Quantenalgorithmen

Alexander May

28. Oktober 2013

Literatur

Mika Hirvensalo Quantum Computing

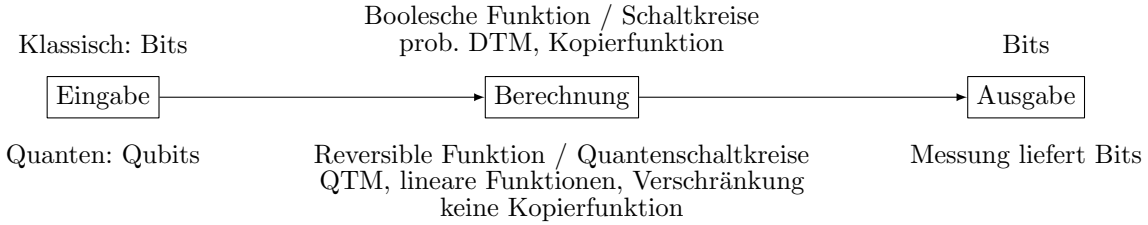
Chuang/Nielsen Quantum Computation and Quantum Information

D. Aharanov Quantum Computation

1 Warum Quantenalgorithmen

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

2 Berechnungen



Probleme bei Implementierung:

- Dekohärenz, Skalierbarkeit
- Quantenfehlerkorrektur

Klassische, probalistische Systeme: Seien $x_1, \ldots, x_n$ Basiszustände

Wahrscheinlichkeitsverteilung eines Zustandsraum :

$p_1[x_1] + p_2[x_2] + \cdots + p_n[x_n]$ mit $0 \leq p_i \leq 1$, $\sum_{i=1}^{n} p_i = 1$

Zustandsübergang :

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

Allgemein :

$p_1[x_1] + p_2[x_2] + \cdots + p_n[x_n] \mapsto p_1(p_{11}[x_1] + \cdots + p_{n1}[x_n] = (p_1p_{11} + p_2p_{21} + \cdots + p_np_{1n})[x_1] + \cdots + (p_np_{n1} + \cdots + p_np_{nn})[x_n]$

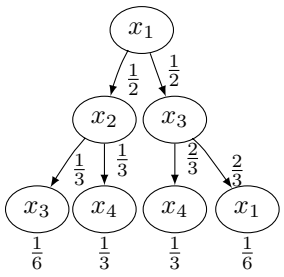
Markov-Matrix :

$$\begin{pmatrix} p_1' \\ \vdots \\ p_n' \end{pmatrix} = \begin{pmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & \ddots & \vdots \\ p_{n1} & \cdots & p_{nn} \end{pmatrix} \cdot \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$$

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

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

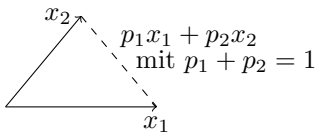
2.

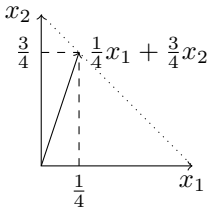


x_1, x_3 : Ws. $\frac{1}{6}$
x_4 : Ws. . $\frac{2}{3}$

Strategie: Maximiere Ws. des gewünschten Endzustands

Vektorraum Interpretation:
- $x_1, x_2, \ldots, x_4$ Basisvektoren eines n-dim. Vektorraums
- Wahrscheinlichkeitsverteilen entsprechen Linearkombinationen



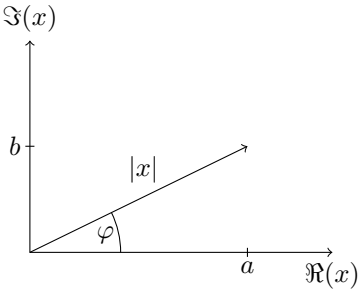


3 1-Qbit Systeme

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

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

Komplexe Zahl :
$|x\rangle \in \mathbb{C}^n \Leftrightarrow |x\rangle = (x_1, \ldots, x_n)^T, x_i \in \mathbb{C}$ "ket"-Notation.
$x = a + ib,\ a, b \in \mathbb{R}, i = \sqrt{-1}$ 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 $|x\rangle = (x_1, \ldots, x_n), \langle x| = (x_1^*, \ldots, x_n^*)$ und $|x\rangle, \langle y|$ orthogonal $\Leftrightarrow \langle x|y\rangle = 0$

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

1. $\langle x_i|x_j\rangle = 0\ \forall i, j$ mit $i \neq j$
2. $||x_i\rangle| = 1\ \forall x_i$

Beispiel: Orthonormale Basen für $\mathbb{C}^2$

- $|0\rangle = (1, 0)^T, |1\rangle = (0, 1)^T$
- $(e^{i\varphi}, 0), (0, e^{i\varphi})$
- $\sqrt{\frac{1}{5}}(1, 2), \sqrt{\frac{1}{5}}(2, -1)$

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

- $|0\rangle = (1, 0, 0, 0)^T, |1\rangle = (0, 1, 0, 0)^T, |2\rangle = (0, 0, 1, 0)^T, |3\rangle = (0, 0, 0, 1)^T$
- $\frac{1}{5}(1, 2, 2, 4)^T, \frac{1}{5}(2, -1, 4, -2)^T, \frac{1}{5}(2, 4, -1, -2)^T, \frac{1}{5}(4, -2, -2, 1)^T$

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

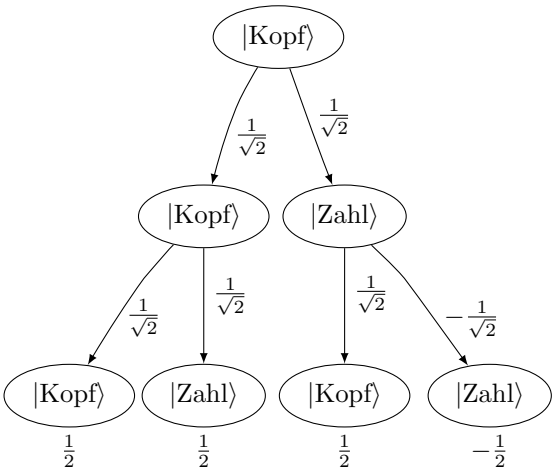
Übung: $|\alpha_0|0\rangle + \alpha_1|1\rangle| = 1 \Leftrightarrow |\alpha_0|^2 + |\alpha_1|^2 = 1$

Allgemein: Seien $|x_1\rangle, \ldots, |x_n\rangle$ eine orthonormale Basis des $\mathbb{C}^n$ (auch H_n für Hilbertraum).
Zustand eines Quantensystems: $\alpha_1|x_1\rangle + \alpha_2|x_2\rangle + \cdots + \alpha_n|x_n\rangle$ mit $|\alpha_1|^2 + \cdots + |\alpha_n|^2 = 1$
Messung: x_i mit $WS|\alpha_i|^2$

Bezeichnung:
- Basisvektoren $|x_i\rangle$ werden Basiszustände genannt.
- α_i heißen Amplituden
- Allg. Zustand ist Superposition der Basiszustände (Überlagerung)
- $\psi(x_i) = \alpha_i$ heist Wellenfunktion.
- $|x >= e^{i\varphi}|y > \Leftrightarrow$ Zustände $|x\rangle$ und $|y\rangle$ heißen äquivalent

Vergleich : Wahrscheinlichkeitsverteilung $P_1[x_1] + \cdots + p_n[x_n]$ $\sum i = 1^n p_i = 1$
Superposition $\alpha_1|x_1\rangle + \cdots + \alpha_n|x_n\rangle$ $\sum_{i=1}^{n} |\alpha_i|^2 = 1$, d.h. $|\alpha_i|^2 WS-$Verteilung. Trotzdem fundamental verschieden!

