Quantenkryptographie (Teil 2)
- Entropie und Monogamie

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Agenda

Entropie der Verschränkung

- Die Entropie ist ein Maß für die Unordnung, die ein System aufweist.
  - Je höher die Entropie, desto höher das Unwissen über das System.
  - Shannon-Entropie ist ein Maß für den Informationsgehalt einer Nachricht.
    - Maß für klassische Systeme.

- Von Neumann hat das Konzept der Entropie auf die Quantenphysik übertragen.
  - "Unwissen" über einen Zustand
  - Die Entropie kann als Maßzahl für die Verschränkung zwischen Teilsystemen interpretiert werden.
  - Basiert auf der Dichtematrix
    - Allgemein gilt : $S(\rho) = -Tr(\,\rho \log_2 \rho\,)$
    - Beachte: $0 \log_2 0 = 1 \log_2 1 = 0$

Eigenschaften der Quanten-Entropie

- Für einen reinen Zustand gilt

$$S(\rho) = -Tr(\,\rho \log_2 \rho\,) = 0$$

- Für zusammengesetzte Systeme gilt allgemein:

$$S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$$

$$|S(\rho_A) - S(\rho_B)| \leq \; S(\rho_{AB})$$ *Araki-Lieb-Ungleichung*

  - Sind die Teilsysteme A und B nicht verschränkt ($\rho_{AB} = \rho_A \otimes \rho_B$), dann gilt

$$S(\rho_{AB}) = S(\rho_A) + S(\rho_B)$$

Berechnung der Entropie

- Da die Dichtematrix hermitesch ist, kann sie immer diagonalisiert werden.
  - Standardoperation der linearen Algebra

$$\rho = \begin{pmatrix} \lambda_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & \lambda_n \end{pmatrix}$$

- Berechnung der Entropie ist dann einfach

$$S(\rho) = -\sum_{i=1}^{n} \lambda_i \log_2 \lambda_i$$

  - Die Entropie ist maximal, wenn gilt $\lambda_i = \frac{1}{n}$ (Gleichverteilung)

Beispiel: Bell-Zustand

- Die Entropie eines Bell-Zustands (maximal verschränkt)

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|0\rangle_A |0\rangle_B + |1\rangle_A |1\rangle_B\right)$$

$$\rho_{AB} = |\Psi\rangle_{AB\ AB}\langle\Psi| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

- Für einen reinen Zustand gilt immer

$$S(\rho) = 0$$

"Teilsystem" eines Bell-Zustands

- Alice "Sicht" auf ihr Teilsystem

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

- Hier erhält man

$$S(\rho_A) = -\frac{1}{2}\log_2\frac{1}{2} - \frac{1}{2}\log_2\frac{1}{2} = 1$$

Berechnung mit Qiskit

```python
import qiskit.quantum_info as qi
import numpy as np
```

```python
# Define state vector
psi = np.array([1,0,0,1])/np.sqrt(2)
psi_AB = qi.Statevector(psi)

print("Bell state: ")
psi_AB.draw(output='latex')
```

Bell state:

$$\frac{\sqrt{2}}{2}|00\rangle + \frac{\sqrt{2}}{2}|11\rangle$$

```python
S_psi = qi.entropy(psi)

print("Entropy : {:>3f}".format(S_psi))
```

Entropy : 0.000000

```python
# Create density matrix
rho = qi.DensityMatrix(psi)
rho.draw('latex',prefix='\\rho_{AB} = ')
```

$$\rho_{AB} = \begin{bmatrix} \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ \frac{1}{2} & 0 & 0 & \frac{1}{2} \end{bmatrix}$$

```python
rho_A = qi.partial_trace(rho,[1])
rho_A.draw('latex',prefix='\\rho_{A} = ')
```

