Übungen zur Kryptologie

Blatt 4 SoS 2024 — H. Kiechle

Präsenzaufgaben

11. Gegeben seien zwei endliche Mengen Q und K, auf denen jeweils eine Wahrscheinlichkeitsfunktion $p_Q : Q \to [0,1]$ bzw. $p_K : K \to [0,1]$ definiert ist. Dann ist

$$p : Q \times K \to [0,1]; (x,k) \mapsto p_Q(x) \cdot p_K(k).$$

eine Wahrscheinlichkeitsfunktion auf $Q \times K$.

Für $k \in K$ bzw. $q \in Q$ seien die Ereignisse $Q_k := \{(x,k)\,;\ x \in Q\}$ und $K_q := \{(q,x)\,;\ x \in K\}$ (als Teilmengen von $Q \times K$) definiert.

(a) Versuchen Sie sich die Situation mit einer Skizze der Mengen zu veranschaulichen.

Zeigen Sie

(b) $P(Q_k) = p_K(k)$ für alle $k \in K$;

(c) $P(K_q) = p_Q(q)$ für alle $q \in Q$;

(d) Die Ereignisse Q_k und K_q sind für alle $(q,k) \in Q \times K$ unabhängig.

Hausaufgaben

Wir untersuchen das folgende einfache Kryptosystem (Q, C, K, f) mit

$$Q := \{0,1\}, \quad C := \{U,V,W,Z\}, \quad K := \{a,b,c,d\} \quad \text{und}$$

$f(.,.)$	a	b	c	d
0	U	V	W	Z
1	V	U	Z	W

.

Z.B. gilt $f(1,c) = Z$. Wie in der Vorlesung setzen wir $D_y := \{(x,k) \in Q \times K\,;\ f(x,k) = y\}$ für jedes $y \in C$.

12. Es soll gezeigt werden, dass wirklich ein Kryptosystem vorliegt.

(a) Erläutern Sie kurz, warum alle Abbildungen f_k verschieden sind.

(b) Füllen Sie die vorgegebene Tabelle aus, die eine zugehörige Entschlüsselungs-Abbildung g definieren soll.

$g(.,.)$	a	b	c	d
U				
V				
W			0	
Z				

Der bestehende Eintrag kommt so zu Stande: Es gilt $f_c(0) = f(0,c) = W$. Daher muss gelten $g(W,c) = g(f_c(0),c) = 0$.

Achtung: Manche Einträge sind zwingend, andere beliebig; welche?

(c) Bestimmen Sie D_U, D_V, D_W und D_Z.

bitte wenden!

13. Nun seien Wahrscheinlichkeitsfunktionen p_Q und p_K auf Q bzw. K gegeben mit

$$p_Q(0) = \frac{1}{3}, \quad p_Q(1) = \frac{2}{3}, \quad \text{und} \quad p_K(a) = p_K(b) = \frac{1}{3}, \quad p_K(c) = p_K(d) = \frac{1}{6},$$

Mit Hilfe dieser Funktionen definieren wir eine Wahrscheinlichkeitsfunktion p auf $Q \times K$ durch $p(x,k) := p_Q(x) \cdot p_K(k)$. (Vgl. Aufgabe 11 und die Vorlesung.)

(a) Zeigen Sie, dass p_Q, p_K und p tatsächlich Wahrscheinlichkeitsfunktionen auf Q bzw. K bzw. $Q \times K$ sind.

Hinweis: Bei p kann man durch geschicktes Ausklammern die Bruchrechnungen vermeiden.

(b) Berechnen Sie $p(D_U)$, $p(D_V)$, $p(D_W)$ und $p(D_Z)$.

(c) Mit $K_0 := \{(0,k)\,;\ k \in K\}$ bestimmen Sie $K_0 \cap D_U$ und $p(K_0 \cap D_U)$.

(d) Folgern Sie, dass K_0 und D_U unabhängig sind.

(e) Überprüfen Sie in analoger Weise die Unabhängigkeit von K_1 und D_Z.