Decoder error probability

1 Error v failure

1.1 Probabilistic channels

Recall the source-channel-reciever diagram
Channels are probabilistic in nature. Errors due to thermal noise, faults, damage...
Impossible to predict how many errors will occur

1.2 Decoder error and failure

If more than t errors occur, two situations could happen

- The decoder cannot find any codeword at a distance $\leqslant$ t from the received vector: Decoder **failure**
- The decoder finds another (wrong) codeword at distance $\leqslant$ t from the received vector: Decoder **error**

Failure: Ask for retransmission. No big deal
Error: the decoder is totally oblivious. Much more problematic.
No failures when using hamming codes - hamming codes are optimal so all sequences will correspond to a codeword.

1.3 Example of decoder error and failure

Consider the code with the following parity-check matrix:

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

This is a (5,2,3)-code. It's codewords are:

$$\{(0,0,0,0,0),(0,1,1,1,1),(1,1,1,0,0),(1,0,0,1,1)\}$$

Suppose we send the all zero codeword C=(0,0,0,0,0)

- If the vector v=(0,1,0,1,0) is received: failure
- If the vector v=(1,1,0,0,0) is received: error

2 Decoder error probability

In general, the decoder error probability (DEP) depends on:

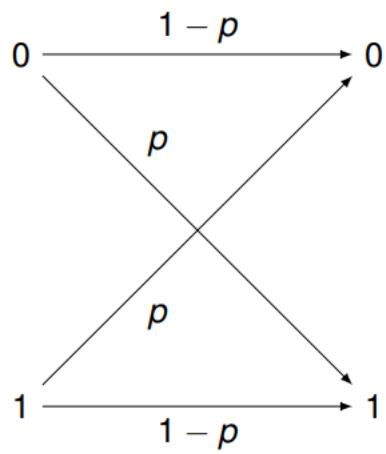
- The channel
- The code we use
- The transmitted codeword

For a given channel and a given code, it can be determined

2.1 Binary symmetric channel

Instead of trying to figure out exactly how the errors occur, we will simplify the channel model

Binary symmetric channel (BSC) with crossover probability p:



2.2 How many errors?

Let E be the number of errors under a BSC, if n bits are transmitted. We have:

$$P(E = w) = \binom{n}{w} p^w (1-p)^{n-w}$$

If we use a code with error correction capability t, the probability of not being able to correct the errors is:

$$\begin{aligned} P(E > t) &= 1 - P(E \le t) \\ &= 1 - \sum_{w=0}^{t} \binom{n}{w} p^w (1-p)^{n-w} \end{aligned}$$

2.3 DEP over the BSC

Theorem: Let $A_i(c)$ be the number of codewords at distance i from the transmitted codeword **c**, then the DEP over a BSC with crossover probability p is

$$DEP = \sum_{w=t+1}^{n} p^w (1-p)^{n-w} \sum_{i=d_{min}}^{n} A_i(\mathbf{c}) \sum_{s=0}^{t} \binom{i}{\frac{w-s+i}{2}} \binom{n-i}{\frac{w+s-i}{2}}$$

Where

$$\binom{a}{b} = \begin{cases} \frac{a!}{b!(a-b)!} & \text{if } 0 \le b \le a \text{ are integers} \\ 0 & \text{otherwise} \end{cases}$$

2.4 Distance distribution of Hamming codes

For any linear code, $A_i(C)$ does not depend on c
For the $(n = 2^r - 1, k = 2^r - r - 1, 3)$-Hamming code

$$A_i = 2^{-r} \binom{2^r - 1}{i} + (1 - 2^{-r}) \sum_{j=0}^{i} (-1)^j \binom{2^{r-1}}{j} \binom{2^{r-1} - 1}{i - j}$$

2.5 DEP of hamming codes

For Hamming codes, you can apply the last two (long) equations.

Alternatively, realise that there are **no failures** when using hamming codes. This, for a BSC channel with crossover probability p

$$DEP_{\text{Hamming}} = P(E > 1) = 1 - (1-p)^n - np(1-p)^{n-1}$$