Основы квантовой коммуникации часть 1

Grundlagen der Quantenkommunikation
Teil 1 – Kapitel 7
Mathematischer Apparat der Quantenkommunikation

A.V. Kozubov, A.A. Gaidash, S.M. Kynew, V.I. Egorov,
A.E. Ivanova, A.V. Gleim, G.P. Miroschnitschenko
Übersetzung: Dipl.- Ing. Björnstjerne Zindler, M.Sc.

www.Zenithpoint.de

Erstellt: 22. März 2023 – Letzte Revision: 25. März 2023

Inhaltsverzeichnis

Literatur

[A.V] A.V. Kozubov, A.A. Gaidash, S.M. Kynew, V.I. Egorov, A.E. Ivanova, A.V. Gleim, G.P. Miroschnitschenko. Grundlagen der Quantenkommunikation, Teil 1.

Университет ИТМО
Санкт Петерсбург 2019

Universität ITMO [1]
Sankt Petersburg 2019

[1] Staatliche Universität für Informationstechnologien, Mechanik und Optik in Sankt Petersburg

7 Mathematischer Apparat der Quantenkommunikation

7.1 Grundlegende Konzepte

7.1.1 Mathematische Interpretation

In diesem Abschnitt werden die grundlegenden mathematischen Konzepte eingeführt, die für das weitere Studium des Kurses erforderlich sind.

Führen wir eine komplexe Zahl $c = a + ib$ ein, so dass $c \in \mathbb{C}$, wobei $a, b \in \mathbb{R}, i = \sqrt{-1}$, dann ist $c^* = a - ib$ ihre komplex Konjugierte. Eine solche Darstellung wird auch im weiteren Verlauf der Quanteninformationstheorie benötigt.

Außerdem ist es notwendig, eine spezielle Darstellung der Vektoren, Bra- und Ket einzuführen. Anfangs mag eine solche Darstellung zu umständlich und mühsam erscheinen, aber später wird die Bequemlichkeit der Verwendung dieser nominalen Darstellung unbestreitbar sein.

- **Definition 5.1.1**

Der Ket-Vektor $|\bullet\rangle$ sei ein d-dimensionaler Spaltenvektor im komplexen Vektorraum $\mathbb{C}^d$, dann ist der Bra-Vektor, $\langle\bullet|$, der d-dimensionale Zeilenvektor, der der komplexen Konjugation des Ket-Vektors entspricht und die Form $\langle\bullet| = \left((|\bullet\rangle)^*\right)^T$, wobei $*$ die komplexe Konjugation und T die Transposition ist.

- **Beispiel 5.1.1**

Sei $|v\rangle \in \mathbb{C}^2$ ein Raum mit folgendem zweidimensionalen Vektor der Form:

$$|v\rangle = |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$\Rightarrow$

$$\langle v| = \left((|v\rangle)^*\right)^T = \left((|0\rangle)^*\right)^T = \begin{pmatrix} 1^* \\ 0^* \end{pmatrix}^T = \begin{pmatrix} 1 & 0 \end{pmatrix}$$

- **Definition 5.1.2 Betrag einer komplexen Zahl**

Sei $c \in \mathbb{C}$ eine komplexe Zahl und habe die Form $c = a + ib$, wobei $a, b \in \mathbb{R}$. Der Betrag oder Betrag von c wird genannt:

$$|c| = \sqrt{c^* c} = \sqrt{a^2 + b^2}$$

- **Beispiel 5.1.2**

$$|c| = 1 + 2i \rightarrow |c| = \sqrt{1^2 + 2^2} = \sqrt{5}$$

- **Definition 5.1.3 Skalarprodukt**

Es gebe zwei d-dimensionale Vektoren

$$|v_1\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}, |v_2\rangle = \begin{pmatrix} b_1 \\ \vdots \\ b_d \end{pmatrix}$$

dann ist das Skalarprodukt dieser Vektoren nichts anderes als $\langle v_1 \mid v_2\rangle = \sum_{i=1}^{d} a_i^* b_i$. Es sei darauf hingewiesen, dass das Skalarprodukt der Vektoren $|v_1\rangle, |v_2\rangle \in \mathbb{C}^d$ im Allgemeinen eine komplexe Zahl ist.

- **Beispiel 5.1.3**

Es seien zwei Vektoren

$$|v_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |v_2\rangle = \begin{pmatrix} 3 \\ 2 \end{pmatrix}$$

dann

$$\langle v_1 \mid v_2\rangle = \begin{pmatrix} 1^* & 0^* \end{pmatrix} \cdot \begin{pmatrix} 3 \\ 2 \end{pmatrix} = 3$$

- **Definition 5.1.4 Vektorlänge**

Es gebe einen Vektor

$$|v\rangle = \begin{pmatrix} a_1 \\ \vdots \\ a_d \end{pmatrix}$$

dann hat die Länge des Vektors folgende Form:

$$\||v\rangle\|_2 = \sqrt{\langle v \mid v\rangle} = \sqrt{\sum_{i=1}^{d} a_i^* \cdot a_i} = \sqrt{\sum_{i=1}^{d} |a_i|^2}$$

Wenn $\||v\rangle\|_2 = 1$, dann ist es üblich zu sagen, dass der Vektor $|v\rangle$ die Norm 1 hat oder $|v\rangle$ ist normalisiert.

