Zusammenfassung der 1. Vorlesung (20.04.09)

1. Klassische Information und Quanteninformation

1.1 *Was ist Information?* : Man kann sagen, Information sei alles, was von der totalen Eintönigkeit abweicht. Ein solcher Sachverhalt lässt sich stets umgangssprachlich beschreiben. Allerdings wnrd diese Beschreibung mehr oder weniger unvolkommen sein. Der Eindruck, den das Anhören eines Musikstücks oder die Betrachtumg eines Gemäldes hinterlässt, kann durch die bloße Beschreibung kaum hervorgerufen werden. Jedenfalls ist die Niederschrift der umgangssprachlichen Beschreibung eine, wenn auch im Allgemeinen grobe, Kodierung der durch den Sachverhalt gegebenen Information, die diese in einer Zeichenreihe darstellt. Andere Kodierungen, wie zum Beispiel die Digitalisierung von Musik oder von Bildern, stellen eine feinere Kodierung dar, die ebenfalls als Zeichenreihe aufgezeichnet werden kann. Zeichenreihen sind der Gegenstand der klassischen Informationstheorie.

1.1.1 *Klassische Information* : Unter klassischer Information versteht man eine Zeichenreihe, etwa $x_1x_2x_3\dots x_N$, mit Zeichen aus einem Alphabet mit M Buchstaben, $\mathcal{A}_M = \{b_0, b_1, b_2, \dots, b_{M-1}\}$. Mit einer Zeichenreihe der Länge N lassen sich M^N Wörter bilden, die sich bei Kennzeicchnung der Buchstaben mit den Indizes $j = 0, 1, 2, \dots, M-1$ in natürlicher Weise numerieren lassen: Das Wort $b_{j_1}b_{j_2}b_{j_3}\dots b_{j_N}$ erhält im M-adischen Zahlsystem die Nummer $j_1j_2j_3\dots j_N$, die im Dezimalsystem

$$Z_{10,M}(j_1j_2j_3\dots j_N) = j_1M^{N-1} + j_2M^{N-2} + j_3^{N-3} + \dots + j_{N-1}M + j_N$$

ist. Eine besondere Bedeutung hat das Alphabet $\mathcal{A}_2 = \{0, 1\}$ mit zwei Buchstaben. Das Zeichen $x \in \{0, 1\}$ drückt eine Alternative aus, "ja" oder "nein". Als *binary digit*, kurz **Bit** genannt, stellt es die kleinste Speicherkapazittät dar, die man sich denken kann. Das Bit wird deshalb als Einheit für die Speicherkapazität benutzt. Eine Zeichenreihe aus Bits der Länge N, die die Bildung von 2^N ensprechenden Wörtern zulässt, hat die Kapazität N Bit. Jeder Buchstabe des Alpabets $\mathcal{A}_M$ hat die Kapazität $\log_2 M$ Bit, eine Zeichenreihe der Länge N also die Kapazität $N \log_2 M = \log_2 M^N$ Bit. Jedes Zeichen kann man sich als einen Speicherplatz denken, der $\log_2 M$ Bit aufnehmen

kann. Veranschlagt man die Anzahl der Buchstaben des umgangssprachlichen lateinischen Alphabets mit Groß- und Kleinschreibung, einer Leerstelle und einigen Interpunktionszeichen mit 64, dann hat jeder Buchstabe die Speicherkapazität 6 Bit.

1.1.2 *Quanteninformation* : Unter Quanteninformation versteht man den Zustand eines *N-partiten* (aus N Teilchen zusammengesetzten) Quantensystems, wobei in Analogie zzur klassischen Information im Allgemeinen angenommen wird, dass die Teilchen die gleiche Anzahl M von Anregungszuständen haben, die als stationär vorausgesetz werden. Der Hilbertraum einer Komponente des System ist der Hilbertraum $\mathbf{C}^M$, in dem die Basis der normierten Eigenzustände $\{|i>\}_{i=0,1,2,\ldots,M-1}$ des Operators $A = \sum_{i=0}^{M-1} i|i><i|$ der Anregungszustäde augezeichnet ist. Die Eigenwerte dieses Operators entsprechen den Buchstaben des klassischen Alphabets $\mathcal{A}_M$. Im Hilbertraum des Gesamtsystems $(\mathbf{C}^M)^{\otimes N} \cong \mathbf{C}^{MN}$ ist die Basis

