ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
Departement Informatik

Open Class – Sieben Wunder der Informatik

Prof. Dr. Juraj Hromkovič

Übungsaufgaben – Quantum-Computing

Zürich, 30. Oktober 2007

Zusammenfassung

Die erste und sehr gut geschriebene deutschsprachige Quelle für Quantum-Computing ist

> Matthias Homeister: *Quantum Computing verstehen.*
> Vieweg 2005, ISBN 3-528-05921-4.

Die ausführlichste unter den hervorragenden Quellen für Quantum-Computing ist

> M.A. Nielsen, I.L. Chuang: *Quantum computation and quantum information.*
> Cambridge University Press 2000, ISBN 0-521-63503-9.

Die Gesetze des Verhaltens von Mikro-Teilchen (der Quantenmechanik) laufen unseren Vorstellungen und Erfahrungen im Umgang mit Gegenständen in der Makro-Welt zuwider. Mindestens die folgenden beiden für die klassische Physik und Weltanschauung unverzichtbaren Prinzipien gelten in der Welt der Mikro-Teilchen nicht:

1. Ein Gegenstand befindet sich zu einem Zeitpunkt (der Relativitätstheorie folgend auch ein subjektiver Begriff) genau an einem Ort. Dies trifft für Teilchen nicht zu. Zum Beispiel kann sich ein Elektron gleichzeitig an mehreren Orten befinden.

2. Das Prinzip der Lokalität besagt, dass Wirkung immer lokal ist: Zwei Teilchen können eine derart starke Verbindung miteinander haben (in der Fachsprache sagt man, sie seien *verschränkt*), dass unabhängig von ihrer Entfernung (von ggf. Millionen von Lichtjahren) eine Änderung an einem der Teilchen sofort die gleiche Änderung an dem anderen Teilchen bewirkt.

Anhand von Erfahrungen aus der Makro-Welt müsste man solche Ereignisse in der Welt der Teilchen als Wunder betrachten. Für uns ist noch ein drittes Wunder wichtig: Zwei Ereignisse, die mit einer Wahrscheinlichkeit grösser null eintreten, können sich gegenseitig völlig auslöschen, so dass keines von beiden eintritt. Zum Beispiel nimmt ein Lichtstrahl von der Sonne zu seinem „Ziel“ (etwa einem Fisch unterhalb der Wasseroberfläche) die schnellste Strecke, weil alle anderen Möglichkeiten, das Ziel zu erreichen, sich gegenseitig auslöschen.

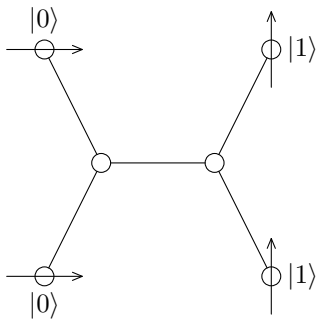

Abbildung 1: Ein Quantenregister

Wie können diese Eigenschaften von Teilchen benutzt werden, um einen Quantenrechner zu bauen? Zunächst ist es erforderlich, einen Speicher für die zu bearbeitenden Daten zu bauen. Wir denken an Register, die einzelne Bits speichern können. Solche Bits nennen wir Quantenbits und bezeichnen sie mit $|0\rangle$ und $|1\rangle$, um sie von klassischen Bits zu unterscheiden.
Es gibt mehrere Möglichkeiten, Quantenbits physikalisch zu realisieren. Eine Möglichkeit beruht auf der *Kernspin-Resonanz.* Abbildung 1 veranschaulicht, wie vier von sechs Atomen eines Moleküls als Quantenregister verwendet werden können.
Wenn sich ein Molekül in einem Magnetfeld befindet, richtet sich der Spin der Atomkerne parallel zu dem Magnetfeld aus. Diese parallele Richtung des Spins interpretieren wir als $|0\rangle$. Eine zu dem ursprünglichen Magnetfeld senkrechte Richtung betrachten wir als $|1\rangle$. Man kann durch oszillierende Felder Operationen auf diesen Quantenbits ausführen, mit denen man dank unterschiedlicher chemischer Eigenschaften der Atome die einzelnen Quantenregister beeinflussen kann.
Eine andere Möglichkeit sind *Ionenfallen.* Ionen sind elektrisch geladene Moleküle oder Atome (in Abbildung 2 sind sie positiv geladen, da ihnen jeweils zwei Elektronen fehlen). Die Ionen werden im Vakuum bei Temperaturen nahe dem absoluten Nullpunkt durch ein elektromagnetisches Feld in einer Ionenfalle festgehalten.
Den Wert $|0\rangle$ ordnen wir dem Grundzustand des Ions zu, und der Wert $|1\rangle$ wird durch einen energetisch angeregten Zustand des Ions realisiert. Die quantenmechanischen Operationen auf diesen Quantenbits kann man einzeln durch Laser-Strahlen realisieren.
Wie rechnet ein Quantenrechner, und was sollen die Vorteile sein? Wenn wir beim klassischen Rechner ein Bit-Register haben, dann kann dieses Register entweder 0 oder 1 beinhalten. Bei einem Quantenregister ist das anders. Es kann gleichzeitig beide Inhalte aufweisen oder jedes zu einem gewissen Teil. Wie beschreibt man dies?
Man sagt, dass sich ein *Quantenbit* (als Inhalt des Quantenregisters) in einer *Superposition* (oder *Überlagerung*) von klassischen Bits $|0\rangle$ und $|1\rangle$ befinden kann und beschreiben dies durch

