Review Week 02

2022-10-03

TUTORIALS:
TUT Ø1 THURSDAY 10 am
TUT Ø2 MONDAY 2 PM
BOTH IN ALAN TURING G.205

Reminder: correcting errors

A decoder for C is a function $\text{DECODE}: F^n \to C$ such that $\text{DECODE}(\underline{y})$ is a nearest neighbour of $\underline{y}$ in C.

Challenge: can an undetected error be corrrected? NO!

$\underline{c} \in C \to$ CHANNEL $\to \underline{y}$

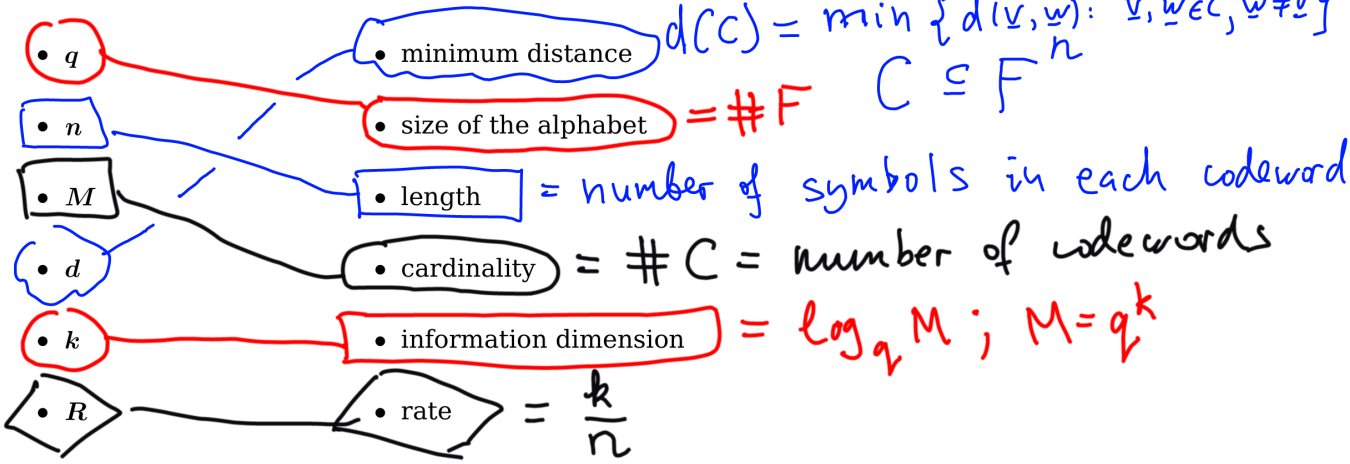
$\underline{y} \neq \underline{c}$ (error)

$\underline{y} \in C$

$d(\underline{y},\underline{y}) = 0$ so $\text{DECODE}(\underline{y}) = \underline{y}$ (a codeword is always decoded to itself)

Parameters of a code

Connect each letter with the parameter it denotes, and define each parameter



Is high rate good or bad?

Is high minimum distance good or bad?

What is an $[n, k, d]_q$ code? [length, inf. dim., min. dist]$_{\text{size of the alphabet}}$

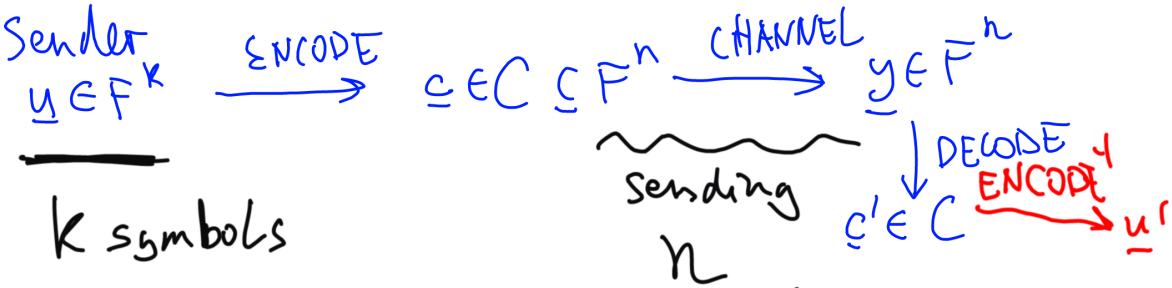
$(n, M, d)_q$

Channel coding: $C \subseteq F^n$ k is an integer.

1 1 0 0 1 0 0 1 1 0 .....

$k=2$ Messages are of length k

ENCODE : $F^k \to C$ bijection



k symbols

n symbols via the channel

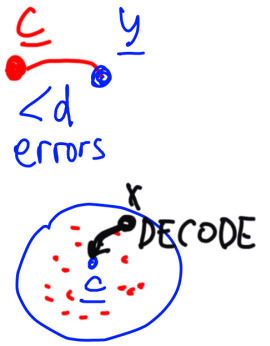
$R = \frac{k}{n}$

High rate (≈ 1) is good.

TRANSMITTED $= R^{-1}$. MESSAGE

How many errors, per codeword, is a code *guaranteed* to detect/correct?

A code of min. distance d
- detects up to $d-1$ symbol errors in a codeword
- corrects up to $t = \left[\frac{d-1}{2}\right]$ symbol errors in a codeword.



Bounds

The Hamming bound: if $(n, M, d)_q$ codes exist, $M \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i}$.

=: perfect

$S_t(\underline{c}) = \{\underline{x} : d(\underline{x}, \underline{c}) \leq t\}$

$\binom{n}{i}$ binomial coeff

$\frac{n!}{(n-i)!\, i!}$

- Codes that *attain* the Hamming bound are called:

The Singleton bound: if $(n, M, d)_q$ codes exist, $M \leq q^{n-d+1}$

- Codes that *attain* the Singleton bound are called: MDS

Examples: the trivial code, the repetition code, the code E_3

Define the above codes. Calculate the parameters. Determine which of these codes are perfect and which of these codes are MDS.

$q = \#F$

trivial: F^n

$[n, n, 1]_q$-code.

$\#F^n = q^n$

$(x_1, \ldots, x_n)$ — q q

$d(F^n) \neq 1 = 1$

$d(aa\ldots a, ba\ldots a) = 1$

Perfect: Hamming bd

$t = \left[\frac{d-1}{2}\right] = \left[\frac{1-1}{2}\right] = 0$

$M \leq \frac{q^n}{\sum_{i=0}^{t} \binom{n}{i}(q-1)^i} = \frac{q^n}{\binom{n}{0}(q-1)^0} = q^n$

$\binom{n}{0} = 1$, $(q-1)^0 = 1$