16-124-836
Marcel Zauder

2.1 Zwei Würfel

Allgemein gilt: $E[Y \mid B] = \frac{E[1_B \cdot Y]}{P(B)}$

a) E[Z|X ist gerade]

P(X ist gerade) = $\frac{1}{2}$
$E[1_{X \text{ ist gerade}} \cdot Z]$ = P(Z=1|X ist gerade)·1 + P(Z=2|X ist gerade)·2 +...+ P(Z=12|X ist gerade)·12
$E[1_{X \text{ ist gerade}} \cdot Z] = \frac{1}{36}\cdot 3 + \frac{1}{36}\cdot 4 + \frac{2}{36}\cdot 5 + \frac{2}{36}\cdot 6 + \frac{3}{36}\cdot 7 + \frac{3}{36}\cdot 8 + \frac{2}{36}\cdot 9 + \frac{2}{36}\cdot 10 + \frac{1}{36}\cdot 11 + \frac{1}{36}\cdot 12 = \frac{135}{36} = 3{,}75$
$\rightarrow$ E[Z|X ist gerade] = $\frac{3{,}75}{\frac{1}{2}} = 7{,}5$

b) E[Z|Y ist ungerade]

P(Y ist ungerade) = $\frac{1}{2}$
$E[1_{Y \text{ ist ungerade}} \cdot Z]$ = P(Z=1|Y ist ungerade)·1 + P(Z=2|Y ist ungerade)·2 +...+ P(Z=12|Y ist ungerade)·12
$E[1_{Y \text{ ist ungerade}} \cdot Z] = \frac{1}{36}\cdot 2 + \frac{1}{36}\cdot 3 + \frac{2}{36}\cdot 4 + \frac{2}{36}\cdot 5 + \frac{3}{36}\cdot 6 + \frac{3}{36}\cdot 7 + \frac{2}{36}\cdot 8 + \frac{2}{36}\cdot 9 + \frac{1}{36}\cdot 10 + \frac{1}{36}\cdot 11 = \frac{117}{36} = 3{,}25$
$\rightarrow$ E[Z|Y ist ungerade] = $\frac{3{,}25}{\frac{1}{2}} = 6{,}5$

c) E[X|Z = 5]

P(Z = 5) = P(X = 1,Y = 4) + P(X = 2,Y = 3) + P(X = 3,Y = 2) + P(X = 4,Y = 1) = $\frac{4}{36} = \frac{1}{9}$
$E[1_{Z = 5} \cdot X]$ = P(X=1|Z=5)·1 + P(X=2|Z=5)·2 +...+ P(X=6|Z=5)·6
$E[1_{Z = 5} \cdot X] = \frac{1}{36}\cdot 1 + \frac{1}{36}\cdot 2 + \frac{1}{36}\cdot 3 + \frac{1}{36}\cdot 4 = \frac{10}{36}$
$\rightarrow$ E[X|Z = 5] = $\frac{\frac{10}{36}}{\frac{1}{9}} = 2{,}5$

d) E[Y|Z > 6]

P(Z > 6) = 1 - P(Z $\leq$ 6) = 1 - [P(X = 1,Y = 1) + P(X = 1,Y = 2) + ...+ P(X = 5,Y = 1)
= 1 - $\frac{15}{36} = \frac{21}{36}$
$E[1_{Z > 6} \cdot Y]$ = P(Y=1|Z>6)·1 + P(Y=2|Z>6)·2 +...+ P(Y=6|Z>6)·6
$E[1_{Z > 6} \cdot Y] = \frac{1}{36}\cdot 1 + \frac{2}{36}\cdot 2 + \frac{3}{36}\cdot 3 + \frac{4}{36}\cdot 4 + \frac{5}{36}\cdot 5 + \frac{6}{36}\cdot 6 = \frac{91}{36}$
$\rightarrow$ E[Y|Z > 6] = $\frac{\frac{91}{36}}{\frac{21}{36}} = \frac{13}{3}$ = 4,3333333...

