Diskrete Wahrscheinlichkeitstheorie – Hausaufgabe 4

Abgabe bis zum 23.5. bis 8:30.

Alle Antworten sind unter Angabe des Rechenwegs zu begründen, soweit nicht anders gefordert! Fragen gerne im infler-Forum posten :).

Aufgabe 4.1 Abzugeben sind (a), (b) und (c) 1P+2P+3P

Wir betrachten eine Multiple-Choice-Aufgabe, die aus genau 3 ja/nein Fragen besteht.

Die Fakultät zwingt uns eines der folgenden Bepunktungssysteme für die Aufgabe zu verwenden:

(1) Antwort richtig: +1 Punkt, Antwort falsch oder keine Antwort: 0 Punkte.

(2) Antwort richtig: +1 Punkt, Antwort falsch oder keine Antwort: -0.5 Punkt. Negative Punkte als Gesamtpunktzahl der Aufgabe sind möglich.

(3) Antwort richtig: +1 Punkt, Antwort falsch: -1 Punkt, keine Antwort: -0.5 Punkte. Erreicht ein Student eine negative Punktezahl, so wird die Aufgabe stattdessen mit 0 Punkten bewertet.

Wir sind natürlich daran interessiert, das System zu finden, bei dem ein ratender Student am schlechtesten abschneidet.

Wir nehmen an, dass ein ratender Student höchstens eine Antwort pro Frage ankreuzt. Sei 1/5 die W'keit, dass ein ratender Student keine Antwort ankreuzt, während er mit W'keit 2/5 "ja" bzw. "nein" ankreuzt.

Sei A_i die ZV, die die Gesamtpunktzahl eines ratenden Studenten unter dem Bepunktungssystem (i) angibt.

(a) Berechnen Sie $\mathbb{E}[A_1]$ und $\mathrm{Var}[A_1]$

(b) Bestimmen Sie Parameter $a, b \in \mathbb{R}$ so, dass $A_2 = a \cdot X + b$ mit $X \sim \mathrm{Bin}(3, 2/5)$. Bestimmen Sie dann $\mathbb{E}[A_2]$ sowie $\mathrm{Var}[A_2]$.

(c) Betrachten Sie nun das System (3). Bestimmen Sie die Dichte von A_3 sowie $\mathbb{E}[A_3]$ und $\mathrm{Var}[A_3]$.

Wie hängt die Dichtefunktion von A_3 mit den Koeffizienten c_j in $(\frac{2}{5}z^2 + \frac{2}{5}z^{-2} + \frac{1}{5}z^{-1})^3 = \sum_{j=-6}^{6} c_j z^j$ zusammen?

Aufgabe 4.2 Abzugeben 4P

Seien W, X, Y, Z (nicht nur paarweise!) unabhängige (diskrete) ZVen mit folgenden Verteilungen:

- $W \sim \mathrm{Bin}(5, 1/3)$.
- $X \sim \mathrm{Geo}(1/2)$.
- $Y \sim \mathrm{Bin}(20, 3/4)$.
- $Z \sim \mathrm{Geo}(2/5)$.

Bestimmen Sie $\mathbb{E}[\frac{(X+Z)(Y+Z)}{W+1}]$. Begründen Sie jeden Ihrer Rechenschritte!

Aufgabe 4.3 Abzugeben sind (a), (b) und (c). 2P+1P+2P

Eine (idealisierte) Hashfunktion ist eine Abbildung $h\colon \{0,1\}^* \to \{0,1\}^l$ für ein festes $l \in \mathbb{N}$. So bildet SHA-512 Strings (quasi) beliebiger Länge auf Hashwerte bestehend aus $l = 512$ Bit ab.

Für kryptographische Anwendungen fordert man, dass es "schwierig" sein muss, eine Kollision zu finden, d.h. zwei Urbilder $u_1, u_2 \in \{0,1\}^*$ mit $u_1 \neq u_2 \wedge h(u_1) = h(u_2)$.