Beispiel: 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 von $|Kopf\rangle$ summieren sich zu $1 \rightarrow$ positive Interferenz
- Amplituden von $|Zahl\rangle$ summieren sich zu $0 \rightarrow$ negative Interferenz

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

Man beachte: Superposition $\alpha_1|x_1\rangle + \cdots + \alpha_n|x_n\rangle$ liefert x_i mit $Ws|\alpha_i|^2$
Wechsel zu anderer orthonormaler Basis $|x'_1\rangle, \ldots, |x'_n\rangle$ mit $|x'_1\rangle = \alpha_1|x_1\rangle + \cdots + \alpha_n|x_n\rangle$ liefert x'_1 mit $Ws1$.

3.1 Zustandsübergänge

Da Quantenzustände stets Einheitsvektoren sind: längenerhaltene Abbildung
Aus den Gesetzen der Quantenphysik: lineare Abbildung, reversibel

Definition (unitäre Abb.): eine lineare Abb. $U : \mathbb{C}^n \rightarrow \mathbb{C}^n$ heißt unitär, falls für alle $|x\rangle \in \mathbb{C}^n$ gilt: $||x\rangle| = \sqrt{\langle x|x\rangle} = \sqrt{\langle U||x\rangle|U|x\rangle >} = |U||x\rangle|$
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 $|x\rangle \in \mathbb{C}^m : |U|x\rangle| = ||x\rangle|$. D.h. U beschreibt eine unitäre Abbildung.

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

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

Beispiel: Hadamard-Walsh-Matrix $W_2 = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$

Übung: $W_2(W_2^*)^T = I$

Anmerkung: W_2 Beschreibt "Quanten-Münzwurf"

3.2 Entwicklung eines Quantenbits

Sei $|0\rangle = (1,0)^T, |1\rangle = (0,1)^T, U = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$

$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = a \begin{pmatrix} 1 \\ 0 \end{pmatrix} + b \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, d.h. $|0\rangle \overset{U}{\longmapsto} a|0\rangle + b|1\rangle$

$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix} = c \begin{pmatrix} 1 \\ 0 \end{pmatrix} + d \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, d.h. $|1\rangle \overset{U}{\longmapsto} c|0\rangle + d|1\rangle$

3.3 Beispiele unitärer Abbildungen

Beispiel 1 (Quanten-Not): $M_\neg = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

$M_\neg$ ist unitär, $(M_\neg^*)^T = M_\neg, M_\neg^2 = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

$\begin{matrix} (1,0) \mapsto (0,1) \\ (0,1) \mapsto (1,0) \end{matrix}$ d.h. $\begin{matrix} |0\rangle \mapsto |1\rangle \\ |1\rangle \mapsto |0\rangle \end{matrix}$

Beispiel 2 (Wurzel des Not): $\sqrt{M_\neg} = \begin{pmatrix} \frac{1+i}{2} & \frac{1-i}{2} \\ \frac{1-i}{2} & \frac{1+i}{2} \end{pmatrix}$

$$\begin{aligned} |0\rangle \overset{\sqrt{M_\neg}}{\longmapsto} \frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle \overset{\sqrt{M_\neg}}{\longmapsto} & \frac{1+i}{2}(\frac{1+i}{2}|0\rangle + \frac{1-i}{2}|1\rangle) + \frac{1-i}{2}(\frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle) \\ &= ((\frac{1+i}{2})^2 + (\frac{1-i}{2})^2)|0\rangle + 2\frac{1-i^2}{4}|1\rangle \\ &= \frac{1+2i+i^2+1-2i+i^2}{4}|0\rangle + \frac{4}{4}|1\rangle = |1\rangle \end{aligned}$$

Äqivalent $|1\rangle \overset{\sqrt{M_\neg}}{\longmapsto} \frac{1-i}{2}|0\rangle + \frac{1+i}{2}|1\rangle \overset{\sqrt{M_\neg}}{\longmapsto} |0\rangle$ wegen $\left|\frac{1+i}{2}\right|^2 = \left|\frac{1-i}{2}\right|^2 = \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$

Übung: $\sqrt{M_\neg}$ ist unitär, $(\sqrt{M_\neg})^2 = M_\neg$.

Beispiel 3 (Haddamard-Walsh Matrix $W_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$

$$\begin{aligned} |0\rangle \overset{W_2}{\longmapsto} \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \overset{W_2}{\longmapsto} & \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) + \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \\ &= \left(\frac{1}{2} + \frac{1}{2}\right)|0\rangle + \left(\frac{1}{2} - \frac{1}{2}\right)|1\rangle = |0\rangle \end{aligned}$$

Beispiel 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: $F_\pi = F$

Definition (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-Qbit-Systems ist ein Einheitsvektor im $\mathbb{C}^4$

4 Exkurs über Tensorprodukte

Definition (Tensorprodukt) Seien $|x\rangle = (x_1, \ldots, x_n) \in \mathbb{C}^n, |y\rangle = (y_1, \ldots, y_m) \in \mathbb{C}^m$. Das Tensorprodukt von $|x\rangle$ und $|y\rangle$ ist definiert als:
$|x\rangle \otimes |y\rangle = (x_1y_1, x_1y_2, \ldots, x_1y_m, x_2y_1, \ldots, x_2y_m, \ldots, x_ny_1, \ldots, x_ny_m) \in \mathbb{C}^{nm}$

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

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

4.1 Rechenregeln für das Tensorprodukt

- Distributivität:
  $\forall\, |x\rangle \in \mathbb{C}^n, |y\rangle, |z\rangle \in \mathbb{C}^m, |x\rangle \otimes (|y\rangle + |z\rangle) = |x\rangle \otimes |y\rangle + |x\rangle \otimes |z\rangle$
  $\forall\, |x\rangle, |y\rangle \in \mathbb{C}^n, |z\rangle \in \mathbb{C}^m, (|x\rangle + |y\rangle) \otimes |z\rangle = |x\rangle \otimes |z\rangle + |y\rangle \otimes |z\rangle$
- Skalare Multiplikation:
  $\forall\, |x\rangle \in \mathbb{C}^n, |y\rangle, \in \mathbb{C}^m, c \in \mathbb{C} : (c|x\rangle) \otimes |y\rangle = c(|x\rangle \otimes |y\rangle) = |x\rangle \otimes (c|y>)$
- 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:
  $\forall\, |x\rangle \in \mathbb{C}^n, |y\rangle \in \mathbb{C}^m : ||x\rangle \otimes |y\rangle|^2 = ||x\rangle|^2 \cdot ||y\rangle|^2$

