Wolfgang K. Seiler
Tel. 2515

B6, B4.08

September 21, 2023

Mathematics and Information, Exercise sheet 2

Problem 1: (*6 points*)

Let $\mathcal{X} = X_1, X_2, \ldots$ be a stationary time invariant Markov chain with transition matrix $A = \begin{pmatrix} p & 1-p \\ 1-q & q \end{pmatrix}$, where $p, q \in [0,\ 1]$.

a) Determine the probability distribution and the entropy for each of the random variables X_i !

b) Compute the entropy rate of $\mathcal{X}$!

c) For which values of p and q is this entropy rate minimal respectively maximal?

Problem 2: (*7 points*)

a) Let X be a random variable with values in an alphabet $A = \{a_1, \ldots, a_n\}$ with probability distribution $(p_1, \ldots, p_n)$. Show that the entropy of X decreases, if for two subscript $i \neq j$ the probability of a_i is set to $p_i + p_j$ and that of a_j to zero!

b) Now let $f\colon A \to B$ a map from A to a second alphabet B, and let $Y = f(X)$ be the random variable with values in B which takes value $f(a)$ whenever X takes the value a. Show that $H(Y) \leq H(X)$!

c) When ist $H(X) = H(Y)$?

d) Give an example where $H(Y) < H(X)$!

Problem 3: (*7 points*)

a) Each of the following cryptograms represents a German word, encrypted with a Caesar cypher. Which of these cryptograms have a unique decryption?

$$c_1 = \texttt{xgas}, \qquad c_2 = \texttt{xql}, \qquad c_3 = \texttt{iold}, \qquad c_4 = \texttt{ma}, \qquad c_5 = \texttt{qh}$$

b) The first 21 letters on the current page of your one time pad are `KRYPTOLOGIEVORLESUNGHS`. Decrypt the message `IFFHCURXTVTNVWZLKVILV`!

c) How would that page begin, if the message were `BRINGEBLUMENFUERMUTTI`?
Hint: Even though cryptographers solved such problem for centuries without any modern utilities, you will probably save much time by writing a short computer program.

Can be submittel till Wednesday, September 27, 2023 at 15.30h