Quantenalgorithmen

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

A. May, M. Vollmer, Maike Ritzenhofen

M. Hirvensalo, Quantum Computing
Chuang/Nielsen, Quantum Computation and Quantum Information
D. Aharonov, Quantum Computation

Übungsbetrieb: 2-wöchentlich, Start: 26.10.
Do. 9:50 - 11:30
Mo. 9:50 - 11:30 A102

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:

Klassisch: Bits | Boolsche Fkt. / Schaltkreise, prob. DTM, Kopierfunktion | Bits

Eingabe ⟶ Berechnung ⟶ Ausgabe

Quanten: Qubits | Reversible Fkt. / Quantenschaltkreise, QTM, lineare Funktionen, Quantenparallelität, Interferenz, Verschränkung, keine Kopierfunktion | 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: $p_1[x_1] + p_2[x_2] + \dots + p_n[x_n]$

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

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

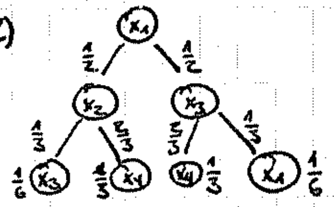
D.h. $\begin{pmatrix} p_1' \\ p_2' \\ \vdots \\ p_n' \end{pmatrix} = \overbrace{\begin{pmatrix} p_{11} & \cdots & p_{1n} \\ & \ddots & \\ p_{n1} & \cdots & p_{nn} \end{pmatrix}}^{\text{Markov-Matrix}} \cdot \begin{pmatrix} p_1 \\ \vdots \\ p_n \end{pmatrix}$

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)



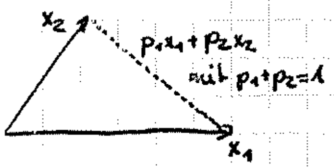
x_1, x_3: Ws. $\frac{1}{6}$

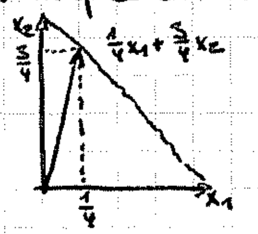
x_4: Ws $\frac{2}{3}$

Strategie: Maximiere Ws. des gewünschten Endzustands.

Vektorraum-Interpretation: • $x_1, x_2, \dots, x_n$ Basisvektoren eines n-dim Vektorraums

• Wahrscheinlichkeitsverteilungen entsprechen konvexen Linearkombinationen





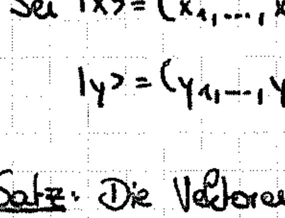
1-Qubit Systeme

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

$|y\rangle = (y_1, \dots, y_n)$ $\langle x|y\rangle = \sum_{i=1}^{n} x_i^* y_i$ $\quad |x\rangle, |y\rangle$ 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.) $||x_i\rangle| = 1$ 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 $|x_1\rangle, \ldots, |x_n\rangle$ eine orthonormale Basis des $\mathbb{C}^n$ (auch H_n für Hilbertraum).

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

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 $p_1[x_1] + \ldots + p_n[x_n]$ $\quad \sum_{i=1}^n p_i = 1$

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

Trotzdem fundamental verschieden!

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

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

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

Zweifacher Münzwurf:

$$\begin{tikzcd}[column sep=small]
 & & & |\text{Kopf}\rangle \arrow[dll, "\frac{1}{\sqrt{2}}"'] \arrow[drr, "\frac{1}{\sqrt{2}}"] & & & \\
 & |\text{Kopf}\rangle \arrow[dl, "\frac{1}{\sqrt{2}}"'] \arrow[dr, "\frac{1}{\sqrt{2}}"] & & & & |\text{Zahl}\rangle \arrow[dl, "\frac{1}{\sqrt{2}}"'] \arrow[dr, "-\frac{1}{\sqrt{2}}"] & \\
|\text{Kopf}\rangle & & |\text{Zahl}\rangle & & |\text{Kopf}\rangle & & |\text{Zahl}\rangle
\end{tikzcd}$$

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