$$\alpha \cdot |0\rangle \quad + \quad \beta \cdot |1\rangle \quad ,$$

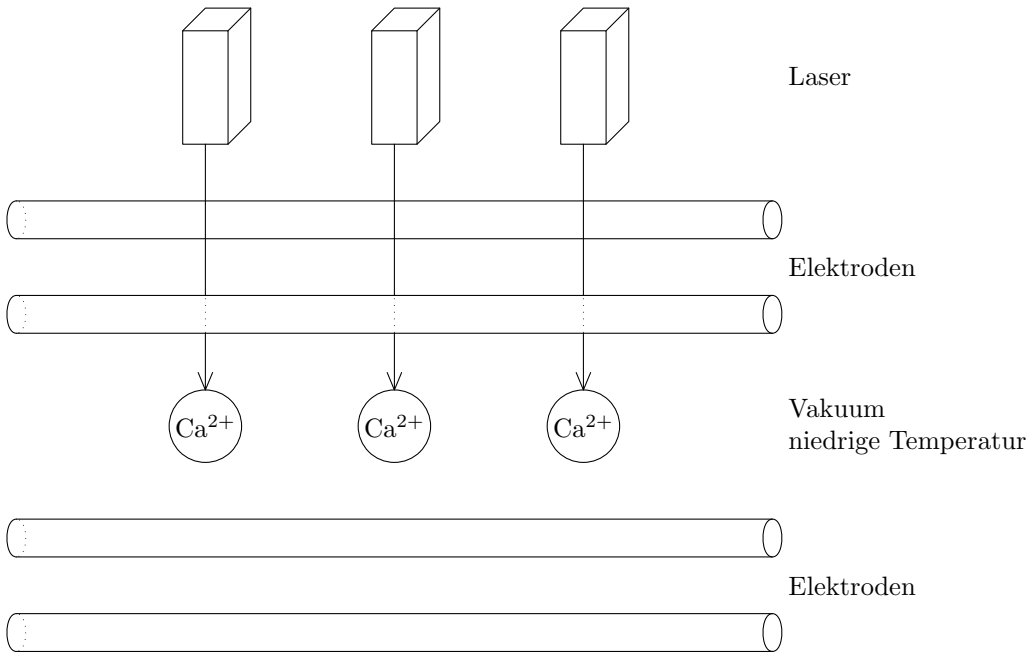

Abbildung 2: Drei Kalzium-Ionen in einer elektromagnetischen Ionenfalle

wobei α und β komplexe Zahlen sind, für die

$$\alpha^2 + \beta^2 = 1$$

gilt. Die Werte α und β heissen *Amplituden* und drücken die Grösse des Anteils aus, zu dem sich das Bit jeweils in $|0\rangle$ bzw. $|1\rangle$ befindet.
Genauer gilt:

α^2 ist die Wahrscheinlichkeit, sich in $|0\rangle$ zu befinden.

β^2 ist die Wahrscheinlichkeit, sich in $|1\rangle$ zu befinden.

