1.4 Basic Math notation and terminology.

1.5 Formal models of communication through noisy channels.

Let M be a finite set of messages and W be a finite set of words that can be transmitted through a channel. A model of communication through a noisy channel is given by M, W and the three functions:

$ENC : M \to W$ encoder (from messages to codewords)

$CH : W \to W$ a function modelling the noise in the channel (sometimes it's a family of functions)

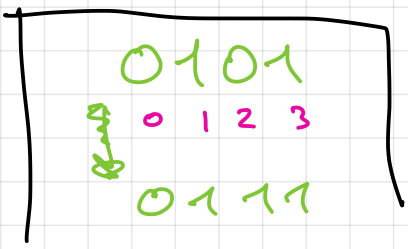
$DEC : W \to M$ decoder (from a codeword to the message).

$$M \xrightarrow{ENC} W \xrightarrow{CH} W \xrightarrow{DEC} M$$

Frequently one models the noise via randomness. In this case $CH : W \to W$ is actually a random function that means $CH = CH(w, \omega)$

$CH : W \times \Omega \to W$ it depends $w \in W$ and chance expressed via a random event $\omega \in \Omega$.

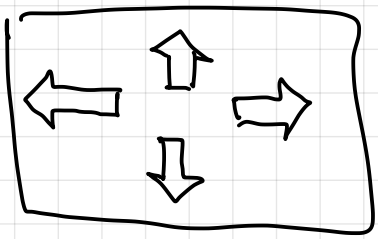
There is also a game-theoretic model for noise, with the



noise that can "think": Alice & Bob play against the noise. The Noise tries to choose CH with given limitations in a way that disrupts communication the most. The objective of Alice & Bob is to have $DEC(CH(ENC(x))) = x$.

Sometimes one also looks at the message as a random variable with some distribution which is given.

Rem. Frequently one discards M completely and focuses on $ENC(M) \subseteq W$.



$CH(\{\uparrow, \downarrow, \rightarrow, \leftarrow\}) = \{000, 101, 011, 110\}$

Just focus on this set.

This can be done in the case of ENC which are injective.

This set $C := ENC(M)$, which is a subset of W, is called a code. It matters more what code we use than what encoding we use. We may have different encodings for the same code.

Def. For finite sets M, W an encoder-decoder scheme is a pair (f, g) of functions $f: M \to W$ and

$$g: W \to M$$

$f(x)$ is the encoding of x, also called the codeword of x. g is the decoder.

The code used here is $C = f(M)$

Def. For a finite set W a code-decoder scheme is a pair (C, g), where $C \subseteq W$ and $g: W \to C$.

Def. For a finite set W a code-error-detector scheme is a pair (C, h), where $C \subseteq W$ and $h: W \to \{0,1\}$ the function $h(w) = \begin{cases} 1 & \text{if } w \in C \\ 0, & \text{if } w \in C|W. \end{cases}$

2 Bounds on block codes.

2.1 Parameters of block codes

Def 2.1 Fix a finite set K of size $q = |K| > 0$ and let $n \in \mathbb{N} := \{1, 2, 3, 4, \dots\}$. A non-empty subset $C \subseteq K^n$ of $K^n := \{(x_1, \dots, x_n) : x_1, \dots, x_n \in K\}$ is called a block code over the alphabet K.

n is called the length of C

$|C|$ is called the size of C

q is called the arity of the code C

($q = 2 \Rightarrow$ binary code

$q = 3 \Rightarrow$ ternary code)

Def 2.2. A function $d: X \times X \to \mathbb{R}$ is called a metric on a set X if the following conditions are satisfied:

(a) $d(u,v) \geq 0$ with $d(u,v) = 0$ iff $u = v$ for all $u, v \in X$.

(b) $d(u,v) = d(v,u)$ for all $u, v \in X$

(c) $d(u,v) \leq d(u,t) + d(t,v)$ for all $u, t, v \in X$ (the triangle inequality)

For $c \in X$ and $\rho \in \mathbb{R}_{\geq 0}$, we call

$$B(c,\rho) = \{x \in X : d(x,c) \leq \rho\}$$

the closed ball with center in c and of radius ρ.

Def 2.3 The function $d: K^n \times K^n \to \mathbb{Z}_{\geq 0}$ given by $d(u,v) := |\{i = 1, \dots, n : u_i \neq v_i\}|$ is called the Hamming distance.

Here, $u = (u_1, \dots, u_n)$

$v = (v_1, \dots, v_n)$.

$d(u, 0) = d(u_1 \dots u_n, 0 \dots 0)$ is called the weight of u (this is defined when $0 \in K$).

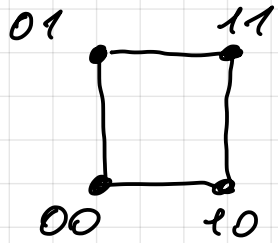
For a code $C \subseteq K^n$, $C \neq \emptyset$.

the minimum

$$\min\{d(u,v) : u,v \in C, u \neq v\}$$

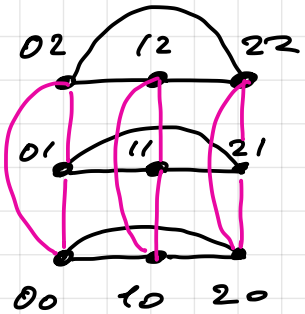
is called the minimum distance of the code C or just the distance.

