

Quantenkanalkapazität

Seminar: Quanteninformation - Entwicklung, Protokolle, Technologien

Marco Möller

24.05.2007

Inhalt

- 1 Information
 - Definition
 - Bedingte -/ Transinformation
- 2 Kodierung ohne Rauschen
 - Problemstellung
 - typische Unterräume
 - Satz von Schumacher
 - Beispiel: Schumacher-Kompression
- 3 Kodierung unter Rauschen
 - klassisch
 - QM
- 4 Ende
 - Literatur
 - Fragen

Information

Definitionen

- *Shannon Entropie*

$$H(X) \equiv - \sum_x p_x \log p_x$$

- *Von Neumann Entropie*

$$S(X) \equiv \text{tr}(\rho \log \rho)$$

Korrolar (Shannon Entropie ist Spezialfall)

falls $\rho = \sum_x p_x |x\rangle \langle x|$ *und* $\langle x|y\rangle = \delta_{xy}$

$$S(X) = H(X)$$

- Einheit ist *bit* bzw. *qubit*
- \log ist zur Basis 2

weitere Informationen

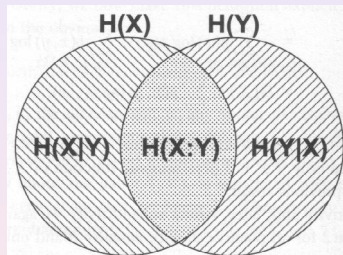
Definitionen

- *bedingte Entropie*

$$H(X|Y) = H(X, Y) - H(Y)$$

- *Transinformation (mutual information)*

$$\begin{aligned} H(X : Y) &= H(X) + H(Y) - H(X, Y) \\ &= H(X) - H(X|Y) \end{aligned}$$



Analog für $S(X)$

Maße für Operatoren

- Wie gleich sind sich zwei Quantenzustände? → benötigen besseres Kriterium als Identität, um Grenzwerte bilden zu können
- Viele Möglichkeiten, so etwas zu definieren

Definition (Fidelity)

- *Statische Fidelity:*

$$F(\rho, \sigma) = \text{tr} \sqrt{\rho^{\frac{1}{2}} \sigma \rho^{\frac{1}{2}}}$$

- *Dynamische Fidelity (ρ verglichen mit $\epsilon(\rho)$): Sei ϵ eine spurerhaltene Quantenoperation mit den Kraus-Operatoren E_i*

$$F(\rho, \epsilon) = \sum_i |\text{tr}(\rho E_i)|^2$$

- $F(\rho, \text{id}) = 1$

Problemstellung klassisch

Quelle entspricht einer Folge von Zufallsvariablen X_1, X_2, \dots über einem endlichen Alphabet

- die Werte entsprechen einer möglichen Ausgabe der Quelle
- die X_i sind identisch verteilt und unabhängig zueinander (independent, identical distributed = i.i.d.)

Frage: wie oft müsste man einen störungsfreien binären Kanal mindestens im Mittel pro generierten Symbol benutzen ($\hat{=}$ Rate).

- Kann auch als *Kompression* aufgefasst werden.

Satz (Shannon: rauschfreie Kanalkodierung)

Sei $\{X_i\}$ eine i.i.d Informationsquelle mit einer Entropierate $H(X)$. Sei $R > H(X)$. Dann existiert ein zuverlässiges Kompressionsschema der Rate R für diese Quelle. Umgekehrt ist wäre jedes Kompressionsschema für $R < H(X)$ nicht zuverlässig.

