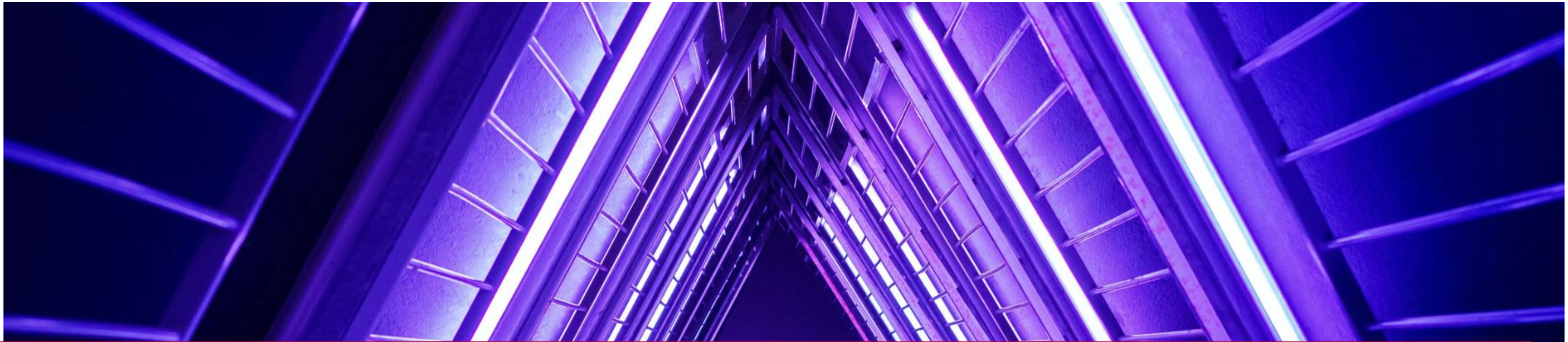


Quantenkryptographie (Teil 2) - Dichtematrix

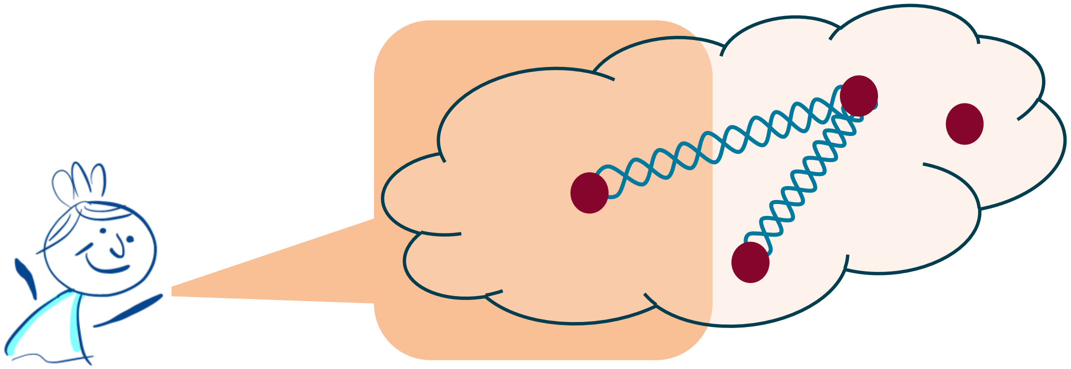
Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Agenda

1. Einführung
2. Wiederholung BB84
3. Qubits und Messbasen
4. Zusammengesetzte Systeme
5. Verschränkung
6. Anwendung von Verschränkung
7. Shared Randomness
8. Schmidt-Darstellung
9. **Dichtematrizen**
10. Partielle Spur
11. Verschränkungsmaß
12. Entropie und Monogamie
13. Entanglement Swapping
14. Entanglement Distillation
15. CHSH-Ungleichung (klassisch)
16. CHSH-Ungleichung (Quantenversion)
17. CHSH-Ungleichung (Simulation)
18. Ekert-Protokoll
19. Sicherheit und DIQKD
20. Zusammenfassung

