

1. einige Grundlagen aus der Quantentheorie

Für die Quanteninformationsverarbeitung sind zwei Elemente der Quantenphysik von besonderer Bedeutung: Zustände und Operationen

0.1.1. Zustände

• reine Zustände

Elemente eines Hilbertraumes $\mathcal{H}$ mit Skalarprodukt

$$(4) \quad c = \langle \varphi | \phi \rangle \quad c \in \mathbb{C}$$

und Norm

$$(5) \quad \|\varphi\| = \sqrt{\langle \varphi | \varphi \rangle}$$

wichtigster Hilbertraum $\mathbb{C}^2$ mit Basis $\{|0\rangle, |1\rangle\}$

$$(6) \quad |\varphi\rangle = \alpha |0\rangle + \beta |1\rangle \quad |\alpha|^2 + |\beta|^2 = 1$$

• gemischte Zustände

Bei unvollständiger Kenntnis über das physikalische System anstelle des Dirac'schen Zustandsvektors $|\varphi\rangle$ der Dichteoperator ρ verwendet werden. Z. B. wenn wir wissen, daß das System in zwei orthogonalen Zuständen mit Wahrscheinlichkeiten p_1 und p_2 vorliegen kann, so ist

$$(7) \quad |\varphi\rangle \rightarrow \rho = p_1 |\varphi_1\rangle\langle\varphi_1| + p_2 |\varphi_2\rangle\langle\varphi_2|$$

nicht korrekt, da dann der Erwartungswert einer Observable $\hat{A}$ gegeben wäre durch

$$\begin{aligned}
 \langle \hat{A} \rangle &= (p_1 \langle \psi_1 | + p_2 \langle \psi_2 |) \hat{A} (p_1 |\psi_1\rangle + p_2 |\psi_2\rangle) \\
 (8) \quad &= p_1^2 \langle \hat{A} \rangle_1 + p_2^2 \langle \hat{A} \rangle_2 + p_1 p_2 \\
 &\quad + p_1 p_2 (\langle \psi_1 | \hat{A} | \psi_2 \rangle + \langle \psi_2 | \hat{A} | \psi_1 \rangle) \\
 &\neq p_1 \langle \hat{A} \rangle_1 + p_2 \langle \hat{A} \rangle_2
 \end{aligned}$$

• Nun gilt, ($d = \text{Dimension von } \mathcal{H}$, $|i\rangle$ ONB.)

$$\begin{aligned}
 \langle \hat{A} \rangle &= \langle \psi | \hat{A} | \psi \rangle = \sum_{i=1}^d \langle \psi | \hat{A} | i \rangle \langle i | \psi \rangle \\
 (9) \quad &= \sum_{i=1}^d \langle i | \psi \rangle \langle \psi | \hat{A} | i \rangle \\
 &= \text{Tr} \{ |\psi\rangle \langle \psi | \hat{A} \}
 \end{aligned}$$

• Statt (7) muß man die Ersetzung

$$\begin{aligned}
 (10) \quad |\psi\rangle \langle \psi| &\longrightarrow p_1 |\psi_1\rangle \langle \psi_1| + p_2 |\psi_2\rangle \langle \psi_2| \\
 &= \hat{\mathcal{G}}
 \end{aligned}$$

Eigenschaften von $\hat{\mathcal{G}}$

• $\hat{\mathcal{G}}, \hat{\mathcal{G}}^\dagger$ sind auf gesamten Hilbertraum definiert

$\hat{\mathcal{G}} = \hat{\mathcal{G}}^\dagger$, d.h. $\hat{\mathcal{G}}$ ist selbstadjungiert

• $\hat{\mathcal{G}}$ ist semipositiv (Eigenwerte ≥ 0)

• $\text{Tr} \{ \hat{\mathcal{G}} \} = 1 = \text{Summe aller Wahrscheinlichkeiten}$