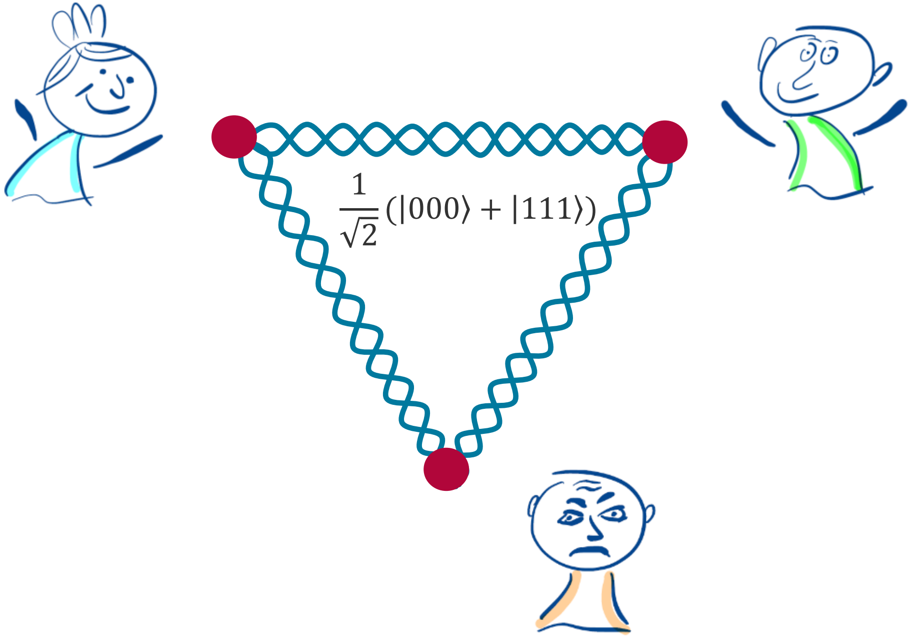
$$\rho_{A} = \begin{bmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{bmatrix}$$

```python
S_rho_A = qi.entropy(rho_A)
print("Entropy : {:>3f}".format(S_rho_A))
```

Entropy : 1.000000

Verschränktes 3-Qubit-System

- Betrachte folgende Situation (GHZ-Zustand).



Partielle Spur

- Alice und Bobs Sicht auf "ihr Teilsystem" von

$$|\Psi\rangle_{ABE} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A |0\rangle_B |0\rangle_E + |1\rangle_A |1\rangle_B |1\rangle_E \Big)$$

- Berechnung der partiellen Spur (*partial trace*)

$$\begin{aligned}\rho_{AB} = \mathrm{Tr}_E(\rho) &= {}_E\langle 0|\rho\,|0\rangle_E + {}_E\langle 1|\rho\,|1\rangle_E \\ &= \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\end{aligned}$$

- Entropie:

$$S(\rho_{AB}) = -\frac{1}{2}\log_2\frac{1}{2} - 0\log_2 0 - 0\log_2 0 - \frac{1}{2}\log_2\frac{1}{2} = 1$$

Entropie des GHZ-Zustands

- Für den (reinen) Zustand

$$|\Psi\rangle_{ABE} = \frac{1}{\sqrt{2}}\Big(|0\rangle_A |0\rangle_B |0\rangle_E + |1\rangle_A |1\rangle_B |1\rangle_E \Big)$$