Motivation: typische Sequenzen

- Im binären Fall:

$$p(x_1, \dots, x_n) = p(x_1) p(x_2) \cdots p(x_n) \approx p^{np} (1-p)^{n(1-p)}$$

- $\log p(x_1, \dots, x_n) \approx np \log p + (1-p)n \log(1-p) = -nH(X)$
- $p(x_1, \dots, x_n) \approx 2^{-nH(X)}$
- Es kann also nur ca. $2^{nH(X)}$ Sequenzen geben, die häufig vorkommen.
- \Rightarrow ein um den Faktor $H(X)$ kürzere umkodierte Sequenz reicht aus, um die typischen Sequenzen zu kodieren.
- Kodierung, die das ausnutzt: Huffman-Kodierung[2]

Problemstellung quantenmechanisch

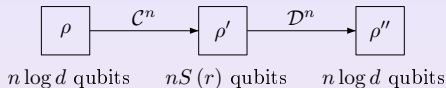


Abbildung: (De)Kompression einer Quanteninformationsquelle [1]

Quelle (i.i.d.) wird durch einen Hilbertraum H und einem Dichteoperator ρ darauf beschrieben

Kompressionsschema der Rate R besteht aus zwei Familien von Quantenoperationen C^n und D^n

Kompression $C^n : H^{\otimes n} \rightarrow 2^{Rn}$

Dekompression $D^n : 2^{Rn} \rightarrow H^{\otimes n}$

Zuverlässig ist ein Kompressionsschema, wenn die Fehlerrate $D^n \circ C^n$ auf $\rho^{\otimes n}$ für große n gegen 0 geht, bzw. $F(\rho^{\otimes n}, D^n \circ C^n) \rightarrow 1$.

Verallgemeinerung von klassischem Fall

Gesetz der großen Zahlen

Satz (Gesetz der großen Zahlen)

Seien X_1, X_2, \dots i.i.d. mit endlichem ersten und zweiten Moment. Dann ist für jedes $\epsilon > 0$

$$\lim_{n \rightarrow \infty} p \left(\left| \frac{1}{n} \sum_{i=1}^n X_i - E(X) \right| \leq \epsilon \right) = 1$$

ϵ -typisch

Definition (ϵ -typisch)

Sei $\rho = \sum_x p(x) |x\rangle \langle x|$ orthonormale Dekomposition. Eine Sequenz x_1, \dots, x_n wird ϵ -typisch genannt, falls

$$\left| \frac{1}{n} \log \left(\frac{1}{p(x_1) p(x_2) \cdots p(x_n)} \right) - S(\rho) \right| \leq \epsilon$$

gilt. Entsprechend wird ein zugehöriger Zustand $|x_1\rangle |x_2\rangle \cdots |x_n\rangle$ ϵ -typisch genannt.

Der Unterraum aller ϵ -typischen Zustände wird $T(n, \epsilon)$ genannt. Der entsprechende Projektor auf diesen Unterraum ist

$$P(n, \epsilon) = \sum_{x \text{ } \epsilon\text{-typisch}} |x_1\rangle \langle x_1| \otimes \cdots \otimes |x_n\rangle \langle x_n|$$

Satz über typische Unterräume

Satz (über typische Unterräume)

- ① Sei $\epsilon > 0$. Für jedes $\delta > 0$ und genügend große n gilt:

$$\text{tr}(P(n, \epsilon) \rho^{\otimes n}) \geq 1 - \delta$$

- ② Für jedes $\epsilon > 0$ und $\delta > 0$ und genügend große n erfüllt die Dimension $|T(n, \epsilon)| = \text{tr}(P(n, \epsilon))$ von $T(n, \epsilon)$

$$(1 - \delta) 2^{n(S(\rho) - \epsilon)} \leq |T(n, \epsilon)| \leq 2^{n(S(\rho) + \epsilon)}$$