- **Beispiel 5.1.4**

Es gebe einen Vektor $|v\rangle \in \mathbb{C}^2$, so dass

$$|v\rangle = \frac{1}{2}\begin{pmatrix} 1+i \\ 1-i \end{pmatrix}$$

dann ist seine Länge

$$\||v\rangle\|_2 = \frac{1}{2} \cdot \sqrt{(1+i)^* \cdot (1+i) + (1-i)^* \cdot (1-i)} = \frac{1}{2} \cdot \sqrt{2 \cdot (1-i) \cdot (1+i)} = \frac{1}{2} \cdot 2 = 1$$

Wenn es um Vektoren geht, ist es logisch anzunehmen, dass die Existenz eines Vektors der folgenden Form $\alpha \cdot |0\rangle + \beta \cdot |1\rangle$ gleich ist. Eine solche Beschreibung eines Vektors ist nichts anderes als eine Darstellung eines **Quantenbits (Qubit)**. Anstatt sich strikt im 0- oder im 1-Zustand zu befinden, befindet sich das Qubit in einem *Überlagerungszustand*. Wenn wir Bits als Vektoren darstellen, können wir sagen, dass ein Quantenbit als $|v\rangle \in \mathbb{C}^2$ beschrieben werden kann.

- **Definition 5.1.5 Quantenbit**

Der reine Zustand eines Qubits kann als zweidimensionaler Ket-Vektor $|\psi\rangle \in \mathbb{C}^2$ dargestellt werden, wobei $|\psi\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$, mit $\alpha, \beta \in \mathbb{C}$ und $|\alpha|^2 + |\beta|^2 = 1$. Die Bedingung für α, β besagt, dass der Vektor $|\psi\rangle$ normiert ist.

In der Darstellung eines Qubits wird vorgeschlagen, die Vektoren $|0\rangle$ und $|1\rangle$ zu verwenden, um klassische Bits zu beschreiben. Es sollte beachtet werden, dass diese Vektoren orthonormal sind, was in der Quantensprache als $\langle 1 \mid 0\rangle = 0$ ausgedrückt werden kann, während $\langle 1 \mid 1\rangle = \langle 0 \mid 0\rangle = 1$ ist. Somit bilden diese Vektoren, $|0\rangle$ und $|1\rangle$ eine Basis in $\mathbb{C}^2$ und jeder Vektor $|v\rangle \in \mathbb{C}^2$ kann als $|v\rangle = \alpha \cdot |0\rangle + \beta \cdot |1\rangle$ dargestellt werden, wobei α, β komplexe Koeffizienten sind.

- **Definition 5.1.6 Standardbasis**

Sei $\mathbb{C}^2$ ein zweidimensionaler komplexer Vektorraum, dann ist die Standardbasis (Rechenbasis) $\mathscr{I} = \{|0\rangle, |1\rangle\}$ eine Orthonormalbasis dieses Raumes mit den Basisvektoren

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Natürlich ist diese Basis nicht die einzige und man kann unendlich viele andere verschiedene Basen wählen.

7.1.2 Operationen auf Qubits

Neben klassischen Bits können auch verschiedene Operationen über Quantenbits durchgeführt werden. Da Quantenbits als Vektoren dargestellt werden, ist es zur Beschreibung von Operationen an ihnen notwendig, den Operator U einzuführen, der wie folgt einen Vektor auf einen anderen Vektor projizieren würde:

$$|\psi_{out}\rangle = U \cdot |\psi_{in}\rangle$$

Wenn der Vektor $|\psi_{in}\rangle \in \mathbb{C}^d$ ist, dann kann der Operator U dargestellt werden als eine mit komplexen Zahlen gefüllte $d \times d$-Matrix.

Außerdem sei daran erinnert, dass für jeden Quantenzustand $|\psi\rangle$ die folgende Bedingung erfüllt sein muss $\langle\psi \mid \psi\rangle = 1$. Die Bedeutung dieser Bedingung liegt darin, dass sie zeigt, dass die Summe der Wahrscheinlichkeiten aller Ergebnisse möglicher Messungen gleich 1 ist. Dies wiederum sagt uns, dass der Operator U das Skalarprodukt bewahrt, d.h:

$$\langle\psi_{out} \mid \psi_{out}\rangle = \langle\psi_{in}| U^\dagger U |\psi_{in}\rangle = \langle\psi_{in}| UU^\dagger |\psi_{in}\rangle = 1$$

Offensichtlich muss der Operator U, um die Wahrscheinlichkeiten zu bewahren, die Länge jedes Vektors erhalten. Diese Bedingung ist dann erfüllt, wenn $U^\dagger U = UU^\dagger = \mathbb{I}$ [2] ist, wobei $\mathbb{I}$ der Identitätsoperator ist. Dieser Operator wird im Folgenden häufig vorkommen, daher definieren wir ihn wie folgt.

- **Definition 5.2.1 Identitätsoperator**

Der Identitätsoperator $\mathbb{I}$ ist eine der Dimension entsprechende Diagonalquadratmatrix, bei der jedes Diagonalelement gleich 1 ist.

$$\mathbb{I} = \begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & \cdots & 0 & 1 \end{pmatrix}$$

- **Definition 5.2.2 Unitarität des Operators**

Der Operator U ist genau dann unitär, wenn

$$U^\dagger U = UU^\dagger = \mathbb{I}$$

- **Beispiel 5.2.1 Operatoreinheitlichkeit**

Betrachten Sie die Matrix:

$$H = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix}$$

Es ist leicht zu sehen, dass $H = H^\dagger$ ist, also $HH^\dagger = H^\dagger H = \mathbb{I}$, was anzeigt, dass der Operator H unitär ist. [3]

- **Definition 5.2.3 linearer Operator**

Sei $\mathbb{C}^d$ ein komplexer d-dimensionaler Vektorraum. Dann kann der lineare Operator $L : \mathbb{C}^d \to \mathbb{C}^{d'}$ als $d' \times d$-dimensionale Matrix dargestellt werden.

$$L = \begin{pmatrix} L_{11} & L_{12} & \cdots & L_{1d} \\ L_{21} & \ddots & \ddots & L_{2d} \\ \vdots & \ddots & \ddots & \vdots \\ L_{d'1} & L_{d'2} & \cdots & L_{d'd} \end{pmatrix}$$

[2] † hier für adjungierte Matrix, hermitesch transponierte Matrix oder transponiert-konjugierte Matrix ist in der Mathematik diejenige Matrix, die durch Transponierung und Konjugation einer gegebenen komplexen Matrix entsteht. Die Notation $\bullet^\dagger$ wird vor allem in der Physik, insbesondere in der Quantenmechanik, verwendet.