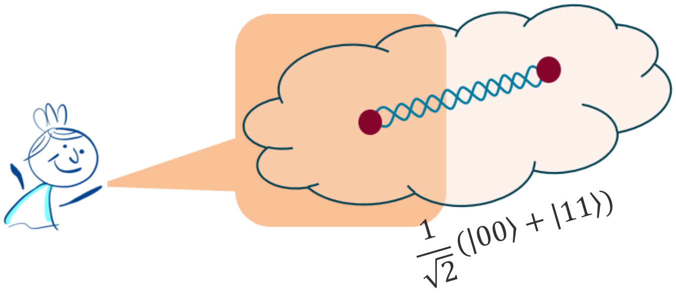
Sicht auf Teilsysteme

- Gegeben ist ein zusammengesetztes Quantensystem, z.B. aus zwei oder drei Photonen (Qubits).
- Frage: Wenn man nur Zugriff auf einen Teil (z.B. ein Photon) hat, wie kann diese "Sicht" mathematisch beschrieben werden?
  - Betrachter kennt nicht das Gesamtsystem.



Beispiel

- Sei das Gesamtsystem in dem Zustand:
  - $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$



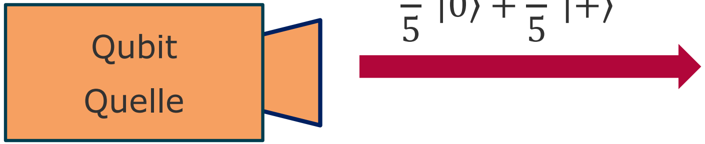
- Aus Alice Sicht besitzt sie ein Qubit
  - $|0\rangle$ oder
  - $|1\rangle$ jeweils mit Wahrscheinlichkeit $\frac{1}{2}$
  - Mögliche Beschreibung: $\left\{\left\{\frac{1}{2}, |0\rangle\right\}; \left\{\frac{1}{2}, |1\rangle\right\}\right\}$
  - Bemerkung: $\frac{1}{2}$ ist hier eine "klassische" Wahrscheinlichkeit, keine Wahrscheinlichkeitsamplitude.
    - Man nennt dies einen gemischten Zustand (*mixed state*)

Gemischte Zustände

- Ein gemischter Zustand ist keine Superposition!
- Ein gemischter Zustand entspricht einer "klassischen Wahrscheinlichkeitsverteilung".
  - $|\Psi\rangle = p_1|\Psi_1\rangle + p_2|\Psi_2\rangle + \cdots + p_n|\Psi_n\rangle$
  - mit $p_1 + p_2 + \cdots + p_n = 1$ (klassische Wahrscheinlichkeiten)

- Dichtematrizen werden zur Beschreibung "realer" physikalischer Systeme benutzt.
  - Beispiel

$$\frac{4}{5}\,|0\rangle + \frac{1}{5}\,|+\rangle$$



Dichtematrix-Darstellung

- Darstellung eines Quantensystems durch eine Matrix (*density matrix*).
  - Entspricht einer alternative Darstellungsform.
- Beispiel für ein Qubit:

$$|\Psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle = \alpha \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$

- Zugehörige Dichtematrix:

$$|\Psi\rangle\langle\Psi| = (\alpha\,|0\rangle + \beta\,|1\rangle)(\bar{\alpha}\,\langle 0| + \bar{\beta}\,\langle 1|) = \alpha\bar{\alpha}\,|0\rangle\langle 0| + \alpha\bar{\beta}\,|0\rangle\langle 1| + \bar{\alpha}\beta\,|1\rangle\langle 0| + \beta\bar{\beta}\,|1\rangle\langle 1|$$

$$\rho = |\Psi\rangle\langle\Psi| = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} \begin{pmatrix} \bar{\alpha} & \bar{\beta} \end{pmatrix} = \begin{pmatrix} \alpha\bar{\alpha} & \alpha\bar{\beta} \\ \bar{\alpha}\beta & \beta\bar{\beta} \end{pmatrix} = \begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{pmatrix}$$

