

<p style="text-align: center;">6. Übungsblatt Diskrete Strukturen (Winter 2019/20)</p>
--

Bauhaus-Universität Weimar, Professur für Mediensicherheit

Dr. Stefan Lucks, Jannis Bossert

URL: <http://www.uni-weimar.de/de/medien/professuren/mediensicherheit/teaching>

Abgabe: Bis zum 21. Januar 2020 vor Beginn der Übung oder per E-Mail an jannis.bossert@uni-weimar.de. Lösungen sind bevorzugt in LaTeX zu verfassen. Ein Template finden Sie auf der Übungsseite der Veranstaltung.

Aufgabe 1 – Bedingte Wahrscheinlichkeit (6 Punkte)

Angenommen, es gibt zwei äußerlich nicht voneinander unterscheidbare Urnen: Die erste Urne beinhaltet drei weiße und drei rote Kugeln; die zweite Urne drei weiße, eine rote und zwei blaue Kugeln. Sie können nicht sehen welche Kugeln wo enthalten sind. Ihre Aufgabe ist es zwei Kugeln ohne Zurücklegen zu ziehen. Sie gewinnen wenn Sie es schaffen zwei gleichfarbige Kugeln zu ziehen.

- a) Sie ziehen zuerst eine weiße Kugel. Mit welcher Wahrscheinlichkeit haben Sie die erste Urne erwischt?
- b) Sie ziehen zuerst eine rote Kugel. Mit welcher Wahrscheinlichkeit haben Sie die erste Urne erwischt?
- c) Ermitteln Sie in Abhängigkeit des Ergebnisses Ihres ersten Zuges eine für Sie optimale Strategie (aus derselben Urne nochmal ziehen oder wechseln) und ermitteln Sie Ihre maximale erwartete Gewinnwahrscheinlichkeit.

Aufgabe 2 – Grundlagen der Statistik (5 Punkte)

Wiederholen Sie aus den Vorlesungsinhalten und selbständig die Bedeutung von Kombination, Permutation und Variation.

Angenommen, Sie haben ein fair gemischtes Doppelkopfspiel mit 48 Karten (es gibt vier Farben und pro Farbe gibt es die folgenden Karten je zwei Mal: 9, 10, Bube, Dame, König und Ass).

- a) Sie ziehen alle 48 Karten nacheinander ohne Zurücklegen. Wieviele mögliche Reihenfolgen der Karten gibt es?
- b) Sie bekommen nacheinander eine Karte bis Sie 10 Karten haben. Nach jedem Zug wird die gezogene Karte wieder in den Stapel gemischt. Wieviele mögliche Ergebnisse gibt es für Ihre 10 Karten (d. h. die Reihenfolge ist irrelevant)?
- c) Sie erhalten 10 Karten aus dem Blatt nacheinander ohne Zurücklegen. Wie viele mögliche Reihenfolgen gibt es (die Reihenfolge ist relevant)?

- d) Wir ignorieren für diese Teilaufgabe die Farbe der Karten und betrachten nur ihren Kartenwert. Sie ziehen abermals alle 48 Karten nacheinander ohne Zurücklegen. Wieviele mögliche Reihenfolgen gibt es?
- e) Sie ziehen nacheinander eine Karte bis Sie eine Herz Zehn ziehen. Nach jedem Zug wird die gezogene Karte wieder in den Stapel gemischt. Wie oft müssen Sie ziehen damit Ihre Wahrscheinlichkeit für eine Herz Zehn ≥ 0.5 ist?

Aufgabe 3 – Passwörter (4 Punkte)

Beurteilen Sie die Sicherheit der folgenden Verfahren zur Passwörterzeugung. Begründen Sie bitte mathematisch, warum es in dem Ihrer Meinung nach sichereren System für einen Angreifer schwerer ist ein Passwort zu erraten. Gehen Sie hierbei davon aus, dass der Angreifer weiß, mit welchem System Sie das Passwort erzeugt haben.

System 1: Man wählt zufällig und gleichverteilt nacheinander 13 Zeichen aus dem Alphabet der Groß- und Kleinbuchstaben ohne Sonderzeichen und der Ziffern 0 - 9. ([a-zA-Z0-9])

System 2: Man wählt zufällig und gleichverteilt fünf Worte aus einem Wörterbuch mit 80000 Einträgen.

Zufällig und gleichverteilt bedeutet, dass bei System 1 jedes Zeichen mit der gleichen Wahrscheinlichkeit gewählt wird wie die anderen Zeichen und bei System 2, dass jedes Wort mit der gleichen Wahrscheinlichkeit gewählt wird wie jedes andere Wort. Das Ziehen erfolgt bei beiden Systemen mit Zurücklegen.