(\mathbb{F}_2^n, +)$.
- Interpretation als Algorithmus zum Finden einer Periode.
- $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$ ist periodisch: $f(x) = f(x \oplus s)$ mit Periode $s \in S$.
- Frage: Können wir $(\mathbb{F}_2, +)$ durch $(\mathbb{Z}, +)$ ersetzen?
  - $(r\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$ für $r \in \mathbb{N}$.
  - D.h. $f : \mathbb{Z} \to \mathbb{Z}$, $f(x) = f(x + r\mathbb{Z})$ mit gesuchter Periode r.

RSA Verschlüsselung und Perioden

RSA Verschlüsselung

Sei $N = pq$ mit p, q prim und $\phi(N) = (p-1)(q-1)$. Ferner sei $e \in \mathbb{Z}^*_{\phi(N)}$. Die *RSA Funktion* ist die Abbildung $f_{RSA} : \mathbb{Z}_N \to \mathbb{Z}_N$ mit

$$m \mapsto m^e \bmod N.$$

Anmerkung:

- Sei $m \in \mathbb{Z}^*_N$. Wir definieren $\mathrm{ord}(m) = \min\{i \in \mathbb{N} \mid m^i = 1 \bmod N\}$.
- Betrachten die Exponentiations-Funktion $f : \mathbb{Z} \to \mathbb{Z}_N$ mit
$$i \mapsto m^i \bmod N.$$
- f ist für jedes $m \in \mathbb{Z}^*_N$ periodisch, denn
$$f(i) = f(i + \mathrm{ord}(m)k) \text{ für } k \in \mathbb{Z}.$$
- D.h. $\mathrm{ord}(m)$ ist die Periode für die Exponentiations-Funktion.
- Unser Ziel ist die effiziente Ermittlung dieser Periode $\mathrm{ord}(m)$.
- *Kleines Problem:* Angreifer kennt nur m^e und nicht m.

Ordnung von Plain- und Chiffretexten

Lemma

Seien N, e RSA Parameter und $m \in \mathbb{Z}_N^*$. Dann gilt $\mathrm{ord}(m) = \mathrm{ord}(m^e)$.

Beweis:

- Sei $\langle m \rangle = \{m, m^2, \ldots, m^{\mathrm{ord}(m)}\}$ die von m erzeugte Untergruppe.
- Es gilt $\mathrm{ord}(m) = |\langle m \rangle|$. Zeigen zunächst $\langle m^e \rangle \subseteq \langle m \rangle$.
- Sei $m^{ei} \in \langle m^e \rangle$. Dann gilt offenbar $m^{ei} \in \langle m \rangle$.
- Andererseits zeigen wir $\langle m \rangle \subseteq \langle m^e \rangle$.
- Nach Satz von Euler gilt $m^{|\mathbb{Z}_N^*|} = m^{\phi(N)} = 1$.
- Die Elementordnung teilt die Gruppenordnung, d.h. $\mathrm{ord}(m) \mid \phi(N)$.
- Wegen $\mathrm{ggT}(e, \phi(N)) = 1$ gilt damit ebenfalls $\mathrm{ggT}(e, \mathrm{ord}(m)) = 1$.
- Damit existieren $d, k \in \mathbb{Z}$ mit $ed + \mathrm{ord}(m)k = 1$.
- D.h. $m = m^{ed + \mathrm{ord}(m)k} = m^{ed} \cdot (m^{ord(m)})^k = (m^e)^d \bmod N$.
- Daraus folgt $m \in \langle m^e \rangle$ und damit auch $m^i \in \langle m^e \rangle$ für alle $i \in \mathbb{N}$.
- Insgesamt: $\langle m \rangle = \langle m^e \rangle$, d.h. $\mathrm{ord}(m) = |\langle m \rangle| = |\langle m^e \rangle| = \mathrm{ord}(m^e)$.

Brechen von RSA mit Hilfe der Ordnung von m

Satz

Seien N, e RSA-Parameter und $m^e \in \mathbb{Z}_N^*$. Mit Hilfe von $\mathrm{ord}(m^e)$ kann m in Zeit $\mathcal{O}(\log^3 N)$ berechnet werden.

Beweis:

- Beweis zuvor liefert $\mathrm{ord}(m) = \mathrm{ord}(m^e)$ und $\mathrm{ggT}(e, \mathrm{ord}(m)) = 1$.
- Der Erweiterte Euklidische Algorithmus liefert bei Eingabe $e, \mathrm{ord}(m) \in \mathbb{Z}_N$ in Zeit $\mathcal{O}(\log^2 N)$ Zahlen d, k mit $ed + \mathrm{ord}(m)k = 1$.
- Wir berechnen $(m^e)^d = m^{1-ord(m)k} = m \cdot (m^{\mathrm{ord}(m)})^{-k} = m \bmod N$ in Zeit $\mathcal{O}(\log^3 N)$.

Motivation Phasenbestimmung

Problem Spezialfall der Phasenbestimmung

Gegeben: Zustand $|\mathbf{z}\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{\mathbf{y}\in\{0,1\}^n} (-1)^{\mathbf{x}\cdot\mathbf{y}} |\mathbf{y}\rangle$

Gesucht: $\mathbf{x} \in \mathbb{F}_2^n$

- Für $n = 1$ ist der Zustand $|\mathbf{z}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^{\mathbf{x}}|1\rangle) = H|\mathbf{x}\rangle$.
- Es gilt $H|\mathbf{z}\rangle = |\mathbf{x}\rangle$, d.h. H dekodiert die Phaseninformation $\mathbf{x}$.
- Für allgemeines n gilt $|\mathbf{z}\rangle = H_n|\mathbf{x}\rangle$ und damit $H_n|\mathbf{z}\rangle = |\mathbf{x}\rangle$.
- D.h. H_n dekodiert Phasen der speziellen Form $(-1)^{\mathbf{x}\cdot\mathbf{y}} = (e^{\pi i})^{\mathbf{x}\cdot\mathbf{y}}$.
- Gibt es ein Analog für Phasen der Form $e^{2\pi i\omega}$ für ein $\omega \in [0, 1)$?

Problem der Phasenbestimmung

Problem Phasenbestimmung

Gegeben: Zustand $|z\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$ für $\omega \in [0,1)$

Gesucht: ω (bzw. eine gute Approximation von ω)

Notation:

- Wir bezeichnen mit $\mathbf{y} \in \mathbb{F}_2^n$ einen n-dimensionalen Vektor.
- Mit $y \in \mathbb{Z}_{2^n}$ bezeichnen wir eine Zahl zwischen 0 und $2^n - 1$.
- Z.B. schreiben wir für $n = 4$ den Zustand $|y\rangle = |3\rangle = |0011\rangle = |\mathbf{y}\rangle$.
- Für $\omega = \sum_k x_k 2^{-k}$ schreiben wir $\omega = 0.x_1x_2x_3\ldots$
- Für $n = 1$ und $\omega = 0.x_1$ folgt

$$|z\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{2\pi i (0.x_1) y} |y\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{\pi i x_1 y} |y\rangle$$

$$= \frac{1}{\sqrt{2}} \sum_{y=0}^{1} (-1)^{x_1 y} |y\rangle = H|x_1\rangle$$

- D.h. $H|z\rangle = |x_1\rangle$ liefert x_1 und damit ω.