Beispiel: Reiner Zustand

- Betrachte

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$$

- Zugehörige Dichtematrix

$$|+\rangle\langle+| = \frac{1}{2}(|0\rangle + |1\rangle)(\langle 0| + \langle 1|)$$

$$= \frac{1}{2}\,(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|)$$

$$= \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

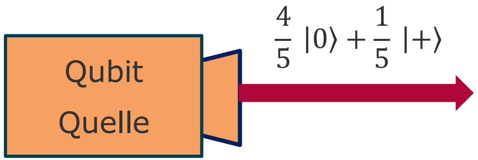
- In Vektorschreibweise

$$|+\rangle\langle+| = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}\frac{1}{\sqrt{2}}\,(1 \;\; 1) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Beispiel: Gemischter Zustand

- Betrachte

$$|\Psi\rangle = \frac{4}{5}\,|0\rangle + \frac{1}{5}\,|+\rangle$$



- Zugehörige Dichtematrix

$$|\Psi\rangle\langle\Psi| = \frac{4}{5}|0\rangle\langle 0| + \frac{1}{5}|+\rangle\langle +|$$

$$= \frac{4}{5}\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix} + \frac{1}{5}\cdot\frac{1}{2}\begin{pmatrix}1 & 1\\ 1 & 1\end{pmatrix} = \frac{1}{10}\begin{pmatrix}9 & 1\\ 1 & 1\end{pmatrix}$$

- Mit

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

Eigenschaften

- Die Dichtematrix besitzt folgende Eigenschaften
  - Spur der Matrix: $Tr(\rho) = 1$
  - Es gilt $\rho = \rho^{\dagger}$ (hermitesch)

$$\begin{pmatrix} |\alpha|^2 & \alpha\bar{\beta} \\ \bar{\alpha}\beta & |\beta|^2 \end{pmatrix}$$

$$Tr(\rho) = |\alpha|^2 + |\beta|^2 = 1$$

- Eigenschaften von *reinen* Zuständen
  - Hier gilt: $Tr(\rho^2) = Tr(\rho \cdot \rho) = 1$
- Eigenschaften von *gemischten* Zuständen
  - Hier gilt: $Tr(\rho^2) < 1$
  - Maß für die Reinheit (purity).

Zusammengesetzte Systeme

- Ist ein Zustand zusammengesetzt

$$|\Psi\rangle = |\Psi_A\rangle \otimes |\Psi_B\rangle$$

- dann gilt mit

$$\rho_A = |\Psi_A\rangle \langle\Psi_A|$$
$$\rho_B = |\Psi_B\rangle \langle\Psi_B|$$

für $\rho = |\Psi\rangle \langle\Psi|$

$$\rho = \rho_A \otimes \rho_B = |\Psi\rangle\langle\Psi|$$

Beispiel: 2-Qubit-System

- Ein separables 2-Qubit-System

$$
\begin{aligned}
|\Psi\rangle &= |\Psi\rangle_1 \otimes |\Psi\rangle_2 \\
&= (\alpha_1 |0\rangle_1 + \beta_1 |1\rangle_1) \otimes (\alpha_2 |0\rangle_2 + \beta_2 |1\rangle_2) \\
&= \alpha_1\alpha_2 |0\rangle_1 |0\rangle_2 + \alpha_1\beta_2 |0\rangle_1 |1\rangle_2 + \beta_1\alpha_2 |1\rangle_1 |0\rangle_2 + \beta_1\beta_2 |1\rangle_1 |1\rangle_2
\end{aligned}
$$

$$
\rho = |\Psi\rangle \langle\Psi| = \begin{pmatrix}
|\alpha_1|^2|\alpha_2|^2 & |\alpha_1|^2\alpha_2\bar{\beta}_2 & |\alpha_2|^2\alpha_1\bar{\beta}_1 & \alpha_1\alpha_2\bar{\beta}_1\bar{\beta}_2 \\
|\alpha_1|^2\beta_2\bar{\alpha}_2 & |\alpha_1|^2|\beta_2|^2 & \alpha_1\beta_2\bar{\beta}_1\bar{\alpha}_2 & |\beta_2|^2\alpha_1\bar{\beta}_1 \\
|\alpha_2|^2\beta_1\bar{\alpha}_1 & \beta_1\alpha_2\bar{\alpha}_1\bar{\beta}_2 & |\beta_1|^2|\alpha_2|^2 & |\beta_1|^2\alpha_2\bar{\beta}_2 \\
\beta_1\beta_2\bar{\alpha}_1\bar{\alpha}_2 & |\beta_2|^2\beta_1\bar{\alpha}_1 & |\beta_1|^2\beta_2\bar{\alpha}_2 & |\beta_1|^2|\beta_2|^2
\end{pmatrix}
$$

