Übung 10

10.1 Datenverarbeitungs-Ungleichung (3pt)

Die Zufallsvariablen $X_1, X_2, X_3, \ldots$, alle mit Alphabet $\mathcal{X}$, bilden eine diskrete *Markovkette*, geschrieben als $X_1 \to X_2 \to X_3 \to \cdots$, sofern die bedingte Verteilung von X_t nur von X_{t-1} abhängt und nicht davon, wie der Wert X_{t-1} zustande kam (für $t \geq 1$). Formal

$$\mathrm{P}[X_t = x | X_{t-1} = x' \cap X_{t-2} = x'' \cap \cdots \cap X_1 = x^*] \;=\; \mathrm{P}[X_t = x | X_{t-1} = x']$$

für alle Werte $x, x', x'', \ldots, x^* \in \mathcal{X}$.

Wir betrachten in der Informationstheorie nur eine Kette $X \to Y \to Z$ der Länge drei. Aus der Markov-Bedingung folgt, dass X und Z bedingt unabhängig sind gegeben Y, d.h. für $x \in \mathcal{X}$, $y \in \mathcal{Y}$ und $z \in \mathcal{Z}$

$$P_{XZ|Y=y}(x,z) = \frac{P_{XYZ}(x,y,z)}{P_Y(y)} = \frac{P_{XY}(x,y)P_{Z|X=x,Y=y}(z)}{P_Y(y)} = P_{X|Y=y}(x)P_{Z|Y=y}(z).$$

Insbesondere gilt auch $X \to Y$ wenn $Y = f(X)$ für eine Funktion f.

Beweisen Sie damit die *Datenverarbeitungs-Ungleichung* für $X \to Y \to Z$ (engl., *data processing inequality*):

$$I(X;Y) \;\geq\; I(X;Z).$$

Die Ungleichung sagt aus, dass Information durch Verarbeitung *nicht erhöht* werden kann. Genauer, die Information welche Y über eine unbekannte Grösse X enthält ist mindestens so gross wie die Information nach der Verarbeitung von Y zu Z, sofern dies ohne Rückgriff auf X geschieht.

10.2 Codierung der Würfelsumme (2pt)

Ein fairer Würfel wird zweimal geworfen; die Summe der resultierenden Zahlen sei Z. Berechnen Sie $H(Z)$ und bestimmen Sie einen binären präfixfreien Code für Z und seine erwartete Codewort-Länge; sie sollte höchstens $H(Z) + 1$ sein.

10.3 Codes (3pt)

Geben sei eine Quelle S mit $K = 5$ Werten und Verteilung:

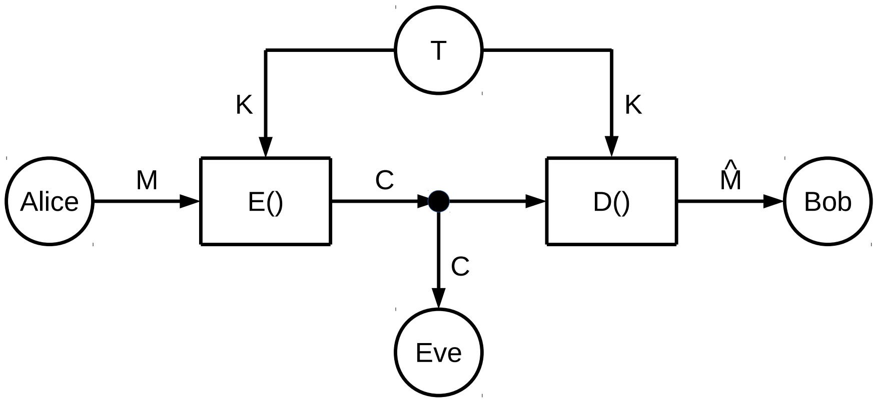
s_1	s_2	s_3	s_4	s_5
0.3	0.3	0.2	0.1	0.1

a) Konstruieren Sie einen Shannon-Code C_A für S und berechnen Sie dessen durchschnittliche Codewort-Länge.
b) Finden Sie einen besseren Code C_B für S (in dem Sinn, dass C_B durchschnittlich kürzere Codewörter als C_A erzeugt).
c) Konstruieren Sie eine Quelle S_C, für welche die erwartete Codewortlänge mit C_B gleich der Unsicherheit der Quelle ist, also $\mathrm{E}[W_C] = H(S_C)$.

$\Longrightarrow$

10.4 Perfekte Sicherheit der Verschlüsselung (2pt)

Shannon publizierte im Jahr 1948 nicht nur die Grundlage der Informations- und Codierungstheorie, sondern gleich im Jahr danach auch ein Modell für die Sicherheit kryptographischer Verschlüsselung [Sha49]. Er führte den Begriff der *perfekten Sicherheit* ein anhand des folgenden Modells eines Verschlüsselungssystems.



Darin erzeugt *Alice* als Sender eine Nachricht M und überträgt diese über einen unsicheren Kanal an den Empfänger *Bob*. Vorgängig haben beide einen Schlüssel K von einer vertrauenswürdigen Partei *T* über einen *sicheren* Kanal erhalten. Das Verschlüsselungssystem besteht aus einem *Encryption*-Algorithmus $E()$, welcher die verschlüsselte Nachricht (*ciphertext*) $C = E(M, K)$ deterministisch aus M und K erzeugt. Alice sendet C über einen *unsicheren*, öffentlichen Kanal, Bob empfängt dieses, entschlüsselt es mittels eines *Decryption*-Algorithmus $D()$ als $\hat{M} = D(C, K)$ und erhält so eine Nachricht $\hat{M}$. Ein Gegner *Eve* hört auf dem unsicheren Kanal mit und erhält so C.

Die Anforderungen an das Verschlüsselungssystem sind:

Vollständigkeit: Bob empfängt die Nachricht von Alice ohne Fehler:

$$\mathrm{P}[\,\hat{M} \neq M\,] \;=\; 0.$$

Perfekte Sicherheit: Eve hat keine Information über M in dem Sinn, dass C statistisch unabhängig von M ist:

$$H(M|C) \;=\; H(M).$$

Formulieren Sie die Anforderungen an $E()$ und $D()$ durch Bedingungen über die Entropien der involvierten Zufallsvarialben und zeigen Sie, dass

$$H(K) \;\geq\; H(M).$$

Dieses Resultat bedeutet, dass der Schlüssel in einem perfekt sicheren Kryptosystem mindestens so viel Entropie enthalten muss wie der Klartext. Insbesondere könnte M ein m-bit String mit maximaler Unsicherheit m bit sein; dann muss der Schlüssel ebenfalls aus mindestens m Zufallsbits bestehen. Verschlüsselung mit perfekter Sicherheit wird deshalb in der Praxis nicht verwendet.

Referenzen

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28:656–715, October 1949.