Universität Rostock
Prof. Dr. H. Kösters

Wintersemester 2019/2020

Übungen zur Stochastik für Informatik

Blatt 2 (Diskrete Wahrscheinlichkeitsräume)

Vorübung 4 (Studienfächer : keine Abgabe)
An einer Universität werden (neben anderen nicht-naturwissenschaftlichen Fächern) die drei Naturwissenschaften Biologie, Chemie und Physik angeboten. Aus den verfügbaren Listen geht hervor, dass ein zufällig ausgewählter Student mit Wahrscheinlichkeit
- 0.4 Biologie
- 0.35 Chemie
- 0.5 Physik
- 0.15 Biologie und Chemie
- 0.1 Biologie und Physik
- 0.15 Chemie und Physik
- 0.05 Biologie und Chemie und Physik

studiert. Bestimmen Sie die Wahrscheinlichkeit dafür, dass ein zufällig ausgewählter Student mindestens eine Naturwissenschaft studiert.

Bemerkung: Auf die Angabe eines W.raums dürfen Sie ausnahmsweise verzichten.

Vorübung 5 (Würfel : keine Abgabe)
Zwei faire Würfel werden gleichzeitig geworfen, und es wird die Augensumme (d. h. die Summe der gewürfelten Augenzahlen) gebildet. Geben Sie einen geeigneten W.raum zur Beschreibung des Wurfs zweier fairer Würfel an, und bestimmen Sie für jeden möglichen Wert k der Augensumme die Wahrscheinlichkeit des Ereignisses A_k : „die Augensumme ist k“. Bestimmen Sie anschließend die Wahrscheinlichkeit des Ereignisses B : „die Augensumme ist ≥ 9“.

Hinweise: Wählen Sie den W.raum so geschickt, dass Sie als W.maß eine Gleichverteilung verwenden können. Vergessen Sie nicht, alle Ereignisse auch formal zu beschreiben.

Vorübung 6 (Geburtstagsparadoxon : keine Abgabe)
In einer Stochastik-Vorlesung sitzen n Studierende. Wie groß ist die Wahrscheinlichkeit, dass es darunter (mindestens) zwei Studierende gibt, die am gleichen Tag Geburtstag haben? Wir wollen dies etwas allgemeiner für den Fall untersuchen, dass das Jahr m Tage besitzt.

(a) Beschreiben Sie die Situation durch einen geeigneten W.raum. Geben Sie an, welche vereinfachenden Annahmen Sie treffen.

(b) Beschreiben Sie das interessierende Ereignis formal, und geben Sie eine exakte Formel für die gesuchte W. an.

(c) Zeigen Sie mit Hilfe der Taylor-Approximation $e^x \approx 1+x$ ($x \approx 0$), dass die gesuchte W. für $1 \ll n \ll m$ näherungsweise $1-\exp(-\frac{n^2}{2m})$ beträgt. (Dabei bedeutet $1 \ll n \ll m$, dass n deutlich größer als 1 und deutlich kleiner als m ist; Sie brauchen dies nicht zu präzisieren!)

(d) Folgern Sie, dass $n \gtrsim \sqrt{2m \log 2}$ sein muss, damit die gesuchte W. $> 1/2$ ist. (Dabei bezeichnet log den natürlichen Logarithmus.)

(e) Wie viele Personen müssen mindestens in der Vorlesung sitzen, damit die gesuchte W. $> 1/2$ ist? Und wie würde sich die Anzahl ändern, wenn das Jahr 100 Tage [1000 Tage] hätte?

Bemerkung: Die Anzahlen sind kleiner, als man naiv erwarten würde. Aus diesem Grund spricht man vom *Geburtstagsparadoxon*.

(f) (*Zusatzaufgabe; falls noch Zeit ist*)

Im Bereich der Computer-Sicherheit werden unter anderem zu Authentifizierungszwecken *kryptographische Hash-Funktionen* eingesetzt. Von der Idee her sind das Funktionen $H : \{0,1\}^* \to \{0,1\}^M$ (wobei $\{0,1\}^* := \bigcup_{n\in\mathbb{N}_0} \{0,1\}^n$ und $M \in \mathbb{N}$), bei denen sich bei gegebener Nachricht x leicht der Hash-Code $H(x)$ berechnen lässt, aber umgekehrt bei gegebenem Hash-Code h nur schwer eine Nachricht x mit $H(x) = h$ finden lässt.

Ein Paar (x, y) von Nachrichten wird *Kollision* genannt, falls $x \neq y$ und $H(x) = H(y)$ gilt. Bei einer „starken“ Hash-Funktion muss es praktisch unmöglich sein, durch „zufälliges“ Ausprobieren eine Kollision zu finden. Dies bedeutet (nach aktuellem Stand der Technik), dass man (mindestens) etwa 2^{128} „zufällige“ Nachrichten erzeugen muss, um mit W. $> \frac{1}{2}$ eine Kollision zu finden.

In einem Buch zur Computer-Sicherheit ist zu lesen: Aufgrund des Geburtstagsparadoxons muss für eine „starke“ Hash-Funktion nicht $M \gtrsim 128$, sondern $M \gtrsim 256$ gewählt werden. Erklären Sie dies!

