Gleichverteilte Zufallsvariablen in Gruppen[1]

Satz 1 *Sei G eine Gruppe mit einem endlichen, translationsinvarianten Maß μ und Ω ein Wahrscheinlichkeitsraum. Seien $X, Y : \Omega \longrightarrow G$ Zufallsvariablen, X sei gleichverteilt, und X, Y seien unabhängig. Sei $Z = X * Y$ (mit der Gruppenoperation $*$). Dann gilt:*

(i) *Z ist gleichverteilt.*

(ii) *Y und Z sind unabhängig.*

Kommentar. Die Unabhängigkeit von X und Y bedeutet

$$P(X^{-1}A \cap Y^{-1}B) = P(X^{-1}A) \cdot P(Y^{-1}B) \quad \text{für alle messbaren } A, B \subseteq G.$$

Die Gleichverteilung von X bedeutet

$$P(X^{-1}A) = \frac{\mu(A)}{\mu(G)} \quad \text{für alle messbaren } A \subseteq G.$$

Insbesondere ist das Maß P_X auf G mit $P_X(A) = P(X^{-1}A)$ translationsinvariant, wenn μ es ist.

Bemerkung. Z ist Zufallsvariable, weil $Z = m^{-1} \circ (X, Y)$ mit der Gruppenoperation $m = *$. Diese ist messbar, weil ihre g-Schnitte,

$$(m^{-1}A)_g = \{h \in G \mid gh \in A\}$$

alle messbar sind und die Funktion

$$g \mapsto \mu(m^{-1}A)_g = \mu(g^{-1}A) = \mu(A)$$

messbar ist. Nach einer Vorform des Satzes von Fubini folgt die Messbarkeit von $m^{-1}A \subseteq G \times G$, und

$$(\mu \otimes \mu)(m^{-1}A) = \int_G (m^{-1}A)_g \, dg = \mu(A) \int_G dg = \mu(A)\mu(G).$$

Anwendung. In der Kryptographie, bei der Bitstrom-Verschlüsselung, ist $G = \mathbb{F}_2^n$ die Menge aller Folgen von n Bits. Der Klartext $y_1 \dots y_n$ wird als Realisierung von Y aufgefasst. Der Schlüssel $x_1 \dots x_n$ soll dann Realisierung einer gleichverteilten Zufallsvariablen X sein. Dann ist die bitweise Summe (XOR) Z von X und Y nicht von einer völlig zufälligen Bitfolge zu unterscheiden und vom Klartext Y stochastisch unabhängig. Statistische Analysen des Kryptoanalytikers müssen also erfolglos bleiben.

[1] Klaus Pommerening, Kryptologie; 27. Juni 1994, letzte Änderung: 16. Juni 2002

Allgemeiner gilt diese Betrachtung auch bei der aperiodischen polyalphabetischen Chiffrierung über einer beliebigen Gruppe.

Gegenbeispiele.

1. Was ist, wenn man die Gleichverteilung von X nicht voraussetzt? Als Beispiel kann man $X = \mathbf{1}$ (Einselement der Gruppe) konstant wählen und Y beliebig; X und Y sind dann unabhängig, aber $Z = Y$ ist im allgemeinen weder gleichverteilt noch von Y unabhängig.

2. Was ist, wenn man die Unabhängigkeit von X und Y nicht voraussetzt? Als Beispiel kann man $Y = X^{-1}$ wählen; das Produkt $Z = \mathbf{1}$ ist im allgemeinen nicht gleichverteilt. Die Wahl $Y = X$ ergibt $Z = X^2$, das im allgemeinen weder gleichverteilt noch von Y unabhängig ist. (Konkretes Beispiel: $\Omega = G = \mathbb{Z}/4\mathbb{Z}, X =$ identische Abbildung $Z =$ Quadrat-Abbildung.)

Allgemeiner Beweis des Satzes

Betrachtet werden die Produktabbildung

$$(X, Y) \colon \Omega \longrightarrow G \times G$$

und die erweiterte Multiplikation

$$\sigma \colon G \times G \longrightarrow G \times G, \quad (g, h) \mapsto (g * h, h).$$

Für $A, B \subseteq G$ gilt nach Definition der Produktwahrscheinlichkeit

$$(P_X \otimes P_Y)(A \times B) = P_X(A) \cdot P_Y(B) = P(X^{-1}A) \cdot P(Y^{-1}B);$$

wegen der Unabhängigkeit von X und Y ist dies weiter

$$\begin{aligned} &= P(X^{-1}A \cap Y^{-1}B) = P\{\omega \mid X\omega \in A, Y\omega \in B\} \\ &= P((X,Y)^{-1}(A \times B)) = P_{(X,Y)}(A \times B). \end{aligned}$$