- ③ Sei $S(n)$ ein Projektor auf einen beliebigen Unterraum von $H^{\otimes n}$ mit Dimension kleiner 2^{nR} . Sei $R < S(\rho)$. Dann gilt für alle $\delta > 0$ und genügend große n

$$\text{tr}(S(n) \rho^{\otimes n}) \leq \delta$$

Beweis: Satz typische Unterräume - Teil 1

- Zu zeigen: $\text{tr}(P(n, \epsilon) \rho^{\otimes n}) \geq 1 - \delta$
- $\text{tr}(P(n, \epsilon) \rho^{\otimes n}) = \sum_{x \in T(n, \epsilon)} p(x_1) p(x_2) \cdots p(x_n) =$ W-keit, dass eine Sequenz ϵ -typisch ist
- Entspricht

$$p \left(\left| \frac{1}{n} \log \left(\frac{1}{p(x_1) p(x_2) \cdots p(x_n)} \right) - S(\rho) \right| \leq \epsilon \right) \geq 1 - \delta$$

- Sei X eine Zufallsvariable mit der Verteilung der x_i .

$$p \left(\left| \sum_{i=1}^n \frac{-\log p(x_i)}{n} - E(-\log X) \right| \leq \epsilon \right) \geq 1 - \delta$$

- Gesetz der großen Zahlen

Beweis: Satz typische Unterräume - Teil 2

- Zu zeigen: $(1 - \delta) 2^{n(S(\rho) - \epsilon)} \leq |T(n, \epsilon)| \leq 2^{n(S(\rho) + \epsilon)}$
- Aus Def. lässt sich Abschätzung gewinnen:

$$\left| \frac{1}{n} \log \left(\frac{1}{p(x_1) p(x_2) \cdots p(x_n)} \right) - S(\rho) \right| \leq \epsilon$$

$$S(\rho) - \epsilon \leq \frac{1}{n} \log \left(\frac{1}{p(x)} \right) \leq S(\rho) + \epsilon$$

$$-n(S(\rho) - \epsilon) \geq \log(p(x)) \geq -n(S(\rho) + \epsilon)$$

$$2^{-n(S(\rho) - \epsilon)} \geq p(x) \geq 2^{-n(S(\rho) + \epsilon)}$$

- $1 \geq \sum_{x \in T(n, \epsilon)} p(x) \geq \sum_{x \in T(n, \epsilon)} 2^{-n(S(\rho) + \epsilon)} = |T(n, \epsilon)| 2^{-n(S(\rho) + \epsilon)}$
- $|T(n, \epsilon)| \leq 2^{n(S(\rho) + \epsilon)}$
- $1 - \delta \leq \sum_{x \in T(n, \epsilon)} p(x) \leq \sum_{x \in T(n, \epsilon)} 2^{-n(S(\rho) - \epsilon)} = |T(n, \epsilon)| 2^{-n(S(\rho) - \epsilon)}$
- $|T(n, \epsilon)| \geq (1 - \delta) 2^{n(S(\rho) - \epsilon)}$

Beweis: Satz typische Unterräume - Teil 3

- Zu zeigen: $|S(n)| < 2^{nR} < 2^{nS(\rho)} \Rightarrow \text{tr}(S(n)\rho^{\otimes n}) \leq \delta$
- Aufteilen der Spur in den typischen Unterraum und den Rest

$$\text{tr}(S(n)\rho^{\otimes n}) = \text{tr}(S(n)\rho^{\otimes n}P(n,\epsilon)) + \text{tr}(S(n)\rho^{\otimes n}(I - P(n,\epsilon)))$$

- Da der Projektor $P(n,\epsilon)$ mit $\rho^{\otimes n}$ kommutiert, gilt:

$$\rho^{\otimes n}P(n,\epsilon) = P(n,\epsilon)\rho^{\otimes n}P(n,\epsilon)$$

- Da die Eigenwerte beschränkt sind, gilt:

$$\begin{aligned} \text{tr}(S(n)P(n,\epsilon)\rho^{\otimes n}P(n,\epsilon)) &\leq 2^{nR}2^{-n(S(\rho)+\epsilon)} \\ &= 2^{-n(S(\rho)-R+\epsilon)} \rightarrow 0 \end{aligned}$$