Produktformel von Griffith-Nui (1996)

Satz Produktformel von Griffith-Nui

Für $\omega = 0.x_1 x_2 \ldots x_n$ gilt

$$|z\rangle = \frac{1}{\sqrt{2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle = \frac{|0\rangle + e^{2\pi i 0.x_n}|1\rangle}{\sqrt{2}} \otimes \ldots \otimes \frac{|0\rangle + e^{2\pi i 0.x_1 x_2 \ldots x_n}|1\rangle}{\sqrt{2}}.$$

Beweis:

$$\begin{aligned}
|z\rangle &= \frac{1}{2^{\frac{n}{2}}} \sum_{y_0=0}^{1} \ldots \sum_{y_{n-1}=0}^{1} e^{2\pi i \omega \sum_{\ell=0}^{n-1} y_\ell 2^\ell} |y_{n-1} \ldots y_0\rangle \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{y_0=0}^{1} \ldots \sum_{y_{n-1}=0}^{1} \bigotimes_{\ell=1}^{n} e^{2\pi i \omega y_{n-\ell} 2^{n-\ell}} |y_{n-\ell}\rangle \\
&= \frac{1}{2^{\frac{n}{2}}} \bigotimes_{\ell=1}^{n} \left(\sum_{y_\ell=0}^{1} e^{2\pi i \omega y_{n-\ell} 2^{n-\ell}} |y_{n-\ell}\rangle \right) = \frac{1}{2^{\frac{n}{2}}} \bigotimes_{\ell=1}^{n} \left(|0\rangle + e^{2\pi i \omega 2^{n-\ell}} |1\rangle \right) \\
&= \frac{1}{2^{\frac{n}{2}}} \left(\left(|0\rangle + e^{2\pi i x_1 x_2 \ldots x_{n-1}.x_n} |1\rangle \right) \otimes \ldots \otimes \left(|0\rangle + e^{2\pi i 0.x_1 x_2 \ldots x_n} |1\rangle \right) \right)
\end{aligned}$$

Bestimmen von zwei Nachkommastellen

Problem Phasenbestimmung mit $n = 2$ Bits

Gegeben: Zustand $|z\rangle = \frac{1}{2}\sum_{y=0}^{2^2-1} e^{2\pi i \omega y}|y\rangle$ für $\omega = 0.x_1x_2$

Gesucht: $\omega = 0.x_1x_2$

- Schreibe $|z\rangle = \left(\frac{|0\rangle + e^{2\pi i 0.x_2}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i 0.x_1x_2}|1\rangle}{\sqrt{2}}\right)$.
- Bestimme x_2 durch Anwendung von Hadamard auf das 1. Qubit.
- Falls $x_2 = 0$, bestimme x_1 durch Hadamard auf das 2. Qubit.
- Falls $x_2 = 1$, dann eliminieren wir zunächst x_2 durch eine Rotation.
- Wir betrachten die Rotation $R_2 = F_{2\pi(0.01)} = \begin{pmatrix} 1 & 0 \\ 0 & e^{2\pi i(0.01)} \end{pmatrix}$.
- D.h. $R_2^{-1}\left(\frac{|0\rangle + e^{2\pi i 0.x_1 1}|1\rangle}{\sqrt{2}}\right) = \left(\frac{|0\rangle + e^{2\pi i(0.x_1 1 - 0.01)}|1\rangle}{\sqrt{2}}\right) = \left(\frac{|0\rangle + e^{2\pi i 0.x_1}|1\rangle}{\sqrt{2}}\right)$.
- Verwenden ein vom 1.Qubit kontrolliertes R_2^{-1}-Gatter auf Qubit 2.
- Anschließend bestimmen wir x_1 mittels eines Hadamard-Gatters.

Bestimmen von 3 Nachkommastellen

Problem Phasenbestimmung mit $n = 3$ Bits

Gegeben: Zustand $|z\rangle = \frac{1}{2^{\frac{3}{2}}} \sum_{y=0}^{2^3-1} e^{2\pi i \omega y} |y\rangle$ für $\omega = 0.x_1x_2x_3$

Gesucht: $\omega = 0.x_1x_2x_3$

- $|z\rangle = \left(\frac{|0\rangle + e^{2\pi i 0.x_3}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i 0.x_2x_3}|1\rangle}{\sqrt{2}}\right) \otimes \left(\frac{|0\rangle + e^{2\pi i 0.x_1x_2x_3}|1\rangle}{\sqrt{2}}\right)$
- Bestimme x_3 und x_2 wie zuvor.
- Definiere Rotation R_k zum Entfernen der k-ten Nachkommastelle

$$R_k = F_{2\pi 2^{-k}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{pmatrix}.$$

- Entferne x_3 in Qubit 3 durch R_3^{-1} kontrolliert durch Qubit 1.
- Entferne x_2 in Qubit 2 durch R_2^{-1} kontrolliert durch Qubit 2.
- Bestimme anschließend x_1 durch ein Hadamard-Gatter.

Die Quanten Fourier Transformation

- Verallgemeinerung auf beliebiges n führt zu einem Schaltkreis C_n mit $\mathcal{O}(n^2)$ Gatter.
- D.h. wir realisieren für $\omega = 0.x_1 \dots x_n = \frac{x}{2^n}$ die Abbildung

$$\frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle \mapsto |x\rangle.$$

Definition Quanten Fourier Transformation (QFT)

Wir bezeichnen die Abbildung

$$\mathrm{QFT}_{2^n} : |x\rangle \mapsto \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{x}{2^n} y} |y\rangle$$

als *Quanten Fourier Transformation* (QFT).

Schaltkreis für QFT_{2^n}

Satz Schaltkreis für QFT_{2^n}

Es gibt einen Quantenschaltkreis für QFT_{2^n} mit $\mathcal{O}(n^2)$ Gattern.

Beweis:

- Verwenden Schaltkreis C_n zur Phasenbestimmung.
- Der Schaltkreis C_n implementiert $\mathrm{QFT}_{2^n}^{-1}$.
- D.h. wir können C_n in umgekehrter Reihenfolge anwenden.

