Diskrete Stochastik und Informationstheorie – 9 Apr 2014

Exercise 16. Let X, Y be the values of two independently thrown dice. Calculate $H(X+Y)$ and $H(X)+H(Y)$ and compare the two values.

Exercise 17.

(a) Assume a password generator per default generates all-lowercase strings of length 10 (uniformly random). What is the entropy ("security") of such a password? What is the entropy per character? How long must such passwords be to achieve a security level of 80 bits? What if the password generator includes uppercase letters, numbers and symbols in the allowed alphabet?

(b) Assume the generator builds simple "pronounceable" passwords (all lowercase) by increasing the number of vowels such that $\frac{1}{2}$ of all letters are vowels and the other $\frac{1}{2}$ are consonants (you can assume that the password length is even). Within each group, letters are still picked uniformly at random. What is the entropy per character, how many characters are necessary for 80-bit security? What changes if the first character is an uppercase letter with probability $\frac{1}{2}$?

(c) Explain `http://xkcd.com/936`. How is the entropy estimated? What assumptions are made? How well are such calculations applicable to humanly-generated passwords?

Exercise 18. Let X, Y be two independent random variables, each taking the value 0 with probability $p = \frac{1}{2}$ and the value 1 otherwise. Calculate the mutual information $I(X;Y)$, $I(X+Y;X)$ and $I(X+Y;X-Y)$ and explain the intuitive meaning of the results.

Exercise 19. Let $(\Omega, \mathcal{A}, \mathbb{P})$ be a probability space with $A, B \in \mathcal{A}$, $A \cap B = \emptyset$ and $\mathbb{P}(A) = \mathbb{P}(B) = \frac{1}{4}$. Let $X, Y : \Omega \to \{0, 1, -1\}$ be random variables defined by

$$X(\omega) = \begin{cases} 1 & \omega \in A \\ -1 & \omega \in B \\ 0 & \text{else} \end{cases} \qquad Y(\omega) = \begin{cases} -1 & \omega \in A \\ 1 & \omega \in B \\ 0 & \text{else} \end{cases}$$

(a) Argue that X and Y are not independent and that

$$H(X) = H(Y) = H(X,Y) = I(X;Y) = \frac{3}{2} \qquad \text{and} \qquad H(X|Y) = H(Y|X) = 0.$$

Whenever possible, avoid numeric calculations such as Shannon's formula and use general, more intuitive properties of entropy and mutual information instead.

(b) Let $Z = X \cdot Y$. Again avoiding calculations as far as possible, argue that

$$H(Z) < H(X,Y) = H(X,Y,Z) \qquad \text{and} \qquad H(Z|X) = 0 \text{ but } H(X|Z) > 0.$$

(c) Calculate $H(X|Z)$ and show that $H(X|Z) = I(X;Y \mid Z)$.