- Es gilt $S(n) \leq I$. Da $S(n)$ und $\rho^{\otimes n}(I - P(n,\epsilon))$ positive Operatoren sind, gilt:

$$0 \leq \text{tr}(S(n)\rho^{\otimes n}(I - P(n,\epsilon))) \leq \text{tr}(\rho^{\otimes n}(I - P(n,\epsilon))) \rightarrow 0$$

□

Satz von Schumacher

Satz (Schumacher: quantenmechanische rauschfreie Kanalkodierung)

Sei $\{H, \rho\}$ eine i.i.d. Quanteninformationsquelle. Für $R > S(\rho)$ existiert ein zuverlässiges Kompressionschema der Rate R für diese Quelle. Umgekehrt ist wäre jedes Kompressionschema für $R < S(\rho)$ nicht zuverlässig.

- Zuverlässig entspricht $F(\rho, \cdot) \rightarrow 1$ für $n \rightarrow \infty$

Beweis: Satz von Schumacher - Existenz - Teil 1

- Zu zeigen: Wenn $R > S(\rho)$, dann $F(\rho, \cdot) \rightarrow 1$
- wähle $\epsilon > 0$ so, dass $S(\rho) + \epsilon \leq R$.
- Aus Theorem über typische Unterräume: Für jedes $\delta > 0$ und genügend große n gilt:

$$\begin{aligned} \text{tr}(\rho^{\otimes n} P(n, \epsilon)) &\geq 1 - \delta \\ |T(n, \epsilon)| &\leq 2^{nR} \end{aligned}$$

- Sei H_c^n ein 2^{nR} -dimensionaler Hilbertraum, der $T(n, \epsilon)$ enthält.

Beweis: Satz von Schumacher - Existenz - Teil 2

- Komprimiere mit $A_i \equiv |0\rangle \langle i|$, wobei $|i\rangle$ orthonormale Basis, die orthogonal zum typischen Unterraum ist; $|0\rangle$ ein beliebiger Vektor aus dem typischen Unterraum.

$$\mathcal{C}^n(\sigma) = P(n, \epsilon) \sigma P(n, \epsilon) + \sum_i A_i \sigma A_i^\dagger$$

- Dekodieren \mathcal{D}^n ist als Identität auf H_c^n definiert.

$$\begin{aligned} F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) &= |\text{tr}(\rho^{\otimes n} P(n, \epsilon))|^2 + \sum_i |\text{tr}(\rho^{\otimes n} A_i)|^2 \\ &\geq |\text{tr}(\rho^{\otimes n} P(n, \epsilon))|^2 \\ &\geq |1 - \delta|^2 \geq 1 - 2\delta \end{aligned}$$

Beweis: Satz von Schumacher - Optimal - Teil 1

- Zu zeigen: Wenn $R < S(\rho)$ dann $F(\rho, \cdot) \rightarrow 0$
- oBdA \mathcal{C}^n bildet in einen 2^{nR} -dim Unterraum von $H^{\otimes n}$ ab (zugehöriger Projektor $S(n)$)
- Seien C_j die Operatorelemente von \mathcal{C}^n und D_k die von \mathcal{D}^n .

$$F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) = \sum_{jk} |\text{tr}(D_k C_j \rho^{\otimes n})|^2$$

- Jeder der Operatoren C_j bildet in den Unterraum von $S(n)$ ab:
 $C_j = S(n) C_j$
- Sei $S^k(n)$ der Projektor auf den Unterraum, auf den $D_k S(n)$ abbildet:

$$S^k(n) D_k S(n) = D_k S(n)$$

$$\begin{aligned} D_k C_j &= D_k S(n) C_j \\ &= S^k(n) D_k S(n) C_j \\ &= S^k(n) D_k C_j \end{aligned}$$