Um eine untere Schranke für die Ausgabelänge l einer Hashfunktion herzuleiten, betrachtet man folgendes Experiment:

$X_1, X_2, \ldots, X_m$ seien unabhängige ZVen, jede gleichverteilt über $\{0,1\}^{2l}$. Also $\Pr[X_i = u] = 2^{-2l}$ für alle $i \in [r]$ und $u \in \{0,1\}^{2l}$.

Weiterhin sei idealisiert angenommen, dass die Hashfunktion die Gleichverteilung erhält, das heißt, dass auch $\Pr[h(X_i) = w] = 2^{-l}$ für alle $i \in [r]$ und $w \in \{0,1\}^l$.

Es sei $K_u := \{\omega \in \Omega \mid |\{X_1(\omega), \ldots, X_m(\omega)\}| < m\}$ das Ereignis, dass eine Kollision bereits in den Urbildern vorliegt.

Entsprechend sei $K_h := \{\omega \in \Omega \mid |\{h(X_1(\omega)), \ldots, h(X_m(\omega))\}| < m\}$.

(a) Zeigen Sie, dass $\Pr[K_h] \geq 1/2 \cdot \binom{m}{2} 2^{-l}$ für $\binom{m}{2} \leq 2^l$.

Hinweise: Argumentieren Sie zunächst, warum Sie die Formel aus Beispiel 20 auf $\Pr\left[\overline{K_h}\right]$ anwenden dürfen. Skizzieren Sie sich dann die Abbildung $1 - e^{-x}$ über dem Intervall $[0, 1]$.

(b) Zeigen Sie, dass auch $\Pr[K_h] \leq \binom{m}{2} 2^{-l}$.

Hinweis: Benutzen Sie die boolsche Ungleichung aus den Folien.

(c) Zeigen Sie, dass $\Pr\left[\overline{K_u} \mid K_h\right] \geq 1 - 2^{-l+1}$.

Aufgabe 4.4 Abzugeben sind (a-i) und (a-ii). 2P+3P

(a) Die kleine Maxi hat vor Kurzem von ihrem Vater Xaver eine CD von Justus Nagetier geschenkt bekommen, obwohl sie sich viel lieber die CD von den Flambierten gewünscht hätte. Dummerweise zwingt Xaver sie auch noch die ganze Zeit, sich diese CD anzuhören.

Um sich davon abzulenken, hat sie sich das folgende spannende Spiel ausgedacht:

Sie wirft eine faire Münze, bis zum ersten Mal das Muster 110 auftritt (1 sei Zahl, 0 sei Kopf).

(i) Wie oft muss Maxi die Münze im Mittel werfen, bis das Spiel endet?

Hinweis: Orientieren Sie sich an den Rechenwegen aus den Beispielen 14 und 15.

(ii) Bestimmen Sie auch die Varianz der entsprechenden ZV aus (i).

Hinweis: Die Varianz lässt sich mit Hilfe des Erwartungswerts darstellen. Gehen Sie dann wie in (i) vor.

(b) Nachdem der kleine Michel zu häufig auf 4chan gelandet ist, lässt ihn sein Vater Xaver nicht mehr an den Computer. Notgedrungen muss er mit seiner kleinen Schwester Maxi spielen:

Michel ist natürlich auch sofort von Maxis Spiel begeistert. Sie wandeln das Spiel daher so ab, dass sie die faire Münze werfen, bis das erste Mal entweder das Muster 110 oder 100 auftritt. Im Fall von 110 gewinnt Maxi, im Fall von 100 gewinnt Michel.

(i) Wie viele Würfe dauert ein Spiel im Mittel?

(ii) Nach ein paar Spielen fängt Michel an, seine kleine Schwester zu beschimpfen, dass sie bei ihrem dummen Spiel viel häufiger gewinnen würde.

Stimmt das?