TU Graz
Graz University of Technology

Department of
Mathematical Structure Theory

Diskrete Stochastik und Informationstheorie
Exercise sheet 11 – 20/6/2013

Hamming codes

Bonus points

The channel coding theorem states the existence of codes that allow to transmit information over a noisy channel. However, it remains the important question how to construct such a code. Two main natural requirements on such a code are that the probability of error is low and that the code is useful or simple to implement. Moreover, it would be desirable that the code is "error-detecting" or even better "error-correcting".
The subject of this exercise sheet is to construct a code that satisfies the above requirements. The question of finding a "good" code relies on the way we can introduce redundancy. Let us first consider the most trivial one.

Exercise 48 *Consider a binary symmetric channel with crossover probabilities. Suppose that you encode* 1 *as* 11111 *and* 0 *as* 00000*. What is the error probability? How can you detect or correct the disturbed signals?*

The above code works but is not very useful and you can detect errors only with some probability. Can we be smart and do better?

Exercise 49 *Give a simple example of a parity check code.*

That is better; but still we can do better. Let us develop the Hamming code. For this end we consider binary codes of length 7 and calculate *mod* 2. The following matrix gives all nonzero binary vectors of length 3 in their columns:

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Exercise 50 *Find all vectors v of length 7 such that $Hv = (0,0,0)^t$. (You may use some linear algebra). These 2^4 vectors will be our codewords. Find the minimum distance of the code, i.e., the minimum number of places in which two codewords differ.*

Exercise 51 *Define a parity check for the above code and summarize the obtained results. Comment on possible improvements.*