

Übungsblatt 2

Wahrscheinlichkeitsrechnung I

Stochastik@AIN2

Prof. Dr. Barbara Staehle

Wintersemester 2021/2022

HTWG Konstanz

Einfache und mittelschwere Aufgaben

AUFGABE 2.1 WÜRFELN MIT EINEM W10

TEILAUFGABE 2.1.1 1 PUNKT

Betrachten Sie den Wurf eines W10 (ein Würfel mit 10 Seiten) und die Ereignisse A = ungerade Augenzahl, $B = \{2\}$, $C = \{2, 3\}$.

- a) Geben Sie die Ereignismenge Ω an.
- b) Sind A und B vereinbar? Begründen Sie Ihre Entscheidung.
- c) Sind B und C vereinbar? Begründen Sie Ihre Entscheidung.
- d) Wie lauten die Gegenereignisse von A, B, C ?

TEILAUFGABE 2.1.2 2 PUNKTE

Wie groß ist die Wahrscheinlichkeit folgender Ereignisse beim Würfeln mit einem fairen W10?

- a) Augenzahl 4
- b) eine ungerade Augenzahl
- c) eine Augenzahl von mindestens 3
- d) Augenzahl 3 oder 4

TEILAUFGABE 2.1.3 2 PUNKTE

Ein fairer W10 wird zweimal geworfen. Wie groß ist die Wahrscheinlichkeit für die folgenden Ereignisse?

- a) zwei mal die 5
- b) wenigstens einmal die 1
- c) Summe der Zahlen gleich 4
- d) Summe der Zahlen größer gleich 19

AUFGABE 2.2 GUMMIBÄRCHENORAKEL 2.0 UND 3.0

Stellen Sie sich vor, in einer Tüte Gummibärchen befinden sich Bärchen in 7 verschiedenen Farben.

TEILAUFGABE 2.2.1 GUMMIBÄRCHENORAKEL 2.0, 2 PUNKTE

Für eine Befragung des Orakels ziehen Sie blind 5 Bärchen aus der Tüte. In der Tüte befinden sich von jeder Farbe mindestens 5 Bärchen.

Wie viele Möglichkeiten für verschiedene Farbkombinationen gibt es, wenn die Reihenfolge in welcher Sie die Bärchen ziehen

- a) nicht wichtig ist?
- b) wichtig ist

TEILAUFGABE 2.2.2 GUMMIBÄRCHENORAKEL 3.0, 2 PUNKTE

Für eine Befragung des Orakels ziehen Sie aus einem Gefäß, in dem sich 7 Bärchen in den 7 verschiedenen Farben befinden, blind 5 Bärchen.

Wie viele Möglichkeiten für verschiedene Bärchen-Anordnungen gibt es, wenn die Reihenfolge in welcher Sie die Bärchen ziehen

- a) nicht wichtig ist?
- b) wichtig ist

AUFGABE 2.3 PINS

Einige Banken errechnen Karten-PINs anhand der Kontonummer des Kunden. Nach einigen Rechenschritten wird am Ende eine vierstellige PIN aus den Ziffern 0-9 erzeugt.

TEILAUFGABE 2.3.1 1 PUNKT

Wie viele solcher PINs gibt es,

- a) wenn jede Ziffer mehrfach vorkommen darf?
- b) wenn jede Ziffer mehrfach vorkommen darf und die erste Stelle keine Null sein darf?

TEILAUFGABE 2.3.2 1 PUNKT

Mit welcher Wahrscheinlichkeit findet ein:e Angreifer:in in höchstens drei Versuchen in denen eine zufällig Zahl geraten wird (dumme:r Angreifer:in, der/die evtl. eine Zahl auch mehrmals wählt), die richtige PIN heraus,

- a) wenn jede Ziffer mehrfach vorkommen darf?
- b) wenn jede Ziffer mehrfach vorkommen darf und die erste Stelle keine Null sein darf?

AUFGABE 2.4 SOCKENSCHUBLADE, 4 PUNKTE

In einer Schublade sind 6 rote und 8 blaue Socken. Bob zieht jeden morgen noch im Dunkeln zufällig zwei Socken aus der Schublade, um pünktlich zur Vorlesung zu kommen.