gilt wieder

$$S(\rho_{ABE}) = 0$$

- Für das Teilsystem ρ_{AB} gilt

$$S(\rho_{AB}) = 1$$

- Auch für das Teilsystem ρ_E von Eve gilt

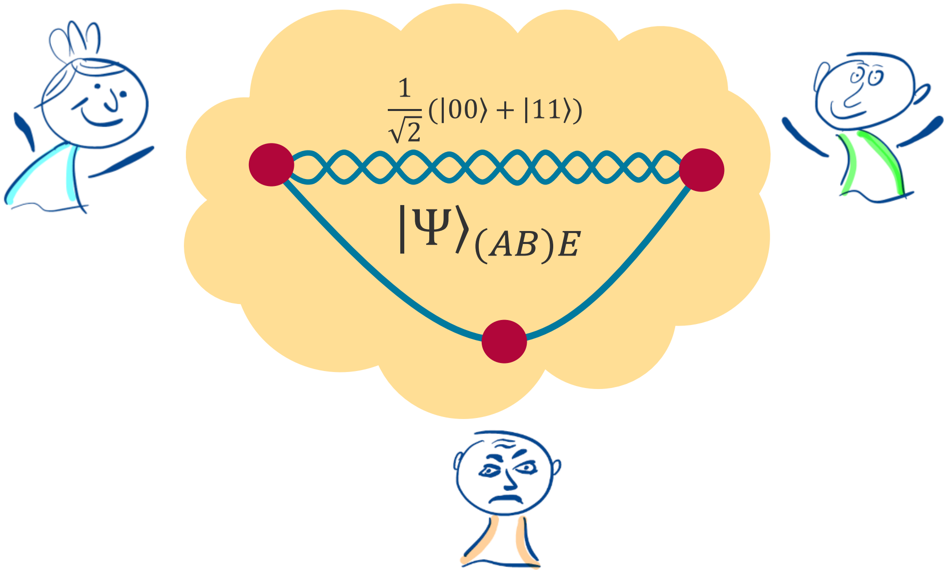
$$S(\rho_E) = 1$$

- Beachte:

$$S(\rho_{ABE}) < S(\rho_{AB}) + S(\rho_E)$$

Verschränktes 3-Qubit-System

- Betrachte nun folgende Situation, in der sich Alice und Bob ein maximal verschränktes Teilsystem teilen.
  - Gesamtzustand sei irgendwie "verschränkt".



Entropiebetrachtungen

- Für den reinen Zustand $\rho_{(AB)E} = |\Psi\rangle\langle\Psi|$ gilt

$$S\big(\rho_{(AB)C}\big) = 0$$

- Und für das Teilsystem von Alice und Bob

$$\rho_{(AB)} = Tr_E\big(\rho_{(AB)E}\big) = \frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\big)$$

gilt ebenfalls

$$S(\rho_{AB}) = 0$$

Wissen von Eve

- Aus den Ungleichungen (hinter einander gereiht)

$$|S(\rho_{AB}) - S(\rho_E)| \leq S\big(\rho_{(AB)E}\big) \leq S(\rho_{AB}) + S(\rho_E)$$

folgt mit $S\big(\rho_{(AB)E}\big) = 0$ und $S(\rho_{AB}) = 0$

$$|0 - S(\rho_E)| \leq 0 \leq 0 + S(\rho_E)$$

- Somit gilt $S(\rho_E) = 0$ und somit gilt $S\big(\rho_{(AB)E}\big) = S(\rho_{AB}) + S(\rho_E)$, also

$$\rho_{(AB)\mathrm{E}} = \rho_{\mathrm{AB}} \otimes \rho_E$$

Monogamie

- Monogamie ist eine der grundlegendsten Eigenschaften der Verschränkung!
- Wenn zwei Qubits A und B maximal verschränkt (quantenkorreliert) sind, können sie nicht mehr mit einem dritten Qubit C verschränkt sein.
- Wenn Qubit A und B jeweils auch mit einem dritten Qubit verschränkt sind, dann kann die Verschränkung zwischen A und B nicht mehr maximal sein.
  - Stichwort: Coffman-Kundu-Wootters (CKW) Monogamie-Ungleichung.

Zusammenfassung

- Das klassische Konzept der (Shannon-) Entropie kann auf die Quantenphysik übertragen werden.
  - Von Neumann-Entropie, basiert auf der Dichtematrix.

- Entropie ist eine Maßzahl für das "Nicht-Wissen" über einen Zustand.
  - Eine Maßzahl für einen gemischten Zustand.
  - Kann als Maß für die Verschränkung des Teilsystems mit dem Restsystem betrachtet werden (Partielle Spur).

- Monogamie ist eine ganz wesentliche Eigenschaft einer maximalen Verschränkung!

Hasso Plattner Institut
Digital Engineering • Universität Potsdam

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik