Wolfgang K. Seiler
Tel. 2515

A5, C201

9. Mai 2001

3. Übungsblatt zur Einführung in die Wahrscheinlichkeitstheorie

Fragen: *(je ein Punkt)*
Die Antworten auf die nachfolgenden Fragen sollten nicht länger als etwa zwei Zeilen sein und lediglich eine kurze *Begründung enthalten. Antworten ohne Begründung werden nicht gewertet.*

1) Geburtstage sind nicht gleichmäßig über das Jahr verteilt. Erhöht oder vermindert dies die Wahrscheinlichkeit, daß unter n Personen zwei den gleichen Geburtstag haben?

Lösung: Es erhöht sie, da sich die Geburtstage zu manchen Zeiten häufen.
(Viel mehr läßt sich mit etwa zwei Zeilen nicht sagen; ein exakter Beweis wäre mindestens eine Seite lang.)

2) *Richtig oder falsch:* Für $A, B, C \subseteq \Omega$ sei $P(A) \le P(B)$. Dann ist auch $P(A \mid C) \le P(B \mid C)$.

Lösung: *Falsch:* Beim Würfeln sei $A = C = \{2,4,6\}$ und $B = \{1,2,3,5\}$. In dieser Situation ist $P(A) = \frac{1}{2} < \frac{2}{3} = P(B)$, aber wegen $A \cap B = \{2\}$ ist $P(A \mid C) = 1 > \frac{1/6}{2/3} = \frac{1}{4} = P(B \mid A)$.

3) *Richtig oder falsch:* Für $A, B \subseteq \Omega$ mit $0 < P(A), P(B) < 1$ ist $P(A) < P(A \mid B)$.

Lösung: *Falsch:* Sei etwa beim Würfeln A das Ereignis *gerade* und B *ungerade*. Dann ist $P(A) = \frac{1}{2} > 0 = P(A \mid B)$.

4) Was ist $P(A \mid A^c)$?

Lösung: Ein Elementarereignis aus $A^c = \Omega \setminus A$ liegt definitionsgemäß nicht in A, also ist die bedingte Wahrscheinlichkeit null.

5) *Richtig oder falsch:* $\mathfrak{P}(\Omega_1) \otimes \mathfrak{P}(\Omega_2) = \mathfrak{P}(\Omega_1 \times \Omega_2)$ für abzählbare Mengen Ω_1, Ω_2.

Lösung: *Richtig:* Für $\omega_1 \in \Omega_1$ und $\omega_2 \in \Omega_2$ liegt $\{(\omega_1, \omega_2)\}$ in $\mathfrak{P}(\Omega_1) \otimes \mathfrak{P}(\Omega_2)$, und nach Definition einer σ-Algebra enthält $\mathfrak{P}(\Omega_1) \otimes \mathfrak{P}(\Omega_2)$ damit auch alle abzählbaren Vereinigungen solcher Mengen, also jede Teilmenge von $\Omega_1 \times \Omega_2$.

Aufgabe 1: (*5 Punkte)*

a) Wie wahrscheinlich ist es, daß 2 von 4 Personen am gleichen Wochentag geboren sind?

Lösung: Die Wahrscheinlichkeit, daß alle vier an verschiedenen Wochentagen geboren sind, ist

$$\frac{7 \cdot 6 \cdot 5 \cdot 4}{7^4} = \frac{6 \cdot 5 \cdot 4}{7^3} = \frac{120}{343};$$

die gesuchte Wahrscheinlichkeit ist komplementär dazu, also

$$1 - \frac{120}{343} = \frac{223}{343} \approx 0{,}65014577 \approx \frac{2}{3}.$$

b) Für elektronische Unterschriften unter größere Dateien wird der Datei zunächst durch eine praktisch nicht umkehrbare Funktion pseudozufällig ein 160 Bit langer Hashwert zugeordnet, und nur dieser wird wirklich „unterschrieben". Bei variabler Datei sind alle 2^{160} Hashwerte gleichwahrscheinlich. Nun erzeugt ein Betrüger zufällig n Dateien. Wie groß ist die Wahrscheinlichkeit, daß zwei davon auf denselben Hashwert führen?

Lösung: Mit $M = 2^{160}$ ist die Wahrscheinlichkeit des komplementären Ereignisses gleich

$$\frac{M(M-1)(M-2)\cdots(M-n+1)}{M^n} = \prod_{j=1}^{n-1} \frac{M-j}{M} = \prod_{j=1}^{n-1}\left(1-\frac{j}{M}\right),$$

die gesuchte Wahrscheinlichkeit also gleich $1 - \prod_{j=1}^{n-1}\left(1-\frac{j}{M}\right)$.

c) Wie groß muß n etwa sein, damit seine Erfolgschance bei mindestens einem Prozent liegt?