Lemma: Sei $|x_1\rangle, \ldots, |x_n\rangle \in \mathbb{C}^n$ eine orthonormale Basis des $\mathbb{C}^n$ und $|y_1\rangle, \ldots, |y_m\rangle \in \mathbb{C}^m$ eine orthonormale Basis des $\mathbb{C}^m$. Dann ist
$|x_1\rangle \otimes |y_1\rangle, |x_1\rangle \otimes |y_2\rangle, \ldots, |x_1\rangle \otimes |y_m\rangle, |x_2\rangle \otimes |y_1\rangle, \ldots, |x_n\rangle \otimes |y_m\rangle \in \mathbb{C}^{mn}$ eine orthonormale Basis des $\mathbb{C}^{nm}$

Beweis: Für $|x_i\rangle, |y_j\rangle$ gilt:
$||x_i\rangle \otimes |y_j\rangle| = ||x_i\rangle| \cdot ||y_j\rangle| = 1 \cdot 1 = 1$
Weiterhin sind die Vektoren paarweise orthogonal:
$\langle |x_i\rangle \otimes |y_j\rangle || x_k\rangle \otimes |y_l\rangle\rangle = \langle x_i||x_k\rangle \cdot \langle y_j||y_l\rangle = 0\ \forall\, i \neq k$ oder $j \neq l$.

Beispiel:

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

$$|0\rangle \otimes |0\rangle = (1,0,0,0)^T \qquad |x\rangle \otimes |x\rangle = \frac{1}{2}(1,-1,-1,1)^T$$

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

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

$$|1\rangle \otimes |1\rangle = (0,0,0,1)^T \qquad |y\rangle \otimes |y\rangle = \frac{1}{2}(1,1,1,1)^T$$

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.

5 2-Quantum Register

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

5.1 Zustand eines 2-Qubit Systems

Ein Zustand eines 2-Qubit Systems ist ein Einheitsvektor
$|v\rangle = c_0|00\rangle + c_1|10\rangle + c_2|10\rangle + c_3|11\rangle \in \mathbb{C}^4$ 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 $Ws.|c_0|^2$
- Basiszustand $|01\rangle$ mit $Ws.|c_1|^2$
- Basiszustand $|10\rangle$ mit $Ws.|c_2|^2$
- Basiszustand $|11\rangle$ mit $Ws.|c_3|^2$

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

Messung eines einzelnen Qubits eines 2-Qubit Systems: Messung des 1. Qubits von $|1\rangle$ 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:

- $\frac{c_0|00\rangle + c_1|01\rangle}{\sqrt{|c_0|^2+|c_1|^2}}$ falls $|0\rangle$ im ersten Qubit gemessen wurde
- $\frac{c_2|10\rangle + c_3|11\rangle}{\sqrt{|c_2|^2+|c_3|^2}}$ falls $|1\rangle$ im ersten 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 $\mathbb{C}^4$

5.2 Separabel/Verschränkt

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

Beispiel (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 $-\frac{1}{\sqrt{2}}$).

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

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

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

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

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

$$\Rightarrow \text{Gleichungssystem} \left| \begin{array}{c|l} \alpha_0\beta_0 = \frac{1}{\sqrt{2}} & \Rightarrow \alpha_0 \neq 0 \wedge \beta_0 \neq 0 \\ \alpha_0\beta_1 = 0 & \Rightarrow \alpha_1 = 0 \vee \beta_0 = 0 \\ \alpha_1\beta_0 = 0 & \Rightarrow \alpha_1 = 0 \vee \beta_0 = 0 \\ \alpha_1\beta_1 = \frac{1}{\sqrt{2}} & \Rightarrow \alpha_1 \neq 0 \wedge \beta_1 \neq 0 \end{array} \right. \lightning \text{ nicht erfüllbar.}$$

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 im 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 Abbildung $U \in \mathbb{C}^{4\times4}$

Beispiel (CNOT): $M_{\texttt{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \begin{array}{lll} |00\rangle & \mapsto & |00\rangle \\ |01\rangle & \mapsto & |01\rangle \\ |10\rangle & \mapsto & |11\rangle \\ |11\rangle & \mapsto & |10\rangle \end{array}$

Controlled-Not: Das zweite Bit wird genau dann invertiert, wenn das 1. Bit (Kontrollbit) gesetzt ist. Man überprüfe, dass $M_{\texttt{CNOT}} \cdot (M^*_{\texttt{CNOT}})^T = I_2$

Definition: $U \in \mathbb{C}^{m\times m}$ heißt Permutationsmatrix $\Leftrightarrow U$ in jeder Zeile und Spalte genau eine Eins und sonst Nullen erhält.

Beispiel: $M_{\texttt{CNOT}}$ ist Permutationsmatrix.

Übung: Permutationsmatrizen sind unitär.

Bez.: Eine unitäre Abbildung, die nur auf einen Teil der Qubits agiert, heißt <u>lokal</u> unitär.
Sei $|z\rangle = (c_0|00\rangle + c_2|10\rangle + c_3|11\rangle)$ 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 eine lokal unitäre Abb. auf dem 2. Qubit

5.3 Tensorprodukt bzw. Kroneker-Produkt von Matrizen

Definition: Seien

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mm} \end{pmatrix} \in \mathbb{C}^{m\times m}, B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \in \mathbb{C}^{n\times n}$$

Dann ist das Tensorprodukt von A und B definiert als:

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1m}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mm}B \end{pmatrix} \in \mathbb{C}^{mn\times mn}$$

Beispiel:

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

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: $(A \otimes B)|z\rangle$

Beweis: 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: $|z\rangle \overset{A\otimes B}{\longmapsto} A|x\rangle \otimes B|y\rangle$.
D.h. lokal unitäre Operationen allein können keine Verschränkung erzeugen.

Beispiel 1: Anwendung von W_2 auf das 1. Qubit: $W_2 \otimes I_2$

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

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

Beispiel 2: $W_4 = W_2 \otimes W_2$

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

Zustandsübergang für Basiszustand $|x_0x_1\rangle, x_0, x_1 \in \{0,1\}$:
$W_4|x_0x_1\rangle = \frac{1}{2}(|00\rangle + (-1)^{x_1}|01\rangle + (-1)^{x_0}|10\rangle + (-1)^{x_0+x_1}|11\rangle)$
$= \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_0}|1\rangle)}_{W_2|x_0\rangle} \otimes \underbrace{\frac{1}{\sqrt{2}}(|0\rangle + (-1)^{x_1}|1\rangle)}_{W_2|x_1\rangle}$

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

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

Beweis: $M_{\texttt{CNOT}}$ ist unitär.