Also ist $P_{(X,Y)} = P_X \otimes P_Y$, und für $S \subseteq G \times G$ gilt nach dem Satz von Fubini

$$P_{(X,Y)}(S) = \int_{h \in G} P_X(S_h) \cdot P_Y(dh).$$

Speziell für $S = \sigma^{-1}(A \times B)$ gilt

$$\begin{aligned} S_h &= \{g \in G \mid (g * h, h) \in A \times B\} = \begin{cases} A * h^{-1}, & \text{falls } h \in B, \\ \emptyset & \text{sonst.} \end{cases} \\ P_X(S_h) &= \begin{cases} P_X(A * h^{-1}) = \frac{\mu(A)}{\mu(G)}, & \text{falls } h \in B, \\ 0 & \text{sonst.} \end{cases} \end{aligned}$$

Also ist

$$\begin{aligned} P(Z^{-1}A \cap Y^{-1}B) &= P\{\omega \in \Omega \mid X(\omega) * Y(\omega) \in A, Y(\omega) \in B\} \\ &= P((X,Y)^{-1}S) = P_{(X,Y)}(S) \\ &= \int_{h\in B} \frac{\mu(A)}{\mu(G)} \cdot P_Y(dh) = \frac{\mu(A)}{\mu(G)} \cdot P(Y^{-1}B). \end{aligned}$$

Im Fall $B = G$ folgt $P(Z^{-1}A) = \frac{\mu(A)}{\mu(G)}$, womit (i) bewiesen ist, und daraus folgt

$$P(Z^{-1}A \cap Y^{-1}B) = P(Z^{-1}A) \cdot P(Y^{-1}B)$$

womit auch (ii) bewiesen ist. $\diamond$

Beweis im abzählbaren Fall

Da der obige Beweis allgemeine Masstheorie verwendete, in der Idee aber sehr einfach ist, wird er hier noch einmal im abzählbaren Fall durchgeführt, wo die Integrale zu Summen werden und die Schlussweisen elementar verständlich sind.

Hilfssatz 1 *Mit G, Ω, X, Y und Z wie im Satz gilt*

$$Z^{-1}(A) \cap Y^{-1}(B) = \bigcup_{h\in B} [X^{-1}(A * h^{-1}) \cap Y^{-1}h]$$

für alle messbaren $A, B \subseteq G$.

Das folgt aus den Gleichungen

$$\begin{aligned} Z^{-1}A &= (X,Y)^{-1}\{(g,h) \in G \times G \mid g * h \in A\} \\ &= (X,Y)^{-1}\left[\bigcup_{h\in G} A * h^{-1} \times \{h\}\right] \\ &= \bigcup_{h\in G} (X,Y)^{-1}(A * h^{-1} \times \{h\}) \\ &= \bigcup_{h\in G} [X^{-1}(A * h^{-1}) \cap Y^{-1}h], \\ Z^{-1}A \cap Y^{-1}B &= \bigcup_{h\in G} [X^{-1}(A * h^{-1}) \cap Y^{-1}h \cap Y^{-1}B] \\ &= \bigcup_{h\in B} [X^{-1}(A * h^{-1}) \cap Y^{-1}h]. \end{aligned}$$

Sei jetzt also G höchstens abzählbar. Dann ist

$$\begin{aligned}
P(Z^{-1}A \cap Y^{-1}B) &= \sum_{h\in B} P[X^{-1}(A * h^{-1}) \cap Y^{-1}h] \\
&= \sum_{h\in B} P[X^{-1}(A * h^{-1})] \cdot P[Y^{-1}h] \quad \text{(da } X, Y \text{ unabhängig)} \\
&= \sum_{h\in B} \frac{\mu(A * h^{-1})}{\mu(G)} \cdot P[Y^{-1}h] \quad \text{(da } X \text{ gleichverteilt)} \\
&= \frac{\mu(A)}{\mu(G)} \cdot \sum_{h\in B} P[Y^{-1}h] \\
&= \frac{\mu(A)}{\mu(G)} \cdot P[\bigcup_{h\in B} Y^{-1}h] \\
&= \frac{\mu(A)}{\mu(G)} \cdot P(Y^{-1}B).
\end{aligned}$$

Im Fall $B = G$ folgt $P(Z^{-1}A) = \frac{\mu(A)}{\mu(G)}$, womit (i) bewiesen ist, und daraus folgt

$$P(Z^{-1}A \cap Y^{-1}B) = P(Z^{-1}A) \cdot P(Y^{-1}B),$$

womit auch (ii) bewiesen ist. $\diamond$