Lösung: Hierzu müssen wir den Ausdruck aus *b)* durch einen Wert der Exponentialfunktion approximieren: Wegen

$$e^x = \lim_{\nu\to\infty}\left(1+\frac{x}{\nu}\right)^\nu \approx \left(1+\frac{x}{M}\right)^M$$

ist $e^{-\frac{j}{M}} \approx 1 - \frac{j}{M}$ und damit

$$\prod_{j=1}^{n-1}\left(1-\frac{j}{M}\right) \approx \prod_{j=1}^{n-1} e^{-\frac{j}{M}} = e^{\sum_{j=1}^{n-1}\frac{j}{M}} = e^{-\frac{(n-1)(n-2)}{2M}} \approx e^{-\frac{n^2}{2M}}.$$

Eins minus diesem Wert wird größer als $1\% = \frac{1}{100}$, sobald der Wert selbst kleiner wird als $99\% = \frac{99}{100}$, und das ist äquivalent zu

$$\frac{n^2}{2M} > -\ln\frac{99}{100} = \ln\frac{100}{99} \quad \text{oder}$$

$$n > \sqrt{2M\ln\frac{100}{99}} = \sqrt{2^{161}\ln\frac{100}{99}} = 2^{80}\sqrt{2\ln\frac{100}{99}} \approx 2^{80}\cdot 0{,}1417768 \approx 1{,}713977\cdot 10^{23}.$$

NB: *Warum sollte ein Betrüger versuchen, zwei Dateien mit gleichem Hashwert zu finden?*

Angenommen, er hat zwei Dateien, deren erste sein Opfer bedenkenlos unterschreiben kann, wohingegen die zweite diesem schwere Nachteile bringt. Falls es der Betrüger schafft, beide Dateien durch Zufallsmodifikationen, die nichts am Sinn ändern, so zu verändern, daß sie denselben Hashwert liefern, läßt er das Opfer die erste unterschreiben und hängt diese Unterschrift (die nur vom Hashwert abhängt) unter die zweite.

Zufallsmodifikationen wie zusätzliche Leerzeichen, Tabulatoren, eventuell auch die Folge Leertaste/Rückwärtstaste lassen sich auch in einem kurzen Text an vielen Stellen einfügen oder oder auch nicht; bei r Stellen ergibt dies 2^r Möglichkeiten mit r deutlich über hundert. Falls jemand die Resourcen hat, um rund 2^{80} Modifikationen jeder der beiden Dateien zu erzeugen und auf ihren Hashwert zu testen, hat er somit Chancen, eine Unterschrift unter einen gefälschten Vertrag erhalten. Beim derzeitigem Stand der Technik haben wohl höchstens Agenturen wie NSA die dazu notwendigen Mittel.

Aufgabe 2: *(5 Punkte)*

Von den Anmeldungen zum Übungsbetrieb für diese Vorlesung entfallen drei Viertel auf den Integrierten Studiengang Mathematik und Informatik sowie je ein Achtel auf Lehramt und auf Wirtschaftspädagogik. Die folgende Tabelle zeigt, mit welcher Wahrscheinlichkeit einige Aussagen auf die einzelnen Studenten zutreffen:

	<4. Sem.	*4. Sem*	*>4. Sem.*	*männlich*	*weiblich*
Math. & Inf.	1/18	8/9	1/18	2/3	1/3
Lehramt	0	2/3	1/3	1/3	2/3
Wirtschaftspäd.	0	0	1	1	0

Bestimmen Sie mittels der BAYESschen Formel die Wahrscheinlichkeit dafür, daß

a) eine zum Übungsbetrieb angemeldete Studentin Mathematik und Informatik studiert

Lösung: Seien MI, LA, WP und W die Ereignisse „studiert Mathematik und Informatik", „studiert für Lehramt", „studiert Wirtschaftspädagogik" und „ist weiblich". Dann ist

$$P(W \mid MI) = \frac{1}{3}, \quad P(W \mid LA) = \frac{2}{3} \quad \text{und} \quad P(W \mid WP) = 0\,.$$

Also ist

$$\begin{aligned} P(W) &= P(MI) \cdot P(W \mid MI) + P(LA) \cdot P(W \mid LA) + P(WP) \cdot P(W \mid WP) \\ &= \frac{3}{4} \cdot \frac{1}{3} + \frac{1}{8} \cdot \frac{2}{3} = \frac{1}{4} + \frac{1}{12} = \frac{1}{3}\,, \end{aligned}$$

und nach der BAYESschen Formel ist

$$P(MI \mid W) = \frac{P(W \mid MI) \cdot P(MI)}{P(W)} = \frac{\frac{1}{3} \cdot \frac{3}{4}}{\frac{1}{3}} = \frac{3}{4}\,.$$

b) jemand aus einem höheren als dem vierten Semester Wirtschaftspädagogik studiert!