$$|x_1x_2x_3\ldots x_N>:= |x_1>\otimes|x_2>\otimes|x_3>\otimes\cdots\otimes|x_N>,$$

die man die *Compiterbasis* nennt, ausgezeichnet und die Eigenwerte der Observablen des Gesamtsystems

$$\begin{aligned}\mathbf{A} &= \sum_{k=0}^{M^N-1} Z_{10,M}(x_1x_2x_3\ldots x_N)|x_1x_2x_3\ldots x_N><x_1x_2x_3\ldots x_N| \\ &= M^{N-1}A\otimes 1\otimes 1\otimes 1\otimes\cdots\otimes 1 + M^{N-2}1\otimes A\otimes 1\otimes 1\otimes\cdots\otimes 1 + \\ &\quad M^{N-3}1\otimes 1\otimes 1\otimes A\otimes 1\otimes\cdots\otimes 1 + \cdots\cdots + \\ &\quad M^1 1\otimes 1\otimes\cdots\otimes 1\otimes A\otimes 1 + M^0 1\otimes 1\otimes\cdots\otimes 1\otimes A\end{aligned}$$

entsprechen den Nummern der klassischen Worte, die mi t $x_i \in \mathcal{A}_M$ als $x_1x_2x_3\ldots x_N$ gebildet werden können. Liegt etwa der reine Zustand $\Psi \in (\mathbf{C}^M)^{\otimes N} \cong \mathbf{C}^{MN}$ des Gesamtsystems vor, und wird $\mathbf{A}$ ideal gemessen, dann ist die Wahrscheinlichkeit für das sich zufällig ergebende Wort $x_1x_2x_3\ldots x_N$

$$p(x_1x_2x_3\ldots x_N) = |<x_1x_2x_3\ldots x_N|\Psi>|^2.$$

Bei Idealmessung erster Art befindet sich das betreffende Quantensysten nmittelbar nach der Messung in dem Eigenzustand von $\mathbf{A}$, der zu dem Messergebnis gehört. Man geht davon aus, dass jeder Zustand des Gesmtsystems präparierbar ist, d.h. dass es ein experimentelles Verfahren gibt,

das eine Gesamtheit von Systemen liefert, so dass bei beliebigen Messungen genau die nach den Gesetzen der Quantenmechnik bestimmten Wahrscheinlichkeiten verifiziert werden. Im Gegensatz zur klassischen Information, wo das gesprochene oder geschriebene eizelne Wort stets erkennbar ist, ist der Quantenzustand im allgemeinen am einzelnen System unerkennbar. Eine Idealmessung erster Art legt nur den Zustand nach der Messung fest, der Zustand vor der Messung bleibt unerkannt, wenn man nicht vorab weiß, dass sich das System in einem der Eigenzustände befunden hat. Ein Quantensystem, das nur zu zwei Anregungszuständen fähig ist, heißt **Qubit**, das als Kapazitätseinheit dient. Der Hilbertraum eines Qubits ist der $\mathbf{C}^2$ und die Kinematik des Qubits ist deshalb besonders durchsichtig. Wir werden dies noch genauer betrachten. Insbesondere wird dabei die größere Reichhaltigkeit der Quantenzustaände gegenüber denen der ensprechen klassischen Systeme deutlich werdern.