Wie groß ist die Wahrscheinlichkeit, dass Bob

- a) zwei rote
- b) zwei blaue
- c) zwei verschiedene
- d) zwei zueinander passende

Socken trägt?

AUFGABE 2.5 KARTENSPIEL, 2 PUNKTE

In einem Kartenstapel befinden sich 8 Herz-, 8 Pik-, 8 Karo- und 8 Kreuz-Karten. Sie ziehen vier Karten, ohne sie anschließend zurückzulegen. Wie groß ist die Wahrscheinlichkeit folgender Ereignisse:

- a) A: Die gezogenen Karten haben alle eine andere Farbe.
- b) B: Die gezogenen Karten sind alles Herz-Karten.
- c) C: Es werden nur Herz- oder Pik-Karten gezogen.
- d) D: Es wird mindestens eine Herz-Karte gezogen.

AUFGABE 2.6 PASSWORTGENERATOR (KLAUSUR WS 18/19)

Da ihr Tinder-Account gehackt wurde, möchte sich Alice einen Passwortgenerator programmieren, der nicht knackbare Passwörter erzeugt. Hierfür geht sie wie folgt vor.

- **Schritt 1:** Wähle aus einer Menge von 36 möglichen Zeichen (Kleinbuchstaben a-z, Ziffern 0-9) 5 verschiedene Zeichen aus.
- **Schritt 2:** Erzeuge Passwort, indem alle 5 ausgewählten Zeichen in einer zufälligen Reihenfolge angeordnet werden.

TEILAUFGABE 2.6.1 2 PUNKTE

Berechnen Sie Anzahl der

- a) Auswahlmöglichkeiten von 5 Zeichen in Schritt 1, N_1
- b) (für eine fixe Auswahl von 5 Zeichen) erzeugbaren Passwörter in Schritt 2, N_2
- c) insgesamt (durch Kombination von Schritt 1 und 2) erzeugbaren Passwörter, N_3

TEILAUFGABE 2.6.2 2 PUNKTE

Verwenden Sie die Annahmen aus Aufgabe 2.6.1 über den Aufbau der erzeugten Passwörter, sowie Ihre Ergebnisse weiter. **Wenn Sie Aufgabe 2.6.1 nicht lösen konnten**, nutzen Sie $N_1 = 10^5$, $N_2 = 10^3$, $N_3 = 10^6$.

Mit welcher Wahrscheinlichkeit errät eine Hackerin ein ihr unbekanntes, von Alice zufällig erzeugtes Passwort

- a) mit nur einem Versuch?
- b) mit nur einem Versuch, wenn sie weiß welche Zeichen in Schritt 1 ausgewählt wurden?

Mittelschwere und schwere Aufgaben

AUFGABE 2.7 ZEITUNGSLESER, 3 PUNKTE

In Entenhausen erscheinen die Lokalblätter „Abendzeitung“ und „Bildpost“. Wir betrachten die Ereignisse

- A : ein Einwohner von Entenhausen liest die Abendzeitung,
- B : ein Einwohner von Entenhausen liest die Bildpost.

Die Wahrscheinlichkeit, dass ein Einwohner

- die Abendzeitung liest sei 0.6
- die Bildpost liest, sei 0.5
- die Abendzeitung oder die Bildpost (oder beide) liest, sei 0.9.

Stellen Sie die gesuchten Ereignisse mit Hilfe der Ereignisse A und B dar und berechnen Sie die Wahrscheinlichkeiten, dass ein Einwohner

- a) beide Lokalblätter liest,
- b) keines der beiden Lokalblätter liest,
- c) ein Lokalblatt, aber nicht beide liest?

AUFGABE 2.8 IM AUTOHAUS

Ein Autohaus will in seiner Neuwagenausstellung 20 verschiedene Autos zeigen.

TEILAUFGABE 2.8.1 2 PUNKTE

Von diesen Autos sollen 5 in Raum 1 nebeneinander (in einer Reihe) ausgestellt werden. Wie viele Möglichkeiten gibt es hierfür, wenn die Anordnung der Autos

- a) wichtig ist?
- b) nicht wichtig ist?

TEILAUFGABE 2.8.2 2 PUNKTE

Die restlichen 15 Autos sollen über die Räume 2 und 3 verteilt und dort ebenso nebeneinander (jeweils in einer Reihe) aufgestellt werden. Wie viele Möglichkeiten gibt es hierfür (für die Verteilung der Autos über die Räume 2 und 3), wenn die Anordnung der Autos

- a) wichtig ist?
- b) nicht wichtig ist?

