Übung 7

7.1 Noch eine unfaire Münze (4pt)

Sie finden eine Münze, welche unfair ist und mit Wahrscheinlichkeit p Kopf zeigt. Sie kennen p nicht, wissen aber, dass bei allen solchen Münzen $p \geq \alpha$ für ein bekanntes α. Sie werfen die Münze n Mal und erhalten βn Mal Kopf. Sie möchten p schätzen, so dass

$$\mathrm{P}[|p - \beta| \geq \gamma p] \ \leq \ \epsilon$$

für gegebene γ und ϵ. Berechnen Sie die dazu mindenstens nötige Anzahl Würfe n mittels eines Chernoff-Bounds in Abhängigkeit von α, γ und ϵ.

Wie gross ist die untere Schranke für n für $\alpha = 0.25$, $\gamma = 0.1$ und $\epsilon = 0.01$?

7.2 Wertebereich (2pt)

Chernoff-Bounds wie besprochen gelten für beliebige Zufallsvariablen $X_1, \ldots, X_n$ mit $X_i \in [0, 1]$ und beschränken die Abweichung von $X = \sum_{i=1}^{n} X_i$ vom Erwartungswert $\mu = \mathrm{E}[X]$. Zum Beispiel, für $\delta > 0$

$$\mathrm{P}[X \geq (1 + \delta)\mu] \ \leq \ e^{-\frac{\mu\delta^2}{3}}.$$

Geben Sie eine analoge Schranke für eine Zufallsvariable $Z = \sum_{i=1}^{n} Z_i$, wobei $Z_i \in [0, a]$ für beliebiges $a > 0$.

7.3 Kommittee (4pt)

Blockchain-Systeme werden betrieben durch *Knoten*, die in einem Peer-to-Peer Netz verbunden sind. In einigen solchen Systemen wählt ein Protokoll durch eine zufällige Lotterie ein Kommittee von Knoten aus, welche dann die Cryptocurrency-Transaktionen validieren.

Angenommen, es gibt insgesamt n Knoten und davon sind mindestens αn ehrlich. Die Knoten im Kommittee werden zufällig gewählt, und zwar so, dass im Erwartungswert das Kommittee insgesamt m Knoten enthält und jeder Knoten unabhängig von allen anderen mit Wahrscheinlichkeit $\frac{m}{n}$ dabei ist. Nun sollen in einem Kommittee mit Wahrscheinlichkeit $1 - \epsilon$ mindestens βm Knoten ehrlich sein für gegebene Parameter ϵ und β (mit $\alpha > \beta > \frac{1}{2}$).

a) Wie gross muss m mindestens sein? Benutzen Sie einen Chernoff-Bound.

b) Rechnen Sie ein numerisches Beispiel für $\alpha = 0.6$, $\beta = 0.55$ und $\epsilon = 0.001$.

(In Protokollen mit *Proof-of-Stake*-Consensus, wie in der *Algorand*-Blockchain oder in *Ouroboros*, dem Protokoll des *Cardano*-Systems, finden kryptographische *Verifiable Random Functions* Verwendung für die Lotterie.)