Annahme: $M_{\texttt{CNOT}}$ sei Tensorprodukt zweier unitärer Abbildungen, d.h. $M_{\texttt{CNOT}} = A \otimes B$.
Beachte: $|00\rangle \overset{W_2\otimes I_2}{\longmapsto} \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \overset{A\otimes B}{\longmapsto} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$.
D.h. wir erhalten ein verschränktes EPR-Paar durch lokal unitäre Abbildungen auf dem separablen Zustand $|00\rangle$. $\lightning$ 5.3

5.4 No-Cloning Theorem

Definition (Quanten-Kopiermaschine): Sei $|x\rangle \in \mathbb{C}^2$ ein Qubit. Eine Quanten-Kopiermaschine ist eine unitäre Abbildung U mit: $U(|z\rangle \otimes |x\rangle) = |z\rangle \otimes |z\rangle$ für alle Qubits $|z\rangle \in \mathbb{C}^2$

Satz (No-Cloning Theorem): Es gibt keine Quantenkopiermaschine.

Beweis: Annahme: 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 seperabel).
Aufgrund der Linearität von U gilt aber ebenfalls:
$U(W_2|0\rangle \otimes |1\rangle) = U(\frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle) = \frac{1}{\sqrt{2}}(U|01\rangle + U|11\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ (ist verschränkt, (EPR-Paar)). $\lightning$

Man beachte: $M_{\texttt{CNOT}} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ ist Kopiermaschine für Basiszustände $|0\rangle, |1\rangle$,
denn $|00\rangle \mapsto |00\rangle, |10\rangle \mapsto |11\rangle$.
Allerdings gilt $(\alpha_0|0\rangle + \alpha_1|1\rangle)|0\rangle \overset{M_{\texttt{CNOT}}}{\longmapsto} \alpha_0|00\rangle + \alpha_1|11\rangle \neq (\alpha_0|0\rangle + \alpha_1|1\rangle)(\alpha_0|0\rangle + \alpha_1|1\rangle)$ für $\alpha_0, \alpha_1 \neq 0$.

6 n-Qubit Zustandssysteme (Register)

Sei $|0\rangle$, $|1\rangle$ eine orthonormale Basis des $\mathbb{C}^2$.
Gemäs Basis-Lemma (4.1): $|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle$ 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 $\mathbb{C}^{2^n}$.

Definition: Ein n-Qubit System ist ein Einheitsvektor im $\mathbb{C}^{2^n}$ der Form
$|z\rangle = \sum_{x \in \{0,1\}^n} c_x |x\rangle$ mit $c_x \in \mathbb{C}$, $\sum_{x \in \{0,1\}^n} |c_x|^2 = 1$.

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

Zustandsübergang:
- n-Qubit Systeme entwickelt sich gemäß unitärer Abb. $U : \mathbb{C}^{2^n} \to \mathbb{C}^{2^n}$
- Lokal unitäre Abbildungen operieren auf einzelnen Qubits des Systems.

Beobachtung:
- n Qubits werden durch 2^n Amplituden beschrieben.
- Unitäre Matrizen $U \in \mathbb{C}^{2^n \otimes 2^n}$ haben Beschränkungsgröße 2^{2n}.

D.h. die Beschreibungsgröße ist exponentiell in der physikalischen Größe n.
Feyman: "Quantenrechner sollten nicht effizient auf klassischen Rechnern simulierbar sein."

Definition (Separabilität): Ein n-Qubit $|z\rangle \in \mathbb{C}^{2^n}$ heißt separabel gdw. $|z\rangle = |x_1\rangle \otimes |x_2\rangle \otimes \dots \otimes |x_n\rangle$ für $|x_i\rangle \in \mathbb{C}^2$.
Nicht separable Zustände heißen verschränkt.

Beispiel: $|z\rangle = \frac{1}{\sqrt{3}}(|000\rangle - |001\rangle - |111\rangle)$ ist verschränkt.
Messung des 1. Qubits: $|0\rangle$ mit $Ws\frac{2}{3}$, $|0\rangle$ 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 $\frac{\frac{1}{\sqrt{3}}|111\rangle}{\sqrt{\frac{1}{3}}} = |111\rangle$.

7 Quanten-Protokolle

7.1 Quantenteleportation

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 Alices, 2. Bit gehört Bob.

Ziel: 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 Rekonstrutkion von Quantenbits aus klassischer Information, so existiert ein Quanten-Kopierer. $\lightning$ (No-Cloning-Theorem (5.4))

Lösung: Nutze Verschränkung zur Übertragung.
Zusammengesetzter Zustand von $|z\rangle$ und $|e\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$:

$$\begin{aligned} |z\rangle \otimes |e\rangle &= (c_0|0\rangle + c_1|1\rangle) \otimes \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ &= \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|100\rangle + c_1|111\rangle) \end{aligned}$$

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

Protokoll für die Teleportation von $|z\rangle$:

1. Alice wendet CNOT auf das 2. Qubit mit dem 1. Qubit als Kontrollbit an:
   $|ze\rangle \overset{\texttt{CNOT}}{\longmapsto} \frac{1}{\sqrt{2}}(c_0|000\rangle + c_0|011\rangle + c_1|110\rangle + c_1|101\rangle)$
2. Alice wendet nun auf das 1. Qubit die Hadamard-Walsh Transformation W_2 an:
   $\frac{1}{\sqrt{2}}(\frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|00\rangle + \frac{c_0}{\sqrt{2}}(|0\rangle + |1\rangle)|11\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|10\rangle + \frac{c_1}{\sqrt{2}}(|0\rangle - |1\rangle)|01\rangle)$
   $= \frac{1}{2}(c_0|000\rangle + c_0|100\rangle + c_0|011\rangle + c_0|111\rangle + c_1|010\rangle - c_1|110\rangle + c_1|001\rangle - c_1|101\rangle)$
   $= \frac{1}{2}(|00\rangle(c_0|0\rangle + c_1|1\rangle) + |01\rangle(c_0|1\rangle + c_1|0\rangle) + |10\rangle(c_0|0\rangle - c_1|1\rangle) + |11\rangle(c_0|1\rangle - c_1|0\rangle))$
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 an Bob.
4. Abhängig von Messergebnis führt Bob folgende Operation aus:
   Für $|00\rangle$: Bobs Qubit ist bereits im gewünschten Zustand.
   $|01\rangle$ NOT Operation $c_0|1\rangle + c_1|0\rangle \overset{\texttt{NOT}}{\longmapsto} c_0|0\rangle + c_1|1\rangle$
   $|10\rangle$ Flip Operation: $c_0|0\rangle - c_1|1\rangle \overset{\texttt{Flip}}{\longmapsto} c_0|0\rangle + c_1|1\rangle$
   $|11\rangle$ Flip $\circ$ NOT $c_0|1\rangle - c_1|0\rangle \overset{\texttt{Flip} \circ \texttt{NOT}}{\longmapsto} c_0|0\rangle + c_1|1\rangle$

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

7.2 Superdense Coding (Bennet, Wiesner 1992)

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

Ziel: übertrage zwei klassische Bits b_0, b_1 mit Hilfe eines einzelnen Qubits.