[3] Hier also $H^\dagger = (H^*)^T = \frac{1}{\sqrt{2}} \cdot \begin{pmatrix} +1 & +1 \\ + & -1 \end{pmatrix}$

→

$H^\dagger H = HH^\dagger = \frac{1}{2} \cdot \begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix} \begin{pmatrix} +1 & +1 \\ +1 & -1 \end{pmatrix} = \frac{1}{2} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$

Wobei jedes Element $L_{ij} \in \mathbb{C}$ ist. Die Menge der linearen Operatoren wird bezeichnet als

$$\mathscr{L}\left(\mathbb{C}^d, \mathbb{C}^{d'}\right)$$

- **Definition 5.2.4 Hermitianischer Operator**

Ein linearer Operator $M \in \mathscr{L}\left(\mathbb{C}^d, \mathbb{C}^{d'}\right)$ ist hermitesch, falls $M^\dagger = M$.

Der Spektralsatz besagt, dass jeder hermitesche Operator $\mathscr{L}\left(\mathbb{C}^d, \mathbb{C}^{d'}\right)$ mit reellen Eigenwerten diagonalisiert werden kann. Das bedeutet, dass es eine orthonormale Basis $\{|v_j\rangle\} \in \mathbb{C}^d$ (Eigenvektoren) und reelle Zahlen λ_j (Eigenwerte) gibt, so dass $M = \sum_j \lambda_j |v_j\rangle \langle v_j|$.

- **Definition 5.2.5 positiver semidefiniter Operator**

Ein hermitescher Operator M ist ein positiver semidefiniter Operator, wenn alle seine Eigenwerte $\{\lambda_j\}_j$ nichtnegativ sind, d.h. $\lambda_j \geq 0$. Diese Bedingung wird als $M \geq 0$ bezeichnet.

- **Definition 5.2.6 Spur des Operators, der Matrix**

Die Spur einer Matrix $M \in \mathscr{L}\left(\mathbb{C}^d, \mathbb{C}^{d'}\right)$ wird betrachtet als

$$\mathrm{Tr}\,(M) = \sum_i \langle i| M |i\rangle$$

wobei $\{|i\rangle\}$ eine beliebige orthonormale Basis auf $\mathbb{C}^d$ ist.

- **Definition 5.2.7 positives operatorenbewertetes Maß**

Ein positives operatorenbewertetes Maß (POM) auf $\mathbb{C}^d$ ist etwas anderes als eine Menge positiver semidefiniter Operatoren $\{M_x\}_{x \in \mathscr{H}}$, so dass

$$\sum_x M_x = \mathbb{I}_{\mathbb{C}^d}$$

Der Index x wird verwendet, um das Messergebnis anzuzeigen. Die Wahrscheinlichkeit p_x, dass das Ergebnis x geworfen wird, kann basierend auf der Born-Regel [4] wie folgt dargestellt werden:

$$p_x = \mathrm{Tr}\,(M_x \rho)$$

[4] Bornsche Wahrscheinlichkeitsinterpretation

7.1.3 Wahrscheinlichkeitstheorie

Bevor wir mit der Beschreibung der Wahrscheinlichkeitstheorie in der Quantensprache fortfahren, ist es notwendig, die Grundkonzepte der klassischen Theorie zu wiederholen.

Stellen Sie sich vor, wir haben eine diskrete Zufallsvariable X, die einen der Werte des Alphabets $\mathscr{H}$ der Größe n annimmt. Dann sei $p(X)$ die Verteilung einer diskreten Zufallsvariablen X, wobei $|X|$ die Dimension des in X verwendeten Alphabets ist und Prob $(X = x)$ die Wahrscheinlichkeit, dass die Zufallsvariable den Wert $x \in \mathscr{H}$ annimmt. Manchmal wird der Einfachheit halber $p_x = p(x) = \text{Prob}(X = x)$ verwendet.

Die Verteilung $p(X)$ wird durch eine Menge nichtnegativer Wahrscheinlichkeiten definiert, nämlich $\forall x \in \mathscr{H}$, $p_x \geq 0$. Außerdem muss $p(X)$ normalisiert werden, was bedeutet, dass $\sum_{x \in \mathscr{H}} p_x = 1$.

Es ist wichtig zu verstehen, dass die Zufallsvariable X mit der Zufallsvariablen Y korreliert werden kann. Das bedeutet, dass sie einen gemeinsamen Verteilung haben $p(XY)$, was im Allgemeinen nicht unbedingt ihr direktes Produkt $p_{xy} \neq p_x \cdot p_y$ ist. Dies bringt uns zum Konzept der bedingten Wahrscheinlichkeit $P(X|Y)$, wobei Prob $(X = x|Y = y)$ die Wahrscheinlichkeit ist, dass die Zufallsvariable X den Wert x annimmt, vorausgesetzt, dass Y den Wert y annimmt.

