Quantum Computation:
Zusammenfassung der 1. Vorlesung (17.10.08)

1 *Klassischer und Quanten- Kalkül*

1.1 *Klassische und Quanten- Information*

Gegenstände der klassischen Informationstheorie sind Zeichenreihen der endlichen Länge N mit Zeichen aus einem Alphabet der endlichen Länge M. Eine bestimmte Zeichenreihe wird auch Wort genannt. Da die Buchstaben in einem Alphabet angeordnet sind, kann man sie von 0 bis $M-1$ durchnumerieren und durch die Nummer der Stelle erzetzen, an der sie stehen. Damit sind unmittelbar auch die möglichen Worte, die gebildetwerden können, durchnumeriert, wenn man die Zeichenreihe

$$b_1 b_2 b_3 \dots b_N$$

als N-adische Zahl liest. Offenbar lassen sich M^N Wörter bilden, die bei Numerierung im Dezimalsystem an k-ter Stelle stehen:

$$0 \leq k = b_1 M^{N-1} + b_2 M^{N-2} + \dots + b_N M^0 \leq M^N - 1.$$

Neben den M^N "reinen" Wörtern werden auch die statistischen Gemische on Wörtern betrachtet. Konkret kann man sich ein solches Gemisch durch einen Zufallsdrucker realisiert denken, der auf Knopfdruck mit der Wahrscheinlichkeit p_k das k-te Wort druckt. Stellt man die k reinen Wörter durch k paarweise verschiedene Punkte Q_k eines affinen Raumes dar, von denen keine drei auf einer Geraden liegen, dann sind nach Wahl eines Ursprungs O die statstischen Gemische durch die Punkte R mit

$$\vec{OR} = \sum_{k=0}^{M^N-1} p_k \vec{OQ}_k, \quad p_k \geq 0, \quad \sum_{k=0}^{M^N-1} p_k = 1$$

dargestellt. Die statistischen Gemische bilden somit die konvexe Hülle der Q_k, die geometrisch die Ecken (Extremalpunkte) eines Polyeders sind.

Gegenstände der Quanteninformationstheorie sind anstelle von Zeichenreihen der endlichen Länge N mit Zeichen aus einem Alphabet der endlichen Länge M Wellenfunktionen

$$\Psi \in (\mathbf{C}^M)^{\otimes N}, \quad \|\Psi\| = 1,$$

genauer gesagt die von Ψ erzeugten Einheitssstrahlen in $(\mathbf{C}^M)^{\otimes N}$, da ein Phasenfaktor keine Rolle spielt. Konkret hat man sich unter Ψ den Zustand eines Systems aus N Atomen mit je M Anregungszuständen vorzustellen. Die Anregungszustände entsprechen den Buchstaben des klassischen Alphabets. An die Stelle von M^N reinen Wörtern tritt das $2(MN-1)$-dimensionale Kontinuum der Zustände Ψ. Im Gegensatz zur klassischen Informatinstheorie, in der ein Wort stets erkennbar ist, ist (am einzelnen System) Ψ ohne Vorkenntnis unerkennbar. Wenn man die Observable

$$A = \sum_{k=0}^{M^N-1} k|(k)><(k)|, \qquad \text{wobei} \quad |(k)>=|b_1>\otimes|b_2>\otimes\cdots\otimes|b_N>$$

und b_i den Anregungszustand des i-ten Atoms bezeichnet, misst, erhält man mit der Wahrscheinlichkeit $p_k = |<(k)|\Psi>|^2$ den Wert k. Pei Idealmessung mit dem Ergebnis k weiß man, dass nach der Messung das System im Zustand $|(k)>$ ist, der dem k-ten klasischen Wort entwpricht. Aber der Zustand Ψ vor der Messung nleibt unerkannt. Selbst wenn man in einer Versuchsreihe die Wahrscheinlichkeiten p_k bestimmt, bleibt Ψ unerkannt. Die Realität eines Zustandes besteht darin, dass man ihn bei Kenntnis beliebig oft präparieren kann, z. B. durch Idealmessung von $|\Psi><\Psi|$ und Selektion nach dem Messwert k. Erkennbar ist der Zustand am einzelnen System nicht. Durch Messung erhält man nur eines der 2^N klassischen Wörter. Man kann sagen, dass der Nutzen der Quantenrechner hauptsächlich in der größeren Vielfalt der Algorithmen, die insbesondere das Überlagerungsprinzip ausnutzen können, besteht.

1.2 *Der Fall M=2: N=1. Bit und Qubit*

Der Fall $M = 2$, $N = 1$, ein Zeichen $x \in \{0, 1\}$, wird (ein) Bit genannt. Ensprechend heisst der Zustand eines 2-Niveau Systems, $\psi \in \mathbf{C}^2$, (ein) Qubit. Wenn wir die länge des latienischen Alphabets mit Klein- und Großbuchstaben, einer Leerstelle und Interpunktionszeichen mit 64 ansetzen, benötigt ein Buchstabe die Speicherkapazität von 6 Bit.

Die große Bedeutung von in Bit ausgedrückter klassischeer Information liegt in der unserem Denken angepassten Verarbeitung, die darin besteht, aus

$$\{0,1\}^N \ni x_1x_2\ldots x_N \mapsto y_1y_2\ldots y_{\tilde{N}} \in \{0,1\}^{\tilde{N}}$$

zu erzeugen, wobei Funktionen

$$y_j = F_j(x_1 x_2 \dots x_N), \quad (j = 1, 2, \dots, \tilde{N})$$

das gewünschte Resultat festlegen. Solche Funktionen werden in der klassischen Aussagenlogik als "Wahrheitswertfunktoren" analysiert und aus elementaren, d.h. im Allgemeinen monadischen und dyadischen, Funktoren aufgebaut. Ein analoges Verfahren für die Verarbeitung der in Qubit ausgedrükten Quanteninformation werden wir noch kennen lernen.

Jede Qubitwellenfunktion lässt sich in der Form

$$\psi = e^{i\tau}(\cos\frac{\Theta}{2}|0> + e^{i\Phi}\sin\frac{\Theta}{2}|1>), \quad \tau \in \mathbf{R}, \quad \tau \text{ beliebig}$$

schreiben. Im Hinblick aud die Darstellung statistischer Gemische von Qubitzuständen ist es praktisch, die reinen Qubitzustände gleich als Projektionsopersatoren vom Rang 1 zu schreiben: $|\psi><\psi|$. Für die Wahrscheinlichkeiten gilt dann $p_i = \mathrm{tr}(|\psi><\psi|x><x|) = |<\psi|x>|^2$, $x \in \{0, 1\}$. Nun ist

$$\begin{aligned}
|\psi><\psi| &= (\cos\frac{\Theta}{2}|0> + e^{i\Phi}\sin\frac{\Theta}{2}|1>)(\cos\frac{\Theta}{2}<0| + e^{-i\Phi}\sin\frac{\Theta}{2}<1|) \\
&= \cos^2\frac{\Theta}{2}|0><0| + \sin^2\frac{\Theta}{2}|1><1| \\
&\quad + (\cos\Phi - i\sin\Phi)\cos\frac{\Theta}{2}\sin\frac{\Theta}{2}|0><1| \\
&\quad + (\cos\Phi + i\sin\Phi)\cos\frac{\Theta}{2}\sin\frac{\Theta}{2}|1><0| \\
&= \frac{1}{2}(1+\cos\Theta)|0><0| + \frac{1}{2}(1-\cos\Theta)|1><1| \\
&\quad + \frac{1}{2}\cos\Phi\sin\Theta(|0><1| + |1><0|) \\
&\quad - \frac{i}{2}\sin\Phi\sin\Theta(|0><1| - |1><0|) \\
&= (|0> |1>)\frac{1}{2}(\mathbf{1} + \vec{e}(\Theta,\Phi)\cdot\vec{\sigma})\begin{pmatrix} <0| \\ <1| \end{pmatrix},
\end{aligned}$$

dabei ist im $\mathbf{R}^3$

$$\vec{e}(\Theta,\Phi) = \cos\Phi\sin\Theta\vec{e_1} + \sin\Phi\sin\Theta\vec{e_2} + \cos\Theta\vec{e_3}, \quad \vec{\sigma} = \sigma_1\vec{e_1} + \sigma_2\vec{e_2} + \sigma_3 e_3,$$

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Damit ist eine bijektive Abbildung der reinen Qubitzustände auf die Einheitssphäre im $\mathbf{R}^3$ definiert, die in diesem Zusammenhang Blochsphäre genannt wird:

$$|\psi><\psi| \mapsto \vec{e}(\Theta, \Phi)$$

Diese Abbildung ist offensichtlich auch affin: Ist $|\phi><\phi|$ ein weiterer reiner Qubitzustand ist und $|\phi><\phi| \mapsto \vec{e}(\Sigma, \Lambda)$, dann gilt

$$p|\psi><\psi| + (1-p)|\phi><\phi| \mapsto p\vec{e}(\Theta, \Phi) + (1-p)\vec{e}(\Sigma, \Lambda), \quad 0 \leq p \leq 1.$$

Die statistischen Gemische von Qubitzuständen werden somit auf das Innere der Einheitskugel im $\mathbf{R}^3$ bijektiv und affin abvgebildet. Die Einheitskugel im $\mathbf{R}^3$ heißt in diesem Zusammenhang Blochkugel. Jeder reine oder statistisch gemischte Qubitzustand ρ kann daher als Dichtematrix eindeutig in der Form

$$\rho == \frac{1}{2}(\mathbf{1} + \vec{r} \cdot \vec{\sigma}), \quad r = \|\vec{r}\| \leq 1$$

geschrieben werden. $\vec{r}$ heißt der Blochvektor von ρ. Die Pole der Blochkugel sind die Bilder der Zustäne $|0>$ und $|1>$, der inerhalb der Blochkugel verlaufende Abschnitt der Polarachse ist die Bildmenge der statistischen Gemische dieser Zustände.

Die Blochkugel ist ein anschauliches Bild der Qubitzustände. Der in der Blochkugel verlaufende Abschitt der Polarachse wird im Allgemeinen mit dem klassischen Bit und seinen statistischen Gemischen identifiziert. Dem entspricht die Qubitobservable $A = |1><1|$ mit den Eigenwerten 0 und 1. Das Ergebnis einer Idealmessung von A an einem Qubit im Zustand $\psi = \cos\frac{\Theta}{2}|0> + e^{i\Phi}\sin\frac{\Theta}{2}|1>$ ist mit der Wahrscheinlichkeit

- $p = \frac{1}{2}(1 - cos\Theta)$ der Wert 1, und in diesem Fall ist der Zustand des Qubits nach der Messung $|1>$,
- $1 - p = \frac{1}{2}(1 + cos\Theta)$ der Wert 0, und in diesem Fall ist der Zustand des Qubits nach der Messung $|0>$,

Ist der Zustand des Qubits vor der Messung unbekannt, dann liefert die Messung keine Kenntnis über diesen Zustand. Nur wenn man vorher schon weiß, dass der Zustand vor der Messung ein Eigenzustand von A ist, bestimmt die Messung diesen Zustand.

Messungen von A in einer Versuchsreihe mit einer Gesamtheit von Qubits in einem unbekannten Zustand ρ erlauben es, die Wahrscheinlichkeit p genähert

zu bestimmen. Da p nur von dem Winkel Θ abhängt, ist im $\mathbf{R}^3$ eine zur Polarachse senkrechte Ebene bestimmt, die diese im Punkt mit den Koordinaten $(0, 0, -\cos\Theta)$ schneidet. Genau die statistischen Gemische von Qubitzuständen, die durch Punkte dieser Ebene in der Blochkugel dargestellt werden, liefern die Wahrscheinlichkeit p. Aus Symmetriegründen gilt dieser geometrische Sachverhalt nicht nur bei Messungen der Observablen $|1><1|$ sondern für jede Qubitobservable. Man überlegt sich leicht, dass es möglich ist, mit drei Versuchsreihen, in denen je eine von drei geeigneten Observablen gemessen wird, den Zustand ρ einer Gesamtheit approximativ zu bestimmen.