Rechenbeispiel (1)

$$|\Psi\rangle_1 = \frac{2}{3}\,|0\rangle_1 + \frac{\sqrt{5}}{3}\,|1\rangle_1$$

$$\begin{aligned}
\rho_1 &= |\Psi\rangle_{1\,1}\langle\Psi| \\
&= \left(\frac{2}{3}\,|0\rangle_1 + \frac{\sqrt{5}}{3}\,|1\rangle_1\right)\left(\frac{2}{3}\,{}_1\langle 0| + \frac{\sqrt{5}}{3}\,{}_1\langle 1|\right) \\
&= \frac{4}{9}\,|0\rangle_{1\,1}\langle 0| + \frac{2\sqrt{5}}{9}\,|0\rangle_{1\,1}\langle 1| + \frac{2\sqrt{5}}{9}\,|1\rangle_{1\,1}\langle 0| + \frac{5}{9}\,|1\rangle_{1\,1}\langle 1|
\end{aligned}$$

$$\rho_1 = \frac{1}{9}\begin{pmatrix} 4 & 2\sqrt{5} \\ 2\sqrt{5} & 5 \end{pmatrix}$$

Rechenbeispiel (1)

$$|\Psi\rangle_2 = \frac{1}{\sqrt{2}}|0\rangle_2 + \frac{1}{\sqrt{2}}|1\rangle_2$$

$$\begin{aligned}
\rho_2 &= |\Psi\rangle_2\,{}_2\langle\Psi| \\
&= \left(\frac{1}{\sqrt{2}}|0\rangle_2 + \frac{1}{\sqrt{2}}|1\rangle_2\right)\left(\frac{1}{\sqrt{2}}\,{}_2\langle 0| + \frac{1}{\sqrt{2}}\,{}_2\langle 1|\right) \\
&= \frac{1}{2}|0\rangle_2\,{}_2\langle 0| + \frac{1}{2}|0\rangle_2\,{}_2\langle 1| + \frac{1}{2}|1\rangle_2\,{}_2\langle 0| + \frac{1}{2}|1\rangle_2\,{}_2\langle 1|
\end{aligned}$$

$$\rho_2 = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Rechenbeispiel (3)

$$|\Psi\rangle = \left(\frac{2}{3}|0\rangle_1 + \frac{\sqrt{5}}{3}|1\rangle_1\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle_2 + \frac{1}{\sqrt{2}}|1\rangle_2\right)$$
$$= \frac{2}{3\sqrt{2}}|0\rangle_1|0\rangle_2 + \frac{2}{3\sqrt{2}}|0\rangle_1|1\rangle_2 + \frac{\sqrt{5}}{3\sqrt{2}}|1\rangle_1|0\rangle_2 + \frac{\sqrt{5}}{3\sqrt{2}}|1\rangle_1|1\rangle_2$$

$$\rho = \begin{pmatrix} \frac{4}{18} & \frac{4}{18} & \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} \\ \frac{4}{18} & \frac{4}{18} & \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} \\ \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} & \frac{5}{18} & \frac{5}{18} \\ \frac{2\sqrt{5}}{18} & \frac{2\sqrt{5}}{18} & \frac{5}{18} & \frac{5}{18} \end{pmatrix}$$

