Quantencomputing I

Hecke Schrobsdorff

Max Punck Institut für Dynamik und Selbstorganisation

Oberseminar Theoretische Informatik SS 2005

Inhalt

Einführung

Hauptidee:

- Miniaturisierung führt zu Quantenphänomenen.
- Kann man das nutzen?

Quantenmechanik

- eröffnet neue Rechenmöglichkeiten,
- vereinfacht einige Berechnungen.

Aber

- nicht alles wird einfacher,
- es gibt Grenzen in der Beschleunigung.

Qubits statt Bits

Ein Quantumbit, kurz **Qubit**, hat die Form

$$|\phi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle \quad \text{mit: } \alpha, \beta \in \mathbb{C}, \quad |\alpha|^2 + |\beta|^2 = 1$$

- $|\cdot\rangle$: **Ket**-Schreibweise bezeichnet einen Basiszustand
  Standard-Orthonormalbasis $|0\rangle$ und $|1\rangle$
- Superposition als Linearkombination der Basis
- kontinuierliche Werte auf dem Einheizkreis
- Wahrscheinlichkeitsinterpretation ($\rightarrow$ Messen) der Amplituden α und β

Rechnen mit Qubits

- Präparation eines Anfangszustands
- Zustandsänderung mittels unitärer Transformationen, die auf den aktuellen Zustand angewendet werden
- Informationsextraktion per Messung

Achtung! Die Messung ist keine unitäre Transformation, sondern höchst nichtlinear.

Messen

- Immer nur bezüglich einer Orthonormalbasis
- Das Ergebnis ist einer der Basiszustände
- Die Amplitudenquadrate bezeichnen die Wahrscheinlichkeiten des Messens des entsprechenden Zustands.

$$
\begin{aligned}
|\alpha|^2 &= P(\mathrm{M}(\phi) = |0\rangle) \\
|\beta|^2 &= P(\mathrm{M}(\phi) = |1\rangle)
\end{aligned}
$$

- Zusammenbruch der Superposition
- Der gemessene Zustand wird angenommen.

“Man kann nichts beobachten, ohne es zu verändern”

Unitäre Transformationen

- Qubits liegen immer auf dem Einheitskreis $\Rightarrow$ alle Transformationen sind unitär

Definition : Eine Matrix M heißt **unitär**,
wenn $M^* := \overline{M}^T = M^{-1}$ gilt.

Dies entspricht den orthogonalen Matrizen, wenn man sich nicht über $\mathbb{C}$ sondern über $\mathbb{R}$ bewegt.

- Reversibilität ist Pflicht
- Basis von 2 Elementen, also 2×2-Matrizen
- Zustände sind als 2er Vektoren darstellbar

Die Hadamardtransformation H_1

$$H_1 := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix}$$

Damit ist:

$$\begin{aligned} H_1|0\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \\ H_1|1\rangle &= \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \end{aligned}$$

und wieder ($H_1^{-1} = H_1$)

$$\begin{aligned} H_1 \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) &= |0\rangle \\ H_1 \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) &= |1\rangle \end{aligned}$$

nochmal Messen

- Eine wichtige Basis ungleich $\{|0\rangle, |1\rangle\}$ ist

$$\begin{aligned}\{|+\rangle, |-\rangle\} &= \{H_1|1\rangle, H_1|0\rangle\} \\ &= \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}\end{aligned}$$

- Zum Messen wird transformiert

$$|\phi\rangle = \frac{1}{\sqrt{2}}((\alpha+\beta)|+\rangle + (\alpha-\beta)|-\rangle)$$

- Die Amplitudenquadrate in dieser Basis geben dann die Wahrscheinlichkeiten an, wenn in dieser Basis gemessen wird.

$$\begin{matrix}\frac{1}{2}|\alpha+\beta|^2 \\ \frac{1}{2}|\alpha-\beta|^2\end{matrix} \quad \text{den Zustand} \quad \begin{matrix}|+\rangle \\ |-\rangle\end{matrix}.$$

Quantenregister

- Mehrere Qubits verschaltet geben ein Quantenregister

$$|x_n\rangle \ldots |x_2\rangle |x_1\rangle =: |x_n \ldots x_2\, x_1\rangle$$

- Im Prinzip äußeres Produkt der einzelnen Hilbärträume
- Hier reicht: Basiszustände des n-Registers sind Binärzahlen der Länge n

