Übung 2

2.1 Zwei Würfel (2pt)

Zwei normale sechsseitige Würfel werden geworfen. Der erste Würfel zeigt die Zufallsvariable X und der zweite Würfel Y. Sei $Z = X + Y$. Berechnen Sie

a) $\mathrm{E}[Z|X \text{ist gerade}]$

b) $\mathrm{E}[Z|Y \text{ist ungerade}]$

c) $\mathrm{E}[X|Z = 5]$

d) $\mathrm{E}[Y|Z > 6]$

2.2 Jensen im Quadrat (2pt)

Beweisen Sie dass für alle geraden $k \geq 2$ gilt, $E[X^k] \geq E[X]^k$.

2.3 Min-Max im Erwartungswert (3pt)

Alice und Bob gehen ins Casino. Ihre Gewinne A und B sind unabhängig voneinander und je eine zufällige ganze Zahl im Intervall $[1, k]$.

a) Was ist $\mathrm{E}[\min(A, B)]$ und $\mathrm{E}[\max(A, B)]$?

b) Zeigen Sie aufgrund des Resultats in a), dass gilt

$$\mathrm{E}[\min(A, B)] + \mathrm{E}[\max(A, B)] \;=\; \mathrm{E}[A] + \mathrm{E}[B].$$

c) Beweisen Sie diese Gleichung ebenfalls durch Herleitung mittels Eigenschaften des Erwartungswertes.

2.4 Ein zufälliger Text (3pt)

Die Katze läuft über die Tastatur und erzeugt zufällige Zeichen. Angenommen es gäbe nur 26 Buchstaben und 6 Sonderzeichen. Wie gross ist die Wahrscheinlichkeit dafür, dass die Katze folgendes tippt:

a) Ihr Passwort (10 Zeichen)?

b) Den 128-bit AES-Schlüssel einer TLS-Verbindung auf dem Internet?

c) Die Kopfzeile dieses Übungsblatts (125 Zeichen)?

Das gesamte Bitcoin-Netzwerk berechnet heute (2019) etwa $40 \cdot 10^{18}$ (Hash-)Operationen pro Sekunde. Angenommen der zufällige Text würde mit dieser Geschwindigkeit erzeugt, wie lange dauert es dann durchschnittlich, bis a)–c) gefunden werden?