Zusammenfassung der 1. Vorlesung (12.04.2010)

1. Klassische Information und Quanteninformation

1.1 *Vorwort* : Die klassische Informationstheorie wurde von dem Mathematiker Claude Elwood Shannon (1916-2001) begründet. Als Ursprung gilt seine Arbeit *A Mathematical Theory of Communication* [Bell System Technical Journal. Short Hills N.J. 27, 379-423, 623-656 (1948)]. Die Quanteninformationstheorie entstand etwa 50 Jahre später und ist weniger scharf zu datieren. Eine wichtige Rolle spielte dabei Charles H.Bennett ($\star$1943), der als Computerwissenschaftler bei IBM gundlegende Ideen zur Quantencommunikation und zu Quantenrechnern entwickelt hat. Zusammen mit Gilles Brassard ($\star$1955) entwickelte er am Ende der achtziger Jahre Konzepte zur Quantenkryptographie. 1993 entdeckten Bennett und Brassard die Teleportation. Diese ermöglicht es zum einen, überhaupt Quantenzustände von einem Quantensystem auf ein zweites zu übertragen, und zum anderen kann sich das zweite Quantensystem in beliebiger Entfernung von ersten befinden, wenn nur die Möglichkeit klassischer Kommunikation zwischen den beiden Orten besteht. Die Teleportation ist eine tiefsinnige Anwendung der von Albert Einstein, Boris Podolsky und Nathan Rosen [Phys. Rev. 47, 777 (1935)] erdachten Situation, in der das Ergebnis einer Messung an einem Teilchen instantan eine bestimmte Zustandsänderung an einem anderen Teilchen verursacht, das sich in raumartiger Entfernung vom ersten befindet. Da für die am ersten Teilchen gemessene Eigenschaft eine Wahlfreiheit zwischen komplmentären Eigenschften besteht und die Zustandsänderung des zweiten Teilchens von der getroffenen Wahl entscheidend abhängt, aber instantane Wirkungsaubreitung unmöglich ist, schlossen Einstein, Podolsky und Rosen (EPR), dass die Quantenmechanik noch keine endgültige Beschreibung der Wirklichkeit liefern kann. Da für EPR nur klassische Korrelationen vorstellbar waren, mussten sie annehmen, dass in den Teilchen komplementäre Eigenschaten realisiert sind, Elemente der Realität, die die Quantenmechanik nicht beschreibt. Dies stand im Widerspruch zur Auffassung von Niels Bohr, der die Quantenmechanik schon als endgültige Theorie anerkannt hatte. Es ist erwähnenswert, dass Erwin Schrödinger [Die Naturwissebscften 23, 807 (1935)] den Zustand des aus zwei Teilchen bestehenden Systems in der EPR-Situation "verschränkt" nannte. So heißt seither die Eigenschaft von Zuständen quantenmechanischer Mehrteilchensysteme, die solche merkwürdigen