1.1.3 *Gegensätzliches* : Ein klsassisches Wort kann stets kopiert werden, gleeichgültig ob der Ausführende den Inhalt, die Information kennt oder nicht. Ein unbekannter Quantenzustand kann prinzipiell nicht kopiert weden, es gilt das sogenannte *No-Cloning*-Theorem. Ein einfaches Argument gegen die Existenz eines Kopieralgorithmus ist die Tatsache, dass für jedes feste $\varphi \in \mathcal{H}$ und beliebiges $\psi \in \mathcal{H}$ die Abbildung

$$\varphi \otimes \psi \mapsto \psi \otimes \psi$$

nicht linear ist, denn

$$\begin{aligned} \varphi \otimes (c_1\psi_1 + c_2\psi_2) &\mapsto (c_1\psi_1 + c_2\psi_2) \otimes (c_1\psi_1 + c_2\psi_2) \\ &\neq (\varphi \otimes c_1\psi_1) + (\varphi \otimes c_2\psi_2), \end{aligned}$$

und damit nicht das Resultat eines Quantenprozesses sein kann. Um ein tiefer liegendes Argument anzudeuten, ist es vorteilhaft, sich das Observablenkozept der Quantenmechanik zu vergegenwärtigen.

Observablen der Quantenmechanik werden als selbstadjungierte Operatoren A des zugrunde ligendan Hilbertraumes dargestellt. Ein solcher Operator legt eindeutig ein projektionswertiges Spetralmaß auf den Borelmengen der reellen Achse fest, so dass $A = \int \lambda E(d\lambda)$ ist. Bei idealen Messungen von A werden die Spektraloperatoren $E(b)$, wobei b eine Borelmenge ist, durch einen Wechselwirkungsprozess des Quantenobjektes mit einem

Vielteilchensystem erzeugt. Der Erwartungswert von $E(b)$ ist dabei die Wahrscheinlichkeit dafür, dass der Messwert in b liegt. Umgekehrt definiert jeder ideale Messapparat ein projektionswertiges Spekralmaß, das den selbstadjungierten Oprator festlegt, der mit diesem Apparat gemessen wird. Im Sinne der Wahrscheilichkeitstheorie deutet man die Borelmengen b als zufällige Ereignisse, die eintreten, wenn der Messwert in b liegt, oder ausbleiben, wenn dies nicht der Fall ist. Ereignisse, die an ein und demselben idalen Messapparat durch ein Objekt hervorgerufen werden können, sind kommensurabel im Sinne der Quantenmechanik, d.h. es treten keine Unschrferelationnen auf. Es ist zu bemerken, dass die letztere Aussage nur für ideale Messapparate oder 'scharf' messende Apparate gilt, die projektionswertige Maße definieren.

Vor diesem Hintergrund kann man nun folgendes Argument gegen die Kopierbarkeit von Quanteninformation geben: Man geht davon aus, dass man den Ort oder auch den Impuls eines Quantenobjektes beliegig scharf messen kann. Nun sind die kanonischen Vertauschungrelationen grundlegend für die Quantenmechanik. Gäbe es einen Kopiealgorithmus der oben beschriebenen Art, dann könnte ein Objekt an einem Apparat, der erst den Zustand kopiert und dann etwa am Original den Ort und an der Kopie den Impuls misst, Ereignisse hervorrufen, die Ort und Impuls beliebig scharf festlegen. Im Idealfall definiert dieser Apparat ein projektionswertges Spektralmaß auf den Borelmengen der (x, p)-Ebene, das die Spektralmaße von Ort und Impuls marginal enthält. Ort und Impuls wären damit kommensurabel, was der kanonischen Vertauschungsrelation widerspricht. Allerdings würde dieser Apparat heine Idealmessungen erster Art zulassen und damit nicht ermöglichen, Gesamtheiten zu präparieren, die der Heisenbergschen Unschärferelation widersprechen. Dies stellt die Tragfähigkeit dieses Arguments in Frage.

1.3 *Reine und gemischte Zustände* : Grundlage einer operational aufgebauten statistischen Theorie ist eine Menge $\mathcal{P}$ von Präparierverfahren und eine Menge $\mathcal{M}$ von Messverfahren, so dass jede Kombination $(\pi, \mu) \in \mathcal{P} \times \mathcal{M}$ eines Präparierverfahrens mit einem Messverfahren einnen Versuchsaufbau definiert. O.B.d.A. kann man sich darauf beschränken, dass jeder Versuch nur die Messergebnisse 0 oder 1 haben kann. Es ist aber zu fordern, dass für jede Kombination eine hinreichend lange Versuchsreihe, die relativen Häufigkeiten Wahrschreilichkeiten $p_{(\pi,\mu)}(0)$ für das Ergebnis 0 bzw.