Protokoll Superdense Codding:

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.

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

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \overset{U}{\longmapsto} \frac{1}{2}(|00\rangle + |10\rangle + |00\rangle - |10\rangle) = |00\rangle$ Interpretation: $(b_0, b_1) = (0, 0)$
$\frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \overset{U}{\longmapsto} \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle + |10\rangle) = |01\rangle$ Interpretation: $(b_0, b_1) = (0, 1)$
$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \overset{U}{\longmapsto} \frac{1}{2}(|00\rangle + |10\rangle - |00\rangle + |10\rangle) = |10\rangle$ Interpretation: $(b_0, b_1) = (1, 0)$
$\frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \overset{U}{\longmapsto} \frac{1}{2}(-|01\rangle + |11\rangle + |01\rangle + |11\rangle) = |11\rangle$ Interpretation: $(b_0, b_1) = (1, 1)$

7.3 Quanten Schlüsselaustausch

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

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
- Alice und Bob besitzen authentisierten klassischen Kanal
- Kanäle werden belauscht und manipuliert durch Eve.

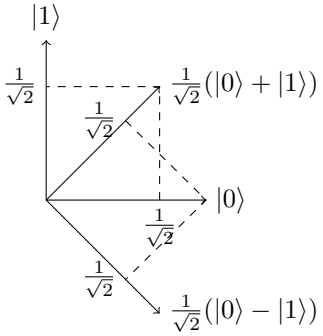
Ziel: Austausch von n klassischen Bits, so dass

- Eve durch Belauschen keine Information erhält
- Manipulation von Eve entdeckt wird

Einfache Lösung: falls Alice und Bob n EPR-Paare $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$teilen:
Messen in derselben Basis $|0\rangle$, $|1\rangle$ liefert n identische Zufallsbits.

Definition(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 liefert $\frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ jeweils mit $Ws.\frac{1}{2}$.



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

Kodierungstabelle:

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

, 0 = Z-Basis, 1 = X-Basis

7.3.1 BB84-Protokoll (Bennet-Brassard)

1. Alice wählt zufällige $4n$-Bit Strings $a = a_1 \dots a_{4n}, a = b_1 \dots b_{4n} \in \{0,1\}^{4n}$.
   Alice sendet 4n Qubits $|z_{a_i b_i}\rangle, i = 1 \dots 4n$ an Bob

2. Bob wählt einen zufälligen Bitstring $b' = b'_1 \dots b'_{4n} \in \{0,1\}$.
   Falls $b_i = 0$ Messe $|z_{a_i b_i}\rangle$ zur Z-Basis. Falls $|0\rangle$, setze $a'_i = 0$, sonst $a'_i = 1$
   Falls $b_i = 1$ 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.

Korrektheit: Falls keine Manipulation der Qubits vorliegt, gilt $Ws(a_i = a'_i | b_i = b'_i) = 1$, denn Bob misst Basiszustand in der korrekt gewählten Basis.

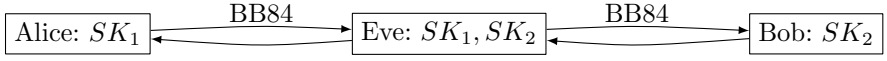
Sicherheit: Eve erhält nur dann das i-te Bit, falls sie $|z_{a_i b_i}\rangle$ misst.

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 $|z_{\tilde{a_i}\hat{b_i}}\rangle$ an Bob, wobei $\tilde{a_i} \in_R \{0,1\}$. Misst Bob in Basis b_i, so erhält er a'_i mit $Ws(a'_i = a_i) = \frac{1}{2}$.
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, das Eves Erfolgswahrscheinlichkeit, 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 Man-in-the-Middle Angriff durchführen.



7.3.2 BB92-Protokoll (Bennet)

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 Ergebnis $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, setze $b = 0$, sonst setze $b = 1$.

   Bob sendet 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

$$\text{Ws.}\,(b=1) = \text{Ws.}\,(b=1|a=a')\cdot\text{Ws.}\,(a=a') + \text{Ws.}\,(b=1|a\neq a')\cdot\text{Ws.}\,(a\neq a') = 0\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}.$$

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 $a = 1 - a'$.

Satz: Ws. $(a = 1 - a'|b = 1) = 1$

Beweis: Es gilt Ws. $(a = 1 - a'|b = 1 \cdot$ Ws. $(b = 1) =$ Ws. $(b = 1|a = 1 - a') \cdot$ Ws. $(a = 1 - a')$
$\Rightarrow$ Ws. $(a = 1 - a'|b = 1) = \frac{\text{Ws.}\,(b=1|a=1-a')\cdot\text{Ws.}\,(a=1-a')}{\text{Ws.}\,(b=1)} = \frac{\frac{1}{2}\cdot\frac{1}{2}}{\frac{1}{4}} = 1$
D.h. falls $b = 1$, so müssen a und a' verschiedene Bits sein. Damit erhalten Alice und Bob dasselbe Bit $a = 1 - a'$

8 Boolesche Schaltkreise, Schaltkreiskomplexitäten

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

Beispiel: Und $\wedge : \mathbb{F}_2^2 \to \mathbb{F}_2, (x_1, x_2) \overset{\wedge}{\longmapsto} x_1 \wedge x_2 = x_1x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$,
$(x_1, \ldots, x_n) \mapsto (((x_1 \wedge x_2) \wedge x_3) \ldots x_n)$

Oder $\vee : \mathbb{F}_2^2 \to \mathbb{F}_2, (x_1, x_2) \overset{\vee}{\longmapsto} x_1 \vee x_2 = x_1 + x_2 + x_1x_2$ bzw. $\mathbb{F}_2^n \to \mathbb{F}_2$,
$(x1, \ldots, x_n) \mapsto (((x_1 \vee x_2) \vee x_3) \ldots x_n)$

Nicht $\neg : \mathbb{F}_2 \to FZ, x \overset{\neg}{\longmapsto} 1 - x$ Schreibweise auch: $\overline{x}$

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

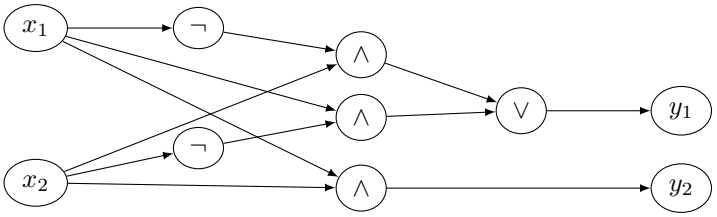
Entscheiden von Sprachen $\mathtt{L} : X_{\mathtt{L}} : \mathbb{F}_2^n \to \mathbb{F}_2, X_{\mathtt{L}}(\omega) = \begin{cases} 1 & \text{falls } \omega \in \mathtt{L} \\ 0 & \text{sonst} \end{cases}$

Definition (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 azyklischer, 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).