Aus dieser Interpretation ergibt sich die Anforderung $\alpha^2 + \beta^2 = 1$, weil es keine andere Möglichkeit für klassische Zustände gibt.
Obwohl sich das Quantenregister mit Sicherheit in einem Zustand (einer Superposition)

$$\alpha \cdot |0\rangle + \beta \cdot |1\rangle$$

befindet, haben wir keine Möglichkeit, uns diese Superposition vollständig anzusehen, d. h. α und β zu messen. Wenn wir eine Messung eines Quantenbits vornehmen, sehen wir nur klassische Resultate, also $|0\rangle$ oder $|1\rangle$, und die Superposition wird dadurch definitiv zerstört. Dies ist genau wie bei einem Elektron, das durch zwei unterschiedliche Fenster gleichzeitig fliegt, aber wenn man es beobachtet, so fliegt es durch nur ein Fenster.
In dieser Interpretation ist α^2 die Wahrscheinlichkeit, mit der wir bei der Messung $|0\rangle$ erhalten, und β^2 ist die Wahrscheinlichkeit, mit der wir bei der Messung $|1\rangle$ sehen werden.

Beispiel. Die Superposition

$$\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$$

drückt aus, dass man mit gleicher Wahrscheinlichkeit in $|0\rangle$ ist wie in $|1\rangle$, denn

$$\alpha^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{(\sqrt{2})^2} = \frac{1}{2} \quad \text{und} \quad \beta^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2} \quad .$$

Beispiel. Die Superposition

$$\frac{1}{\sqrt{3}} \cdot |0\rangle + \sqrt{\frac{2}{3}} \cdot |1\rangle$$

drückt aus, dass man bei der Messung mit der Wahrscheinlichkeit

$$\alpha^2 = \left(\frac{1}{\sqrt{3}}\right)^2 = \frac{1}{3}$$

die $|0\rangle$ sieht und mit der Wahrscheinlichkeit

$$\beta^2 = \left(\sqrt{\frac{2}{3}}\right)^2 = \frac{2}{3}$$

die $|1\rangle$ erhält.

Aufgabe 21

Schreiben Sie die Superposition eines Quantenbits nieder, bei der man mit einer Wahrscheinlichkeit von $\frac{1}{4}$ den klassischen Wert $|1\rangle$ und mit einer Wahrscheinlichkeit von $\frac{3}{4}$ den klassischen Wert $|0\rangle$ messen wird. **5 Punkte**

Wie sieht dies allgmeiner aus? Wenn wir n Quantenregister haben, dann haben wir potenziell 2^n mögliche Inhalte. Und eine Superposition von n Quantenbits bedeutet, sich gleichzeitig in allen 2^n vielen möglichen klassischen Registerzuständen zu befinden, und zwar in jedem mit einer gewissen Wahrscheinlichkeit, so dass diese 2^n vielen Wahrscheinlichkeitswerte aufsummiert den Wert 1 ergeben.

Beispiel. Betrachten wir zwei Quantenregister. Alle möglichen Inhalte von zwei Bit-Registern sind die vier Inhalte

$$00 \quad , \quad 01 \quad , \quad 10 \quad \text{und} \quad 11 \quad .$$

Damit befindet sich der Quantenspeicher aus zwei Quantenregistern in einer Superposition

$$\alpha \cdot |00\rangle + \beta \cdot |01\rangle + \gamma \cdot |10\rangle + \delta \cdot |11\rangle$$

mit

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1 \quad .$$

Die konkrete Superposition

$$\frac{1}{2} \cdot |00\rangle + \frac{1}{2} \cdot |01\rangle + \frac{1}{2} \cdot |10\rangle + \frac{1}{2} \cdot |11\rangle$$

mit $\alpha = \beta = \gamma = \delta = \frac{1}{2}$ beschreibt die Situation, in der alle vier klassisch möglichen Inhalte dieselbe Wahrscheinlchkeit von

$$\alpha^2 = \beta^2 = \gamma^2 = \delta^2 = \left(\frac{1}{2}\right)^2 = \frac{1}{4}$$

haben, bei einer Messung gesehen zu werden.
Betrachten wir die Superposition

$$0 \cdot |00\rangle + 0 \cdot |01\rangle + 0 \cdot |10\rangle + 1 \cdot |11\rangle \quad ,$$

so liefert, weil $\alpha = \beta = \gamma = 0$ und $\delta^2 = 1^2 = 1$, jede Messung mit Sicherheit den klassischen Inhalt

$$|1\rangle \quad .$$

Bei der Superposition

$$\frac{1}{\sqrt{2}} \cdot |00\rangle + 0 \cdot |01\rangle + 0 \cdot |10\rangle + \frac{1}{\sqrt{2}} \cdot |11\rangle$$

können nur die zwei Resultate $|00\rangle$ und $|11\rangle$ gemessen werden, und zwar beide mit der gleichen Wahrscheinlichkeit von $\frac{1}{2}$.