$p_{(\pi,\mu)}(1) = 1 - p_{(\pi,\mu)}(0)$ für das Ergebnis 1 annähern, die nur von π und μ abhängigen dürfen. Man definiert $\pi \sim \pi'$, falls $p_{(\pi,\mu)} = p_{(\pi',\mu)}$ für alle $\mu \in \mathcal{M}$ gilt und nennt die Äquivalenzklassen Zustände. $\mathcal{Z}$ sei die Menge der Zustände. Analog definiert man $\mu \sim \mu'$ falls $p_{(\pi,\mu)} = p_{(\pi,\mu')}$ für alle $\pi \in \mathcal{P}$ gilt und nennt die Äquivalenzklassen $Effekte$. $\mathcal{E}$ sei die Menge der Effekte. Wir schreiben $p_{(z,e)} := p_{(\pi,\mu)}$ falls $z = [\pi] \in \mathcal{Z}$ und $e = [\mu] \in \mathcal{E}$ gelten. $\mathcal{Z}$ trennt $\mathcal{E}$ indem $(\forall z \in \mathcal{Z}) p_{(z,e)} = p_{(z,e')}. \Rightarrow .e = e'$ und $\mathcal{E}$ trennt $\mathcal{Z}$ indem $(\forall e \in \mathcal{E}) p_{(z,e)} = p_{(z',e)}. \Rightarrow .z = z'$.

Seien nnun $z, z' \in \mathcal{Z}$, λ eine rationale Zahl, $0 \leq \lambda \leq 1$. Macht man in einer Versuchsreihe den Bruchteil λ der Versuche mit den Aufbau (π, μ), $\pi \in z$ und den Bruchteil $1 - \lambda$ der Versuche mit den Aufbau (π', μ), $\pi' \in z'$, dann wird man unabhängig von der Reihenfolge, in der man die verschiedenen Präparierverfahren anwendet, für das Ergebnis 0 die Wahrscheinlichkeit $\lambda p_{(\pi,\mu)}(0) + (1-\lambda) p_{(\pi',\mu)}(0) = \lambda p_{z,e)}(0) + (1-\lambda) p_{(z',e)}(0)$ erhalten, falls $\mu \in e$ ist, und entsprechendes für das Ergebnis 1. Auf diese Weise ist für rationale λ operational ein gemischter Zustand definiert worden. Diese Überlegung motiviert das Mischungsaxiom.

Mischungaxiom: Die Menge der Zustände $\mathcal{Z}$ einer statistischen Theorie trägt eine konvexe Struktur, d.h. mit $0 \leq \lambda_i \in \mathbf{R}$, $z_i \in Z$, $i = 1, 2, 3, \ldots, n$, $\sum_i \lambda_i = 1$ gibt es einen Zustand $\zeta(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n; z_1, z_2.z_3, \ldots, z_n) \in \mathcal{Z}$, wobei gilt $\zeta(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n; z, z.z, \ldots, z) = z$. In Bezug auf diese Strukttur sind die Funktionale $E : \mathcal{Z} \to [0.1]; z \mapsto p_{(z,e)}(0)$, die durch die Effekte $e \in \mathcal{E}$ gegeben sind, affin, d.h. $E(\zeta(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n; z_1, z_2.z_3, \ldots, z_n)) = \sum_i \lambda_i E(z_i)$.

