Privatdozent Dr. C. Diem
diem@math.uni-leipzig.de
http://www.math.uni-leipzig.de/∼diem/krypto

# KRYPTOGRAPHIE
# ÜBUNGSBLATT NR. 1

Wir benutzen die Definitionen aus der Vorlesung.

**Aufgabe 1** Es sei $z$ eine Zufallsvariable mit Werten in $\mathcal{Z}$, $\mathcal{A} \subseteq \mathcal{Z}$. Zeigen Sie:

$$\mathbf{P}[z \in \mathcal{A}] = \sum_{z^{(0)}} \mathbf{P}[z \in \mathcal{A} \mid z = z^{(0)}] \cdot \mathbf{P}[z = z^{(0)}]$$

Über welche Elemente $z^{(0)}$ muss hier die Summe gehen?

Wenn Sie wollen, können Sie $z$ ganz weglassen.

**Aufgabe 2** Es sei nun, zusätzlich zu Aufgabe 1, $\mathcal{B} \subseteq \mathcal{Z}$.
Zeigen Sie:
$\mathcal{A}$ und $\mathcal{B}$ sind genau dann zueinander stochastisch unabhängig (bezüglich $z$), wenn gilt:

$$\mathbf{P}[z \in \mathcal{B}] > 0 \rightarrow \mathbf{P}[z \in \mathcal{A} \mid z \in \mathcal{B}] = \mathbf{P}[z \in \mathcal{A}]$$

(Der Pfeil "$\rightarrow$" zeigt eine Implikation an.)

**Aufgabe 3** Es seien nun $u$ und $v$ Zufallsvariablen mit Werten in endlichen / abzählbaren Mengen, deterministisch abhängig vom selben Zufall.
Zeigen Sie, dass äquivalent sind:

- $u$ und $v$ sind zueinander stochastisch unabhängig.
- Für alle möglichen Werte $u^{(0)}$ und $v^{(0)}$ von $u$ bzw. $v$ gilt:

  $$\mathbf{P}[v = v^{(0)}] > 0 \rightarrow \mathbf{P}[u = u^{(0)} \mid v = v^{(0)}] = \mathbf{P}[u = u^{(0)}]$$

- Für alle möglichen Werte $u^{(0)}$ von $u$ und $v^{(0)}, v^{(1)}$ von $v$ gilt:

  $$(\mathbf{P}[v = v^{(0)}] > 0 \wedge \mathbf{P}[v = v^{(1)}] > 0) \rightarrow \mathbf{P}[u = u^{(0)} \mid v = v^{(0)}] = \mathbf{P}[u = u^{(0)} \mid v = v^{(1)}]$$