Vergleich zur Diskreten Fourier Transformation (DFT)

Definition Diskrete Fourier Transformation

Sei $\alpha(x) = \sum_{\ell=0}^{2^n-1} a_i x^i \in \mathbb{C}[x]$. Sei $\beta_y = \alpha(e^{2\pi i \frac{y}{2^n}})$ für $y \in \mathbb{Z}_{2^n}$. Dann bezeichnen wir $\beta = (\beta_0, \ldots, \beta_{2^n-1})$ als *Diskrete Fourier Transformierte (DFT)* von $\alpha(x)$.

Zusammenhang mit QFT:

- DFT liefert $\beta_y = \sum_{\ell=0}^{2^n-1} \alpha_\ell e^{2\pi i \frac{y}{2^n}\ell}$.
- Betrachten allgemeinen Quantenzustand $|z\rangle = \sum_{\ell=0}^{2^n-1} \alpha_\ell |\ell\rangle$.

$$\begin{aligned}
\mathrm{QFT}_{2^n}(|z\rangle) &= \sum_{\ell=0}^{2^n-1} \alpha_\ell \mathrm{QFT}_{2^n}(|\ell\rangle) = \sum_{\ell=0}^{2^n-1} \alpha_\ell \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{\ell}{2^n} y} |y\rangle \\
&= \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} \sum_{\ell=0}^{2^n-1} \alpha_\ell e^{2\pi i \frac{y}{2^n}\ell} |y\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} \beta_y |y\rangle
\end{aligned}$$

- D.h. die Amplituden β_y sind die DFTs der Amplituden α_ℓ.

Vergleich zum klassischen Ansatz

Speedup:

- Berechnung der DFT entspricht Auswerten eines Polynoms vom Grad kleiner als 2^n an 2^n verschiedenen Stellen.
- Komplexität mit Horner-Schema: $2^n \cdot \mathcal{O}(2^n) = \mathcal{O}(2^{2n})$.
- Schnelle Fourier Transformation (DiMaI): $\mathcal{O}(n2^n)$.
- Berechnung der QFT benötigt dagegen nur $\mathcal{O}(n^2)$ Gatter.
- D.h. wir erhalten einen exponentiellen Speedup.
- **Aber:** QFT liefert die Amplituden nicht explizit. Aus $\mathrm{QFT}_{2^n}(|z\rangle)$ kann daher die DFT nicht einfach bestimmt werden.

Approximieren von ω

Szenario:

- Bisher war ω stets von der Form $\omega = \frac{x}{2^n}$.
- **Frage:** Was geschieht für allgemeines ω?

Fakt Approximation von ω

Sei $|z\rangle = \frac{1}{2^{\frac{n}{2}}} \sum_{y=0}^{2^n-1} e^{2\pi i \omega y} |y\rangle$ für $\omega \in [0,1)$. Dann liefert $\mathrm{QFT}^{-1}(|z\rangle)$ mit Wahrscheinlichkeit mindestens $\frac{4}{\pi^2}$ ein x mit $|\frac{x}{2^n} - \omega| \leq \frac{1}{2^{n+1}}$.

- D.h. wir erhalten mit Ws $\frac{4}{\pi^2}$ dasjenige ganzzahlige Vielfache von $\frac{1}{2^n}$, das am nächsten zu ω ist.

Definition Periodischer Zustand

Sei $|z_{r,b}\rangle$ ein Quantenzustand der Form $|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |kr + b\rangle$ mit $b \in \mathbb{Z}_r$. Dann heißt $|z_{r,b}\rangle$ *periodischer Zustand* mit *Periode* r, *Vielfachheit der Periode* m und *Shift* b.

Finden der Periode mit Vielfachheit

Problem Finden der Periode mit Vielfachheit

Gegeben: mr, periodischer Zustand $|z_{r,b}\rangle$ mit $b \in_R \mathbb{Z}_r$
Gesucht: r

Lösung:

- Messen von $|z_{r,b}\rangle$ liefert jeden Zustand $|x\rangle$, $x \in \mathbb{Z}_{mr}$ mit Ws $\frac{1}{mr}$.
- D.h. Messung von $|z_{r,b}\rangle$ liefert keine Information über r.
- Berechnen stattdessen $\mathrm{QFT}_{mr}|z_{r,b}\rangle = \frac{1}{\sqrt{r}} \sum_{\ell=0}^{r-1} e^{2\pi i \frac{b}{r}\ell} |m\ell\rangle$.
  (Lemma auf nächster Folie)
- Messung liefert nur Basiszustände $|m\ell\rangle$, die Vielfache von m sind.
- Wir berechnen $\frac{m\ell}{mr} = \frac{\ell}{r}$. Falls $\gcd(\ell, r) = 1$ liefert dies r.
- Es gilt $\gcd(\ell, r) = 1$ mit Wahrscheinlichkeit $\Omega(\frac{1}{\log\log r})$.

QFT entfernt den Shift

Lemma Entfernen des Shifts durch QFT

$$\mathrm{QFT}_{mr}|z_{r,b}\rangle = \frac{1}{\sqrt{r}}\sum_{\ell=0}^{r-1} e^{2\pi i \frac{b}{r}\ell}|m\ell\rangle$$

Beweis:

- Es gilt $\mathrm{QFT}_{mr}|z_{r,b}\rangle = \frac{1}{\sqrt{m}}\sum_{k=0}^{m-1}\mathrm{QFT}_{mr}|kr+b\rangle$. Umformung liefert
$$\frac{1}{\sqrt{m^2 r}}\sum_{y=0}^{mr-1}\sum_{k=0}^{m-1} e^{2\pi i \frac{kr+b}{mr}y}|y\rangle$$
- Wir ziehen den vom Shift b abhängigen Term aus der 1. Summe
$$\frac{1}{\sqrt{m^2 r}}\sum_{y=0}^{mr-1} e^{2\pi i \frac{by}{mr}}\sum_{k=0}^{m-1} e^{2\pi i \frac{ky}{m}}|y\rangle.$$
- Für $y = m\ell$, $\ell \in \mathbb{Z}_r$ erhalten wir $e^{2\pi i \frac{by}{mr}} = e^{2\pi i \frac{b}{r}\ell}$ und $\sum_{\ell=0}^{m-1} e^{2\pi i \frac{ky}{m}} = m$. Dies liefert sofort die geforderte obige Formel.
- Übungsaufgabe: Rechnen Sie nach, dass für $m \not| y$ gilt
$$\sum_{k=0}^{m-1}\left(e^{2\pi i \frac{y}{m}}\right)^k = 0.$$
- D.h. die restlichen Amplituden heben sich gegenseitig auf.