Quantenkorrelationen beinhalten, wie sie in der EPR-Situation beschrieben sind. Die Verschränktheit (engl. entanglement), die es in der klassischen Physik nicht gibt, spielt heute eine Zentrale Rolle bei der Verarbeitung von Quanteninformation. Kann es, wie Einstein, Podolski und Rosen behauptet haben, Elemente der Wirklichkeit geben, die die Quantenmechanik micht beschreibt? Nachdem David Bohm die EPR-Situation für Spinsysteme formuliert und damit durchsichtiger gestaltet hatte, stellte John Stewart Bell [*On the Einstein-Podolsky-Rosen paradox*, Physics. 1, No. 3, 195-200 (1964)] eine Ungleichung für Korrelationen auf, die erfüllt sein muss, wenn solche Elemente vorhanden sind, aber verletzt, wenn es solche Elemente nicht gibt. Alain Aspect, Jean Dalibard, Gérard Roger [*Experimental Test of Bell's Inequalities Using Time-Varying Analyzers*, Phys. Rev. Lett.. 49, No. 25, 1804-1807 (1982)] hat entsprechende Experimente mit Photonenpaaren, deren Polarisation veschränkt ist, durchgefüht und die Verletzung der Bellschen Ungleichung nachgewiesen. Es ist erstaunlich, dass erst im Zuge der auf das experimentelle Egebnis von Alain Aspect neu entfachten Diskussion über die Quantenmechanik die Quanteninformationstheorie entstanden ist, nachdem das von Einstein, Podolski und Rosen beschriebene zentrale Werkzeug, die Quantenkorrelation, ein halbes Jahrhundert trotz heftiger Diskussionen ungenutzt geblieben war. Allerdings ging es EPR damals nicht um das Aufzeigen von Quantenkorrelationen, sie hatten lediglich auf Korrelationen in der Quantenmechanik hingewiesen, die klassisch nicht verständlich sind, ohne die Quntenmechanik als vorläufige Theorie anzusehen. Die eigentliche Bedeutung der Quantenkorrelationen wurde erst erkannt, nachdem experimentell erwiesen war, dass die Quantenmechanik die Bellsche Ungleichung nicht erfüllt.- Neben der Teleportation wird als bedeutender früher Erfolg der Quantenalgorithmus von Peter Shor ($\star$1959) [*Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer*, SIAM Journal on Computing 26, 1484-1509 (1997)] angesehen. Klassische Rechner benötigen zur Faktrisierung Laufzeiten, die mit der Stellenzahl exponentiell anwachsen, während die Laufzeit des Shor-Algoritmus dazu nur logarithmisch mit der Stellenzahl anwächst.

Gegenstand der klassischen Informationstheorie sind Zeichenreihen einer Länge N mit Zeichen aus einem Alphabet, das M parrweise unterscheidbare Zeichen enthält,

$$x_1x_2x_3\ldots x_N, \qquad x_i \in \mathcal{A}_M = \{b_0, b_1, b_2, \ldots, b_{M-1}\}.$$

Jede bestimmte Zeichenreihe heißt ein Wort. Das Wort ist eine Kombination mit Wiederholung und mit Berücksintigung der Reihenfolge, es lassen sich also M^N Wörter bilden. Zum Beispiel ist beim lateinischen Alphabet mit Groß- und Kleinschreibung, einigen Interpunktionszeichen und einer Leerstelle ungefähr $M = 64$. Man darf sich in der Informationstheorie aber nicht dazu verleiten lassen, mit einigen Wörtern Assoziationen zu verbinden: Die Informationstheorie kümmert sich nicht um die semiotische Bedeutung der Wörter, sondern nur darum, was quantitativ an Information in einem Wort enthalten ist. Dabei kommt es nicht auf die Reihenfolge der Zeichen an, sonder nur au die Wahrscheinlichkeiten, mit denen die einzelnen Buchstaben im Wort anzutreffen sind. Es ist einsichtig, dass in einem Wort, in dem nur wenige der M Zeichen vorkommen, weniger Information enthält als ein Wort, das mehr der M Zeichen enthält. Den geringsten Informationsgehalt haben Wörter, in denen nur ein und dasselbe Zeichen (mit der Wahrscheinlichkeit 1) vorkommt. Plausible Axiome über die Information führen auf die Shannon Entropie

$$S = \sum_{0}^{M-1} p_i \log \frac{1}{p_i} = -\sum_{0}^{m-1} p_i \log 1 p_i$$

als Maß für den Informationsgehalt. Ein Wort in dem nur ein Zeichen vorkommt enthält demnach keine Information. Ein Wort, in dem alle Zeichen mit gleicher Wahrscheinlichkeit vorkommen, entwa im Fall $N = kM$, $k \in \mathbf{N}$, hat die maximale Information $S = \log M$, also 1, wenn der Logarithmus zur Basis M genommen wird. Neben der Shannon Entropie gibt es weitere Informationsmaße, die verschienen Fragestellungen angepasst sind. Ein wichtiges Problem, das die Informationstheorie behandelt, ist die unwillkürliche Veränderung von Zeichenreihen, die auftritt, wenn Information übertragen wird. Der sogenannte Informationskanal kann Störungen verursachen, die darin bestehen, dass vom Sender (heute im Allg. mit Alice bezeichnet) ausgehende Zeichen vom Empfänger (heute im Allg. mit Bob bezeichnet) nicht unterschieden werden können (Äquivokation). Dies mindert die empfangene Information. Andererseits vermehrt Rauschen die von Bob empfangene Information, die aber irrelevant ist, weil sie von Alice nicht gesendet wurde. Wieviel Information wird wirklich übertragen (Transinformation (engl. mutual information)? Diese Frage wurde von Shannon in seiner eingangs zitierten ursprünglichen Arbeit behandelt. Ein ebenso wichtiges Problem ist die willkürliche Veränderung von Zeichenreihen nach Gesetzen der formalen Logik (Algorithmen), die in Rechnern vollzugen wird.