Für $n = 2$ ist

$$\begin{aligned} R &= \alpha_0 \cdot |0\rangle|0\rangle + \alpha_1 \cdot |0\rangle|1\rangle + \alpha_2 \cdot |1\rangle|0\rangle + \alpha_3 \cdot |1\rangle|1\rangle \\ &= \alpha_0 \cdot |00\rangle + \alpha_1 \cdot |01\rangle + \alpha_2 \cdot |10\rangle + \alpha_3 \cdot |11\rangle \end{aligned}$$

n allgemein: $R = \sum_{i=0}^{2^n-1} \alpha_i \cdot |i\rangle$ mit $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$

wobei $|i\rangle \hat{=} |b_n b_{n-1} \ldots b_1\rangle$ und $(b_n b_{n-1} \ldots b_1) = bin(i)$

Transformation von Registern

Manipulationen an Registern werden nun durch unitäre $2^n \times 2^n$-Matrizen (!) beschrieben.
Beispiel: $n = 2$

$$XOR : |x, y\rangle \mapsto |x, x \oplus y\rangle$$

$$\Rightarrow \quad XOR \mathrel{\hat{=}} \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array}\right)$$

- Die klassische Form $|x, y\rangle \mapsto |x \oplus y\rangle$ ist nicht reversibel.
- gesteuertes *NOT*: Das zweite Bit wird genau dann negiert, wenn das erste Bit x den Wert 1 hat.

Die allgemeine Hadamardtransformation

- Sei $|x\rangle$ eim n-Qubit Quantenregister $|x_n x_{n-1} \ldots x_1\rangle$.
  Verallgemeinerte Hadamardtransformation:

$$H_n|x\rangle = \frac{1}{\sqrt{2}} \sum_{y \in \{|0\rangle, |1\rangle\}^n} (-1)^{x \cdot y} |y\rangle, \text{ wobei } x \cdot y = \bigoplus_{i=1}^{n} x_i y_i$$

- Die Summe läuft über alle möglichen Zustände des Registers. $|x\rangle$ taucht nur noch im Vorzeichen auf.

Beispiele:

- gleichgewichtete Superposition aller Zustände:

$$H_n|0\rangle = H_n|00\ldots0\rangle = \frac{1}{\sqrt{2}} \sum_{y=0}^{2^n-1} (-1)^0 |y\rangle$$

- $H_2|01\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$

Lokalität

- Jede Transformation eines n-Quantenregisters zerfällt in n Transformationen, die je auf einem Qubit arbeiten.

$$H_2 = H_1 \otimes H_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} H_1 & H_1 \\ H_1 & -H_1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

- Das liegt an der Struktur des äußeren Produktes.
- Dadurch wird die Anzahl der verschiedenen Gatter sehr eingeschränkt.

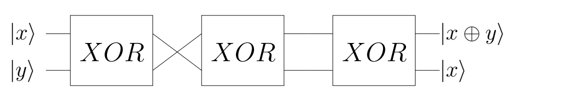
Entkopplung der Transformationen

Wir hatten: $H_2|01\rangle = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$
Das lässt sich auch lokal berechnen:

$$
\begin{aligned}
|01\rangle \xrightarrow{\substack{H_1\text{ aufs}\\ \text{erste Qubit}}} \quad & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|1\rangle \\
= \quad & \frac{1}{\sqrt{2}}|01\rangle + \frac{1}{\sqrt{2}}|11\rangle \\
\xrightarrow{\substack{H_1\text{ aufs}\\ \text{zweite Qubit}}} \quad & \frac{1}{\sqrt{2}}|0\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) + \frac{1}{\sqrt{2}}|1\rangle\left(\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right) \\
= \quad & \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)
\end{aligned}
$$

Quantenschaltkreise

- Schaltkreise liefern eine gute Übersicht von Quantenalgorithmen
- Sie definieren die Komplexität eines Quantenalgorithmus über die Anzahl der Einqubit-Gatter.

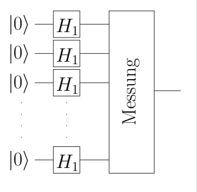


Hier passieren folgende Zustandsübergänge:

$$\begin{aligned}
|x, y\rangle &\rightarrow |x, x \oplus y\rangle \xrightarrow{\text{tausch}} |x \oplus y, x\rangle \\
&\rightarrow |x \oplus y, x \oplus x \oplus y\rangle = |x \oplus y, y\rangle \\
&\rightarrow |x \oplus y, x \oplus y \oplus y\rangle = |x \oplus y, x\rangle
\end{aligned}$$

Zufall

- Ein Quantencomputer kann echte Zufallszahlen generieren.
- Durch Messen einer gleichgewichteten Superposition



- Registerinhalt nach dem ersten Schritt:

$$|0..0\rangle \xrightarrow{H_n} \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle$$

- Messen ergibt: $|i\rangle$ mit Wahrscheinlichkeit $P = \frac{1}{\sqrt{2^n}}$

Das Deutsch-Problem
Problemstellung

Gegeben sei eine Blackbox, die eine Funktion $f : \{0,1\} \mapsto \{0,1\}$ berechnet. Davon gibt es vier verschiedene.