Finden der Ordnung von 2 in $\mathbb{Z}_{15}^*$

Beispiel: Finden der Periode von 2 in $\mathbb{Z}_{15}^*$

Gegeben: $mr = |\mathbb{Z}_{15}^*| = 8$
Gesucht: $r = \operatorname{ord}_{\mathbb{Z}_{15}^*}(2)$

- Sei $f(x) = 2^x \bmod 15$ mit reversibler Einbettung U_f.
- Auf $|0^3\rangle|0^3\rangle$ wird $H_3 \otimes I_3$ und U_f angewendet. Dies liefert
$$\frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle|2^x \bmod 15\rangle = \frac{1}{\sqrt{8}} \Big(|0\rangle|1\rangle + |1\rangle|2\rangle + |2\rangle|4\rangle + |3\rangle|8\rangle + |4\rangle|1\rangle + |5\rangle|2\rangle + |6\rangle|4\rangle + |7\rangle|8\rangle \Big).$$
- Angenommen wir messen $|2\rangle$ im rechten Teil.
- Dann steht in den ersten 3 Qubits der periodische Zustand
$$|z_{4,1}\rangle = \frac{1}{\sqrt{2}}(|1\rangle + |5\rangle).$$
- $\mathrm{QFT}_8(|z_{4,1}\rangle) = \frac{1}{2} \sum_{\ell=0}^{3} e^{2\pi i \frac{1}{4}\ell} |2\ell\rangle = \frac{1}{2}(|0\rangle + i|2\rangle - |4\rangle - i|6\rangle)$.
- Bei Messung von $m\ell = 6$ erhalten wir $\frac{m\ell}{mr} = \frac{6}{|\mathbb{Z}_{15}^*|} = \frac{3}{4}$.
- Der Nenner impliziert $4 \mid \operatorname{ord}(2)$.
- Wir prüfen $2^4 = 1 \bmod 15$, d.h. $\operatorname{ord}(2) = 4$.

Finden der Periode ohne Vielfachheit

Problem Finden der Periode

Gegeben: n, periodischer Zustand $|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k:0 \leq kr+b<2^n} |kr+b\rangle$ mit geeignetem m, $r \leq m \leq \frac{2^n}{r}$, so dass $\| |z_{r,b}\rangle \| = 1$.

Gesucht: r

Idee der Lösung:

- Es gilt $\mathrm{QFT}_{2^n}(|z_{r,b}\rangle) = \frac{1}{\sqrt{m2^n}} \sum_{y=0}^{2^n-1} e^{2\pi i \frac{by}{2^n}} \sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y} |y\rangle$.
- Amplitude $\sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y}$ wird groß, falls y nahe einem Vielfachem von $\frac{2^n}{r}$ ist. Wir zeigen $\left| y - \frac{2^n}{r} \cdot \ell \right| \leq \frac{1}{2}$ für ein $\ell \in \mathbb{Z}_r$ mit hoher Ws.
- Wegen $2^n \geq r^2$ folgt damit $\left| \frac{y}{2^n} - \frac{\ell}{r} \right| \leq \frac{1}{2 2^n} \leq \frac{1}{2r^2}$.
- Damit kommt $\frac{\ell}{r}$ in der Kettenbruchentwicklung von $\frac{y}{2^n}$ vor.
- Zeigen alternativ, dass man $\frac{r}{\gcd(\ell,r)}$ mittels Gittern finden kann.
- 2 Durchgänge des Algorithmus liefern $r_1 = \frac{r}{\gcd(\ell_1,r)}$, $r_2 = \frac{r}{\gcd(\ell_2,r)}$.
- Mit Ws $\geq \frac{6}{\pi^2}$ gilt $r = \mathrm{kgV}(r_1, r_2)$.

Messung von y

Lemma Gemessenes y approxiert Vielfaches von $\frac{2^n}{r}$

Mit Ws mindestens $\frac{4}{\pi^2} \geq 0.4$ erhalten wir ein y mit $\left| y - \frac{2^n}{r} \cdot \ell \right| \leq \frac{1}{2}$.

Beweisskizze:

- Sei $y_\ell = \frac{2^n}{r}\ell + \delta_\ell$ für $|\delta_\ell| \leq \frac{1}{2}$ und $p(y_\ell) = \frac{1}{m2^n} \left| \sum_{k=0}^{m-1} e^{2\pi i \frac{kr}{2^n} y_\ell} \right|^2$.
- Für die Berechnung von $p(y_\ell)$ trägt nur der Term δ_ℓ bei.
- Übung: $m2^n \cdot p(y_\ell) = \left| \frac{e^{2\pi i \frac{r}{2^n} m \delta_\ell} - 1}{e^{2\pi i \frac{r}{2^n} \delta_\ell} - 1} \right|^2 = \frac{\sin^2(\pi \frac{r}{2^n} m \delta_\ell)}{\sin^2(\pi \frac{r}{2^n} \delta_\ell)}$.
- Wegen $m \approx \frac{2^n}{r}$ und $sin(x) \approx x$ für kleine x erhalten wir
$$p(y_\ell) \approx \frac{1}{m2^n} \left(\frac{\sin(\pi \delta_\ell)}{\pi \frac{r}{2^n} \delta_\ell} \right)^2 \approx \frac{1}{r} \left(\frac{\sin(\pi \delta_\ell)}{\pi \delta_\ell} \right)^2.$$
- Es gilt $\sin(x) \geq \frac{2}{\pi} x$ für $x \in [0, \frac{\pi}{2}]$, d.h. $p(y_\ell) \geq \frac{1}{r} \left(\frac{\frac{2}{\pi} \pi \delta_\ell}{\pi \delta_\ell} \right)^2 = \frac{1}{r} \frac{4}{\pi^2}$.
- Ws gilt für alle $p(y_\ell)$ mit $\ell \in \mathbb{Z}_r$, d.h. wir messen ein y mit Ws $\geq \frac{4}{\pi^2}$.

Berechnen von $r/\gcd(\ell, r)$

Lemma Berechnen von ℓ und r

Sei $y \in \mathbb{Z}$ mit $\left|y - \frac{2^n}{r} \cdot \ell\right| \leq \frac{1}{2}$ und $\ell \in \mathbb{Z}_r$, $r^2 \leq 2^n$. Dann kann $\frac{r}{\gcd(\ell,r)}$ in Zeit $\mathcal{O}(n^2)$ berechnet werden.

Beweisskizze:

- Es gilt $yr - 2^n\ell = x$ für ein $x \in \mathbb{Z}$ mit $|x| \leq \frac{r}{2}$.
- Seien r', ℓ', x' die durch $\gcd(\ell, r)$ gekürzten Unbekannten r, ℓ, x.
- Definieren $f(r', x') = yr' - x'$ mit $f(r', x') = 0 \bmod 2^n$.
- f ist modulares lineares Polynom mit Nullstelle (r', x'), so dass
$$|r' \cdot x'| \leq r' \cdot \frac{r}{2} \leq 2^{n-1}.$$
- Vorlesung Kryptanalyse: r', x' werden in Zeit $\mathcal{O}(n^2)$ gefunden, sofern $|r' \cdot x'|$ kleiner als der Modul 2^n ist.
- Sei $B = \begin{pmatrix} 1 & y \\ 0 & 2^n \end{pmatrix}$. Dann gilt $(r', -\ell') \cdot B = (r', x')$ und (r', x') ist eine kürzeste ganzzahlige Linearkombination von Vektoren aus B.
- D.h. ein kürzester Vektor liefert $r' = \frac{r}{\gcd(\ell,r)}$.