Sei nun für $\alpha, \beta \in \mathbf{R}$, $e, f \in \mathcal{E}$, $E(z) = p_{(z,e)}(0)$ und $F(z) = p_{(z,f)}(0)$

$$(\alpha E + \beta F)(z) := \alpha E(z) + \beta F(z),$$

dann spannen die durch $\mathcal{E}$ gegebenen Funktionale einen rellen Vektorraum $\mathcal{S}$ auf. Die Zustände $z \in Z$ treten dann als lineare Funktionale

$$z(\sum_i \alpha_i E_i) := \sum_i \alpha_i E_i(z) = \sum_i \alpha_i p_{(z,e_i)}$$

auf $\mathcal{S}$ auf. Sie sind damit Elemente des algebraischen Dualraums $\mathcal{S}^*$ von $\mathcal{S}$

und überdies gilt für $0 \leq \lambda_i \in \mathbf{R}$, $z_i \in Z$, $i = 1, 2, 3, \ldots, n$, $\sum_i \lambda_i = 1$

$$\begin{aligned} & \zeta(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n; z_1, z_2.z_3, \ldots, z_n)(\sum_i \alpha_i E_i) \\ = & \sum_i \alpha_i E_i(\zeta(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n; z_1, z_2.z_3, \ldots, z_n)) \\ = & \sum_i \alpha_i \sum_k \lambda_k E_i(z_k) = \sum_k \lambda_k \sum_i \alpha_i E_i(z_k) = \sum_k \lambda_k z_k (\sum_i \alpha_i E_i). \end{aligned}$$

Es gilt also

$$\zeta(\lambda_1, \lambda_2, \lambda_3, \ldots, \lambda_n; z_1, z_2.z_3, \ldots, z_n) = \sum_k \lambda_k z_k,$$

so dass die Zustände als konvexe Menge in den Vektorraum $\mathcal{S}^*$ eingebettet sind. Wir definieren in $\mathcal{S}^*$ eine Teilordnung. Für $x, y, \in \mathcal{S}^*$ sei

$$x \geq y \quad :\Leftrightarrow \quad x - y \in \mathcal{C} := \{c | c = \alpha z, 0 \leq \alpha \in \mathbf{R}, z \in \mathcal{Z}\}.$$

Der positive Kegel $\mathcal{C}$ ist konvex, aber nicht notwendig erzeugend, d.h. es mag Elemente $x \in \mathcal{S}^*$ mit $x \notin \mathcal{C} - \mathcal{C} := \{y | y = y_1 - y_2,\ y_l \in \mathcal{C},\ i = 1, 2\}$ geben. Jedenfalls ist $\mathcal{C} - \mathcal{C}$ einen Vektorraum in dem $\mathcal{C}$ erzeugend ist, und man überlegt sich leicht, dass die konvexe Hülle $\mathrm{conv}\{\mathcal{Z} \cup (-\mathcal{Z})\}$ absorbierend ist, d.h. jeder Vektor $x \in \mathcal{C} - \mathcal{C}$ kann in der Form $x = \alpha y,\ 0 \leq \alpha \in \mathbf{R},\ y \in \mathrm{conv}\{\mathcal{Z} \cup (-\mathcal{Z})\}$ geschrieben werden. Das Infimum solcher α definiert eine Norm

$$\|x\| = \inf\{\alpha | x = \alpha y,\ 0 \leq \alpha \in \mathbf{R},\ y \in \mathrm{conv}\{\mathcal{Z} \cup (-\mathcal{Z})\}, \}$$

die Basisnorm heißt, weil $\mathcal{Z}$ eine Basis des Kegels $\mathcal{C}$ ist. Der *Zustandsraum* der so aufgebauten statistischen Theorie ist dann die mit dieser Norm vervollständigte Hülle von $\mathcal{C} - \mathcal{C}$. $\mathcal{V} = \overline{\mathcal{C} - \mathcal{C}}$ ist ein teilweise geordneter Banachraum. Die Extremalpunkte von $\mathcal{Z}$, d.h. diejenigen Zustände z, für die aus $z = \lambda z_1 + (1 - \lambda) z_2$, $z_1, z_2 \in \mathcal{Z}$, $z_1 \neq z_2$ folgt $\lambda \in \{0, 1\}$, heißen *reine Zustände*, alle anderen *gemischte Zustände*. Stets ist $\mathcal{Z}$ die konvexe Hülle der reinen Zustände.