Aufgabe 22

Wie sehen im allgemeinen die Superpositionen von drei Quantenbits aus?

(a) Schreiben Sie eine Superposition von drei Quantenbits nieder, in der alle Inhalte von drei Registern dieselbe Wahrscheinlichkeit haben, gemessen zu werden.

(b) Geben Sie einer Superposition von drei Quantenbits an, in der der Inhalt $|111\rangle$ mit Wahrscheinlichkeit $\frac{1}{2}$, der Inhalt $|000\rangle$ mit Wahrscheinlichkeit $\frac{1}{4}$ und alle restlichen Inhalte mit der jeweils gleichen Wahrscheinlichkeit gemessen werden können.

5+10 Punkte

Welche Operationen sind in der Quantenwelt möglich? Wie kann eine Superposition in einem Quantenrechenschritt in eine andere Superposition übergehen? Es sind alle Rechenschritte möglich, die man durch die Multiplikation der Superpositionen als Vektoren mit

gewissen speziellen Matrizen realisieren kann. Diese Matrizen haben die besondere Eigenschaft, aus jeder Superposition in jedem Fall wieder eine Superposition zu erzeugen.
Wir fahren nun für an der Mathematik besonders Interessierte fort.
Eine Superposition

$$\alpha_1 \cdot |00\rangle + \alpha_2 \cdot |01\rangle + \alpha_3 \cdot |10\rangle + \alpha_4 \cdot |11\rangle$$

kann man als einen Spaltenvektor

$$\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix}$$

darstellen. Einen Zeilenvektor kann man mit einem Spaltenvektor wie folgt multiplizieren:

$$(\beta_1, \beta_2, \beta_3, \beta_4) \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \alpha_1\beta_1 + \alpha_2\beta_2 + \alpha_3\beta_3 + \alpha_4\beta_4 \quad .$$

Das Resultat ist nur eine komplexe Zahl (kein Vektor). Eine $n \times n$-Matrix kann man als n Zeilenvektoren ansehen. Zum Beispiel besteht die 4×4-Matrix

$$M = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{pmatrix}$$

aus den vier Zeilenvektoren

$$\begin{array}{c} (a_{11}, a_{12}, a_{13}, a_{14}) \\ (a_{21}, a_{22}, a_{23}, a_{24}) \\ (a_{31}, a_{32}, a_{33}, a_{34}) \\ (a_{41}, a_{42}, a_{43}, a_{44}) \end{array}$$

Nun ergibt die Multiplikation von M mit $\alpha = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)^{tr}$ wieder einen Vektor $\mu = (\mu_1, \mu_2, \mu_3, \mu_4)^{tr}$, in dem die i-te Position dem Produkt des i-ten Zeilenvektors von M mit α entspricht. Genauer:

$$M \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \mu_3 \\ \mu_4 \end{pmatrix} \quad ,$$

wobei

$$\begin{aligned}\mu_i &= (a_{i,1}, a_{i,2}, a_{i,3}, a_{i,4}) \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{pmatrix} \\ &= a_{i,1} \cdot \alpha_1 + a_{i,2} \cdot \alpha_2 + a_{i,3} \cdot \alpha_3 + a_{i,4} \cdot \alpha_4 \quad .\end{aligned}$$

Die Anwendung von M auf eine Superposition betrachtet man als einen Rechenschritt. Wenn für jede Superposition α (als Spaltenvektor) das Resultat $M \cdot \alpha$ auch eine Superposition ist (in unserem Beispiel bedeutet dies: $\mu_1^2 + \mu_2^2 + \mu_3^2 + \mu_4^2 = 1$), dann ist M als eine Rechenoperation erlaubt.
Im folgenden Beispiel zeigen wir, wie ein Quantenrechner zufällige Bits generieren kann.