Ein solcher Formalismus reicht jedoch nicht aus, um die Quantenzustände des Systems zu beschreiben und folglich ist ein allgemeinerer Ansatz erforderlich. Insbesondere erlaubt uns die klassische Beschreibung von Wahrscheinlichkeiten nicht, solche Zustände wie den EPR [5] eines Paares zu beschreiben oder Situationen, in denen der Zustand $|\psi_1\rangle$ mit Wahrscheinlichkeit p_1 und $|\psi_2\rangle$ mit Wahrscheinlichkeit p_2 herausfällt. Um den Gesamtzustand genau zu beschreiben, müssen wir den gesamten Satz von Zuständen und Wahrscheinlichkeiten $\{|\psi_i\rangle, p_i\}$ berücksichtigen. Lässt sich der Zustand, der durch einen solchen Prozess entsteht, mathematisch genau beschreiben?

Ja, es stellt sich heraus, dass es einen solchen Weg gibt und man nennt ihn den Formalismus der Dichtematrizen. Stellen Sie sich vor, dass es einen Quantenzustand eines Systems $|\psi\rangle$ gibt und schreiben Sie ihn als Matrix $\rho = |\psi\rangle\langle\psi|$. Es ist erwähnenswert, dass dies eine Matrix mit dem Rang 1 ist, was bedeutet, dass sie nur einen (gleich einem) Nicht-Null-Eigenwert mit dem entsprechenden Eigenzustand (Vektor) $|\psi\rangle$ hat.

- **Beispiel 5.3.1**

Die Zustandsdichtematrix $|0\rangle$ lautet wie folgt:

$$|0\rangle\langle 0| = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

Um auf die oben gestellte Frage zur Beschreibung eines Quantenzustands zurückzukommen, wie kann uns ein solcher Formalismus helfen, den Fall zu beschreiben, wenn jemand einen der beiden Quantenzustände $|\psi_1\rangle$ und $|\psi_2\rangle$ mit gleicher Wahrscheinlichkeit p_1 bzw. p_2 präpariert? Offensichtlich wird die Superpositionsbeschreibung nicht korrekt genug sein, da der Zustand mit Wahrscheinlichkeit $1/2$ genau in einem der Zustände liegt. Und doch können wir diesen Allgemeinzustand als eine Mischung aus $|\psi_1\rangle$ und $|\psi_2\rangle$ beschreiben. Bei gleichen Wahrscheinlichkeiten $|\psi_1\rangle$ und $|\psi_2\rangle$ sieht dieser gemischte Zustand folgendermaßen aus:

$$\rho = \frac{1}{2} \cdot |\psi_1\rangle\langle\psi_1| + \frac{1}{2} \cdot |\psi_2\rangle\langle\psi_2|$$

Im allgemeinen Fall, wenn die Quelle den Zustand $|\psi_x\rangle$ mit der Wahrscheinlichkeit p_x vorbereitet, hat der resultierende Zustand des Systems die folgende Form:

$$\rho = \sum_x p_x |\psi_x\rangle\langle\psi_x|$$

Um den Zustand eines Quantensystems korrekt zu beschreiben, muss die Dichtematrix die folgenden zwei wichtigen Eigenschaften erfüllen, sie muss ein positiv semidefiniter Operator sein und ihre Spur muss gleich 1 sein.

[5] Das Einstein-Podolsky-Rosen-Paradoxon, auch EPR-Paradoxon oder EPR-Effekt, ist ein quantenmechanisches Phänomen. Mancherorts wird auch vom EPR-Argument gesprochen. Es zeigt, dass die Quantenmechanik gegen die Annahme der klassischen Lokalität, die Eigenschaft, dass Vorgänge Auswirkungen nur auf ihre direkte Umgebung haben, verstößt.

- **Definition 5.3.1 Eigenschaften der Dichtematrix**

Stellen Sie sich ein Quantensystem im Zustandsraum $\mathbb{C}^d$ vor. Dann ist die *Dichtematrix* ρ ein linearer Operator $\rho \in \mathscr{L}\left(\mathbb{C}^d, \mathbb{C}^{d'}\right)$, so dass:

- $\rho \geq 0$
- $\mathrm{Tr}\left(\rho\right) = \sum_i^d \rho_{ii} = 1$

Wenn $\mathrm{rang}\left(\rho\right) = 1$, dann ist ρ ein reiner Zustand, ansonsten ein gemischter Zustand.

Eine nützliche Technik ist die Möglichkeit, die Wahrscheinlichkeitsverteilung in der klassischen Zeile $\mathbf{x}$ in Form von Dichtematrizen zu schreiben. Stellen wir uns vor, wir hätten eine klassische Wahrscheinlichkeitsverteilung von Symbolen aus dem Alphabet $\mathscr{H} = \{0, \ldots, d-1\}$, wobei p_x die Wahrscheinlichkeit des Auftretens eines bestimmten x ist. Indem wir klassische Bits (oder einfach nur Zahlen) mit Elementen der Standardbasis $\{|0\rangle, \ldots, |d-1\rangle\}$ korrelieren, können wir die Quelle, die jeden Zustand $|x\rangle$ vorbereitet, mit der Wahrscheinlichkeit p_x in der Form $\rho = \sum_{x=0}^{d-1} p_x |x\rangle \langle x|$ beschreiben. In diesem Fall liegen die Wahrscheinlichkeiten p_x auf der Hauptdiagonale der Dichtematrix und alle anderen Elemente sind gleich 0.