Gaußalgorithmus

Definition Gitter

Sei $B \in \mathbb{Z}^{2\times 2}$. Wir bezeichnen mit $L(B) = \{\mathbf{x} \in \mathbb{Z}^2 \mid \mathbf{a}B = \mathbf{x}, \mathbf{a} \in \mathbb{Z}^2\}$ das von den Vektoren von B aufgespannte *Gitter*. Wir verwenden für die Länge von Gittervektoren $\mathbf{x} = (x_1, x_2)$ die ℓ_2-Norm $\|\mathbf{x}\| = \sqrt{x_1 + x_2}$.

Algorithmus Gaußalgorithmus

EINGABE: Basis $B = \begin{pmatrix} \mathbf{b_1} \\ \mathbf{b_2} \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ mit $\|\mathbf{b}_1\| \geq \|\mathbf{b}_2\|$

1. Bestimme $k \in \mathbb{Z}$, das $\|\mathbf{b}_1 - k \cdot \mathbf{b}_2\|$ minimiert.
2. Setze $\mathbf{b}_1 := \mathbf{b}_1 - k \cdot \mathbf{b}_2$. Falls $k \neq 0$, gehe zu Schritt 1.

AUSGABE: Basis $\mathbf{b}_1, \mathbf{b}_2$ minimaler Länge

Gaußalgorithmus liefert kürzeste Vektoren

Fakt Gaußalgorithmus

Der Gaußalgorithmus liefert bei Eingabe einer Basis B mit maximalem Basiseintrag b_m in Zeit $\mathcal{O}(\log^2 b_m)$ eine reduzierte Basis mit kürzestem Gittervektor in $L(B)$.

Shor's Algorithmus (1994)

Algorithmus Shor's Algorithmus zum Finden der Ordnung

EINGABE: a, N

1. Benötigen $2^n \geq N^2 \geq \phi^2(N)$, d.h. wähle $n = \lceil 2 \log N \rceil$.
2. Sei U_f die reversible Einbettung von $f(x) = a^x \bmod N$.
3. Wende auf $|0^n\rangle|0^n\rangle$ zunächst $H_n \otimes I_n$ dann U_f an. Liefert
$$\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle|a^x \bmod N\rangle = \sum_{b=0}^{r-1} \left(\frac{1}{\sqrt{2^n}} \sum_{k=0}^{m-1} |kr+b\rangle \right) |a^b \bmod N\rangle.$$
4. Messen der hinteren n Register liefert in den ersten n Registern
$$|z_{r,b}\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |kr+b\rangle.$$
5. Berechne $\mathrm{QFT}_{2^n}(|z_{r,b}\rangle)$ und messe ein y_1.
6. Wiederhole Schritte 1-5 für ein y_2.
7. Berechne $r_1 = \frac{r}{\gcd(\ell_1, r)}$, $r_2 = \frac{r}{\gcd(\ell_2, r)}$ aus y_1, y_2 mit Gauß-Alg.
8. Berechne $r = \mathrm{kgV}(r_1, r_2)$. Falls $a^r \neq 1 \bmod N$, Ausgabe "Fehler".

AUSGABE: $r = \mathrm{ord}_{\mathbb{Z}_N*}(a)$

Finden der Ordnung von 2 in $\mathbb{Z}_{21}^*$

Beispiel: Finden der Periode von 2 in $\mathbb{Z}_{21}^*$

- Wähle der Einfachheit halber nur $n = 6$. Wir erhalten
$$\frac{1}{8}\sum_{x=0}^{63}|x\rangle|2^x \bmod 21\rangle = \frac{1}{8}\Big(|0\rangle|1\rangle + |1\rangle|2\rangle + \quad \ldots \quad + |5\rangle|11\rangle$$
$$\vdots$$
$$+|60\rangle|1\rangle + |61\rangle|2\rangle + |62\rangle|4\rangle + |63\rangle|8\rangle\Big).$$
- Messung von $|4\rangle$ im rechten Teil liefert im linken Teil
$$|z_{6,2}\rangle = \frac{1}{\sqrt{11}}\sum_{i=0}^{10}|6k+2\rangle.$$
- $\mathrm{QFT}_{2^6}(|z_{6,2}\rangle)$ und Messung liefert ein $y = 11\ell$ mit Ws $\geq \frac{4}{\pi^2}$.
- Bei Messung von $y = 11 \cdot 1$ erhalten wir die Gitterbasis
$$B = \begin{pmatrix} 1 & 11 \\ 0 & 64 \end{pmatrix}.$$
- Gaußalgorithmus liefert kürzesten Vektor
$$(6,2) = (6,-1)\cdot B = (r,x) \text{ in } L(B).$$
- Wir prüfen $2^r = 2^6 = 1 \bmod 21$.

Komplexität und Vergleich mit klassischen Algorithmen

Satz Komplexität von Shor's Algorithmus

Shor's Algorithmus benötigt $\tilde{\mathcal{O}}(\log^2 N)$ Gatter.

Beweis:

- Anwendung von H_n benötigt $n = \mathcal{O}(\log N)$ Hadamard-Gatter.
- Anwednung von U_f benötigt $\mathcal{O}(n^2 \log n \log\log n) = \tilde{\mathcal{O}}(\log^2 N)$ Gatter.
- QFT_{2n} in Schritt 5 benötigt $\mathcal{O}(n^2)$ Gatter.
- Schritt 7 benötigt ebenfalls $\mathcal{O}(n^2)$ Gatter.

Klassisch:

- Bester beweisbarer Algorithmus $e^{\mathcal{O}(\sqrt{\log N \log\log N})}$.
- Bester heuristischer Algorithmus $e^{\mathcal{O}(\log^{\frac{1}{3}} N \log\log^{\frac{2}{3}} N)}$ (Number Field Sieve)

Finden der Ordnung und Faktorisieren

Satz Faktorisieren mittels Ordnung

Sei $N = pq$, p, q prim. Gegeben sei ein Algorithmus, der bei Eingabe $(a, N) \in \mathbb{Z}_N^* \times \mathbb{N}$ die Ordnung $\mathrm{ord}_{\mathbb{Z}_N*}(a)$ in Zeit $T(N)$ berechnet. Dann kann N in erwarteter Laufzeit $\mathcal{O}(\log^3 N \cdot T(N))$ faktorisiert werden.

Beweis: Übungsaufgabe.