Ziel des Spiels ist es nun, zu entscheiden, ob

f konstant ($f(0) = f(1)$) oder
f balanciert ($f(0) \neq f(1)$) ist.

- Orakelabfragen sind erlaubt
- Ein klassischer Computer muss zwei solcher Abfragen tätigen
- Quantencomputer müssen nur einmal schauen.

Das Deutsch-Problem
Die Idee

- Erzeuge eine gleichgewichtete Superposition der beiden Basiszustände
- Wende f darauf an.
- Messe bezüglich der Basis, deren reine Zustände die beiden Ergebnisse der Rechnung sind.

Das Deutsch-Problem
Eine Transformation für f

eine unitäre Form des Funktionsaufrufes ist

$$U_f : |x, y\rangle \mapsto |x, y \oplus f(x)\rangle$$

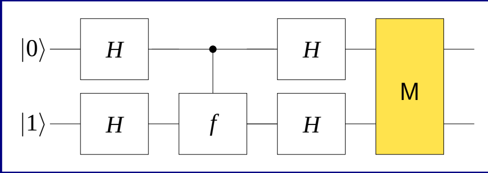
- f ist an sich nicht reversibel
- U_f schon.
- Es ist $U_f^{-1} = U_f$.

Das Deutsch-Problem
Algorithmus

1. $R = |x, y\rangle \leftarrow |01\rangle$
2. $R \leftarrow H_2 R$
3. $R \leftarrow U_f R$
4. Messe das erste Bit $|x\rangle$ bezüglich der Basis

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

Sage “konstant“ falls das Ergebnis $|-\rangle$ ist, sonst “balanciert“.



Das Deutsch-Problem

Analyse

$$|01\rangle \xrightarrow{H_2} \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$$

$$\xrightarrow{U_f} \tfrac{1}{2}\left(|0\rangle \cdot (|0 \oplus f(0)\rangle - |1 \oplus f(0)\rangle) + |1\rangle \cdot (|0 \oplus f(1)\rangle - |1 \oplus f(1)\rangle)\right)$$

$$= \frac{1}{2|0,f(0)\rangle - \frac{1}{2}|0,1+f(0)\rangle + \frac{1}{2}|1,f(0)\rangle - \frac{1}{2}|1,1+f(1)\rangle}$$

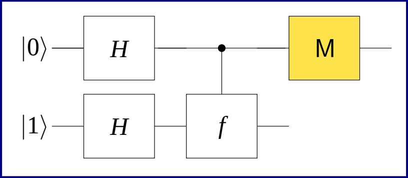
$$= \frac{1}{2\Big(|0\rangle \cdot (-1)^{f(0)}(|0\rangle - |1\rangle) + |1\rangle \cdot (-1)^{f(1)}(|0\rangle - |1\rangle)\Big)}$$

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

$$= \begin{cases} \left.\begin{array}{r} \frac{1}{2}(|0\rangle + |1\rangle) \cdot (|0\rangle - |1\rangle) \\ \text{oder } -\frac{1}{2}(|0\rangle + |1\rangle) \cdot (|0\rangle - |1\rangle) \end{array}\right\} \text{falls} f(0) = f(1) \\ \\ \left.\begin{array}{r} \frac{1}{2}(|0\rangle - |1\rangle) \cdot (|0\rangle - |1\rangle) \\ \text{oder } -\underbrace{\frac{1}{2}(|0\rangle - |1\rangle)}_{|x\rangle} \cdot \underbrace{(|0\rangle - |1\rangle)}_{|y\rangle} \end{array}\right\} \text{falls} f(0) \neq f(1) \end{cases}$$

Das Deutsch-Problem
Alternativer Algorithmus

1. $R = |x, y\rangle \leftarrow |01\rangle$
2. $R \leftarrow H_2 R$
3. $R \leftarrow U_f R$
4. $|x\rangle \leftarrow H_1 |x\rangle$
5. Messe das erste Bit $|x\rangle$ bezüglich der Basis $\{|0\rangle, |1\rangle\}$ Sage "konstant" falls das Ergebnis $|1\rangle$ ist, sonst "balanciert".