Beweis: Satz von Schumacher - Optimal - Teil 2

- Damit ergibt sich (mit Cauchy-Schwarz-Ungleichung)

$$\begin{aligned}
 F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) &= \sum_{jk} |\text{tr}(D_k C_j \rho^{\otimes n} S^k(n))|^2 \\
 &\leq \sum_{jk} \text{tr}(D_k C_j \rho^{\otimes n} C_j^\dagger D_k^\dagger) \text{tr}(S^k(n) \rho^{\otimes n} S^k(n))
 \end{aligned}$$

- Nach dem Satz über typische Unterräume gilt mit der Spurerhaltung von C_j, D_k :

$$\begin{aligned}
 F(\rho^{\otimes n}, \mathcal{D}^n \circ \mathcal{C}^n) &\leq \delta \sum_{jk} \text{tr}(D_k C_j \rho^{\otimes n} C_j^\dagger D_k^\dagger) \\
 &= \delta
 \end{aligned}$$

□

Beispiel: Schumacher-Kompression 1

- Sei ein i.i.d. Quantenquelle, die

$$\begin{aligned}
 |\psi_0\rangle &= |0\rangle \\
 |\psi_1\rangle &= \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle)
 \end{aligned}$$

jeweils mit Wahrscheinlichkeit $\frac{1}{2}$ emittiert

- dies entspricht der Dichtematrix

$$\begin{aligned}
 \rho &= \frac{1}{2} |\psi_0\rangle \langle \psi_0| + \frac{1}{2} |\psi_1\rangle \langle \psi_1| \\
 &= \frac{1}{4} \begin{bmatrix} 3 & 1 \\ 1 & 1 \end{bmatrix}
 \end{aligned}$$

Beispiel: Schumacher-Kompression 2

- mit orthonormaler Dekomposition:

$$\begin{aligned}\rho &= p |\bar{0}\rangle \langle \bar{0}| + (1-p) |\bar{1}\rangle \langle \bar{1}| \\ |\bar{0}\rangle &= \cos \frac{\pi}{8} |0\rangle + \sin \frac{\pi}{8} |1\rangle \\ |\bar{1}\rangle &= -\sin \frac{\pi}{8} |0\rangle + \cos \frac{\pi}{8} |1\rangle \\ p &= \frac{1}{4} \left(3 + \tan \frac{\pi}{8} \right) \approx 0.85\end{aligned}$$

- Bzgl. dieser Basis lässt sich ein Block aus n qubits schreiben als

$$\sum_{x=\{\bar{0}\bar{0}\dots\bar{0}, \bar{0}\bar{0}\dots\bar{0}\bar{1}, \dots, \bar{1}\bar{1}\dots\bar{1}\}} c_x |X\rangle$$

- Nur typische Sequenzen $|X\rangle$ müssen übertragen werden. Bei diesen ist das Hamminggewicht (Anz. $\bar{1}$ en) ca. $n(1-p)$
- Da $p \gg (1-p)$ müssen nur die $|X\rangle$ berücksichtigt werden, die viele $\bar{0}$ en enthalten

Beispiel: Schumacher-Kompression 3

- Bsp. $n = 3$. Sortiere alle Möglichkeiten aufsteigend nach Hamminggewicht und ordne ihnen eine Kodierung zu

000 → 000	011 → 100
001 → 001	101 → 101
010 → 010	110 → 110
100 → 011	111 → 111

- Erwartetes Hamminggewicht liegt bei $(1 - p) 3 \approx 0.44$.
- Da $3S(p) = 3(-p \log p - (1 - p) \log(1 - p)) \approx 1.8 < 2$, reicht folgende Zuordnung

000 → 00	011 → 11
001 → 01	101 → 11
010 → 10	110 → 11
100 → 11	111 → 11

- Dieser Code ist “relativ” zuverlässig. Im Grenzwert $n \rightarrow \infty$ geht die Fehlerwahrscheinlichkeit gegen 0.
- Dies ist nicht der optimale Algorithmus → quantum arithmetic coding