Beispiel. Wir haben ein Quantenbitregister zur Verfügung, beginnen mit der „klassischen“ Superposition

$$|0\rangle = 1 \cdot |0\rangle + 0 \cdot |1\rangle$$

und führen einen Rechenschritt aus, indem wir die *Hadamard-Matrix*

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

mit dieser Superposition multiplizieren:

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \cdot \frac{1}{\sqrt{2}} + 0 \cdot \frac{1}{\sqrt{2}} \\ 1 \cdot \frac{1}{\sqrt{2}} + 0 \cdot \left(-\frac{1}{\sqrt{2}}\right) \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \quad .$$

Also erhalten wir die Superposition

$$\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle \quad .$$

Wenn wir nun messen, so erhalten wir die beiden klassischen Bits $|0\rangle$ und $|1\rangle$ mit derselben Wahrscheinlichkeit von $\frac{1}{2}$.
Wenn wir stattdessen mit der „klassischen“ Superposition

$$|1\rangle = 0 \cdot |0\rangle + 1 \cdot |1\rangle$$

starten und wiederum einen Rechenschritt durch die Multiplikation mit H_2 durchführen, so erhalten wir

$$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \cdot \frac{1}{\sqrt{2}} + 1 \cdot \frac{1}{\sqrt{2}} \\ 0 \cdot \frac{1}{\sqrt{2}} + 1 \cdot \left(-\frac{1}{\sqrt{2}}\right) \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} \quad .$$

Das Resultat ist die Superposition

$$\frac{1}{\sqrt{2}} \cdot |0\rangle - \frac{1}{\sqrt{2}} \cdot |1\rangle \quad .$$

Weil $\alpha^2 = \left(\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ und $\beta^2 = \left(-\frac{1}{\sqrt{2}}\right)^2 = \frac{1}{2}$ gilt, liefert eine Messung wieder die beiden klassischen Bits $|0\rangle$ und $|1\rangle$ mit der gleichen jeweiligen Wahrscheinlichkeit von $\frac{1}{2}$. Was bedeutet dies? Wir erhalten in beiden Fällen ein zufälliges Bit, aber wir können nicht erkennen, welche der beiden Superpositionen $\frac{1}{\sqrt{2}} \cdot |0\rangle + \frac{1}{\sqrt{2}} \cdot |1\rangle$ und $\frac{1}{\sqrt{2}} \cdot |0\rangle - \frac{1}{\sqrt{2}} \cdot |1\rangle$ wir gemessen haben.

Aufgabe 23

Geben Sie noch mindestens zwei weitere Superpositionen eines Quantenbits an, in welchen bei einer Messung beide Messwerte $|0\rangle$ und $|1\rangle$ gleichwahrscheinlich sind. **10 Punkte**

Bonus-Aufgabe 8

Beweisen Sie, dass H_2 die Eigenschaft hat, dass

$$\begin{pmatrix} \gamma \\ \delta \end{pmatrix} := H_2 \cdot \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

für jede Superposition $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ wieder eine Superposition ist, dass also $\gamma^2 + \delta^2 = 1$ gilt. **10 Bonus-Punkte**

Bonus-Aufgabe 9

Alle Berechnungen eines Quantenrechners sind reversibel. Wenn man nicht misst, wodurch die erreichte Superposition zerstört würde, besteht immer die Möglichkeit, die Berechnung durch zulässige Rechenschritte zum Ausgangspunkt zurückzuführen. In unserem Beispiel bedeutet dies, dass es eine 2×2-Matrix M gibt, so dass

$$M \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \text{und} \quad M \cdot \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad .$$

Finden Sie die Matrix M. **10 Bonus-Punkte**

Ihre Lösungen zu den Aufgaben können Sie entweder persönlich bei der Open-Class-Veranstaltung am 18. Januar 2006 abgeben oder bis zum 18. Januar per E-Mail (möglichst als PDF-Datei) an `hjb@inf.ethz.ch` oder per Post an folgende Adresse schicken:

Dr. Hans-Joachim Böckenhauer
Informationstechnologie und Ausbildung
ETH Zentrum CAB F 11.1
Universitätsstrasse 6
8092 Zürich

Bitte vergessen Sie nicht, Ihre Lösung mit Ihrem Namen und Ihrer E-Mail-Adresse zu versehen.
Falls Ihre Lösung uns bis zum 16. Januar 2006 erreicht, können Sie die korrigierte Lösung bereits in der Veranstaltung am 18. Januar abholen (sonst bei der nächsten Veranstaltung).