Beispiel: 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	1	1



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

$y_1 = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})$
$y_2 = x_1 \wedge x_2$

8.1 Universelle Mengen

Definition (universell): Sei S eine Menge von Booleschen Funktionen, 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 Funktion $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ mittels S realisiert werden.

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

Beweis: Wir definieren die Funktion $M_a, a = (a_1, \ldots, a_n) \in \mathbb{F}_2^n$. Vermöge $M_a(x_1, \ldots, x_n) = \varphi_1(x_1) \wedge \varphi_2(x_2) \wedge \cdots \wedge \varphi_n(x_n)$ für $\varphi_i(x_i) = \begin{cases} x_i & \text{für } a_i = 1 \\ \overline{x_i} & \text{für } a_i = 0 \end{cases}$

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

Sei $\mathtt{T} = \{a \in \mathbb{F}_2^n | f(a) = 1\}$. Dann gilt $f = \bigvee_{a \in \mathtt{T}} M_a(x_1, \ldots, x_n) = \neg(\bigwedge_{a \in \mathtt{T}} \neg M_a(x_1, \ldots, x_n))$.

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

Beispiel (obiger Addierer): Für Ausgabebit y_1 gilt:
$\mathtt{T} = \{(0,1),(1,0)\} \Rightarrow y_1 = \bigvee_{a \in \mathtt{T}} M_a(x_1 x_2) = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2}) = \neg(\neg((\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})))$
$= \neg(\overline{(\overline{x_1} \wedge x_2)} \wedge \overline{(x_1 \wedge \overline{x_2})})$

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.

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

Satz: $S = \{\text{nand}, \mathtt{c}\}$ 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)
$\wedge$: $\text{nand}(\text{nand}(x_1, x_2), \text{nand}(x_1, x_2)) = \text{nand}(\overline{x_1 \wedge x_2}, \overline{x_1 \wedge x_2}) = x_1 \wedge x_2$.

8.2 Uniforme / nicht-Uniforme Schaltkreisfamilien

Bezeichnung Wir bezeichnen mit C_n Schaltkreise mit n Eingabeknoten.
Wir nennen $C = \{C_n\}_{n \in \mathbb{N}}$ eine Schaltkreisfamilie.

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

Beobachtung Nach 8.1 können alle Funktionen $\mathbb{F}_2^n \to \mathbb{F}_2$ 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 Touringmaschinen-Modell nicht entscheidbare Halteproblem.
Problem: Konstruktion von C_n erfordert die Kenntnis der Funktionswerte der f_n.

Definition (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 Funktion $f_n, n \in \mathbb{N}$ hat uniforme Schaltkreiskomplexität $\mathcal{O}(g(n))$, falls es eine uniforme Schaltkreisfamilie $\{C_n\}_{n \in \mathbb{N}}$ gibt, die f_n berechnet.

8.3 Die Klasse $\mathcal{P}$

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

Definition ($\mathcal{P}$): Die Klasse $\mathcal{P}$ besteht aus allen booleschen Funktionen $f_n, n \in \mathbb{N}$ mit uniformer Schaltkreiskomplexität $\text{poly}(n)$

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

8.4 Die Klasse $\mathcal{BPP}$

Definition ($\mathcal{BPP}$): Die Klasse $\underline{\mathcal{BPP}}$ besteht aus allen booleschen Funktionen $f_n, n \in \mathbb{N}$, für die es eine uniforme Schaltkreisfamile $\{C_n\}_{n\in\mathbb{N}}$ gibt mit:

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

Beispiel: 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. $(C(x,y) = f_n(x)) \geq \frac{3}{4}$

8.5 Die Klasse $\mathcal{NP}$

Definition ($\mathcal{NP}$): Die Klasse $\mathcal{NP}$ besteht aus allen booleschen Funktionen $f_n, n \in \mathbb{N}, \mathbb{F}_2^n \to \mathbb{F}_2$, für die es eine uniforme Schaltkreisfamilie $\{C_n\}_{n\in\mathbb{N}}$ gibt mit:

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

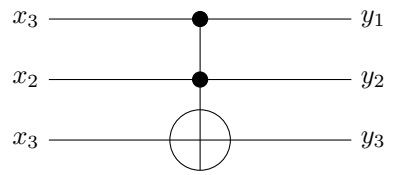
Beispiel: $f_n = X_{\texttt{SAT}}(\langle\phi\rangle) = \begin{cases} 1 & \text{falls } \langle\phi\rangle \in \texttt{SAT} \\ 0 & \text{sonst} \end{cases}$
$X_{\texttt{SAT}} \in \mathcal{NP}$, denn für jedes $\langle\phi\rangle \in \texttt{SAT}$ mit m Variablen gibt es eine erfüllbare Belegung $y \in \mathbb{F}_2^m$. Der Schaltkreis C_n wertet ϕ mit Belegung y aus.

9 Quantenschaltkreiskomplexitäten

9.1 Reversible Schaltkreise

Definition (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 Funktion. Sie werden durch Permutationsmatrizen beschrieben.

Beispiel: $\wedge : \mathbb{F}_2^2 \to \mathbb{F}_2, (x_1, x_2) \mapsto x_1 x_2$
$\texttt{T} = U_\wedge : \mathbb{F}_2^3 \to \mathbb{F}_2^3, (x_1, x_2, x_3) \mapsto (x_1, x_2, x_1 x_2 + x_3) = (x_1, x_2, x_1 \wedge x_2 \oplus x_3)$
Toffoli-Funktion T



NOT auf $x_3 \Leftrightarrow x_1 = x_2 = 1$

$I : \mathbb{F}_2 \to \mathbb{F}_2, x_1 \mapsto x_1$
$\texttt{CNOT} = U_I : \mathbb{F}_2^2 \to \mathbb{F}_2^2, (x_1, x_2) \mapsto (x_1, x_1 + x_2)$
Man beachte: $\texttt{CNOT}(x_1, 0) \mapsto (x_1, x_1)$ liefert Kopierfunktion c für $x_1 \in \mathbb{F}_2$

Definition (r-universell): sei R eine Menge von reversieblen booleschen Funktionen, die auf einer konstanten Anzahl von Bits operieren. R heißt r-universell, falls jede reversible Funktion als Verknüpfung von Elementen aus R, Hilfsvariablen und Konstanten $0, 1$ dargestellt werden kann.

Satz: $\{\mathtt{T}\}$ ist r-universell.

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

9.2 Die Klassen $\mathcal{QP}$ und $\mathcal{BQP}$

Definition (einbettbar): Seien $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ und $U_f : \mathbb{F}_2^{n+l} \to \mathbb{F}_2^{m+k}$ boolesche Funktionen. Wir nennen f einbettbar in U_f, falls es ein $h \in \mathbb{F}_2^2$ gibt mit $U_f(x, h) = (h', f(x))$ 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 aus 9.1: $U_f(x, y) \mapsto (x, f(x)+y)$. 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.