- Hinweis: Sei $\mathrm{ord}(a) = 2^k t$ mit t ungerade.
- Falls $a^{2^i t} \neq \pm 1$ und $a^{2^{i+1} t} = 1$ für ein $i \in \mathbb{Z}_k$, berechne
$$\mathrm{ggT}(a^{2^i t} \pm 1, N).$$

Finden einer Periode und Diskrete Logarithmen

Definition Diskretes Logarithmus Problem (DLP)

Gegeben: Abelsche Gruppe G, $a \in G$ und $b \in \langle a \rangle$
Gesucht: $k = \log_b a \in \mathbb{Z}_{\mathrm{ord}(a)}$ mit $a^k = b$

Lösung mittels Finden einer Periode:

- $\mathrm{ord}(a)$ kann mit Hilfe von Shors Algorithmus berechnet werden.
- Wir definieren die Funktion $f(x_1, x_2) = a^{x_1} b^{x_2} = a^{x_1 + kx_2}$.
- Es gilt $f(x_1 + k\ell, x_2 - \ell) = a^{x_1 + k\ell + kx_2 - k\ell} = f(x_1, x_2)$ für $\ell \in \mathbb{Z}_{\mathrm{ord}(a)}$.
- D.h. f ist periodisch mit Periode $(k, 1)$.
- Finden der Periode führt zur Lösung des DLPs.
- Der Quantenschaltkreis für DLP unterscheidet sich von Shor's Schaltkreis lediglich durch die beiden Eingaberegister für x_1, x_2.

Datenbanksuche

Definition Problem der Datenbanksuche

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2$ mit $f(a) = 1$ für genau ein $a \in \mathbb{F}_2^n$
Gesucht: $a \in \mathbb{F}_2^n$

Klassisch:

- Sei $N = 2^n$. Wir benötigen $\Omega(N)$ Aufrufe, um a zu bestimmen.

Idee für einen Quantenschaltkreis:

- Erzeuge eine Superposition $|\psi\rangle$ aller möglichen Eingaben $x \in \mathbb{F}_2^n$.
- Drehe $|\psi\rangle$ sukzessive in Richtung des gesuchten $|a\rangle \in \mathbb{F}_2^n$.
- Bestimme die Anzahl der notwendigen Drehungen.
- Falls Vektor hinreichend nahe an $|a\rangle$ ist, messe a mit hoher Ws.

Aufwand dazu wird nur $\mathcal{O}(\sqrt{N})$ betragen.

Die Drehung V

Definition der Drehung V:

- Starte mit Zustand $|0^n\rangle|1\rangle$. Sei $|\psi\rangle = H_n|0^n\rangle$.
- Anwendung von H_{n+1} auf $|0^n\rangle|1\rangle$ liefert die Superposition
$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$
- Reversible Einbettung U_f führt zum Zustand
$$\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$
- Effekt von U_f auf die ersten n Register entspricht der Abbildung
$$V|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & \text{für } x \neq a \\ -|x\rangle & \text{für } x = a. \end{cases}$$

Anmerkung:

- Sei $|z\rangle = \sum_{x\in\{0,1\}^n}\alpha_a|x\rangle$ ein beliebiger Quantenzustand.
- V flippt das Vorzeichen des zu $|a\rangle$ parallelen Anteils $\alpha_a|a\rangle$.
- Der Anteil orthogonal zu $|a\rangle$ bleibt unverändert.
- D.h. $V|z\rangle = |z\rangle - 2\alpha_a|a\rangle$ und $V|\psi\rangle = |\psi\rangle - \frac{2}{\sqrt{2^n}}|a\rangle$.

Projektionen

Definition $a^\perp$

Wir betrachten die von $|a\rangle$, $|\psi\rangle$ aufgespannte 2-dimensionale Ebene.
Wir bezeichnen mit $|a^\perp\rangle$ den zu $|a\rangle$ orthogonalen Einheitsvektor.

Anmerkung:

- V spiegelt den Vektor $|\psi\rangle$ an $|a^\perp\rangle$.

Alternative Darstellung von V:

- Sei $|z\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle$.
- Anwendung von $\langle a|$ auf beiden Seiten liefert
$$\langle a|z\rangle = \sum_{x\in\{0,1\}^n} \alpha_x \langle a|x\rangle = \alpha_a.$$
- D.h. die Projektion von $|z\rangle$ auf $|a\rangle$ ist
$$\alpha_a|a\rangle = \langle a|z\rangle|a\rangle = |a\rangle\langle a|z\rangle = |a\rangle\langle a||z\rangle.$$
- Wir können die Operation von V auf $|z\rangle$ schreiben als
$$V|z\rangle = |z\rangle - 2\cdot|a\rangle\langle a||z\rangle = \Big(I_n - 2|a\rangle\langle a|\Big)|z\rangle.$$

Die zweite Drehung W

Definition Projektionsoperator

Sei $|x\rangle \in \mathbb{C}^k$. Dann heißt $|x\rangle\langle x| \in \mathbb{C}^{k\times k}$ *Projektionsoperator* auf $|x\rangle$.

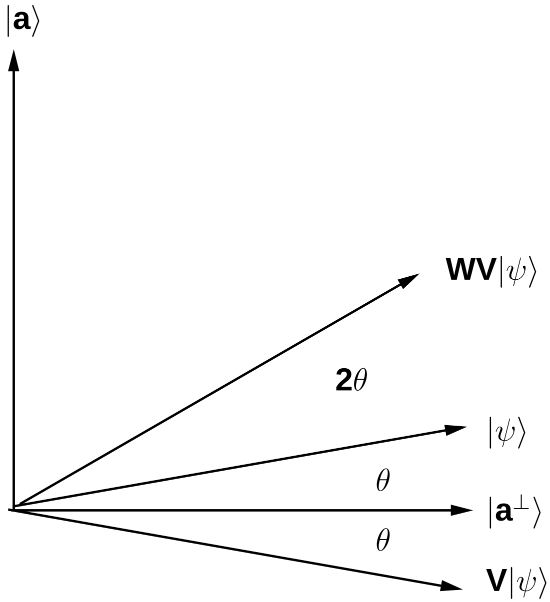
Definition der Drehung W:

- Sei $|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$ die Gleichverteilung.
- Wir definieren die zweite Drehung W wie folgt.
- Die Drehung W erhält den Anteil eines Vektors parallel zu $|\psi\rangle$.
- W flippt das Vorzeichen des Anteil orthogonal zu $|\psi\rangle$.
- Die Drehung W entspricht also einer Spiegelung an $|\psi\rangle$.
- Analog zu V definieren wir $W = (-I_n + 2|\psi\rangle\langle\psi|)$.

Definition Grover-Iteration

Seien $V = (I_n - 2|a\rangle\langle a|)$ und $W = (-I_n + 2|\psi\rangle\langle\psi|)$. Dann nennen wir die Abbildung WV eine *Grover-Iteration*.