Hinweis: Der Auswahlprozess funktioniert als **zweistufiges Verfahren**: zuerst werden 9 Autos für Raum 2 ausgewählt und aufgestellt, dann werden die restlichen 6 Autos in Raum 3 aufgestellt.

TEILAUFGABE 2.8.3 3 PUNKTE

Von den 20 Autos des Autohauses sind 2 von BMW, 10 von Mercedes, 3 von VW und 5 von Opel.
Mit welcher Wahrscheinlichkeit steht in Raum 1 (siehe 2.8.1)

- a) genau ein Mercedes?
- b) ein Opel ganz links?
- c) ein BMW oder ein VW auf dem Platz in der Mitte?

AUFGABE 2.9 Kfz-KENNZEICHEN (KLAUSUR WS 17/18)

Ignorieren Sie Ihre Kenntnisse über Kfz-Kennzeichen und arbeiten Sie mit den folgenden Annahmen!

Angenommen britische, deutsche und französische Kfz-Kennzeichen sind jeweils nach dem folgenden Schema aufgebaut:

- a) Britische Kennzeichen bestehen **immer** aus 5 Zeichen, deren **Reihenfolge wichtig** ist. Zuerst kommen 1 Großbuchstabe, dann 2 Ziffern, gefolgt von 3 Großbuchstaben. Alle Zeichen dürfen **mehrfach** vorkommen (z.B. Y53JEP, L51LLB, A66NOP, ...) (Anzahl N_b).
- b) Deutsche Kennzeichen bestehen **4, 5 oder 6** Zeichen, deren **Reihenfolge wichtig** ist. Zuerst kommen **1-, 2 oder 3** Großbuchstaben, dann nochmals 1 Buchstabe, dann 2 Ziffern. Die Buchstaben dürfen **mehrfach**, die Ziffern jeweils **nur einmal** vorkommen (z.B. KNX57, MM01, FFBX42, ...) (Anzahl N_d)
- c) Französische Kennzeichen bestehen **immer** aus 5 Zeichen, deren **Reihenfolge wichtig** ist. Jedes Kennzeichen besteht aus 4 Ziffern und 1 Großbuchstabe. Alle Zeichen dürfen **nur einmal** vorkommen, jedoch ist es egal, an welcher Stelle sich der Buchstabe befindet (z.B. A7209, 58X93, 7J583...) (Anzahl N_f).

Hinweis: Es gibt 26 verschiedene Großbuchstaben und 10 verschiedene Ziffern.

TEILAUFGABE 2.9.1 3 PUNKTE

Berechnen Sie die Anzahl der möglichen Kfz-Kennzeichen N_b, N_d, N_f .

TEILAUFGABE 2.9.2 3 PUNKTE

Verwenden Sie die Annahmen aus Aufgabe 2.9.1 über die Struktur der Kfz-Kennzeichen weiter.
Dann und nur dann, wenn Sie N_f nicht berechnen konnten, verwenden Sie $N_d = N_b = N_f = 650000$.
Berechnen Sie die Wahrscheinlichkeit

- a) dass ein **britisches** Kennzeichen mindestens einmal die Ziffer 5 enthält.
- b) dass ein **deutsches** Kennzeichen mit 3 Buchstaben beginnt.
- c) dass ein **französisches** Kennzeichen die Ziffernfolge 42 enthält.

AUFGABE 2.10 NUTZERNAMEN

TEILAUFGABE 2.10.1 4 PUNKTE

Wie viele verschiedene theoretisch mögliche Nutzernamen gibt es, wenn folgende Typen von Nutzernamen erlaubt sind?

- a) Typ 1: der Nutzernamen besteht aus zwei **verschiedenen** Kleinbuchstaben (N_1).
- b) Typ 2: der Nutzernamen besteht aus drei Kleinbuchstaben, die alle **mehrfach** vorkommen dürfen (N_2).
- c) Typ 3: der Nutzernamen besteht aus **vier oder fünf** Kleinbuchstaben, die sich innerhalb des Benutzernamens **nicht wiederholen dürfen** (N_3).

Hinweis: Es gibt 26 verschiedene Kleinbuchstaben.