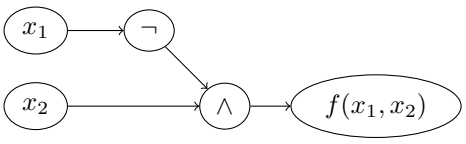
Satz: Sei $C = \{C_n\}_{n\in\mathbb{N}}$ eine uniforme Schaltkreisfamilie über $S = \{\wedge, \neg\}$ der Größe $\mathcal{O}(g(n))$, die $f_n, n \in \mathbb{N}$ berechnet. Dann gibt es eine uniforme reversible Schaltkreisfamilie C_r über $\{\mathtt{T}, 0, 1\}$ der Größe $\mathcal{O}(g(n))$, die $f_n^r : \mathbb{F}_2^{n+m+l} \to \mathbb{F}_2^{n+m+l}$ mit $(x, y, z \mapsto (x, f_n(x) + y, z')$ 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 Schatkrleis C_n auf einer DTM konstruieren. Wir ersetzen in C_n die

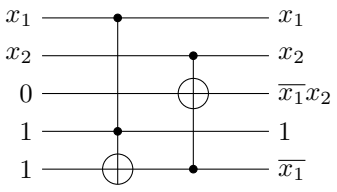
- $\wedge$-Gatter mit $\mathtt{T}(x_1, x_2, 0) = (x_1, x_2, x_1x_2)$
- $\neg$-Gatter mit $\mathtt{T}(x_1, 1, 1) = x_1, 1, 1 - x_1)$

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 $\mathcal{O}(g(n))$.

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



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



Definition (Quantenschaltkreis-Familie): 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 boolesche Funktion $f_n, n \in \mathbb{N}$ hat uniforme Quanten-Schaltkreiskomplexität $\mathcal{O}(g(n))$ bezüglich S, falls es eine uniforme QC-Familie über S gibt, die f_n berechnet.

Definition ($\mathcal{QP}$): Die Klasse $\mathcal{QP}$ ist die Klasse aller booleschen Funktionen $f_n, n \in \mathbb{N}$, für die es ein $g(n) \in$ poly(n) und eine uniforme QC-Familie $Q_{g(n)}$ bezüglich $S_2 = \{\mathtt{H}, \mathtt{CNOT}, \mathtt{T}\}$ 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: $\mathcal{P} \subseteq \mathcal{QP}$

Beweis: Sei $f_n \in \mathcal{P}$. Dann gibt es eine uniforme Schaltkreisfamile C mit Größe poly(n) die f_n berechnet.
$\overset{9.2}{\Rightarrow} \exists$ 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 $\{\mathtt{T}, 0, 1\}$ definiert.
Ersetzung der booleschen Gatter `T` durch unitäre Gatter, die `T` beschreiben, transformiet C_r in einen Quantenschaltkreis. Damit ist die Funktion $f_n \in \mathcal{QP}$.

Definition ($\mathcal{BQP}$): Die Klasse $\mathcal{BQP}$ ist die Klasse aller booleschen Funktionen $f_n, n \in \mathbb{N}$, für die es ein $g(n) \in$ poly(n) und eine uniforme QC-Familie $Q_{g(n)}$ bezüglich $\{\mathtt{H}, \mathtt{CNOT}, \mathtt{T}\}$ gibt mit:

- $Q_{g(n)}$ hat Größe poly(()n)
- $\exists k \in$ 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.

Definition (H_k): Sei $x = |x_0 x_1 \dots x_{k-1}\rangle$. Dann ist
$H_k|x\rangle = H_k|x_0 \dots x_{k-1}\rangle = H|x_0\rangle \otimes H|x_1\rangle \otimes \dots \otimes H|X_{k-1}\rangle$ die Hadamard-Abbildung auf ein k-Qubit-Register.

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

Beweis: $k = 1, 2$: siehe 5.3, $k = 3$: siehe Übung. Beliebiges k: induktiv.

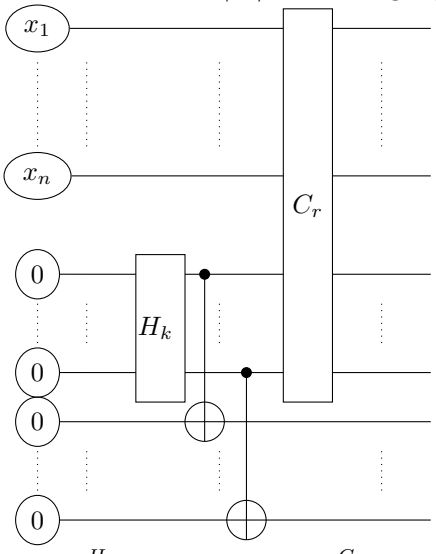
Korollar: $H_k|0^k\rangle = \frac{1}{2^{\frac{k}{2}}} \sum\limits_{y \in \{0,1\}^k} |y\rangle$ liefert gleichmäßige Überlagerung der Basiszustände.

Satz: $\mathcal{BPP} \subseteq \mathcal{BQP}$

Beweis: Sei $f \in \mathcal{BPP}$ und C die Schaltkreisfamilie polynomieller Größe mit Ws.$_y(C(x, y) = f_n) \geq \frac{2}{3}$.
Analog zum Beweis $\mathcal{P} \subseteq \mathcal{QP}$:

- Transformiere C in reversible Familie C_r über $\{\mathtt{T}, 0, 1\}$ polynomieller Größe, die f_n^r berechnet.
- Transformire 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:



$|x0^{2k}\rangle \overset{H_k}{\longmapsto} \frac{1}{2^{\frac{k}{2}}} \sum\limits_{y \in \{0,1\}^k} |xyy\rangle \overset{C_r}{\longmapsto} \frac{1}{2^{\frac{k}{2}}} \sum\limits_{y \in \{0,1\}^k} C_r|xy\rangle \otimes |y\rangle$

Aber $C_r|xy\rangle = f(x) \; \forall x$ und mindestens $\frac{2}{3}$ 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. $\geq \frac{2}{3}$

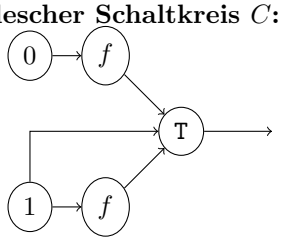
10 Quanten -schaltkreise und -algorithmen

10.1 Deutsch-Josza Problem

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

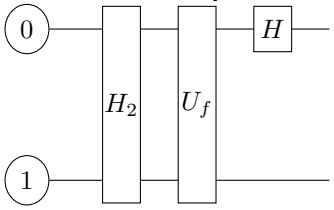
Gesucht: Schaltkreis, der entscheidet ob $f(0) = f(1)$ mit minimaler Anzahl von f-Gattern

Boolescher Schaltkreis C:



$C(0,1) = \mathtt{T}(f(0), 1, f(1)) = f(0) + f(1) \Rightarrow C(0,1) = 0 \Leftrightarrow f(0) = f(1)$. 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 entscehidet das Deutsch-Josza Problem.