$$\begin{aligned}
\rho &= |\Psi\rangle\langle\Psi| \\
&= \left(\frac{2}{3\sqrt{2}}|0\rangle_1|0\rangle_2 + \frac{2}{3\sqrt{2}}|0\rangle_1|1\rangle_2 + \frac{\sqrt{5}}{3\sqrt{2}}|1\rangle_1|0\rangle_2 + \frac{\sqrt{5}}{3\sqrt{2}}|1\rangle_1|1\rangle_2\right) \\
&\quad \otimes\left(\frac{2}{3\sqrt{2}}\,{}_1\langle 0|\,{}_2\langle 0| + \frac{2}{3\sqrt{2}}\,{}_1\langle 0|\,{}_2\langle 1| + \frac{\sqrt{5}}{3\sqrt{2}}\,{}_1\langle 1|\,{}_2\langle 0| + \frac{\sqrt{5}}{3\sqrt{2}}\,{}_1\langle 1|\,{}_2\langle 1|\right) \\
&= \frac{4}{18}|0\rangle_1|0\rangle_2\,{}_1\langle 0|\,{}_2\langle 0| + \frac{4}{18}|0\rangle_1|0\rangle_2\,{}_1\langle 0|\,{}_2\langle 1| + \frac{2\sqrt{5}}{18}|0\rangle_1|0\rangle_2\,{}_1\langle 1|\,{}_2\langle 0| + \frac{2\sqrt{5}}{18}|0\rangle_1|0\rangle_2\,{}_1\langle 1|\,{}_2\langle 1| \\
&\quad + \frac{4}{18}|0\rangle_1|1\rangle_2\,{}_1\langle 0|\,{}_2\langle 0| + \frac{4}{18}|0\rangle_1|1\rangle_2\,{}_1\langle 0|\,{}_2\langle 1| + \frac{2\sqrt{5}}{18}|0\rangle_1|1\rangle_2\,{}_1\langle 1|\,{}_2\langle 0| + \frac{2\sqrt{5}}{18}|0\rangle_1|1\rangle_2\,{}_1\langle 1|\,{}_2\langle 1| \\
&\quad + \frac{2\sqrt{5}}{18}|1\rangle_1|0\rangle_2\,{}_1\langle 0|\,{}_2\langle 0| + \frac{2\sqrt{5}}{18}|1\rangle_1|0\rangle_2\,{}_1\langle 0|\,{}_2\langle 1| + \frac{5}{18}|1\rangle_1|0\rangle_2\,{}_1\langle 1|\,{}_2\langle 0| + \frac{5}{18}|1\rangle_1|0\rangle_2\,{}_1\langle 1|\,{}_2\langle 1| \\
&\quad + \frac{2\sqrt{5}}{18}|1\rangle_1|1\rangle_2\,{}_1\langle 0|\,{}_2\langle 0| + \frac{2\sqrt{5}}{18}|1\rangle_1|1\rangle_2\,{}_1\langle 0|\,{}_2\langle 1| + \frac{5}{18}|1\rangle_1|1\rangle_2\,{}_1\langle 1|\,{}_2\langle 0| + \frac{5}{18}|1\rangle_1|1\rangle_2\,{}_1\langle 1|\,{}_2\langle 1|
\end{aligned}$$

Berechnung mit Qiskit

Berechnung von Dichtematrizen

In [1]:
```
import qiskit.quantum_info as qi
import numpy as np
```

In [2]:
```
# Erzeugung des ersten Zustandsvektors
psi1 = np.array([2/3,np.sqrt(5)/3])
psi_A = qi.Statevector(psi1)
display( psi_A.draw('latex') )
```

$$\frac{2}{3}|0\rangle + \frac{\sqrt{5}}{3}|1\rangle$$

In [3]:
```
# Erzeugung des zweiten Zustandsvektors
psi2 = np.array([1, 1])/np.sqrt(2)
psi_B = qi.Statevector(psi2)
display( psi_B.draw('latex') )
```

$$\frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|1\rangle$$

In [4]:
```
# Bildung des Tensorprodukts
psi_AB = psi_A.tensor(psi_B)
display( psi_AB.draw('latex') )
```

$$\frac{\sqrt{2}}{3}|00\rangle + \frac{\sqrt{2}}{3}|01\rangle + \frac{\sqrt{10}}{6}|10\rangle + \frac{\sqrt{10}}{6}|11\rangle$$