- **Definition 5.3.2. klassischer Zustand**

Stellen Sie sich ein System X mit dem Zustandsraum $\mathbb{C}^d$ vor und sei $\{|x\rangle\}_{x=0}^{d-1}$ die Standardbasis auf $\mathbb{C}^d$. Ein System X befindet sich in einem klassischen Zustand, wenn die zugehörige Dichtematrix diagonal im Zustandsraum X steht und folgende Form hat:

$$\rho_X = \sum_{x=0}^{d-1} p_x |x\rangle \langle x|_X$$

Wobei $\{p_x\}_{x=0}^{d-1}$ die normalisierte Wahrscheinlichkeitsverteilung ist.

In der Quantenkryptographie werden wir jedoch häufig Zustände begegnen, die teils klassisch, teils quantenmechanisch sind.

- **Definition 5.3.3 klassischer Quantenzustand**

Der klassische Quantenzustand hat die Form:

$$\rho_{XQ} = \sum_{x=0}^{d-1} p_x |x\rangle \langle x|_X \otimes \rho_x^Q$$

Dieser Zustand hat ein klassisches Register X und ein Quantenregister Q. Wenn es kein Quantenregister gibt, dann ist dies nur ein klassischer Zustand.

7.1.4 Informationstheorie

Stellen Sie sich vor, wir haben einen Zustand $\rho_x = \sum_{x=0}^{d-1} p_x |x\rangle \langle x|_X$. Beachten Sie, dass dies bedeutet, dass wir effektiv die Wahrscheinlichkeitsverteilung p_x über die Zeilen x betrachten. Wie können wir die inhärente p_x Unsicherheit messen? Apropos verschiedene Arten von Kommunikation, eines der wichtigen Maße ist die von Neumann- oder Shannon-Entropie $H(X) = -\sum_x p_x \log p_x$. Doch ist diese Maßnahme zur Auswertung im Kontext der Kryptografie geeignet?

Leider kann dieses Maß im Kontext der Kryptographie nicht verwendet werden, da wir hier eine Mittelung über alle möglichen Ergebnisse verwenden, während wir die schlechteste der möglichen Optionen betrachten müssen. Heute gibt es jedoch eine alternative Maßnahme, die in diesem Abschnitt verwendet werden kann.

- **Definition 5.4.1. Minimumentropie**

Für jede Wahrscheinlichkeitsverteilung $\{p_x\}$ wird die *Minimumentropie* H_{min} geschätzt als

$$H_{\min}(X) = -\log \max_x p_x$$

Im Allgemeinen wird die Wahrscheinlichkeit, dass wir die gesamte Bitfolge erraten, als $P_{guess}(X) = \max_x p_x$ geschätzt. In diesem Fall,

$$P_{guess}(X) = -\log P_{guess}(X)$$

Können wir auch die Unsicherheit über X quantifizieren, wenn wir ein zusätzliches Quantenregister E haben? Es stellt sich heraus, dass es wie bei der von Neumann-Entropie eine bedingte Variante $H_{\min}(X|E)$ für die Minimumentropie gibt. Der einfachste Weg, über die bedingte Minimumentropie nachzudenken, ist die Wahrscheinlichkeit, mit der Eve es schafft X zu raten, indem sie auf ihr Quantenregister E zugreift.

- **Definition 5.4.2 bedingte Minimumentropie**

Stellen Sie sich einen zweiseitigen klassischen Quantenzustand ρ_{XE} vor, wobei X das klassische Register ist. Dann kann die *bedingte Minimumentropie* $H_{\min}(X|E)^{\varepsilon}$ geschrieben werden als

$$H_{\min}(X|E) = -\log P_{guess}(X|E)$$

wobei $P_{guess}(X|E)$ die Wahrscheinlichkeit ist, dass Eve x errät, maximiert über alle möglichen Quantendimensionen. Es kann dargestellt werden als:

$$P_{guess}(X|E) = \max_{\{M_x\}} x \sum_x p_x \mathrm{Tr}\left[M_x \rho_x^E\right]$$

wobei die Maximierung über alle POMs [6] übernommen wird $\{M_x \geq 0 | \sum_x M_x = \mathbb{I}\}$. In diesem Zusammenhang wird E als Drittinformation über X bezeichnet.

Aufgrund der Unvollkommenheit des Protokolls oder der Algorithmen können wir jedoch oft nicht genau den Zustand ρ_{XE} erzeugen, den wir wollen, sondern wir können versuchen, einen ähnlichen (ε-nahen) Zustand ρ'_{XE} zu schaffen. Aus diesem Grund ist es meist physikalischer, die geglättete Minimumentropie zu betrachten, die uns den Maximalwert von $H_{\min}(X|E)$ über alle $\rho'_{XE} \in \mathscr{B}^{\varepsilon}(\rho_{XE})$ liefert.

- **Definition 5.4.3 geglättete bedingte Minimumentropie**

Stellen Sie sich einen zweiseitigen klassischen Quantenzustand ρ_{XE} vor, wobei X das klassische Register ist. Dann kann die *geglättete bedingte Minimumentropie* $H_{\min}(X|E)^{\varepsilon}$ geschrieben werden als:

$$H_{\min}(X|E)^{\varepsilon}_{\rho} = \max_{\rho' \in \mathscr{B}(\rho')} H_{\min}(X|E)_{\rho'}$$

In der klassischen Informationstheorie kann die Unsicherheit über eine Variable **A** bei gegebener Fremdinformation **B** durch die Anzahl der Bits quantifiziert werden, die zusätzlich zu **B** bekannt sein müssen, um **A** zu rekonstruieren. Obwohl diese Zahl unterschiedlich sein kann, ist sie (mit Ausnahme der Wahrscheinlichkeit der Ordnung $\varepsilon > 0$) nicht mehr als die ε-glatte Minimumentropie $H_{\min}(\mathbf{A}|\mathbf{E})$, geschätzt für eine gemeinsame Verteilung ρ für **A** und **B**. Mit anderen Worten, die

[6] siehe Definition 5.2.7

Anzahl der Bits, die zum Wiederherstellen von **A** aus **B** mit Wahrscheinlichkeit $1-O(\varepsilon)$ erforderlich sind, liegt im Intervall

$$I = \left[H^{\varepsilon}_{\min}(\mathbf{A}|\,\mathbf{B})_{\rho}, H^{\varepsilon}_{\max}(\mathbf{A}|\,\mathbf{B})_{\rho}\right]$$

dessen Grenzen durch ε-glatte Entropien definiert sind.

Derselbe Ansatz kann auch angewendet werden, wenn **A** und **B** Quantensysteme sind. Die erforderliche Anzahl von Bits zum Eliminieren der Unsicherheit liegt ebenfalls im Intervall, mit einem Unterschied ρ hier ist ein Dichteoperator, der den gemeinsamen Zustand von **A** und **B** beschreibt.

Die Grenzen dieses Intervalls zu finden, ist eines der zentralen Probleme der Informationstheorie. Trotzdem ist die Berechnung glatter Entropien für große Systeme **A** mit großen Schwierigkeiten verbunden. Um dieses Problem zu lösen, ist es üblich, bestimmte Näherungen zu verwenden. Eine besonders beliebte Methode sowohl in der klassischen als auch in der Quanteninformationstheorie ist die Annäherung, die davon ausgeht, dass das System aus einer Menge voneinander unabhängiger und gleich wahrscheinlicher Prämissen besteht. Genauer gesagt erfordert diese Näherung, dass das System die Form $A = A_1^n = A_1 \otimes \ldots \otimes A_n$ hat. Die dritte Information hat eine ähnliche Struktur $B = B_1^n = B_1 \otimes \ldots \otimes B_n$ und der gemeinsame Zustand des Systems $\rho_{A_1 B_1 \ldots A_n B_n} = \nu_{AB}^{\otimes n}$, wobei $\nu_{AB}^{\otimes n}$ ein willkürlicher Dichteoperator ist. Ein grundlegendes Ergebnis der Informationstheorie, die asymptotische Gleichverteilungseigenschaft zeigt, dass das Unsicherheitsintervall den folgenden Ausdruck erfüllt:

$$I \subset \left[n\left(H(\mathbf{A}|\,\mathbf{B})_{\nu} - \frac{c_{\varepsilon}}{\sqrt{n}}\right), n\left(H(\mathbf{A}|\,\mathbf{B})_{\nu} + \frac{c_{\varepsilon}}{\sqrt{n}}\right)\right]$$

Wobei c_{ε} eine von n unabhängige Konstante, $H(A|\,B)_{\nu}$ die für den Zustand $\nu_{AB}^{\otimes n}$ geschätzte bedingte von Neumann-Entropie ist. Mit anderen Worten, für große n ist die Gesamtunsicherheit von A_1^n bei gegebenem B_1^n gut angenähert durch $n \cdot H(\mathbf{A}|\,\mathbf{B})_{\nu} = \sum_i H(\mathbf{A_i}|\,\mathbf{B_i})_{\rho}$. Somit wird die Entropie des individuellen Systems $\mathbf{A_i}$ durch die Entropie des allgemeinen Systems A_1^n akkumuliert.

7.2 Mathematische Beschreibung von Quantenkanälen

7.2.1 Allgemeine Eigenschaften von Informationskanälen

Die Quanten- und damit auch die klassische Informationstheorie betrachtet wechselseitige Übergänge zwischen verschiedenen Informationsressourcen. Ressourcen können Quanten oder klassisch, statisch oder dynamisch, verrauscht oder ideal sein. Ressourcen werden auch durch die Anzahl der Benutzer geteilt, meistens werden Zwei-Benutzer-Ressourcen als einfachster Fall herausgegriffen (Ressourcen eines Benutzers gelten als unbegrenzt). Lassen Sie uns die Notation für Ressourcen einführen: c klassisch, q Quantum, $\{\bullet\}$ mit Rauschen, $[\bullet]$ ideal, $\rightarrow$ dynamisch.

Dynamische Ressourcen sind vier Arten von Kanälen, die durch die quantenmechanische/klassische Natur der Eingabe-/Ausgabedaten bestimmt werden. So ist zum Beispiel $\{c \rightarrow c\}$ ein klassischer Kommunikationskanal, der durch eine beliebige stochastische Matrix definiert ist, $\{q \rightarrow q\}$ ist ein Quantenkommunikationskanal, der durch eine beliebige vollständig positive spurerhaltende Abbildung definiert ist, $\{c \rightarrow q\}$ ist der Präparation eines Quantenzustands mit einem beliebigen Quant Das Alphabet $\{\rho_x\}$, $\{q \rightarrow c\}$ ist eine verallgemeinerte Quantenmessung mit einem klassischen Ergebnis, das durch ein beliebiges positives definites Maß gegeben ist. Das Ersetzen von geschweiften Klammern durch eckige Klammern ergibt die entsprechenden idealen Kanäle mit Einheitsbandbreite (unter Beibehaltung der entsprechenden Dimensionen Bit/Qubit und Qubit/Bit).