Beweis:

$$
\begin{aligned}
|01\rangle &\overset{H_2 = H \otimes H}{\longmapsto} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&= \frac{1}{2}(|0\rangle \otimes (|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle) \\
&\overset{U_f}{\longmapsto} \frac{1}{2}(|0\rangle \otimes (|0 + f(0)\rangle - |1 + f(0)\rangle) + |1\rangle(|0 + f(1)\rangle - |1 + f(1)\rangle)) \\
&= \frac{1}{2}(|0\rangle \otimes (-1)^{f(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes (-1)^{f(1)}(|0\rangle - |1\rangle)) \\
&= \frac{1}{2}(((-1)^{f(0)}|0\rangle + (-1)^{f(1)}|1\rangle) \otimes (|0\rangle - |1\rangle)) \\
&\overset{H \otimes I}{\longmapsto} \frac{1}{2^{\frac{3}{2}}}(((-1)^{f(0)} + (-1)^{f(1)})|0\rangle + ((-1)^{f(0)} - (-1)^{f(1)})|1\rangle) \otimes (|0\rangle - |1\rangle)
\end{aligned}
$$

Für $f(0) = f(1)$: $(-1)^{f(0)} \frac{1}{\sqrt{2}}|0\rangle \otimes (|0\rangle - |1\rangle)$
$\Rightarrow$ Messung liefert 0 im 1. Qubit

Für $f(0) \neq f(1)$: $(-1)^{f(0)} \frac{1}{\sqrt{2}}|1\rangle \otimes (|0\rangle - |1\rangle)$
$\Rightarrow$ Messung liefert 1 im 1. Qubit.

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

Orakel-Modell: Information über $f : \mathbb{F}_2^n \to \mathbb{F}_2^m$ durch Auswerten von f.

10.2 Verallgemeinertes Deutsch-Josza Problem

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

- konstant, d.h. $f(x) = c \; \forall c \in \mathbb{F}_2, \; \forall x \in \mathbb{F}_2^n$
- 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:

1. `Setze` $c = f(0^n)$
2. `FOR i = 1 TO` 2^{n-1}
   - `Falls` $f(i) \neq c$, `Ausgabe ‘‘balanciert’’ und EXIT.`
3. `Ausgabe: ‘‘Konstant’’`

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

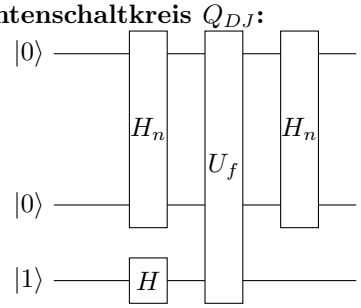
Probalistischer Algorithmus:

1. `Setze` $c = f(0^n)$
2. `FOR i-1 zufällige Werte` $x_j \in \{1, 2, \ldots, 2^{n-1}\}$
   - `Falls` $f(x_i) \neq c$, `Ausgabe ‘‘balanciert’’ und EXIT.`
3. `Ausgabe: ‘‘Konstant’’`

Fehlerwahrscheinlichkeit: $\underbrace{\text{Ws. (Ausgabe “balanciert”}|f \text{ konstant)}}_{=0} + \text{Ws. (Ausgabe “konstant”}|f \text{ balanciert)}$

$= \text{Ws.}\,(x_1 = x_2 = \cdots = x_{i-1} = f(0)|f \text{ balanciert}) = \prod_{j=1}^{i-1} \frac{2^{n-1}-j}{2^n} \leq \left(\frac{1}{2}\right)^{i-1}$

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-Josza Problem.

Beweis:

$$
\begin{aligned}
|0^n 1\rangle &\overset{H_n \otimes H}{\longmapsto} \frac{1}{2^{\frac{n}{2}}} \sum_{x\in\{0,1\}^n} |x\rangle \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \\
&\overset{U_f}{\longmapsto} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x\in\{0,1\}^n} |x\rangle(|0+f(x)\rangle - |1-f(x)\rangle) \\
&= \frac{1}{2^{\frac{n+1}{2}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle \otimes (|0\rangle - |1\rangle) \\
&\overset{H_n}{\longmapsto} \frac{1}{2^{\frac{2n+1}{2}}} \sum_{x\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)+xy}|y\rangle \otimes (|0\rangle - |1\rangle) = |z\rangle
\end{aligned}
$$

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:
$\frac{1}{2^{\frac{2n+1}{2}}} \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}(-1)^{xy}|y\rangle = \frac{1}{2^{\frac{2n+1}{2}}}(-1)^{f(0^n)}(2^n|0^n\rangle + \sum_{y\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{xy}|y\rangle$
$\Rightarrow |z\rangle = \frac{1}{\sqrt{2}}(-1)^{f(0^n)}|0^n\rangle \otimes (|0\rangle - |1\rangle)$
D.h für konstantes f liefert die Messung der ersten n Qubits 0^n.

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

$\Rightarrow$ Messung der 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

10.3 Bernstein-Vazirani Problem (1983)

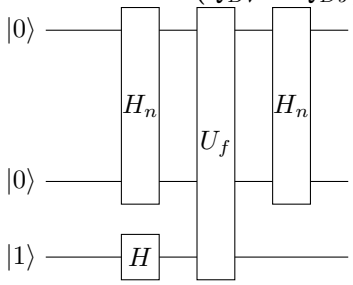
Gegeben: Funktion $f_a : \mathbb{F}_2^n \to \mathbb{F}_2, x \mapsto ax = \sum_{i=1}^{n} a_i x_i \bmod 2$ mit $a \in \{0,1\}^n$ im Orakel-Modell

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 $e_i, i = 1 \ldots n$ die Einheitsvektoren.
Optimaler klassischer Algorithmus:

- `Werte` f_a `an` $e_i, i = 1 \ldots n$ `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:

$$
\begin{aligned}
|0^n 1\rangle &\overset{H_n\otimes H}{\longmapsto} \frac{1}{2^{\frac{n+1}{2}}}\sum_{x\in\{0,1\}^n}|x\rangle\otimes(|0\rangle-|1\rangle)\\
&\overset{U_{f_a}}{\longmapsto} \frac{1}{2^{\frac{n+1}{2}}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle\otimes(|0\rangle-|1\rangle)\\
&\overset{H_n\otimes I_2}{\longmapsto} \frac{1}{2^{\frac{n+1}{2}}}\sum_{y\in\{0,1\}^n}\sum_{x\in\{0,1\}^n}(-1)^{xa}(-1)^{xy}|y\rangle\otimes(|0\rangle-|1\rangle) = |z\rangle
\end{aligned}
$$

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

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

10.4 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 $x_1, \ldots, x_k$ 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: $x_{ij} = \begin{cases} 1 & \text{falls } f(x_i) = f(x_j) \\ 0 & \text{sonst} \end{cases}$, $\text{Ws.}\,(x_{ij} = 1) = \frac{1}{2^n - 1}$

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

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