Wichtige Hinweise:

- Um die Verteilung einer Zufallsgröße $X : \Omega \to \mathcal{X}$ auf einem diskreten W.raum anzugeben, reicht es aus, die Werte $\mathbb{P}(X = x)$, $x \in \mathcal{X}$, anzugeben.
- Die folgenden Aufgaben sollen nach Möglichkeit <u>ohne</u> Verwendung von Baumdiagrammen gelöst werden.

Die folgende Übung kann ab der 2. Vorlesung (incl. Satz 1.9 / Bem. 1.10) bearbeitet werden.

Übung 5 (Garderobe : 2 + 2 + 2 + 4 + 2* = 10 + 2* Punkte)
Sie besuchen – in einer Gruppe von k Bekannten – eine Aufführung mit n Besuchern ($n \geq k$), die alle ihre Jacke an der Garderobe abgeben. Leider fällt während der Aufführung mehrmals der Garderobenständer um, so dass die Jacken völlig durcheinander geraten. Dadurch erhält nach der Aufführung jeder Besucher irgendeine zufällige Jacke.
Wir wollen die Besucher von 1 bis n nummerieren, wobei Sie selbst Besucher Nr. 1 sind und Ihre Gruppe (einschließlich Ihnen selbst) aus den Besuchern Nr. 1 – k besteht. Dann lässt sich der Vorgang durch die Grundmenge

$$\Omega := \{\omega = (\omega_1, \ldots, \omega_n) \in \{1, \ldots, n\}^n \,|\, \omega_i \neq \omega_j \text{ für alle } i, j \in \{1, \ldots, n\} \text{ mit } i \neq j\}$$

(wobei $\omega_i = j$ bedeuten soll, dass der Besucher Nr. i die Jacke von Besucher Nr. j erhält) und das W.maß $\mathbb{P} = \mathcal{U}_\Omega$ (da die Jacken völlig durcheinander geraten sind) beschreiben.
Beschreiben Sie die folgenden Ereignisse formal, und berechnen Sie ihre Wahrscheinlichkeit:

(a) Sie erhalten Ihre eigene Jacke zurück.

(b) Jeder in Ihrer Gruppe (von k Bekannten) erhält seine eigene Jacke zurück.

(c) Jeder in Ihrer Gruppe (von k Bekannten) erhält eine Jacke aus der Gruppe zurück.

(d) Irgendeiner von den n Besuchern erhält seine eigene Jacke zurück.

(e) (*Sternchen-Aufgabe*) Zeigen Sie, dass die W. in Teil (c) für $n \to \infty$ gegen $1 - e^{-1} \approx 0.632$ konvergiert.

Die folgenden Übungen können ab der 4. Vorlesung (am 07.11.2019) bearbeitet werden.

Übung 6 (Tetraeder : 5 + 2 + 2 + 1 = 10 Punkte)
Drei „faire“ tetraederförmige Würfel, auf deren Seitenflächen jeweils die Zahlen 1 – 4 stehen, werden gleichzeitig geworfen. Es interessieren die folgenden Zufallsgrößen:

- Z : Anzahl der unterschiedlichen Ergebnisse (also z. B. $Z(4, 1, 4) = 2$, $Z(2, 2, 2) = 1$)
- S : Summe der drei Ergebnisse (also z. B. $S(4, 1, 4) = 9$, $S(2, 2, 2) = 6$)

(a) Beschreiben Sie die Situation durch einen diskreten W.raum $(\Omega, \mathfrak{P}(\Omega), \mathbb{P})$ und formal definierte Zufallsgrößen Z und S.

(b) Zeigen Sie: $\mathbb{P}(Z = 2) = \frac{36}{64}$ und $\mathbb{P}(S = 9) = \frac{10}{64}$.

(c) Geben Sie für die Zufallsgrößen Z und S jeweils ohne Beweis die Verteilung an.

(d) Bestimmen Sie $\mathbb{P}(\{Z = 2\} \cap \{S = 9\})$.

Übung 7 (Zusammengesetzte Zufallsgrößen : 1 + 3 + 1 = 5 Punkte)
Die Verteilung einer zusammengesetzten Zufallsgröße (X, Y) sei durch die folgende Tabelle gegeben:

$\mathbb{P}(X = x, Y = y)$	$y = -2$	$y = -1$	$y = +1$	$y = +2$
$x = 1$	0.15	0.1	0.1	0
$x = 2$	0.1	0.25	0.2	0.1

(a) Erläutern Sie, warum durch die Werte in der Tabelle eine diskrete Wahrscheinlichkeitsverteilung (*auf welcher Menge?*) gegeben ist.

(b) Bestimmen Sie die Verteilungen von X, von Y und von Y^2.

(c) Berechnen Sie die Wahrscheinlichkeit $\mathbb{P}(\{X = Y\})$. (Das Ereignis $\{X = Y\}$ haben wir streng genommen noch nicht eingeführt, aber Sie können bestimmt erraten, was darunter zu verstehen ist.)

Abgabe: 14.11.2019 um 13:10 vor der Vorlesung