Übungsblatt 2 - mit Lösungen

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?

Lösung

a) $\Omega = \{1,2,\ldots,9,10\}$

b) $A \cap B = \emptyset$, daher sind A und B unvereinbar.

c) $B \cap C = \{2\}$, daher sind B und B vereinbar.

d) $\bar{A} = \Omega \setminus A = \{2,4,6,8,10\}, \bar{B} = \Omega \setminus B = \{1,3,4,5,6,7,8,9,10\}, \bar{C} = \Omega \setminus C = \{1,4,5,6,7,8,9,10\}$

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

LÖSUNG

Würfeln mit einem fairen Würfel ist Laplace-Experiment. $\Omega = \{1, 2, \ldots, 9, 10\}, n = 10$ damit

a) $P(4) = \frac{\text{günstige Fälle}}{\text{mögliche Fälle}} = \frac{1}{10} = 0.1$

b) $P(\text{ungerade}) = \frac{|\{1,3,5,7,9\}|}{5} = \frac{5}{10} = 0.5$

c) $P(\text{mindestes 3}) = \frac{|\{3,4,5,6,7,8,9,10\}|}{10} = \frac{8}{10} = 0.8$

d) $P(3,4) = P(3) + P(4) = \frac{2}{10} = 0.2$, da Ereignisse unvereinbar

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

LÖSUNG

Zweifaches Würfeln mit einem fairen Würfel ist Laplace-Experiment.
$\Omega = \{(1,1), (1,2), \ldots, (1,10), (2,1), \ldots, (10,9), (10,10)\}, n = 100$ damit

a) $P((5,5)) = \frac{\text{günstige Fälle}}{\text{mögliche Fälle}} = \frac{1}{100} = 0.01$

b) $P(\text{mindestens eine 1}) = \frac{|\{(1,1),(1,2),\ldots,(1,10),(2,1),\ldots(10,1)\}|}{100} = \frac{19}{100} = 0.19$

c) $P(\text{Summe} = 4) = \frac{|\{(3,1),(1,3),(2,2)\}|}{100} = \frac{3}{100} = 0.03$

d) $P(\text{Summe} \geq 19) = \frac{|\{(9,10),(10,9),(10,10)\}|}{100} = \frac{3}{100} = 0.03$

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

LÖSUNG

a) $N = C^W(7,5) = \binom{7+5-1}{5} = \binom{11}{5} = 462$

b) $N = P^W(7,5) = 7^5 = 16807$

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

Lösung

a) $N = C(7,5) = \binom{7}{5} = 21$

b) $N = P(7,5) = \frac{7!}{2!} = 2520$

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?

Lösung

a) $N_1 = 10^4 = 10000$

b) $N_2 = 9 \cdot 10^3 = 9000!$

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?

Lösung

Ansatz: Laplace - 3 günstige Möglichkeiten geteilt durch Anzahl aller Möglichkeiten. Ansatz die Wahrscheinlichkeiten für einen Erfolg im 1., 2. oder 3. Versuch aufzuaddieren ergibt fast genau die gleichen Zahlen.

a) $P_1 = \frac{3}{N_1} = \frac{3}{10000} = 0.0003 = 0.003\%$

b) $P_2 = \frac{3}{N_2} == \frac{3}{9000} = 0.000333 \approx 0.0003 = 0.003\%$

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?

Lösung

In der Schublade sind $n = 14$ Socken, davon $n_r = 6$ rote und $n_b = 8$ blaue. Es handelt sich um ein Laplace-Experiment.