Es gibt drei Arten von statischen Ressourcen: klassische cc, Quanten- qq und gemischte quantenklassische cq. Der erste Typ ist ein korreliertes Paar von Zufallsvariablen X und Y, die auf der Menge $\mathcal{X} \times \mathcal{Y}$ definiert sind und eine gemeinsame Wahrscheinlichkeitsverteilung $p(x,y) = \Pr\{X = x, Y = y\}$ haben. Der Quantentyp $\{qq\}$ ist das Zwei-Teilchen-Quantensystem $\mathcal{AB}$, das auf dem Hilbert-Raum $\mathcal{H}_\mathcal{A} \otimes \mathcal{H}_\mathcal{B}$ definiert ist und den Dichteoperator $\rho^{\mathcal{AB}}$ hat. Die Ressource $\{cq\}$ ist ein hybrides quantenklassisches System $\mathcal{XQ}$, das durch das Ensemble $\{\rho_x, p(x)\}$ beschrieben wird, wobei p_x auf der Menge $\mathcal{X}$ definiert ist und ρ_x die Menge der Dichteoperatoren des Systems $\mathcal{Q}$ sind im Hilbertraum $\mathcal{H}_\mathcal{Q}$. Der Zustand des Systems $\mathcal{Q}$ wird mit dem Wert der klassischen Variablen X korreliert. Zur Beschreibung der Ressource $\{cq\}$ verwenden sie den „erweiterten Hilbertraum“ (GSE), wobei die Erweiterung als Ergänzung eines Subsystems $\mathcal{A}$ verstanden wird, das die klassische Variable in der Quantensprache beschreibt. Somit kann das Ensemble $\{\rho_x, p(x)\}$ durch einen einzigen Dichteoperator $\rho^{\mathcal{AQ}} = \sum_x p(x) |x\rangle \langle x|^\mathcal{A} \otimes \rho_x^\mathcal{Q}$ dargestellt werden, wobei $\{|x\rangle : x \in \mathcal{X}\}$ eine orthonormale Basis im Hilbertraum $\mathcal{H}_\mathcal{A}$ des Systems $\mathcal{A}$ ist.

Die ideale Ressource $[cc]$ ist eine vollständig korrelierte Zufallsvariable, die $\mathcal{X} = \mathcal{Y}$ und $p(x,y) = p(x)\,\delta(x,y)$ erfüllt. Die Ressource $[qq]$ ist ein vollständig verschränkter Zustand

$$|\psi\rangle_{\mathcal{AB}} = \frac{1}{\sqrt{2}} \left(|0\rangle_\mathcal{A}|0\rangle_\mathcal{B} + |1\rangle_\mathcal{A}|1\rangle_\mathcal{B}\right)$$

des Systems $\mathcal{AB}$.

So können verschiedene Quanteninformatikprotokolle als Ressourcentransformationsprozesse dargestellt werden, zum Beispiel $\{qq\} + [cc] \Rightarrow [qq]$ ist die Verschränkungsverstärkung, $\{c \rightarrow c\} \Rightarrow [c \rightarrow c]$ ist das Shannon-Theorem, $[c \rightarrow c] + [qq] \Rightarrow [q \rightarrow q]$ die Quantenteleportation usw. usf. Die Quantenkommunikations- und Kryptografieprotokolle wiederum können als die folgenden sequentiellen Transformationen von Ressourcen dargestellt werden:

$$\{c \rightarrow q\} + \{q \rightarrow q\} + \{q \rightarrow c\} + [c \rightarrow c] \Rightarrow [cc]$$

Wobei $\{c \rightarrow q\}$ die Präparation von Zuständen durch Alice ist, $\{q \rightarrow q\}$ die Verteilung von Zuständen durch den Quantenkanal ist, $\{q \rightarrow c\}$ die Messung von Zuständen durch Bob (und Eva) ist, $[c \rightarrow c]$ ist die klassische Nachbearbeitung des „rohen“ Schlüssels und erhöhte Geheimhaltung. Als Nächstes werfen wir einen genaueren Blick auf die $\{q \rightarrow q\}$-Stufe und die damit verbundenen Funktionen.

7.2.2 Signalausbreitung in Quantenkanälen

Stellen Sie sich ein Quantensystem vor, das aus einem Subsystem S einem Quantensignal E der äußeren Umgebung (einschließlich des Kanals selbst) besteht. Jedes der Subsysteme ist auf dem entsprechenden Hilbert-Raum $\mathcal{H}_{\mathcal{S}}$ und $\mathcal{H}_{\mathcal{E}}$ definiert. Der Hamiltonoperator des allgemeinen Systems wird ausgedrückt als

$$\widehat{H} = \widehat{H}_S \otimes \widehat{I}_E + \widehat{I}_S \otimes \widehat{H}_E + \widehat{H}_I$$

wobei $\widehat{H}_S$ und $\widehat{H}_E$ die Hamiltonoperatoren der entsprechenden Subsysteme sind, $\widehat{H}_I$ der Wechselwirkungshamiltonoperator ist, $\widehat{I}_S$ und $\widehat{I}_E$ die Identitätsoperatoren der entsprechenden Subsysteme sind. Die zeitliche Entwicklung, die die Transformation des gemeinsamen Zustands ρ_{SE} beschreibt, ist einheitlich (wenn man den gemeinsamen Zustand als rein betrachtet) und sieht folgendermaßen aus:

$$\rho_{SE}(t) = \widehat{U}(t) \cdot \rho_{SE} \cdot \widehat{U}^{\dagger}(t)$$

Wobei $\widehat{U}(t) = e^{-\frac{i\widehat{H}t}{\hbar}}$ der unitäre Entwicklungsoperator ist. Unter der Annahme, dass zum Anfangszeitpunkt das Signalteilsystem und das Umgebungsteilsystem nicht vermischt sind, d.h. $\rho_{SB} = \rho_S \otimes \rho_B$, so wird die Entwicklung aussehen

$$\rho_{SB}(t) = \widehat{U}(t) \cdot \rho_S \otimes \rho_B \cdot \widehat{U}^{\dagger}(t)$$