Lösung: Sei H das Ereignis „studiert in einem höheren als dem vierten Semester"; dann ist

$$\begin{aligned} P(H) &= P(MI) \cdot P(H \mid MI) + P(LA) \cdot P(H \mid LA) + P(WP) \cdot P(H \mid WP) \\ &= \frac{3}{4} \cdot \frac{1}{18} + \frac{1}{8} \cdot \frac{1}{3} + \frac{1}{8} \cdot 1 = \frac{1}{24} + \frac{1}{24} + \frac{1}{8} = \frac{5}{24}\,. \end{aligned}$$

Damit läßt sich wieder die BAYESschen Formel anwenden:

$$P(WP \mid H) = \frac{P(H \mid WP) \cdot P(WP)}{P(H)} = \frac{1 \cdot \frac{1}{8}}{\frac{5}{24}} = \frac{3}{5}\,.$$

c) Wie viele Studenten sind zum Übungsbetrieb angemeldet?

Lösung: Wenn alle Wahrscheinlichkeiten exakt angegeben sind, muß die Anzahl N der angemeldeten Studenten auf jeden Fall durch acht teilbar sein, denn sonst wäre die Anzahl der Lehramtskandidaten und der Wirtschaftspädagogen nicht ganzzahligen.

Die Anzahl $\frac{3}{4}N$ der Studenten im integrierten Studiengang muß wegen der nicht im vierten Semester Studierenden durch 18 teilbar sein, N selbst also durch $\frac{4}{3} \cdot 18 = 24$. Damit sind alle Teilbarkeitsbedingungen erfüllt: Ist nämlich $N = 24k$, so gibt es $18k$ Studenten im integrierten Studiengang, von denen jeweils k nicht im vierten Semester sind und von denen $12k$ männlich und $6k$ weiblich sind. Entsprechend gibt es $3k$ Lehramtskandidaten, 2k davon im vierter Semester, k männlich und 2k weiblich. Die 3k Wirtschaftspädagogen sind allesamt männlich und in höheren Semestern.

Die Frage ist jetzt nur noch, wie groß k ist. Falls man davon ausgeht, daß die meisten angemeldeten Studenten zur Übung kommen und es im Hörsaal HS103 mit seinen 42 Stühlen noch eine ganze Reihe freier Plätze gibt, kommt eigentlich nur $k = 1$ in Frage; also haben sich 24 Studenten angemeldet.

d) Falls Sie nicht dazugehören: *Melden Sie sich an!*

Lösung: Diese Teilaufgabe wurde sechsmal bearbeitet, in 5/6 der Fälle korrekt. (Das restliche Sechstel war schon angemeldet.) Zur nachträglichen Bearbeitung finden Sie ein Formular unter

http://hilbert.math.uni-mannheim.de/~seiler/EinfWT/anmeldung.html

Mit den neuen Zahlen wären die Zahlenwerte in der Aufgabe unangenehmer gewesen: Jetzt haben die Häufigkeiten der drei Studiengänge allesamt die Primzahl 29 als Nenner.

Aufgabe 3: *(5 Punkte)*

F sei ein Ereignis mit $P(F) > 0$. Zwei Ereignisse A, B heißen F-*unabhängig*, falls gilt: $P(A \cap B \mid F) = P(A \mid F) \cdot P(B \mid F)$. Man beweise oder widerlege durch Gegenbeispiel:

a) Sind A und B unabhängig, so sind sie auch F-unabhängig.

Lösung: Wenn man etwas mit der Definition der bedingten Wahrscheinlichkeit herumspielt und versucht, die F-Unabhängigkeit aus der Abhängigkeit zu folgern, stößt man schnell auf Schwierigkeiten, so daß man anfangen sollte, auch an die Möglichkeit eines Gegenbeispiels zu denken.

Beim Werfen zweier unterscheidbarer Würfel sei A das Ereignis „Augenzahl des ersten Würfels ist gerade“ und B das Ereignis „Augenzahl des zweiten Würfels ist ungerade“. Dann sind A und B offensichtlich unabhängig: $P(A) = P(B) = \frac{1}{2}$ und $P(A \cap B) = \frac{1}{4}$.

Mit dem neuen Ereignis F: „Beide Augenzahlen sind gleich“ ist aber $P(A \cap B \mid F) = 0$, während $P(A \mid F)$ und $P(B \mid F)$ beide gleich $\frac{1}{2}$ sind; A und B sind also nicht F-unabhängig. Wegen der Positivität von $P(F) = \frac{1}{6}$ ist damit ein Gegenbeispiel gefunden.

b) Sind A und B F-unabhängig bezüglich aller F mit $P(F) > 0$, so sind sie unabhängig.

Lösung: Nehme $F = \Omega$; dann ist $P(E \mid F) = P(E)$ für jedes Ereignis E, insbesondere also für A, B und $A \cap B$. Damit folgt die gewöhnliche Unabhängigkeit aus der F-Unabhängigkeit für $F = \Omega$.