Klassisch: Verrauschter Kanal

Satz (Shannon: verrauschte Kanalkodierung)

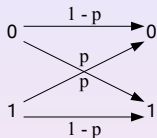
Für einen verrauschten Kanal \mathcal{N} ist die Kapazität gegeben durch

$$C(\mathcal{X}) = \max_{p(x)} H(X : Y)$$

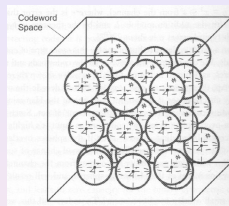
wobei das Maximum über alle Eingangsverteilungen $p(x)$ für X gebildet wird und Y die zugehörige induzierte Zufallsvariable am Ausgang des Kanals ist.

- Kanal wird durch einen Satz von bedingten Wahrscheinlichkeiten $p(x|y) \geq 0$ beschrieben.

Klassischer binärer verrauschter Kanal



klassischer binärer Kanal mit Fehlerwahrscheinlichkeit p



Optimal ist eine Gleichverteilung am Eingang

$$\begin{aligned}
 C(\mathcal{X}) &= \max_{p(x)} H(X : Y) \\
 &= \max_{p(x)} (H(Y) - H(Y|X)) \\
 &= \max_{p(x)} \left(H(Y) - \sum_x p(x) H(Y|X = x) \right) \\
 &= 1 - H_{bin}(p)
 \end{aligned}$$

Beweis: Shannon - verdrauschte Kanalkodierung - Teil 1

- Zu zeigen: für Raten $R < C$ geht die Fehlerwahrscheinlichkeit gegen 0
- Sei $p(x)$ Verteilung, mit der wir ein Wörterbuch generieren.
- Wörterbuch (ist Sender und Empfänger bekannt)

$$\mathcal{C} = \begin{bmatrix} x_1(1) & x_2(1) & \dots & x_n(1) \\ \vdots & \vdots & \ddots & \vdots \\ x_1(2^{nR}) & x_2(2^{nR}) & \dots & x_n(2^{nR}) \end{bmatrix}$$

- Wahrscheinlichkeit, ein spezielles Wörterbuch zu generieren

$$\Pr(\mathcal{C}) = \prod_{\omega=1}^{2^{nR}} \prod_{i=1}^n p(x_i(\omega))$$

- Nachrichten werden gleichverteilt übertragen:

$$\Pr(W = \omega) = 2^{-nR}, \quad \omega = 1, 2, \dots, 2^{nR}$$

Beweis: Shannon - verdrauschte Kanalkodierung - Teil 2

- Empfänger empfängt y^n mit Wahrscheinlichkeit

$$P(y^n | x^n(\omega)) = \prod_{i=1}^n p(y_i | x_i(\omega))$$

- Dekodieren: Es wurde Nachricht \hat{W} geschickt, falls
 - $(X^n(\hat{W}), Y^n)$ gleichzeitig typisch sind
 - es keinen anderen Index k gibt, so dass $(X^n(k), Y^n)$ gleichzeitig typisch sind
- Falls es kein solches \hat{W} gibt, wird ein Standardeintrag ausgegeben.
- Dekodierfehler bei $W \neq \hat{W}$: entspricht dem Ereignis \mathcal{E}

Beweis: Shannon - verdrauschte Kanalkodierung - Teil 3

- Fehlerwahrscheinlichkeit hängt nicht vom Sendewort ab:

$$\begin{aligned}
 \Pr(\mathcal{E}) &= \sum_{\mathcal{C}} P(\mathcal{C}) P_e^{(n)}(\mathcal{C}) \\
 &= \sum_{\mathcal{C}} P(\mathcal{C}) \lambda_1(\mathcal{C}) \\
 &= \Pr(\mathcal{E} | W = 1)
 \end{aligned}$$