Der Wechselwirkungs-Hamiltonoperator kann ausgedrückt werden als

$$\widehat{H}_I = \sum_i \widehat{S}_i \otimes \widehat{E}_i$$

Wobei $\widehat{S}_i \otimes \widehat{E}_i$ eine Menge von Operatoren ist, die auf den kombinierten Raum beider Subsysteme wirken, $\widehat{S}_i$ und $\widehat{E}_i$ Operatoren sind, die auf den Raum des entsprechenden Subsystems wirken.

Die vorgestellte Beschreibung der Wechselwirkung eines Signals mit der Außenwelt (und/oder einem Quantenkanal) ist die allgemeinste. Es kann verwendet werden, um verschiedene physikalische Phänomene und Prozesse zu beschreiben, die bei Quantenzuständen auftreten, wie z. B. Dämpfung, Dekohärenz, Depolarisation usw.

- **Beispiel 6.2.1.**

Betrachten Sie den Prozess der Dekohärenz. Die Interaktion mit der Außenwelt führt zu einer Dekohärenz des Quantenzustands, seiner Zerstörung. Nachdem wir das Subsystem der E-Umgebung entzogen haben, mit anderen Worten, das Umweltsubsystem verworfen haben und betrachten nur die Entwicklung des Signalsubsystems, ergibt sich

$$\rho_S(t) = \mathrm{Tr}_E\left(\widehat{U}(t)\,\rho_S \otimes \rho_E \widehat{U}^{\dagger}(t)\right)$$

Wobei $\rho_S(t)$ eine degenerierte Dichtematrix ist, die nur ein Signalsubsystem beschreibt. Wenn das Umweltsubsystem zum Anfangszeitpunkt durch die orthogonale Basis (im Raum des Subsystems) beschrieben wird, d.h. sein Dichteoperator ist diagonalisiert $\rho_E(0) = \sum_i a_i |i\rangle\langle i|$ dann kann eine teilweise Spur (nach dem Subsystem) unter Verwendung von Kraus-Operatoren [7] beschrieben werden

$$\rho_E(t) = \sum_j \widehat{A}_j \cdot \rho_S(0) \cdot \widehat{A}_j^{\dagger}$$

Wobei $\widehat{A}_j = \sqrt{a_i}\,\langle j|\,\widehat{U}\,|i\rangle$ der Operator von Kraus ist, beschrieben durch die sogenannte Zersetzung der Einheit, d.h. $\sum_j \widehat{A}_j^{\dagger}\widehat{A}_j = \widehat{I}_S$, mit der Eigenschaft $\mathrm{Tr}[\rho_S(t)] = 1$. Trotz der Tatsache, dass im allgemeinen System die Transformation $\widehat{U}$ einheitlich war, erfährt das Subsystem eine neuere Transformation, die im allgemeinen Fall zur teilweisen oder vollständigen (abhängig von der Zeit und Stärke der Wechselwirkung) Zerstörung des Quantenzustands führt.

[7] Die Kraus-Darstellung ist eine Darstellungsform von Quantenkanälen, die die Dynamik eines Quantensystems beschreibt.

- **Beispiel 6.2.2.**

Betrachten Sie den Prozess der Depolarisation eines willkürlichen Zustands ρ, der im Allgemeinen beschrieben werden kann als

$$\rho \to (1-\delta)\,\rho + \frac{\delta}{3}\sum_i \sigma_i \rho \sigma_i$$

Wobei σ_i ein vollständiger Satz von Pauli-Matrizen ist [8], die verschiedene Polarisationskomponenten eines Quantenzustands transformieren, δ der Depolarisationskoeffizient ist, der eine sehr wichtige Rolle in den Polarisationsprotokollen der Quantenkommunikation und Kryptografie spielt.

- **Beispiel 6.2.3.**

Betrachten Sie den kohärenten Zustand $\rho = |\alpha\rangle\langle\alpha|$ und der Vorgang seiner Dämpfung durch die Lindblad-Operatoren [9]

$$\tilde{\rho} = e^{-\gamma a^\dagger a}\,|\alpha\rangle\langle\alpha|\,e^{-\gamma a a^\dagger} = |\gamma\alpha\rangle\langle\gamma\alpha|$$

wobei γ der Dämpfungsfaktor der Amplitude ist. Es ist erwähnenswert, dass dieser Faktor kein allgemein akzeptierter Leistungsdämpfungsfaktor η ist, der oft in *dB* ausgedrückt wird. Das Verhältnis dieser Koeffizienten wird ausgedrückt als $\gamma = 10^{-\frac{\eta}{10}}$.

[8] Die Pauli-Matrizen $\sigma_1, \sigma_2, \sigma_3$ sind spezielle komplexe hermitesche 2×2-Matrizen. Zusammen mit der 2×2-Einheitsmatrix bilden sie eine Basis des 4-dimensionalen reellen Vektorraums.

[9] In der Quantenmechanik bezeichnet als die nichtunitäre Evolution des Dichteoperators ρ, spurerhaltend und komplett positiv für alle Anfangsbedingungen.

8 Quantenkommunikation im freien Raum und in Weltraum

9 Quanten-Zufallszahlengeneratoren

LaTeX 2_ε