TEILAUFGABE 2.10.2 2 PUNKTE

Mit welcher Wahrscheinlichkeit

- a) beinhaltet ein zufällig ausgewählter Typ 1 Nutzernamen mindestens einmal den Buchstaben X?
- b) beinhaltet ein zufällig ausgewählter Typ 2 Nutzernamen den Buchstaben X überhaupt nicht?
- c) lautet ein zufällig ausgewählter Typ 3 Nutzernamen „xxxx“ oder „xxxxx“?
- d) lautet ein zufällig ausgewählter Typ 3 Nutzernamen „abcd“ oder „vwxyz“?

AUFGABE 2.11 NUTZERNAMEN UND COMMIT-IDS (KLAUSUR SS21), 8 PUNKTE

Charlie arbeitet beim Webhoster Host123 und ist für das Kunden-Management zuständig. Die gängige Praxis ist die, dass jede:r Entwickler:in einer Kundenfirma einen **Nutzernamen**, welcher **den ersten 10 Zeichen** des SHA1-Hashes ihres/seines vollen Namens entspricht, erhält. Zusätzlich zum Nutzernamen ist jede:r Nutzer:in eine **Commit-ID** für das Repository zugeordnet, welche aus den **ersten 5 Zeichen** des Nutzernamens besteht.

Bob beobachtet, dass dieses Verfahren beim automatisierten Buildprozess manchmal für Probleme sorgt, weil es passieren kann, dass die Commit-ID nur aus Zahlen besteht, oder dass zwei Entwickler:innen die selbe Commit-ID zugeordnet bekommen.

Charlie nimmt vereinfacht an, dass eine SHA1-Hash eine Hexadezimal-Zahl ist, also aus den Ziffern 0-9 sowie den Buchstaben a-f besteht, wobei die einzelnen Zeichen mehrmals vorkommen können. Dann überlegt er sich Folgendes:

- a) (1 Punkt) Wie viele mögliche Nutzernamen N_N gibt es?
- b) (1 Punkt) Wie viele mögliche Commit-IDs N_C gibt es?
- c) (2 Punkte) Mit welcher Wahrscheinlichkeit $P(Z)$ besteht eine Commit-ID nur aus Ziffern?
- d) (2 Punkte) Mit welcher Wahrscheinlichkeit $P(G)$ haben zwei Nutzer:innen die selbe Commit-ID?
- e) (2 Punkte) Eine Umstellung des Verfahrens der Nutzernamen und Commit-ID Zuordnung ist zeitaufwändig und teuer, aber einige Kunden beschwerten sich über Probleme beim Buildprozess. Würden Sie an Charlies Stelle die gängige Praxis weiterlaufen lassen oder würden Sie eine andere Strategie wählen? Begründen Sie Ihre Meinung Hilfe Ihrer obigen Überlegungen.

Digitalaufgaben

AUFGABE 2.12 PASSWORTKNACKEN, 4 PUNKTE

Sie möchten demonstrieren, wie unsicher ein System ist, welches nur Passwörter zulässt, die genau 5 Zeichen lang. Die verwendbaren Zeichen sind lateinische (unsere üblichen) Klein- und Großbuchstaben (ohne Umlaute) und Ziffern von 0-9 die sich beliebig wiederholen dürfen.

- Berechnen Sie, wie viele unterschiedlichen Passwörter mit dieser Struktur es gibt.
- Versuchen Sie anschließend, ein Passwort zu knacken, welches nach genau diesem Schema aufgebaut ist. Der von <http://www.sha1-online.com/> berechnet SHA1 Hash des Passworts ist

39228d06a988045c5caaa97bf0a6158893d51862

Wie lautet das Passwort?

- Geben Sie an, wie lange Ihr Programm gelaufen ist.

Hinweise:

- Teamgröße: 3-5 (ein Team darf identische Lösungen abgeben, Namen der Teammitglieder bitte in der Lösung angeben)
- Bewertung: 1 Punkt für korrekte Anzahl, bis zu 3 Punkte für geknacktes Passwort, gut dokumentieren Code und Erwähnung der Laufzeit.
- Verwenden Sie eine Programmiersprache und eine SHA1-Implementierung, bzw. ein nicht selbst geschriebenes Tool Ihrer Wahl.