Die Menge $S(\mathcal{H})$ aller Dichteoperatoren heißt Zustandsraum.
Der Zustandsraum ist konvex, d.h. falls $\rho_1, \rho_2 \in S(\mathcal{H})$
und λ reell mit $0 \leq \lambda \leq 1$, dann gilt

$$(11) \quad \lambda \rho_1 + (1-\lambda) \rho_2 \in S(\mathcal{H})$$

Reinen Zuständen entsprechen Projektoren $\hat{\rho} = |\psi\rangle\langle\psi|$, d.h.

$$(12) \quad \hat{\rho}^2 = \hat{\rho}$$

Jeder gemischte Zustand $\hat{\rho}$ erlaubt eine Darstellung der Form

$$(13) \quad \hat{\rho} = \sum_{i=1}^d p_i |\psi_i\rangle\langle\psi_i|$$

wobei $0 \leq p_i \leq 1$, $\sum_i p_i = 1$ und $\{|\psi_i\rangle\}$ eine ONB ist.

Die p_i 's in (13) haben die Bedeutung von Wahrscheinlichkeiten das System im Zustand $|\psi_i\rangle$ zu finden. Man beachte aber, daß die Zerlegung (13) nicht eindeutig ist.

② reine Zwei-Parteiensysteme (Verschränkung)

Wir werden sehen, daß in der Q-Inf.-verarbeitung (QIV) Zwei-Parteiensysteme $A = \text{Alice}$, $B = \text{Bob}$ eine wichtige Rolle spielen. Es sei also

$$(14) \quad \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$$

Reine Zustände die sich in der Form

$$(15) \quad |\varphi\rangle = |\phi\rangle_A \otimes |\phi\rangle_B$$

darstellen lassen, wollen wir Produktzustände, separabel oder faktorisierbar nennen. Außerdem falls heißen sie verschränkt.

Schmidt Theorem: Sei $\dim(\mathcal{H}_A) = N$ und $\dim(\mathcal{H}_B) = M$ mit $N \leq M$. Dann gibt es für jeden Zustand $|\varphi\rangle$ eine Zerlegung in ONB'en $\{|i\rangle_A\}$, $\{|i\rangle_B\}$ der folgenden Form

$$(16) \quad |\varphi\rangle = \sum_{i=1}^N c_i |i\rangle_A |i\rangle_B \quad \sum_{i=1}^N |c_i|^2 = 1$$

Beweis: $|\varphi\rangle = \sum_{i=1}^N \sum_{j=1}^M \alpha_{ij} |i\rangle_A |j\rangle_B$

(17) es sei $\sum_{j=1}^M \alpha_{ij} |j\rangle_B \equiv \tilde{|i\rangle}_B$ ein unnormalisierter Zustand

$\{\tilde{|i\rangle}_B : i=1, \dots, N\}$ Satz unnormalisierter, nichtorthogonaler Zustände in $\mathcal{H}_B$. Mit Hilfe des Schmidtschen Orthogonalisierungsverfahren läßt sich aus (17) stets ein Satz von N orthonormalen Zuständen konstruieren:

$$|1\rangle_B = \frac{1}{\sqrt{\sum_{j=1}^M |\alpha_{1j}|^2}} \sum_{j=1}^M \alpha_{1j} |j\rangle_B$$

$$|2'\rangle_B = |\tilde{2}\rangle_B - \frac{\langle 1|\tilde{2}\rangle_B}{\langle 1|1\rangle_B} |1\rangle_B \quad |2'\rangle_B \perp |1\rangle_B$$

Normierung etc.

$$\Rightarrow |2\rangle_B = \sum_{i=1}^N C_i |i\rangle_A |i\rangle_B \quad \square$$

Mit Hilfe der Schmidt'schen Zerlegung kann festgestellt werden, ob ein Zweiteilchenzustand verschränkt ist oder nicht.