Lösung mit Hilfe der Kombinatorik:

a) $P(\text{2rote}) = \frac{\text{günstige Fälle}}{\text{mögliche Fälle}} = \frac{\binom{6}{2}}{\binom{14}{2}} = \frac{15}{91} = 0.165$

b) $P(\text{2blaue}) = \frac{\text{günstige Fälle}}{\text{mögliche Fälle}} = \frac{\binom{8}{2}}{\binom{14}{2}} = \frac{28}{91} = 0.308$

c) $P(\text{2verschiedene}) = 1 - (P(\text{2rote} \cup \text{2blaue}) = 1 - (P(\text{2rote}) + P(\text{2blaue})) = 0.527$

d) $P(\text{2gleiche}) = 1 - (P(\text{2verschiedene})) = 0.473$

Für eine alternative Lösung über bedingte Wahrscheinlichkeiten, definiere folgende Ereignisse:

- $R1$: erste Socke ist rot, $R2$: zweite Socke ist rot
- $B1$: erste Socke ist blau, $B2$: zweite Socke ist blau

Damit

a) $P(\text{2rote}) = P(R1) \cdot P(R2|R1) = \frac{6}{14} \cdot \frac{5}{13} = \frac{15}{91} = 0.165$

b) $P(\text{2blaue}) = P(B1) \cdot P(B2|B1) = \frac{8}{14} \cdot \frac{7}{13} = \frac{28}{91} = 0.308$

c) $P(\text{2verschiedene}) = P(R1) \cdot P(B2|R1) + P(B1) \cdot P(R2|B1) = \frac{6}{14} \cdot \frac{8}{13} + \frac{8}{14} \cdot \frac{6}{13} = \frac{48}{91} = 0.527$

d) $P(\text{2gleiche}) = 1 - (P(\text{2verschiedene})) = 0.473$

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.

Lösung

Alle Karten sind gleich wahrscheinlich, verwende Daher LaPlace-Wahrscheinlichkeiten.

a) erste Karte beliebig, in den nächsten Schritten jeweils eine beliebige Karte einer anderen Farbe: $P(A) = \frac{32}{32} \cdot \frac{24}{31} \cdot \frac{16}{30} \cdot \frac{8}{29} = 0.114$

b) es dürfen nur 4 der 8 Herz-Karten gezogen werden: $P(B) = \frac{8}{32} \cdot \frac{7}{31} \cdot \frac{6}{30} \cdot \frac{5}{29} = 0.002$

c) es dürfen nur 4 der 16 Herz- oder Pik-Karten gezogen werden: $P(C) = \frac{16}{32} \cdot \frac{15}{31} \cdot \frac{14}{30} \cdot \frac{13}{29} = 0.051$

d) Berechnung via Gegenereignis: für keine Herzkarten gibt es 24 Möglichkeiten: $P(D) = 1 - P(\bar{D}) = 1 - \frac{24}{32} \cdot \frac{23}{31} \cdot \frac{22}{30} \cdot \frac{21}{29} = 1 - 0.294 = 0.7045$

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

Lösung

a) $N_1 = C(36,5) = \binom{36}{5} = 376992 = 3.7699 \times 10^5$

b) $N_2 = 5! = 120$

c) $N_3 = N_1 \cdot N_2 = 45239040 = 4.523 \times 10^6$ (Produktregel)

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?

Lösung

a) $P_{H1} = \frac{1}{N_3} = 3.1831 \times 10^{-4}$

b) $P_{H2} = \frac{1}{N_2} = \frac{1}{120} = 0.008$

|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?

Lösung

Die gegebenen Wahrscheinlichkeiten übersetzen sich zu

- $P(A) = 0.6$
- $P(B) = 0.5$
- $P(A \cup B) = 0.9$

Damit berechnen sich die gesuchten Wahrscheinlichkeiten zu

a) $P(\text{beide Lokalblätter}) = P(A \cap B) = P(A) + P(B) - P(A \cup B) = 0.6 + 0.5 - 0.9 = 0.2$

b) $P(\text{keines der beiden Lokalblätter}) = P(\bar{A} \cap \bar{B}) = P(A \bar{\cup} B) = 1 - P(A \cup B) = 1 - 0.9 = 0.1$

c) $P(\text{ein Lokalblatt aber nicht beide}) = P((A \cup B) \setminus (A \cap B)) = P(A \cup B) - P(A \cap B) = 0.9 - 0.2 = 0.7$

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?

LÖSUNG

a) Ansatz: Variationen ohne Wiederholung, $n = 20, k = 5$
$N_2 = P(n,k) = P(20,5) = \frac{20!}{15!} = 1860480$

b) Ansatz: Kombinationen ohne Wiederholung, $n = 20, k = 5$
$N_1 = C(n,k) = C(20,5) = \binom{20}{5} = 15504$

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.