Graphische Darstellung



Grover-Iteration ist Rotation in der Ebene

- Wir wenden WV sukzessive auf den Zustand $|\psi\rangle$ an.
- Die Definition von V und W hängt nur von $|a\rangle$ und $|\psi\rangle$ ab.
- Wir spiegeln abwechselnd an $|a^\perp\rangle$ und $|\psi\rangle$.
- Damit liefert die Grover-Iteration eine 2-dimensionale Rotation in der Ebene aufgespannt durch die Vektoren $|a\rangle$ und $|\psi\rangle$.
- D.h. wir können jeden durch Grover-Iteration erhaltenen Vektor als Linearkombination von $|a\rangle$ und $|\psi\rangle$ darstellen.
- Wegen $\langle a|\psi\rangle = \langle\psi|a\rangle = \frac{1}{\sqrt{2^n}}$ erhalten wir stets reelle Amplituden.

Grover-Iteration rotiert in Richtung $|a\rangle$

- Wir betrachten die erste Grover-Iteration auf $|\psi\rangle$.
- Wegen $\langle a|\psi\rangle = \frac{1}{\sqrt{2^n}}$ sind $|a\rangle$ und $|\psi\rangle$ nahezu orthogonal.
- Sei θ der von $|\psi\rangle$ und $|a^\perp\rangle$ eingeschlossene Winkel.
- V spiegelt $|\psi\rangle$ an $|a^\perp\rangle$.
- D.h. V dreht den Vektor $|\psi\rangle$ um den Winkel 2θ in Richtung $|a^\perp\rangle$.
- W spiegelt an $|\psi\rangle$, d.h. dreht um den Winkel 4θ in Richtung $|a\rangle$.
- D.h. eine Iteration dreht $|\psi\rangle$ insgesamt um 2θ in Richtung $|a\rangle$.
- Da WV eine Rotation ist, wird $|\psi\rangle$ in jeder Iteration um 2θ in Richtung $|a\rangle$ gedreht.

Anzahl der benötigten Grover-Iterationen

Lemma Benötigte Grover-Iterationen

Der Vektor $|\psi\rangle$ ist parallel zum gesuchten $|a\rangle$ nach ca. $\frac{\pi}{4}\sqrt{N}$ Grover-Iterationen.

Beweis:

- Zu Beginn gilt $\cos\gamma := \langle a|\psi\rangle = \frac{1}{\sqrt{2^n}} = \frac{1}{\sqrt{N}}$.
- D.h. der von $|\psi\rangle$ und $|a^\perp\rangle$ eingeschlossene Winkel $\theta = \frac{\pi}{2} - \gamma$ erfüllt
$$\sin\theta = \cos\gamma = \frac{1}{2^{\frac{n}{2}}}.$$
- Wegen $sin(x) \approx x$ für kleine x gilt $\theta \approx 2^{-\frac{n}{2}}$ für große n.
- Jede Grover-Iteration vergrößert den Winkel um 2θ.
- D.h. nach k Iterationen ist der Winkel $(2k+1)\theta$.
- Damit ist nach ca. $\frac{\pi}{4}2^{\frac{n}{2}}$ Grover-Iterationen $|\psi\rangle$ orthogonal zu $|a^\perp\rangle$.

Grover-Algorithmus

Algorithmus von Grover

EINGABE: $f : \mathbb{F}_2^n \to \mathbb{F}_2$ mit $f(a) = 1$ für genau ein $a \in \mathbb{F}_2^n$

1. Berechne $|z\rangle = H_{n+1}|0^n 1\rangle$.
2. Führe auf den ersten n Registern $\frac{\pi}{4} \cdot 2^{\frac{n}{2}}$-mal WV aus.
3. Messe die ersten n Register. Sei $|a\rangle$ das Ergebnis.
4. Falls $f(a) \neq 1$, gehe zurück zu Schritt 1.

AUSGABE: $a \in \mathbb{F}_2^n$

Verallgemeinerung von Grover

Definition Verallgemeinertes Problem der Datenbanksuche

Gegeben: $f : \mathbb{F}_2^n \to \mathbb{F}_2$ mit $f(a) = 1$ für $a_1, \ldots, a_m \in \mathbb{F}_2^n$
Gesucht: $a_i \in \mathbb{F}_2^n$ mit $i \in [m]$

Modifikation im Grover-Algorithmus:

- Analog gilt
$$V|x\rangle = (-1)^{f(x)}|x\rangle = \begin{cases} |x\rangle & \text{für } x \notin \{a_1, \ldots, a_m\} \\ -|x\rangle & \text{für } x \in \{a_1, \ldots, a_m\}. \end{cases}$$
- Wir definieren $|\bar{a}\rangle = \frac{1}{\sqrt{m}} \sum_{i=1}^{m} |a_i\rangle$.
- V und W rotieren ψ in der 2-dimensionalen Ebene aufgespannt durch die beiden Vektoren $|\bar{a}\rangle$ und $|\psi\rangle$.
- Der Winkel zwischen $|\bar{a}^{\perp}\rangle$ und $|\psi\rangle$ beträgt nun
$$\sin\theta = \langle \bar{a}^{\perp}|\psi\rangle = m \cdot \frac{1}{\sqrt{m2^n}} = \sqrt{\frac{m}{2^n}}.$$
- D.h. für $m \ll 2^n$ benötigt der Grover-Algorithmus etwa $\frac{\pi}{4} \cdot \frac{2^{\frac{n}{2}}}{\sqrt{m}}$ Iterationen.

Unbekanntes m

Frage: Können wir Grover auch anwenden, falls m unbekannt ist?

- Die Grover-Iteration ist eine periodische Funktion.
- Der ursprüngliche Zustand $|\psi\rangle$ wird nach ca. $\pi \frac{2^{\frac{n}{2}}}{\sqrt{m}}$ vielen Grover-Iterationen wieder angenommen.
- D.h. wir können die Quanten-Fouriertransformation verwenden, um m zu bestimmen.

Fehlerkorrektur

Notwendigkeit und Probleme der Quanten-Fehlerkorrektur

- Qbits müssen komplett isoliert von der Rechnerumgebung sein.
- Unmöglich, d.h. die Umgebung degeneriert Quantenzustände.
- Beobachtung von Fehlern durch Messung zerstört Zustand.
- Amplituden sind nicht diskret.
- Bitflips sind nicht die einzigen möglichen Fehler.
- Z.B. können einfache Phasenflips $|0\rangle + |1\rangle \mapsto |0\rangle - |1\rangle$ auftreten.
- Diese Fehler sind durch Messung nicht zu erkennen.

Klassisch:

- Auftretende Fehler sind ausschließlich Bitflips.
- Einfachste Lösung ist ein Repetitionscode der Länge 3.
- Wir codieren $0 \mapsto 000$ und $1 \mapsto 111$.
- Code erkennt zwei Fehler und korrigiert einen Fehler.