The notation: $d(C)$

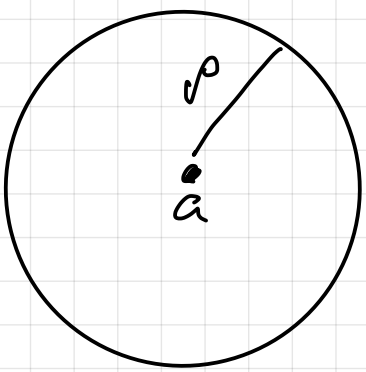


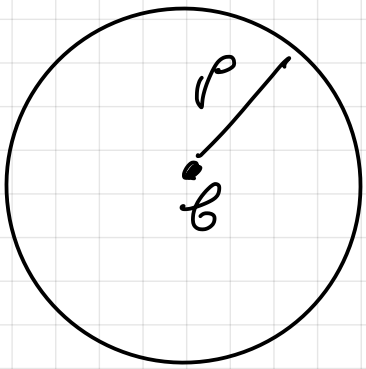
$d(00,00) = 0$
$d(00,01) = 1$
$d(00,11) = 2$

$K = \{0,1\}$, $q = 2$
$n = 2$



$K = \{0,1,2\}$, $q = 3$
$n = 2$





LQ3

Show that $d(a,b) > 2\rho \Rightarrow B(a,\rho) \cap B(b,\rho) = \emptyset$ holds for a metric $d: X \times X \to \mathbb{R}$, $a, b \in X$ and $\rho \in \mathbb{R}_{>0}$

Prop 2.4 The Hamming distance is a metric.

Proof: DIY, return in paper in the next lecture **LQ4** (and LQ1 – LQ3 if you did it).

Remark 2.5 It starts to feel like a space.

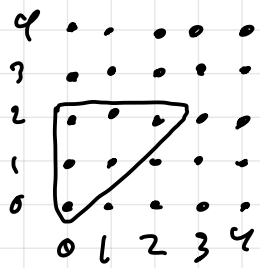
K^n - our space we take the code from

n - Dimension (sort of)

$d(u,v)$ - Hamming distance between $u, v \in K^n$

Note: K (the alphabet) is finite.

So, the space K^n is actually finite set.



$K = \{0,1,2,3,4\}$

$n = 2$

The size of a subset $C \subseteq K^n$, i.e. the number of elements, plays a role of the discrete version of volume.

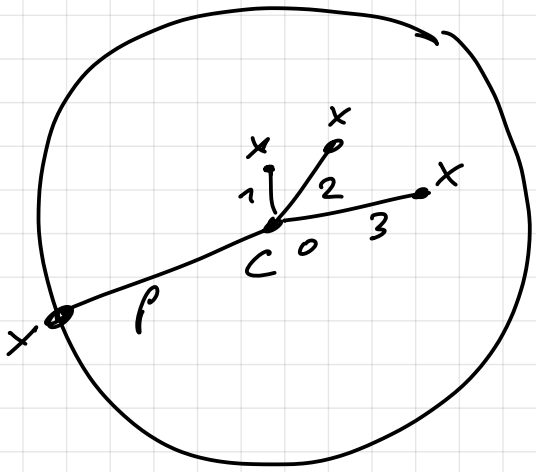
Prop 2.6 Let $n \in \mathbb{N}$, let K be an alphabet of finite size $q \geq 2$ and let d be the Hamming distance on K^n. Then the size of the ball $B(c,\rho)$ with respect to the distance d, which has its center in $c \in K^n$ and radius $\rho \in \{0,1,2,\dots,n\}$ is:

$$|B(c,\rho)| = \sum_{j=0}^{\rho} \binom{n}{j} (q-1)^j$$

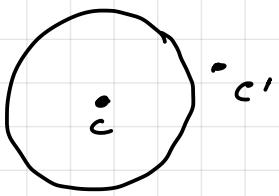
Proof: In $B(c,\rho)$ each word has a unique

distance $j = 0, 1, \dots, \rho$ to the center c of the ball. So, we can count the words with a given distance j separately and then sum those counts up.

A word $x = x_1 \dots x_n$ with distance j to the center $c = c_1 \dots c_n$ has a uniquely defined set $I := \{i = 1, \dots, n : x_i \neq c_i\}$ of positions, in which x and c differ. This set I has size j. So, for the choice of I we have $\binom{n}{j}$ possibilities.



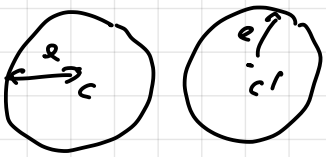
Def 2.7. For a finite alphabet K of size $q \geq 2$, for $n \in \mathbb{N}$, we consider a code $C \subseteq K^n$.



C is called t-error-detecting if $d(C) > t$, which means $d(c, c') > t$ for all $c, c' \in C$, $c \neq c'$.

C is called e-error-correcting if

$$d(C) \geq 2e + 1.$$



Here: t, e are consecutive integers.

Recall: $d(C) = \min\{d(c, c') : c, c' \in C, c \neq c'\}$.