In [5]:
```
# Berechnung der Dichtematrix
rho = qi.DensityMatrix(psi_AB)
display( rho.draw('latex',prefix='\\rho_{AB} = ') )
```

$$\rho_{AB} = \begin{bmatrix} \frac{2}{9} & \frac{2}{9} & 0.24845 & 0.24845 \\ \frac{2}{9} & \frac{2}{9} & 0.24845 & 0.24845 \\ 0.24845 & 0.24845 & 0.27778 & 0.27778 \\ 0.24845 & 0.24845 & 0.27778 & 0.27778 \end{bmatrix}$$

Dichtematrix-Darstellung

- Beispiel für einen Bell-Zustand

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

- Dichtematrix:

$$\rho = |\Psi\rangle\langle\Psi| = \frac{1}{2}\left(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right)$$

$$\rho = |\Psi\rangle\langle\Psi| = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}$$

Berechnung mit Qiskit

Dichtematrix für einen Bell-Zustand

In [6]:
```
# Dichtematrix kann direkt aus einem Array erzeugt werden
psi_bell = np.array([1,0,0,1])/np.sqrt(2)
rho = qi.DensityMatrix(psi_bell)
display( rho.draw('latex',prefix='\\rho_{Bell} = ') )
```

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

In [9]:
```
# Anzeige des zugehörigen Zustandsvektors
display( qi.Statevector(psi_bell).draw('latex') )
```

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

Visualisierung der Dichtematrix

- Quantum Tomography

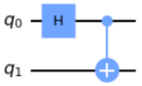
Beispiel Bell-Zustand

In [1]:
```python
from qiskit import QuantumCircuit
import qiskit.quantum_info as qi
from qiskit.visualization import plot_state_city

import numpy as np
```

In [2]:
```python
qc_ERP = QuantumCircuit(2)
qc_ERP.h(0)
qc_ERP.cx(0,1)
qc_ERP.draw('mpl')
```

Out[2]:



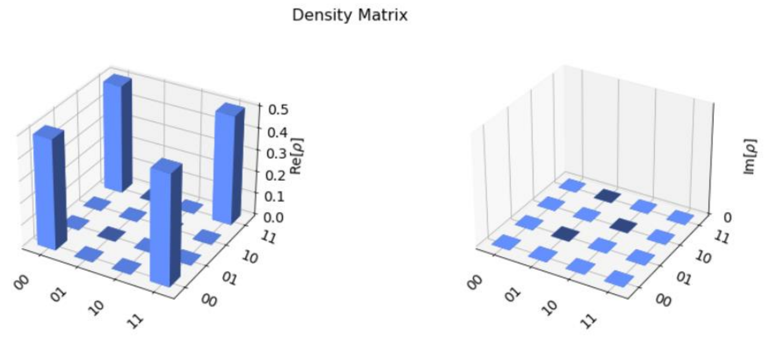
In [3]:
```python
rho_ERP = qi.DensityMatrix.from_instruction(qc_ERP)
rho_ERP.draw('latex', prefix='\\rho_{ERP} = ')
```

Out[3]:

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

In [4]:
```python
plot_state_city(rho_ERP.data, title='Density Matrix')
```

Out[4]:



Zusammenfassung

- Dichtematrizen sind eine alternative Beschreibungsform für Quantensysteme.
  - Sind in der Physik sehr gebräuchlich, um die Ergebnisse von Experimenten vorherzusagen.
    - Man kann nicht immer reine Zustände präparieren.

- Quanten-Tompgraphy ist experimenteller Zugang zur Verschränkung.
  - Experimentelle Bestimmung der Dichtematrix möglich.

- Wir werden Dichtematrizen dazu nutzen, um "die Sicht" auf Teile von einem verschränkten Systems zu extrahieren.
  - Siehe nächste Videos.

Vielen Dank
für die Aufmerksamkeit!

Prof. Dr. Jörg Hettel
Hochschule Kaiserslautern
Fachbereich Informatik

Hasso Plattner Institut
Digital Engineering · Universität Potsdam