Schließlich ist die Verschlüsselung von Zeichenreihen, die Cryptographie, ein wichtiges Problem.

Man denke sich nun ein Quantensystem, das M stationäre Anregungszustänede hat. Ein solches System wird in einem Hilbertraum $\mathcal{H}$ der Dimension M etwa mit dem Hamiltonoperator

$$H = \sum_{k=0}^{M-1} k|k><k|$$

beschrieben, dessen Eigenwerte der Eifachheit halber als $k = 0, 1, 2, 3, \ldots, M-1$ angenommen werden, wobei $|k>$ die Basis der normiertef Eigenzustände ist und $|k><k|$ Die Eigenprojektoren sind, $|k><k|\psi := |k><k|\psi>$, so dass

$$H|j>= j|j>$$

ist. Man kann sich nun anstelle des Zeichens $x_1 = b_j$ das System im j-ten Anregungszustand denken. Das Zeichen b_j ist dann zwar nicht mehr direkt erkennbar, aber wenn man weiß, dass sich das System in einem Eigenzustand von H befindet, ist das Ergebnis einer Idealmessung von H der Eigenwert, ohne dass der Zstuand des Systems durch die Messung verändert wird. Betrachtet man nun ein System, das aus N solcher Atome zusammengesetzt ist und sich ein jedes dieser Atome in einem Eigenzustand von H befindet, dann stallt dieses System ein klassisches Wort $x_1x_2x_3 \ldots x_N$ dar, das durch Idealmessung von H an jedem Teilsystem festgestellt werden kann, ohne den Zustand des Systems zu verändern. Auf ndiese Weise ist klassische Informatio durch den Zustand eines Quantensystem dargestellt.

Nun müssen die Zustände der Teilsysteme nicht Eigenzustände von H sein, sondern der Zustan d des l-ten Teilsystems kann

$$\psi_l = \sum_{k=0}^{M-1} c_l|k>, \qquad \sum_{k=0}^{M-1} |c_l|^2 = 1,$$

sein. Dann liefert die oben beschriebene Messung zwar auch ein Wort, aber dieses ist vor der Messung unbestimmt. Eine Idealmessung von H am l-ten Teilsystem ergibt bekanntlich mit der Wahrscheinlichkeit

$$p_l(k) = | < \psi_l|k > |^2$$

den Wert k. Die kombinierte Messung von H an allen Teilsystemen liefert dann mit der Wahrscheinlichkeit

$$p(x_1x_2x_3\ldots x_N) = \prod_{l=1}^{N} | < \psi_l|k_i > |^2$$

das Wort $x_1x_2x_3\ldots x_N$. Dies ist aber noch nicht alles, was die Quaanteninformation von der klassischen unterscheidet. Der bisher betrachtete Zustand des Quantensystems ist 'separabel', er enthält keinerlei Korrelationen von Eigenschaften der verschiedenen Teilsysteme. Der Zustand kann aber Verschränkungen enthalten, die Quantenkorrelationen von Eigenschaften verschiedener Teilsysteme beinhalten. Schließlich muss der bestrachtete Zustand nicht 'rein' sein, er kann auch ein v. Neumann Gmisch sein. Statistische Gemische von Zuständen sind in der klassischen Physik bekannt, die Mischungskomponenten wie auch die Mischungsverhältnisse liegen dabei stets eindeutig fest. Dies ist bei statistischen Gemischen von Quantenzuständen nicht so. Deshalb tragen sie den Namen V. Neumann Gemische. Ein und dasselbe v. Neumann Gemisch kann aus unterschiedlichen Komponenten statistisch zusammengemischt werden und auch nach unterschedlichen Komponenten sortiert werden.

Dazu ist noch ein kurzer Kommentar am Platze: Ein Skatspiel besteht aus 32 Karten und stellt ein statistisches Gemich aus den vier Farben dar, die gleich verteilt sind. Nach dem Mischen ist mit der Wahrscheilichkeit (1/4) die obere Karte Herz. Bei den gegebenen ll Karten sind die Farben anders verteilt, es ist ein anderes statistisches Gemisch aus den vier Farben. Spielkarten in den vier Farben liegen als Mischungskomponenten fest. Dies ist bei v, Neumann Gemischen der Quantetheorie nicht so: Wären die Spielkarten Quantenobjekte, dann könnte es sein, das ein und dasselbe Gemisch sowohl durch die Farben Kreuz und Piek, wie auch durch die Farben Herz und Karo zusammengesetzt werden könnte. Anders ausgedrückt, ein v. Neumann Gemisch aus den Farben Kreuz und Piek könnte nach den Farben Herz und Karo sortiert werden.

An die Stelle von M^N Zeichenreihen in der klassischen Informationstheorie treten also alle Zustände eines Quantensystems, das in einem Hilbertraum $\mathcal{H}$ der Dimension M^N beschrieben wird, als Gegenstand der Quanteninformationstheorie. Die maximal M^N paarweise verschiedenen Eigenwerte einer Observablen stellen klassische Information dar. Das Ergebnis einer Messung

dieser Observablen ist im Allgemeinen zufällig. An die Stelle von Gesetzen der formalen Logik treten geteuerte Prozesse der Schrödingerdynamik, d.h. unitäre Operationen, und Messoperationen bei der willkürlichen Veränderung des Quantenzustandes. Während die logischen Operationen der klassiscen Informationstheorie auch irreversibel sein können, indem von der sich ergebenen Zeichenreihe nicht auf die ursprüngliche zurückgeschlossen weden kann, sind unitäre Operationen stets reversibel. Bei den unwillkürlichen Veränderungen des Zustandes ist die Dekohärenz zu erwähnen, wobei Wechselwirkungen mit der Umgebung den Übergang reiner Zustände in v. Neumann Gemische verursachenund somit Verschränktheiten zerstören.

Die Zustände der Quantenmechanik bilden eine konvexe Menge, deren Extremalpunkte 'reine' Zustände genannt werden. Bevor wir dies am Beispiel eines Qubits, das ein Quantensystem mit nur zwei Anregungszuständen ist, genauer betrachten, wollen wir noch auf die operationale Definition statistischer Gemische eingehen und die Darstellung der v. Neumann Gemische im Hilbertraum eingehen. Bisher hatten wir nur reine Zustände der Quantenmechanik betrachtet, die durch Vektoren $\psi \in \mathcal{H}$, $\|\psi\| = 1$ dargestellt waren. Der Erwartungswert eines selbstadjungierten Operators A ist dann

$$< A >_\psi =< \psi, A\psi > .$$

Da wir hier Hilberträume endlicher Dimension betrachten, können wir für jeden linearen Operator B mit einer Orthonormalbasis $\{\phi_j\}$ die Spur

$$\mathrm{tr}(B) = \sum_j < \phi_j, B\phi_j >$$

bilden und es gilt

$$\mathrm{tr}(AB) = \sum_{jk} < \phi_j, A\phi_k >< \phi_k, B\phi_j >= \mathrm{tr}(BA).$$

Aus der letzten Gleichung folgt, weil jede andere Orthonormalbasis $\{\varphi_j\}$ mit einem unitären Operator U durch $\varphi_j = U\phi_j$ darstellbar ist,

$$\sum_j < \varphi_j, B\varphi_j >= \sum_j < U\phi_j, BU\phi_j >=$$
$$\sum_j < \phi_j, U^+BU\phi_j >= \mathrm{tr}(U^+BU) = \mathrm{tr}(UU^+B) = \mathrm{tr}(B).$$

Die Spur ist also wohldefiniert (unabhängig von der Basis, in der sie berechnet wird) und ist ein lineares Funktional auf den linaren Operatoren auf $\mathcal{H}$.