- Definiere Ereignis $E_i = \{(X^n(i), Y^n) \text{ sind gleichzeitig typisch}\}$. Für genügend große n und $R < H(X : Y) - 3\epsilon$ gilt:

$$\begin{aligned}
 \Pr(\mathcal{E} | W = 1) &= P(E_1^c \cup E_2 \cup \dots \cup E_{2^{nR}}) \\
 &\leq P(E_1^c) + \sum_{i=2}^{2^{nR}} P(E_i) \\
 &\leq \epsilon + \sum_{i=2}^{2^{nR}} 2^{-n(H(X:Y) - 3\epsilon)} \\
 &\leq 2\epsilon
 \end{aligned}$$

Beweis: Shannon - verdrauschte Kanalkodierung - Teil 4

- Da die durchschnittliche Fehlerwahrscheinlichkeit über alle Wörterbücher $\leq 2\epsilon$ ist, gibt es mindestens ein \mathcal{C}^* mit $P_e^n(\mathcal{C}^*) \leq 2\epsilon$.
- Verwerfe im Wörterbuch die schlechteste Hälfte der Zuordnungen.

Aus

$$P_e^n(\mathcal{C}^*) = \frac{1}{2^{nR}} \sum_i \lambda_i(\mathcal{C}^*) \leq 2\epsilon$$

folgt, das für alle übrigen Zuordnungen gilt: $\lambda_i(\mathcal{C}^*) \leq 4\epsilon$.

- Somit haben wir nur noch 2^{nR-1} Wörterbucheinträge, womit die Rate von R auf $R - \frac{1}{n}$ gesunken ist.
- Insgesamt haben wir einen Code konstruiert mit $R' = R - \frac{1}{n}$ und Fehlerwahrscheinlichkeit $\lambda^{(n)} \leq 4\epsilon$.

□

Beweis: Shannon - verdrauschte Kanalkodierung - Umkehrung

- Umgekehrt gilt:
- $nR = H(W) = H(W|Y^n) + H(W : Y^n)$
- $\leq H(W|Y^n) + I(X^n(W)|Y^n)$
- Fanos Ungleichung
 $\leq 1 + P_e^{(n)} nR + I(X^n(W)|Y^n)$
- $\leq 1 + P_e^{(n)} nR + nC$
- $P_e^{(n)} \geq 1 - \frac{1}{nR} - \frac{C}{R} \geq 0 \Rightarrow R > C$
 \square

HSW-Theorem

Satz (Holevo-Schumacher-Westmoreland (HSW))

Sei ε eine spurerhaltende Quantenoperation. Die Produktzustandskapazität ist

$$C^{(1)}(\varepsilon) = \max_{\{p_j, \rho_j\}} \left[S \left(\varepsilon \left(\sum_j p_j \rho_j \right) \right) - \sum_j p_j S(\varepsilon(\rho_j)) \right]$$

wobei das Maximum über alle Ensemble $\{p_j, \rho_j\}$ von möglichen Eingangszuständen ρ_j des Kanals gebildet wird.

- Semiklassisch: Alice hat eine Menge von Symbolen $\{i\}$ in Form von Dichteoperatoren ρ_i kodiert.
- Eine Sequenz der Länge n bildet Alice per Produktzustand

$$\rho_M = \rho_{M_1} \otimes \rho_{M_2} \otimes \dots \otimes \rho_{M_n}$$

- Bob kann beliebige Operationen auf $\varepsilon^{\otimes n}(\rho_M)$ durchführen.

Literatur



Michael A. Nielsen and Isaac L. Chuang.
Quantum Computation and Quantum Information.
Cambridge University Press, October 2000.



Wikipedia.
Shannon-Fano-Kodierung — Wikipedia, Die freie Enzyklopädie,
2007.
[Online; Stand 18. Mai 2007].

Fragen?

Kuhle Sache:

**Mit KUHbits
gibt's eimerweise
tolle Prämien ...**




www.milchwirtschaft.de