Quantenalgorithmen

Alexander May

28. Oktober 2013

Literatur

Mika Hirvensalo Quantum Computing

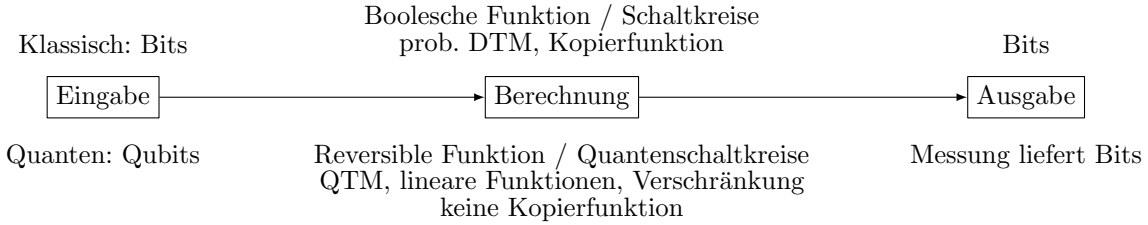
Chuang/Nielsen Quantum Computation and Quantum Information

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 :

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

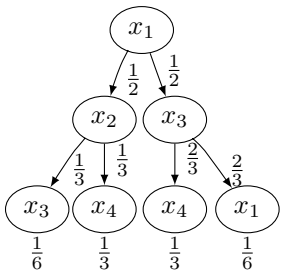
Markov-Matrix :

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

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

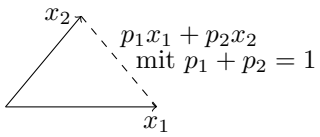
2.

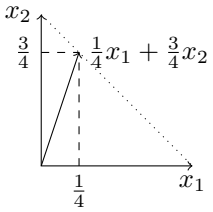


x_1, x_3 : Ws. $\frac{1}{6}$
x_4 : Ws. . $\frac{2}{3}$

Strategie: Maximiere Ws. des gewünschten Endzustands

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



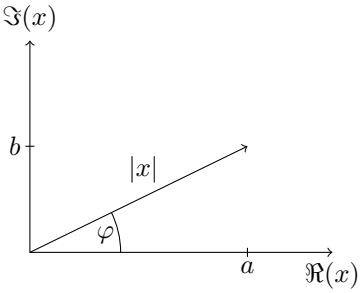


3 1-Qbit Systeme

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: $\alpha_0|0\rangle + \alpha_1|1\rangle,\ \alpha_0, \alpha_1 \in \mathbb{C}$

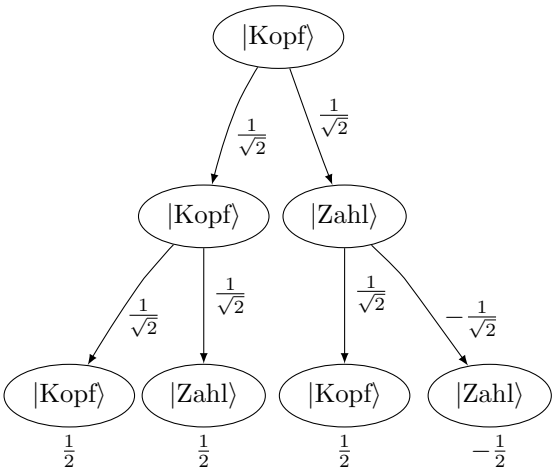
Übung: $|\alpha_0|0\rangle + \alpha_1|1\rangle| = 1 \Leftrightarrow |\alpha_0|^2 + |\alpha_1|^2 = 1$

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.