LÖSUNG

a) Ansatz: Variationen ohne Wiederholung und Produktformel, $n_1 = 15, k_1 = 9, n_2 = 6, k_2 = 6$
$N_4 = P(n_1,k_1) \cdot P(n_2,k_2) = P(15,9) \cdot P(6,6) = \frac{15!}{6!} \cdot 6! = 15! = 1.308 \times 10^{12}$

b) Ansatz: Kombinationen ohne Wiederholung und Produktformel, $n_1 = 15, k_1 = 9, n_2 = 6, k_2 = 6$
$N_3 = C(n_1,k_1) \cdot C(n_2,k_2) = C(15,9) \cdot C(6,6) = \binom{15}{9} \cdot 1 = 5005$

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?

LÖSUNG

Ansatz: Laplace - Anzahl günstiger Fälle durch Anzahl möglicher Fälle und Produktformel

a) $P_1 = \frac{C(10,1) \cdot C(10,4))}{N_1} = \frac{\binom{10}{1} \cdot \binom{10}{4}}{\binom{20}{5}} = 0.135$
(hypergeometrische Verteilung resultiert aus Anwendung der Produktformel)

b) $P_2 = \frac{5 \cdot P(19,4)}{N_2} = \frac{5 \cdot \frac{19!}{15!}}{\frac{20!}{15!}} = \frac{5 \cdot 19!}{20!} = \frac{5}{20} = \frac{1}{4}$

c) $P_3 = \frac{5 \cdot P(19,4)}{N_2} = \frac{5 \cdot \frac{19!}{15!}}{\frac{20!}{15!}} = \frac{5 \cdot 19!}{20!} = \frac{5}{20} = \frac{1}{4}$

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.

Lösung

a) $N_b = P^W(26,1) \cdot P^W(10,2) \cdot P^W(26,3) = 26 \cdot 10^2 \cdot 26^3 = 45697600$

b) $N_d = P^W(26,1) \cdot P^W(26,1), \cdot P(10,2) + P^W(26,2) \cdot P^W(26,1), \cdot P(10,2) + P^W(26,3) \cdot P^W(26,1), \cdot P(10,2) = (P^W(26,1) + P^W(26,2) + P^W(26,3)) \cdot P^W(26,1) \cdot P(10,2) = (26 + 26^2 + 26^3) \cdot 26 \cdot 10 \cdot 9 = 42770520$

c) $N_f = 26 \cdot 5 \cdot P(10,4) = 26 \cdot 5 \cdot \frac{10!}{6!} = 26 \cdot 5 \cdot 10 \cdot 9 \cdot 8 \cdot 7 = 655200$

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.

Lösung

Verwende Annahme, dass es alles Laplace-Experimente sind, also alle Elementarereignisse gleich wahrscheinlich sind.

a) **Ansatz 1:** $P_b = P(\text{5 kommt ein oder zweimal vor}) = P(\text{5 kommt einmal vor}) + P(\text{5 kommt zweimal vor}) = \frac{2 \cdot 1 \cdot 9}{10 \cdot 10} + \frac{1 \cdot 1}{10 \cdot 10} = \frac{19}{100} = 0.19$
Ansatz 2: $P_b = 1 - P(\text{5 kommt gar nicht vor}) = 1 - \frac{9}{10} \cdot \frac{9}{10} = 1 - \frac{81}{100} = \frac{19}{100} = 0.19$

b) $P_d = P(\text{genau 3 Buchstaben am Anfang}) = \frac{26^3}{26+26^2+26^3} = 0.9616$

c) $P_f = P(42 \text{ kommt an einer von 4 möglichen Position vor}) = \frac{4 \cdot 3 \cdot 26 \cdot 8 \cdot 7}{N_f} = \frac{4 \cdot 3 \cdot 26 \cdot 8 \cdot 7}{26 \cdot 5 \cdot 10 \cdot 9 \cdot 8 \cdot 7}$
$\frac{4 \cdot 3}{5 \cdot 10 \cdot 9} = \frac{2}{75} = 0.0267$

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 Nutzername besteht aus zwei **verschiedenen** Kleinbuchstaben (N_1).

b) Typ 2: der Nutzername besteht aus drei Kleinbuchstaben, die alle **mehrfach** vorkommen dürfen (N_2).

c) Typ 3: der Nutzername besteht aus **vier oder fünf** Kleinbuchstaben, die sich innerhalb des Benutzernamens **nicht wiederholen dürfen** (N_3).

