

## 6 Binäre Summen binärer Zufallsvariablen

**Satz 1 („Piling Up Lemma“)** Sei  $\Omega$  ein Wahrscheinlichkeitsraum und

$$X_1, \dots, X_r : \Omega \longrightarrow \mathbb{F}_2$$

unabhängige Zufallsvariablen mit  $p_i := P(X_i = 0) = P(X_i^{-1}(0))$ . Sei  $X = X_1 + \dots + X_r$  (binäre Summe in  $\mathbb{F}_2$ ) und  $p := P(X = 0)$ . Sei  $\lambda_i = (2p_i - 1)^2$  für  $i = 1, \dots, r$  und  $\lambda = (2p - 1)^2$ . Dann gilt  $\lambda = \lambda_1 \cdots \lambda_r$ .

*Beweis.* Es reicht, den Beweis für  $r = 2$  zu führen. Für  $\omega \in \Omega$  ist  $X(\omega) = 0$  genau dann, wenn  $X_1(\omega)$  und  $X_2(\omega)$  beide 0 oder beide 1 sind. Also ist

$$\begin{aligned} p &= p_1 p_2 + (1 - p_1)(1 - p_2) = 1 - p_1 - p_2 + 2p_1 p_2, \\ 2p - 1 &= 4p_1 p_2 - 2p_1 - 2p_2 + 1 = (2p_1 - 1)(2p_2 - 1), \\ \lambda &= \lambda_1 \lambda_2, \end{aligned}$$

wie behauptet.  $\diamond$

Für die Wahrscheinlichkeiten ist die Formel etwas komplizierter:

**Korollar 1** Mit den Bezeichnungen von Satz 1 gilt

$$p = \frac{1}{2} + 2^{r-1} \cdot \prod_{i=1}^r \left(p_i - \frac{1}{2}\right).$$

**Korollar 2** Ist ein  $p_i = \frac{1}{2}$ , so  $\lambda = 0$ ,  $p = \frac{1}{2}$ .

**Korollar 3** Mit wachsendem  $r$  ist  $\lambda$  monoton fallend.