2.2 Jensen im Quadrat

zu Beweisen: $\mathrm{E[X^k] \geq E[X]^k}$ $\quad\quad$ $\mathrm{k \geq 2; k \in N}$

Wir wissen: Wenn die Funktion f(x) zweimal differenzierbar ist, mit f"(x) $\geq 0 \;\forall$ x, dann ist sie konvex.
Sei nun f(x) := $\mathrm{x^{2k}}$ mit k $\in$ N. Dann ist:

$$f''(x) = k * (k-1) * x^{k-2} \geq 0$$

Somit folgt, dass f(x) = $\mathrm{x^k}$ konvex ist für alle geraden k.
Durch die Jensen-Ungleichung wissen wir, dass für eine konvexe Funktion f und $\lambda_i > 0$ mit $\sum_{i=1}^{n} \lambda_i = 1$ gilt:

$$f(\sum_{i=1}^{n} \lambda_i x_i) \leq \sum_{i=1}^{n} \lambda_i f(x_i)$$

Sei nun $\lambda_i := P(X=x)$, $f(x) = x^k$:

$$E[X]^k = (\sum_{i=1}^{n} P(X=x_i) * x_i)^k = f(\sum_{i=1}^{n} \lambda_i * x_i) \leq \sum_{i=1}^{n} \lambda_i * f(x_i) = \sum_{i=1}^{n} P(X=x_i) * x_i^k = E[X^k]$$

2.3 Min-Max im Erwartungswert

a) Was ist E[min(A,B)] und E[max(A,B)]?

$$E[max(A,B)] = \sum_a \sum_b max(a,b) \cdot \frac{1}{k} \cdot \frac{1}{k} = \frac{1}{k^2} \sum_a \sum_{b \leq a} a + \sum_{b>a} b$$

$$E[min(A,B)] = \sum_a \sum_b min(a,b) \cdot \frac{1}{k} \cdot \frac{1}{k} = \frac{1}{k^2} \sum_a \sum_{b \leq a} b + \sum_{b>a} a$$

b) zu Zeigen: E[min(A,B)] + E[max(A,B)] = E[A] + E[B]

$$E[max(A,B)] + E[min(A,B)] = \frac{1}{k^2} \sum_a \sum_{b \leq a} a + \sum_{b>a} b + \frac{1}{k^2} \sum_a \sum_{b \leq a} b + \sum_{b>a} a$$

$$= \frac{1}{k^2} \cdot \sum_a \left(\sum_b b + \sum_b a \right) = \frac{1}{k^2} \cdot \sum_a \sum_b a + b = E[A] + E[B]$$

c) Beweis durch Eigenschaften des Erwartungswertes

$$E[max(A,B)] + E[min(A,B)] = E[max(A,B) + min(A,B)] = E[A+B] = E[A] + E[B]$$

2.4 Ein zufälliger Text

weitere Annahmen sind zu treffen, da sonst die Aufgabe nicht zu lösen ist:

(i) Die Katze trifft bei jedem Schritt genau ein Zeichen

(ii) der nächste Buchstabe ist unabhängig von der vorherigen Eingabe (ein Zeichen kann auch doppelt hintereinander eingegeben werden)

(iii) Wir beachten nicht, dass die Katze auch weniger oder mehr Zeichen eingeben kann, sondern, dass sie immer genau die angegebene Zeichenanzahl erreicht

a) Ihr Passwort (10 Zeichen)
P(Passwort) = $(\frac{1}{32})^{10}$ = 8,88 · 10^{-16}

b) Den 128-bit AES-Schlüssel einer TLS-Verbindung auf dem Internet
Der AES-Schlüssel besteht in diesem Beispiel aus 26 Zeichen, also:
P(Passwort) = $(\frac{1}{32})^{26}$ = 7,35 · 10^{-40}

c) Die Kopfzeile dieses Übungsblattes (125 Zeichen)
P(Passwort) = $(\frac{1}{32})^{125}$ = 7,18 · 10^{-189}

d) **Zusatz:** Computer mit $40 \cdot 10^{18}$ Operationen pro Sekunde

(i) Passwort
T_{max}(Passwort) $= \frac{1}{2} \cdot \frac{32^{10}}{40 \cdot 10^{18}} = 1,41 \cdot 10^{-5}$ sec

(ii) AES-Schlüssel
T_{max}(Passwort) $= \frac{1}{2} \cdot \frac{32^{26}}{40 \cdot 10^{18}} = 1,70 \cdot 10^{19}$ sec

(iii) Kopfzeile
T_{max}(Passwort) $= \frac{1}{2} \cdot \frac{32^{125}}{40 \cdot 10^{18}} = 1,74 \cdot 10^{168}$ sec (sehr sehr lange)