Hinweis: Es gibt 26 verschiedene Kleinbuchstaben.

Lösung

a) $N_1 = P(26, 2) = \frac{26!}{24!} = 26 \cdot 25 = 650$

b) $N_2 = P^W(26, 3) = 26^3 = 17576$

c) $N_3 = P(26, 5) + P(26, 4) = \frac{26!}{21!} + \frac{26!}{22!} = 8252400$

Teilaufgabe 2.10.2 2 Punkte

Mit welcher Wahrscheinlichkeit

a) beinhaltet ein zufällig ausgewählter Typ 1 Nutzername mindestens einmal den Buchstaben X?

b) beinhaltet ein zufällig ausgewählter Typ 2 Nutzername den Buchstaben X überhaupt nicht?

c) lautet ein zufällig ausgewählter Typ 3 Nutzername „xxxx“ oder „xxxxx“?

d) lautet ein zufällig ausgewählter Typ 3 Nutzername „abcd“ oder „vwxyz“?

Lösung

Ansatz: Laplace-Experiment, jeder mögliche Nutzername tritt mit der gleichen Wahrscheinlichkeit auf.

a) $P_1 = \frac{1 \cdot 25 + 25 \cdot 1}{N_1} = \frac{50}{650} = \frac{1}{13} \approx 0.0769$
alternativ: $P_1 = 1 - P(\text{X kommt nicht vor}) = 1 - \frac{25 \cdot 24}{26 \cdot 25} = 1 - \frac{24}{26} = 1 - \frac{12}{13} = \frac{1}{13} \approx 0.0769$

b) $P_2 = \frac{25^3}{N_2} = \frac{15625}{17576} \approx 0.888996$

c) $P_3 = 0$, da solche Nutzernamen qua Definition ausgeschlossen sind (Buchstaben dürfen sich nicht wiederholen)

d) $P_4 = P(\text{Nutzername ist abcd}) + P(\text{Nutzername ist vwxyz}) = \frac{1}{P(26,4)} + \frac{1}{P(26,5)} = \frac{22!}{26!} + \frac{22!}{26!} \frac{2}{8252400} \approx 2.9137 \cdot 10^{-6}$

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-Hashs 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 beschweren 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.

LÖSUNG

a) $k = 10, n = 10 + 6 = 16 \Rightarrow N_N = P^W(n,k) = n^k = 16^{10} = 1099511627776$

b) $k = 5, n = 10 + 6 = 16 \Rightarrow N_N = P^W(n,k) = n^k = 16^5 = 1048576$

c) $P(Z) = \frac{10^5 \cdot 16^5}{16^{10}} = \frac{10^5}{16^5} = 0.09537$

d) $P(G) = \frac{10^5 \cdot 16^5}{16^{10}} \cdot \frac{1 \cdot 16^5}{16^{10}} = \frac{10^5}{16^{10}} = 9.09495 \times 10^{-8}$

e) Ich würde an Charlies Stelle mit der gängigen Praxis weiterarbeiten, da die Wahrscheinlichkeiten doch recht gering sind. Vielleicht bei einem Redesign des Prozesses mal was ändern. Hier gibt es aber keine richtig richtige oder falsche Antwort, diese hängt stark von der Begründung ab.

|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.

a) Berechnen Sie, wie viele unterschiedlichen Passwörter mit dieser Struktur es gibt.

b) 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?

c) 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.

LÖSUNG

a) Anzahl Zeichen: $26 + 26 + 10 = 62$
Anzahl Passwörter: $62^5 = 916132832 \approx 0.9 \times 10^9$

b) Passwort: S0nN3