Universidade de Aveiro

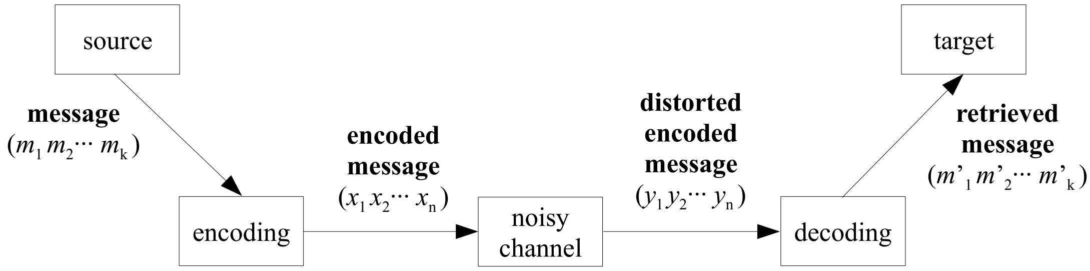
Mestrado Integrado em Engenharia de Computadores e Telemática

Arquitectura de Computadores Avançada

Assignment 1 – Hamming codes

Academic year 2018/2019

THEORETICAL BACKGROUND



A message $\boldsymbol{m}$, generated by a given *source*, is expressed in k symbols of alphabet Σ and is further encoded into a word $\boldsymbol{x}$, using a *block code*, through expansion to length n by addition of redundant information; that is, a specific code word is built by the interspersing of $n-k$ symbols of alphabet Σ to the k symbols of the message, following some definite rule.

The encoded message $\boldsymbol{x}$ is next transmitted over a *noisy channel*, where the symbols may be changed according to certain probabilities that are characteristic of the channel. The received message $\boldsymbol{y}$ is finally decoded into the message $\boldsymbol{m}'$, which is retrieved by the *target*. Bear in mind that the *channel* concept must be taken in a broad sense: it can be a data transmitting medium in the traditional sense, such as copper, optical fiber, or air signal propagation, or a data storage device, such as a hard disk, a flash memory, or a dynamic RAM.

One can define the *information rate* R, which measures the slow down of the effective data transmission, as k/n. On the other hand, given the channel characteristics, one defines the *capacity* C *of the channel* as something which, as Claude Shannon has shown, has the property that, for $R < C$, it is possible to find an *encoding* / *decoding* scheme such that the probability that $\boldsymbol{m} \neq \boldsymbol{m}'$ can be made arbitrarily small. If, however, $R > C$, no such scheme exists.

Claude Shannon, however, did not show how to build such *encoding* / *decoding* schemes. This has been the pioneering work of Richard Hamming. Presently, however, the case for the best codes in terms of the maximal number of errors that one can correct for a given information rate and code length is not clear. Existence theorems are known, but the exact bound is still an open problem.

HAMMING CODES

The binary case will be considered here where the alphabet Σ is the set $\{0,1\}$, the block code C is a subspace of the linear space F_2^n, F_2 being the 2-element field. By taking the number of redundant symbols, *parity bits*, to be r, one gets $n = 2^r - 1$ for the *code length* and $k = n - r$ for the *message length*, giving rise to a $[n, k, 3]$ block code, with a minimum distance between code words of 3, which enables the error detection and correction of 1 bit of the received message.

The *encoding* process is described by

$$\boldsymbol{x} = \boldsymbol{m} \cdot \boldsymbol{G}$$

where $\boldsymbol{m}$ is the message, $\boldsymbol{x}$ its encoding and $\boldsymbol{G}$ the k x n *code generating matrix*, defined as

$$\boldsymbol{G} = \| \boldsymbol{I}_k \mid -\boldsymbol{A}^T \| \ .$$

The *decoding* process, on the other hand, is described by

$\boldsymbol{H} \cdot \boldsymbol{y}^T = \boldsymbol{0} \quad \Rightarrow$ message bits of $\boldsymbol{y}$ are correct (there is no error)
$\boldsymbol{H} \cdot \boldsymbol{y}^T \neq \boldsymbol{0} \quad \Rightarrow$ error on bit whose position is the column number whose contents is $\boldsymbol{H} \cdot \boldsymbol{y}^T$

where $\boldsymbol{y}$ is the received encoded message and $\boldsymbol{H}$ the r x n *parity check matrix*, defined as

$$\boldsymbol{H} = \| \boldsymbol{A} \mid \boldsymbol{I}_r \|$$

and has as columns all the pairwise linear independent vectors of length r.

Design a digital circuit, called the *encoder*, which performs the encoding for a $[15,11,3]$ Hamming code (either combinatorial or synchronous). Design also a digital circuit, called the *decoder*, which detects and corrects a 1-bit error on the received code word (either combinatorial or synchronous).

The assignment entails that some investigation should be made on finding the best possible algorithms for the implementation of the operations.

GRADING

- full specification of the *encoder* and proof of correctness of its design by VHDL simulation in Quartus – 14 valores
- full specification of the *decoder* and proof of correctness of its design by VHDL simulation in Quartus – 17 valores.

DELIVARABLES

- an archive, named `HAM_T$G#.zip` (where $, equal to 1, … ,4, means the lab number and #, equal to 1, …, 10, means the group number), of the VHDL files of your solution
- a pdf file, up to 4 power point like pages, where the main ideas of the design are presented.

DEADLINE

- November, 25, at midnight.