- Ist die Schmidtzahl s , d.h. die Zahl der von null verschiedenen Komponenten C_i größer als 1 ist der Zustand verschränkt. Verschränkung spielt eine zentrale Rolle in der QIV. Daher ist es nützlich ein Kriterium zu besitzen, das anzeigt ob ein Zustand verschränkt ist oder nicht. Die Schmidtzahl ist ein solches einfaches Kriterium. Wie wir noch sehen werden stellt die Verallgemeinerung dieses Kriteriums auf gemischte Zweiteilchenzustände ein enormes Problem dar. Für gemischte Mehrparteiensysteme ist bis heute noch kein allgemeingültiges Verfahren gefunden worden.

1.2. Operationen

In der Q-Theorie unterscheidet man prinzipiell zwei Klassen von Operationen, unitäre Evolutionen gemäß der Schrödingergleichung und Messungen, wobei bei letzteren verschiedene Typen unterschieden werden.

- unitäre Evolution (dynamical map)

$$(18) \quad \rho(0) \rightarrow \rho(t) = U(t) \rho(0) U^\dagger(t)$$

Eine unitäre Evolution bildet reine Zustände auf reine Zustände ab

$$\rho(0)^2 = \rho(0) \Rightarrow$$

$$(19) \quad \begin{aligned} \rho(t)^2 &= U(t) \rho(0) \underbrace{U^\dagger(t) U(t)}_{=1} \rho(0) U^\dagger(t) \\ &= U(t) \rho(0)^2 U^\dagger(t) = U(t) \rho(0) U^\dagger(t) = \rho(t) \end{aligned}$$

- projektive Messung

Seien $i=1, \dots, k$ Indizes die den Ausgang der Messung einer bestimmten Observable charakterisieren (Klasswerte sind Eigenwerte $\{\lambda_1, \lambda_2, \dots, \lambda_k\}$). $\hat{\pi}_i$ seien Projektoren auf die zugehörigen Eigenzustände. Im Falle eines nicht entarteten Eigenwertes λ_i ist $\hat{\pi}_i$ eindimensional

$$(20) \quad \hat{\pi}_i = |\lambda_i\rangle \langle \lambda_i|$$

Für entartete Eigenwerte mit Entartungsgrad ℓ ist $\hat{\pi}_i$ ein ℓ -dimensionaler Projektor. In jedem Fall gilt

$$(21) \quad \hat{\pi}_i \hat{\pi}_j = \delta_{ij} \hat{\pi}_i \quad \sum_{i=1}^k \hat{\pi}_i = 1$$

Hauptunterschied selektive projektive Messungen

die der Abbildung dimensional sind.

$$(22) \quad \rho \rightarrow \rho' = \frac{\hat{\pi}_i \rho \hat{\pi}_i}{\text{tr}\{\hat{\pi}_i \rho \hat{\pi}_i\}}$$

entsprechen, sowie nicht-selektiven Messungen (z.B.:
(man macht eine Messung und ignoriert das Ergebnis))

$$(23) \quad \rho \rightarrow \rho' = \sum_{i=1}^K \hat{\pi}_i \rho \hat{\pi}_i$$

$$\begin{aligned} \text{Man beachte } \text{Tr} \left\{ \sum_{i=1}^K \hat{\pi}_i \rho \hat{\pi}_i \right\} &= \sum_{i=1}^K \text{Tr} \{ \hat{\pi}_i \rho \hat{\pi}_i \} \\ &= \sum_{i=1}^K \text{Tr} \{ \hat{\pi}_i^2 \rho \} = \sum_{i=1}^K \text{Tr} \{ \hat{\pi}_i \rho \} \\ &= \text{Tr} \left\{ \sum_{i=1}^K \hat{\pi}_i \rho \right\} = \text{Tr} \{ \rho \} = 1 \end{aligned}$$

Die Wahrscheinlichkeit des Meßresultats "i" bei einer selektiven Messung ist

$$(24) \quad p_i = \text{Tr} \{ \hat{\pi}_i \rho \hat{\pi}_i \} = \text{Tr} \{ \hat{\pi}_i \rho \}$$

Im 1-dimensionalen Fall (20) geht (24) über in

$$(25) \quad p_i = \text{Tr} \{ |z_i\rangle \langle z_i| \rho \} = \langle z_i | \rho | z_i \rangle$$

Sind alle Projektoren $\hat{\pi}_i$ 1-dimensional, heißt eine selektive Messung vollständig. Nach einer solchen Messung weiß man exakt in welchem Zustand sich das System befindet.

