Institut für Informatik
Algorithmen und Komplexität II
Prof. Dr. Johannes Köbler SS 2001

Übungen zur Kryptologie II

7. Übung

Aufgabe 1

Seien $\mathbf{X}$, $\mathbf{Y}$ Zufallsvariablen mit endlichem Wertebereich $\mathcal{W}$. Zeigen Sie das *Lemma von Gibb*:

$$H(\mathbf{X}) \leq -\sum_{w\in\mathcal{W}} \Pr[\mathbf{X}=w]\log_2 \Pr[\mathbf{Y}=w].$$

(*Hinweis:* Verwenden Sie die Ungleichung $\ln x \leq x-1$.)

Aufgabe 2

Seien $\mathbf{X}$, $\mathbf{Y}$ und $\mathbf{Z}$ Zufallsvariablen mit endlichem Wertebereich $\mathcal{W}$. Zeigen Sie:

i) $0 \leq H(\mathbf{X}) \leq \log_2 \|\mathcal{W}\|$

ii) $H(\mathbf{X} \mid \mathbf{Y}) \leq H(\mathbf{X})$ und $H(\mathbf{X} \mid \mathbf{Y},\mathbf{Z}) \leq H(\mathbf{X} \mid \mathbf{Z})$

iii) Falls $\mathbf{X}$ und $\mathbf{Y}$ unabhängig sind, dann gilt $H(\mathbf{X} \mid \mathbf{Y}) = H(\mathbf{X})$.

iv) Falls $(\mathbf{X},\mathbf{Z})$ und $\mathbf{Y}$ unabhängig sind, dann gilt $H(\mathbf{X} \mid \mathbf{Z}) = H(\mathbf{X} \mid \mathbf{Z},\mathbf{Y})$.

v) $H(\mathbf{X},\mathbf{Y}) = H(\mathbf{Y}) + H(\mathbf{X} \mid \mathbf{Y})$ und $H(\mathbf{X},\mathbf{Y} \mid \mathbf{Z}) = H(\mathbf{Y} \mid \mathbf{Z}) + H(\mathbf{X} \mid \mathbf{Y},\mathbf{Z})$, insbesondere gilt also $H(\mathbf{X} \mid \mathbf{Z}) \geq H(\mathbf{X} \mid \mathbf{Y},\mathbf{Z})$.

(*Hinweis:* Verwenden Sie bei i) und ii) das Lemma von Gibb.)

Aufgabe 3

Zeigen Sie, daß bei einem Secret-Sharing-System die folgenden Bedingungen erfüllt sind. (Hierbei bezeichne $\mathbf{K}$ eine Zufallsvariable mit Wertebereich $\mathcal{K}$, und für eine Gruppe von Teilnehmern B sei $\mathbf{B} = \mathcal{D}_B(\mathbf{K})$.)

a) Für jede Gruppe $B \in \Gamma$ gilt: $H(\mathbf{K} \mid \mathbf{B}) = 0$.

b) Für jede Gruppe $B \notin \Gamma$ gilt: $H(\mathbf{K} \mid \mathbf{B}) = H(\mathbf{K})$.

Aufgabe 4 (2 Punkte)

Es soll ein optisches $(4, 4)$-Schwellenverfahren erstellt werden. Bestimmen Sie dafür die Kollektionen $\mathcal{C}_0$, $\mathcal{C}_1$ von booleschen Matrizen (der Dimension 4×9).

Aufgabe 5 (2 Punkte)

Entwerfen Sie für die Zugriffsstruktur Γ mit der Basis $\Gamma_0 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$ ein optisches Secret Sharing Verfahren.