The Hamming Code

A very little coding theory

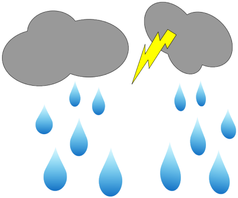
Prof Hans Georg Schaathun

Høgskolen i Ålesund

2nd January 2014

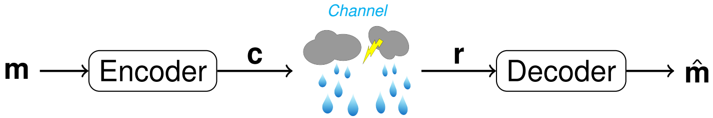
Error-Control Coding

- Noise damages information



- How do we get robust communication?

Communications with Error-Control



The Hamming Code

- The $[7, 4, 3]$ Hamming Code

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix} \tag{1}$$

- Encoding Function $\mathbf{c} = \mathbf{m} \cdot G$

HØGSKOLEN I ÅLESUND
Aalesund University College

Properties

- The Hamming code is a set $C \subset \mathbb{Z}_2^7$
- The elements of C are valid codewords
  - $\#C = 2^k = 2^4$ valid words
  - $2^n = 2^7$ possible 7-bit words
  - A fraction $2^k/2^n = 2^{-3}$ of the words are valid
- Take two distinct words $c_1, c_2 \in C$
  - The Hamming distance $d(c_1, c_2) \geq 3$
- At least three bit errors to risk confusion with another codeword

Error Detection and Error Correction

Error Detection if $\mathbf{r} \notin C$, we have detected an error.

- We can for instance ask for a retransmission.
- The Hamming code can detect up to two errors

Error Correction if $\mathbf{r} \notin C$, we try to find the most likely $\mathbf{c} \in C$, which could be received as $\mathbf{r}$

- The Hamming Code can correct one error
- It never corrects more than one error

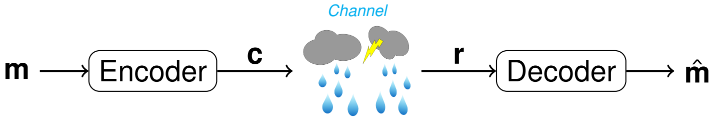
Note that if we use the Hamming code for error correction, we cannot also detect two errors.

Reading

Mathematical Introduction *A First Course in Coding Theory* by Raymond Hill

Comprehensive Engineering Textbook *Error-Control Coding* by Lin and Costello

Summary



Exercise

Using the generator matrix G from slide 4, encode the message (0011).