Neben unitären Transformationen und Messungen sind noch zwei weitere Operationen wichtig

- Erweiterung des Systems durch Anzillazustände

ρ in $\mathcal{H}_A$ und ω in $\mathcal{H}_B$

$$(26) \quad \rho \rightarrow \rho \otimes \omega$$

- Reduzierung des Systems auf ein Untersystem

ρ in $\mathcal{H}_A \otimes \mathcal{H}_B$

$$(27) \quad \rho \rightarrow \sigma = \text{Tr}_B \{ \rho \}$$

Ist A ein (kleines) System und B ein (großes) Reservoir die in Wechselwirkung stehen, beschreibt die Zeitentwicklung von σ z.B. Dissipationsvorgänge

Alle quantenmechanisch erlaubten Operationen (unitäre Evolution, Messung, Erweiterung und Reduktion) lassen sich zusammenfassen zu vollständig positiven, linearen, spärerhaltenden Abbildungen

$$(28) \quad \mathcal{E}: \rho(\mathcal{H}) \rightarrow \rho(\mathcal{H})$$

$\mathcal{E}$ muß linear sein, damit die Konvexitätsbeziehung (11) erhalten bleibt, $\mathcal{E}$ muß positiv sein, damit die Positivität von g erhalten bleibt. Schließlich ist die Spurerhaltung eine Konsequenz der Erhaltung der Gesamtwahrscheinlichkeit.

Eine Abbildung $\mathcal{E}$ ist vollständig positiv, falls

$$(29) \quad \mathcal{E} \otimes \mathbb{1}_N \quad \forall N$$

positiv ist. $\mathbb{1}_N$ ist der Einheitsoperator im N dimensionalen Hilbertraum. Hinter der Forderung nach vollständiger Positivität steckt die Möglichkeit ein System um ein weiteres N dimensionales zu erweitern. Eine Operation auf dem ursprünglichen System wirkt dann auf der Erweiterung wie der Einheitsoperator. (29) ist tatsächlich strenger als die bloße Forderung nach Positivität.

Beispiel: Transposition

$$(30) \quad \mathcal{E}(g) = g^T \quad \text{ist natürlich positiv}$$

aber nicht vollständig positiv. Betrachten $\mathcal{E}$ im 2-dim. Hilbertraum (Spin $1/2$) und die Erweiterung auf $2 \times \text{Spin } 1/2$ Systeme.

$$(31) \quad (1_2 \otimes \varepsilon)$$

angewandt auf $\rho = |\varphi\rangle\langle\varphi|$ mit $|\varphi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|0\rangle + |1\rangle|1\rangle)$

d.h.

$$(32) \quad \rho = \frac{1}{2} \begin{matrix} & \begin{matrix} 00 & 01 & 10 & 11 \end{matrix} \\ \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} & \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \end{matrix}$$

$\Rightarrow$

$$(33) \quad (1_2 \otimes \varepsilon)(\rho) = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Eigenwerte: $(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2})$ nicht vollständig positiv!

D.h. die Transposition einer Dichtematrix ist kein physikalisch erlaubter Prozeß.