Repetition für Quanten

3-Qubit Repetition

Gegeben: Zustand $|z\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$
Gesucht: Zustand $|r\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$

Lösung:

- Verwende zwei Hilfsbits in Zustand $|0\rangle$, d.h. $|z00\rangle$.
- Kopiere die Basiszustände mittels CNOT.
- Sei C_{ij} ein CNOT auf Qubit j mit Kontrollbit i. Es gilt

$$|r\rangle = C_{12}C_{13}(\alpha_0|000\rangle + \alpha_1|100\rangle) = \alpha_0|000\rangle + \alpha_1|111\rangle.$$

Fehlermodell:

- Wir nehmen vereinfachend an, dass nur Bitflips auftreten.
- D.h. unsere fehlerbehafteten Zustände sind

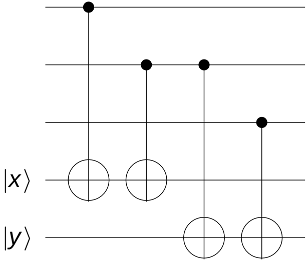
$$\begin{aligned} |e_1\rangle &= \alpha_0|100\rangle + \alpha_1|011\rangle \\ |e_2\rangle &= \alpha_0|010\rangle + \alpha_1|101\rangle \\ |e_3\rangle &= \alpha_0|001\rangle + \alpha_1|110\rangle. \end{aligned}$$

- Wir müssen Fehler beobachten, ohne zu messen.

Beobachten von Fehlern

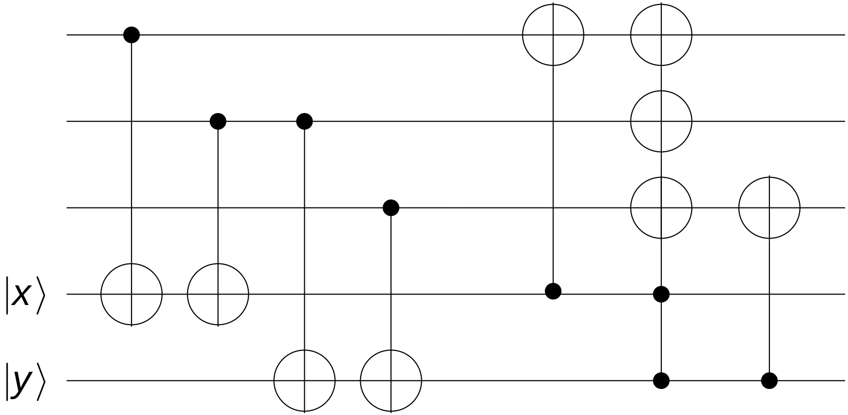
Beobachtung von Bitflips

- Wir verwenden zwei weitere Hilfsbits $|xy\rangle$, initialisiert mit $|0\rangle$.
- Das folgende Gatter erhält als Eingabe $|r\rangle = \alpha_0|000\rangle + \alpha_1|111\rangle$.
- Auftretende Bitflips werden mit CNOT-Gattern wie folgt kopiert.



- **Fall 1** fehlerfrei: $|xy\rangle = |00\rangle$.
- **Fall 2** Bitflip $|e_1\rangle$: $|xy\rangle = |10\rangle$.
- **Fall 3** Bitflip $|e_2\rangle$: $|xy\rangle = |11\rangle$.
- **Fall 4** Bitflip $|e_3\rangle$: $|xy\rangle = |01\rangle$.
- D.h. durch *Messung der Hilfsbits* $|xy\rangle$ erkennen wir einen Fehler.
- Wir nutzen nur Relationen zwischen den ursprünglichen Bits.
- Der ursprüngliche Zustand bleibt in seiner Superposition erhalten.

Korrektur der Fehler



Korrigieren allgemeiner Fehler

Fakt 5-Qubit Code

Es existiert ein 5-Qubit Code zum Korrigieren eines generellen 1-Qubit Fehlers.

- Code korrigiert nicht nur Bit-Flips, sondern auch Phasenfehler.

Bit Commitments

Bit Commitment informal

1. **Commitment-Phase:**
   - Alice platziert ein Bit $b \in \{0, 1\}$ in einem Safe.
   - Alice sendet den Safe an Bob.
   - Bob kann den Safe nicht einsehen, lernt also nichts über *b*. **(Concealing Eigenschaft)**
2. **Revealing-Phase:**
   - Alice öffnet den Safe und zeigt Bob das Bit *b*.
   - Alice kann ihr Bit dabei nicht ändern. **(Binding Eigenschaft)**

Realisierung mittels Qubits

Protokoll Quanten Bit Commitment

Sicherheitsparameter: n

Commitment-Phase:

- Alice wählt $\mathbf{x} \in_R \{0,1\}^n$.
- **Fall 1** $b = 0$: Alice sendet $|\mathbf{y}\rangle = |\mathbf{x}\rangle$ an Bob.
- **Fall 2** $b = 1$: Alice sendet $|\mathbf{y}\rangle = H_n|\mathbf{x}\rangle$ an Bob.

Revealing-Phase:

- Alice sendet b und $\mathbf{x}$ an Bob.
- Bob misst $H_n^b|\mathbf{y}\rangle$ in der Standardbasis und vergleicht mit $|\mathbf{x}\rangle$.

Anmerkungen:

- **Conceiling:** Falls Bob in der Standard- oder der Hadamardbasis misst, erhält er 0 bzw. 1 jeweils mit Ws $\frac{1}{2}$.
- **Binding:** Falls $b' \neq b$, gilt $\mathbf{x} = \mathbf{y}$ nur mit Ws 2^{-n}.

Betrügerische Alice

Protokoll Betrügerische Alice

Sicherheitsparameter n

Commitment-Phase:

- Alice wählt n EPR-Paare $|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
- Alice sendet jeweils das zweite Bit an Bob.

Revealing-Phase:

- **Fall 1:** $b = 0$: Alice misst ihr erstes Bit aller n Paare $|e\rangle$.
- **Fall 2:** $b = 1$: Alice berechnet $H|e\rangle$ und misst ihre n Qubits.
- Sei $\mathbf{x}$ das Ergebnis der Messung. Sende $b, |\mathbf{x}\rangle$ an Bob.

Anmerkung:

- Für $b = 0$ misst Bob aufgrund der Verschränkung dasselbe.
- Für $b = 1$ gilt $(H \otimes H)|e\rangle = |e\rangle$.
- D.h. auch in diesem Fall messen Alice und Bob dasselbe.

Sicheres Quanten Bit Commitment

Offenes Problem Quanten Bit Commitment

Existiert ein sicheres Quanten Bit Commitment Protokoll?

Anmerkung:

- Mayers 1996: Generische Attacke gegen Quanten BC Protokolle.
- Vermutung: Sichere Quanten-BC Protokolle sind nicht ohne weitere Annahmen konstruierbar.