Das Deutsch-Problem
Analyse

Nach **GS3** haben wir den folgenden Zustand:

$$\frac{1}{\sqrt{2}}\Big((-1)^{f(0)}|0\rangle - (-1)^{f(1)}|1\rangle\Big)\cdot\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\xrightarrow{H_1 auf |x\rangle}$$

$$\frac{1}{\sqrt{2}}\Big((-1)^{f(0)}\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) + (-1)^{f(1)}\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\Big)\cdot\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$=1\frac{}{\sqrt{2}\Big(\big((-1)^{f(0)}+(-1)^{f(1)}\big)|0\rangle+\big((-1)^{f(0)}+(-1)^{f(1)}\big)|1\rangle\Big)\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)}$$

$$= \begin{cases} \pm|1\rangle\cdot\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) & \text{falls} f(0) = f(1) \\ \underbrace{\pm|0\rangle}_{|x\rangle}\cdot\underbrace{\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)}_{|y\rangle} & \text{falls} f(0) \neq f(1) \end{cases}$$

Deutsch-Jozsa
Problem

Gegeben sei wieder eine Blackbox, die eine Funktion $f : \{0,1\}^n \mapsto \{0,1\}$ berechnet.

Wir wissen, dass f entweder

konstant $f(i) = f(j) \forall i,j \in \{0,1\}^n$ oder

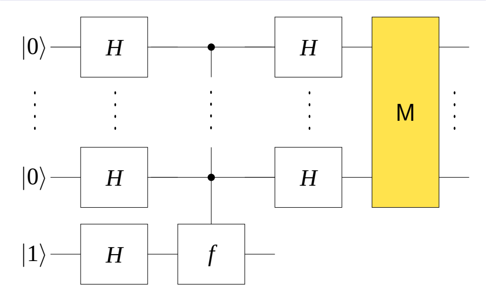
balanciert ist.

Im letzteren Fall werden gleich viele Eingaben auf 0 wie auf 1 abgebildet. Dann ist also $|f^{-1}(0)| = |f^{-1}(1)| = 2^{n-1}$.

- Ein klassischer Computer muss im schlechtesten Fall $2^{n-1} + 1$ solcher Abfragen tätigen
- Quantencomputer müssen nur einmal schauen.

Deutsch-Jozsa
Algorithmus

1. $R = |x_{n-1} \dots x_0\rangle|y\rangle \leftarrow |0\dots 0\rangle|1\rangle$
2. $R \leftarrow H_{n+1}R$
3. $R \leftarrow U_f R$
4. $|x\rangle|y\rangle \leftarrow (H_n|x\rangle)|y\rangle$
5. Messe $|x\rangle$. Sage “konstant” falls das Ergebnis $|0\dots 0\rangle$ ist, sonst “balanciert”.



Deutsch-Jozsa
Analyse

- $$|0\dots0\rangle|1\rangle \xleftarrow{h_{n+1}} \left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle\right)\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = |\phi_2\rangle$$
- $$|x\rangle\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \xrightarrow{U_f} |x\rangle\frac{1}{\sqrt{2}}(|f(x)\rangle-|1\oplus f(x)\rangle)$$
  $$= (-1)^{f(x)}\cdot|x\rangle\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$
- $$|\phi_2\rangle \xrightarrow{U_f} \left(\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|x\rangle\right)\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)$$
- $$\xrightarrow{H_n} \left(\frac{1}{2^n}\sum_{z=0}^{2^n-1}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot z}|z\rangle\right)\cdot\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) = |\phi_4\rangle$$

Deutsch-Jozsa
Analyse

$M(|x_{n-1}\dots x_0\rangle) = |\phi_4'\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}(-1)^{x\cdot z}|z\rangle$, für festes $|z\rangle$

Fall: konstant Für $z = 0$ gilt $x \cdot z = 0$:

$$|\phi_4'\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1} \pm|0\rangle = \pm|0\rangle.$$

Da $|\phi_4'\rangle$ ansonsten symmetrisch ist verschwindet die Amplitude von jedem $|z\rangle$ mit $z \neq 0$.

Fall: balanciert Für $z = 0$ ist $|\phi_4'\rangle = \frac{1}{2^n}\sum_{x=0}^{2^n-1}(-1)^{f(x)}|0\dots 0\rangle$.

Für die eine Hälfte der x ist $f(x) = 0$, für die andere ist $f(x) = 1$. Also ist die Amplitude von $|0\rangle$ gleich 0.

Zusammenfassung

- Die Quantenmechanik bietet neue Möglichkeiten für Algorithmen.
- Es ist gewöhnungsbedürftig, aber nicht schwer.
- Manche Verfahren sind überraschend

$$|cat\rangle = \frac{1}{\sqrt{2}}|dead\rangle + \frac{1}{\sqrt{2}}|alive\rangle$$