- Jede vollständig positiv, lineare und spurerhaltende Abbildung hat die Form

$$(34) \quad \mathcal{S}(\rho) = \sum_{i=1}^K E_i \rho E_i^\dagger$$

mit

$$(35) \quad \sum_{i=1}^K E_i^\dagger E_i = 1$$

(35) garantiert die Spurerhaltung, da

$$\begin{aligned} (36) \quad \text{Tr}\{\mathcal{S}(\rho)\} &= \text{Tr}\left\{\sum_{i=1}^K E_i \rho E_i^\dagger\right\} \\ &= \sum_{i=1}^K \text{Tr}\{E_i \rho E_i^\dagger\} = \sum_{i=1}^K \text{Tr}\{E_i^\dagger E_i \rho\} \\ &= \text{Tr}\{\rho\} = 1 \end{aligned}$$

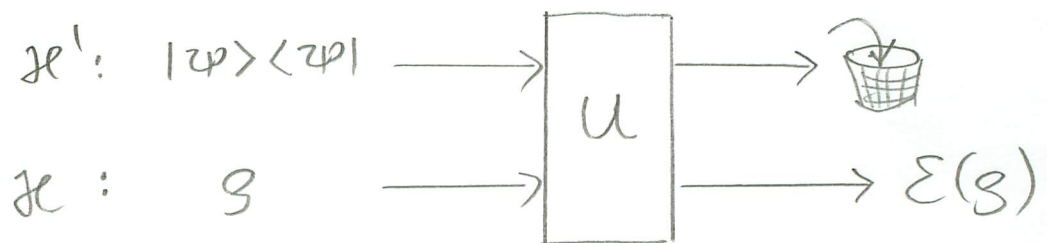
Die Operatoren E_i sind i.A. nicht hermitesch. Es gilt folgendes interessantes Theorem:

Theorem von Stinespring

Gegeben Hilbertraum $\mathcal{H}$ mit $\dim(\mathcal{H}) = N$ und vollst. pos. lineare und spurenhaltende Abb. $\mathcal{E}: \mathcal{S}(\mathcal{H}) \rightarrow \mathcal{S}(\mathcal{H})$.
Dann existiert ein Hilbertraum $\mathcal{H}'$ mit $\dim(\mathcal{H}') \leq N^2$ so daß für jeden beliebigen Zustand $|\varphi\rangle \in \mathcal{H}'$ eine unitäre Operation U auf $\mathcal{H} \otimes \mathcal{H}'$ existiert mit

$$(37) \quad \mathcal{E}(g) = \text{Tr}_{\mathcal{H}'} \{ U [g \otimes |\varphi\rangle\langle\varphi|] U^\dagger \}$$

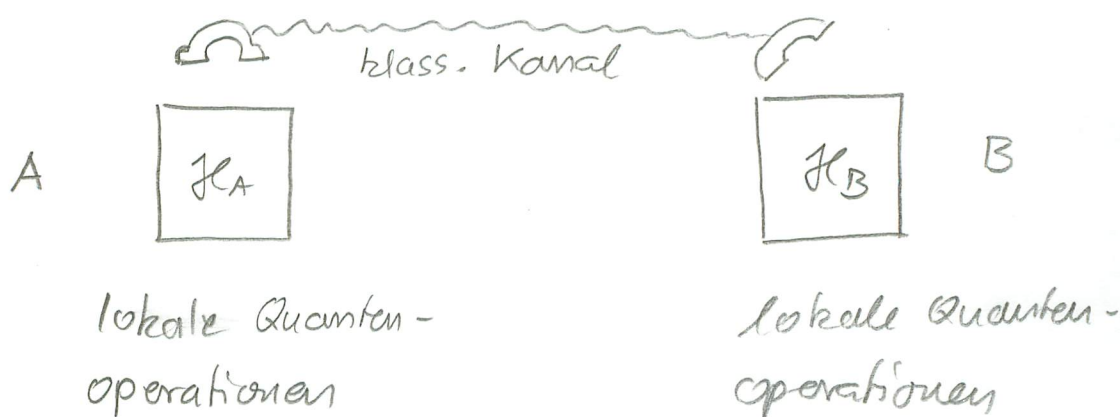
D.h. jede erlaubte Operation kann als unitäre Evolution auf einem geeignet erweiterten Hilbertraum betrachtet werden



1.3. Operationen in Zwei-Parteiensystemen

Eine spezielle Klasse erlaubter Operationen in einem Zwei-Parteiensystem A, B (Alice und Bob) die eine zentrale Rolle in der QIV spielt soll abschließend

nicht kurz definiert werden. Es handelt sich um "local quantum operations with classical communication" (LOCC) Oper



• lokale Operationen

$$(38) \quad \rho \rightarrow \mathcal{E}(\rho) = \sum_{i=1}^K \sum_{j=1}^L (\hat{A}_i \otimes \hat{B}_j) \rho (\hat{A}_i \otimes \hat{B}_j)^\dagger$$

$\hat{A}_i$ wirkt nur in $\mathcal{H}_A$ und $\hat{B}_j$ nur in $\mathcal{H}_B$

• lokale Operation mit "one-way" klass. Kommunikation

Jetzt sendet Alice Informationen an Bob z.B. über ihre Meßresultate. Bob kann dann Operationen ausführen, die von diesen Meßresultaten abhängen

$$(39) \quad \rho \rightarrow \mathcal{E}(\rho) = \sum_{i=1}^K \sum_{j=1}^L (1_A \otimes B_j^{(i)}) (A_i \otimes 1_B) \rho (A_i \otimes 1_B)^\dagger (1_A \otimes B_j^{(i)})^\dagger$$

- lokale Operationen mit "two-way" klass. Kommunikation

$$\equiv \text{LOCC}$$

1.4. Meßbarkeit unbekannter Quantenzustände und no-cloning Theorem

- (i) Ein gänzlich unbekannter Zustand eines einzelnen Quantensystems kann durch Messung nicht vollständig bestimmt werden

Bspl: 2 dim Hilbertraum: Messung

vollständige Messung

$$\hat{\pi}_0 = |0\rangle\langle 0|, \quad \hat{\pi}_1 = |1\rangle\langle 1|$$

$\{|0\rangle, |1\rangle\}$ ist beliebige ONB

$$\rho = |\psi\rangle\langle\psi|$$

$$\frac{\hat{\pi}_0 \rho \hat{\pi}_0}{\text{Tr}\{\hat{\pi}_0 \rho \hat{\pi}_0\}}$$

$$\frac{\hat{\pi}_1 \rho \hat{\pi}_1}{\text{Tr}\{\hat{\pi}_1 \rho \hat{\pi}_1\}}$$

Messung liefert
1 bit an
klass. Information

Es bedarf weit mehr als ein bit an Information
um den Quantenzustand

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

zu rekonstruieren.

Bem: Besitzt man eine große Anzahl identisch präparierter Systeme existieren optimale Strategien zur Bestimmung von $|\psi\rangle$ ("state estimation")

(ii) Ein unbekannter Quantenzustand kann i.A. nicht vervielfältigt werden (no cloning)

Bew: Xerox: $|\alpha\rangle|0\rangle \xrightarrow{?} |\alpha\rangle|\alpha\rangle$
für beliebiges $|\alpha\rangle$

$$U[|\alpha\rangle|0\rangle] = |\alpha\rangle|\alpha\rangle$$

$$U[|\beta\rangle|0\rangle] = |\beta\rangle|\beta\rangle$$

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

$|\gamma\rangle$ ist nicht orthogonal zu $|\alpha\rangle$ und $|\beta\rangle$

$$\begin{aligned} U[|\gamma\rangle|0\rangle] &= U\left[\frac{1}{\sqrt{2}}|\alpha\rangle|0\rangle + \frac{1}{\sqrt{2}}|\beta\rangle|0\rangle\right] \\ &= \frac{1}{\sqrt{2}}|\alpha\rangle|\alpha\rangle + \frac{1}{\sqrt{2}}|\beta\rangle|\beta\rangle \neq |\gamma\rangle|\gamma\rangle \end{aligned}$$

$\Rightarrow$ nur orthogonale Zustände sind kopierbar

Bem: Es existieren optimale Strategien für approximatives clonen ("optimum cloning")