We obviously want to transmit as fast as possible, as much as possible with as few errors as possible

So for a linear $[n, m, d]$-code over a field $\mathbb{F}_q$.

One wants to increase both m/n (message encoded per bits used) and d/n (capable to detect more errors with less bits per code word)

Cannot increase both as much as we want because there are inequalities to be respected between those parameters.

One of those is the sphere packing boundary.

Minimum distance is d then one can draw around each code word c in $\mathbb{F}_q^n$ a sphere with radius $(d-1)/2$.

$$B_c := \left\{ x \in \mathbb{F}_q^n \mid d(x,c) \leq \frac{d-1}{2} \right\}$$

All those spheres are non-intersecting because if

$$x \in B_{c_1} \cap B_{c_2}$$

then by the triangle inequality

$$d(c_1, c_2) \leq d(c_1, x) + d(x, c_2) \leq \frac{d-1}{2} + \frac{d-1}{2} \leq d-1$$

there are two code words with distance $< d$ which is impossible

In each of these spheres there are exactly

$$\sum_{0 \leq i \leq \frac{d-1}{2}} \binom{n}{i} (q-1)^i \text{ words}$$

remainder: $\binom{n}{i} = \frac{n!}{(n-i)!\,i!}$

this sum corresponds to the number of words up to $\frac{d-1}{2}$ errors

$\binom{n}{i}$ counts the possible ways to choose the i error locations and $(q-1)^i$ counts the possible errors we can use in each location.

Each sphere contains different elements and there are q^m spheres

so the union of the balls contains

$$q^m \left(\sum_{i=0}^{\frac{d-1}{2}} \binom{n}{i} (q-1)^i \right) \text{ elements}$$

there are only q^n elements so the above expression is smaller than q^n

theorem: $\forall$ linear $[n, m, d]$-code over $\mathbb{F}_q$ we have that $\sum_{i=0}^{\frac{d-1}{2}} \binom{n}{i} (q-1)^i \leq q^{n-m}$

this lets us say:

A linear $[n, m, d]$-code over $\mathbb{F}_q$ is perfect if the balls B_c cover whole $\mathbb{F}_q^n$. This happens if and only if

$$\sum_{i=0}^{\frac{d-1}{2}} \binom{n}{i} (q-1)^i = q^{n-m}$$

Lemma: a linear code is perfect if and only if for every syndrome there is a unique error vector of weight $\leq \frac{d-1}{2}$

proof: $\forall$ linear $[n, m, d]$-code there are always q^{n-m} syndromes.

Error vectors inside the ball B_0 all have a different syndrome because the code is $\frac{d-1}{2}$ error correcting.

10 pigeons in 9 boxes => 2 pigeons in 1 box

By the pigeon-hole principle every syndrome as a unique error vector as soon as the number of elements in the ball equals the number of syndromes i.e. SPB reached

A CODE CAN NEVER BE PERFECT IF $D \% 2 = 0$

Repetition codes

trivial.

A binary repetition code consists of two code words

$$C := \{00\dots0, 11\dots1\}$$

parameters $[n,1,n]$ easy to check if it's perfect

> **theorem**
> a binary $[n,1,n]$ - repetition code is perfect if and only if n is odd

proof: we already know n has to be odd ($n = 2t+1$), let's use the binomial formula of Newton

$$\sum_{i=0}^{t} \binom{n}{i} (2-1)^i = \sum_{i=0}^{t} \frac{1}{2}\left(\binom{n}{i} + \binom{n}{n-i}\right) 1^i = \frac{1}{2}\sum_{i=0}^{n} \binom{n}{i} = 2^{n-1}$$

(perfect)

Hamming Codes

A binary code is a HC if it has parity check matrix $H \in \mathrm{Mat}_{r \times (2^r-1)}(\mathbb{F}_2)$ consisting of all possible column vectors of $\mathbb{F}_2^r \setminus \{0\}$.

we note it has $\mathrm{Ham}(r,2)$.

example: $r=2$

$$H := \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \Rightarrow G := (1\ 1\ 1)$$

(for example) $C := \{000, 111\}$

so $\mathrm{Ham}(2,2)$ is the binary repetition $[3,1,3]$ code.

this is the only HC which is a repetition code

example: $r=3$, we can put H in standard form like:

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

$$\Downarrow$$

$$G := \begin{pmatrix} 1&0&0&0&0&1&1 \\ 0&1&0&0&1&0&1 \\ 0&0&1&0&1&1&1 \\ 0&0&0&1&1&1&0 \end{pmatrix}$$

> **Lemma** two HC with the same parameters are equivalent

proof: if H and H' are parity check matrixes for HCs then they have the same columns

This means there is a permutation matrix P such that $H = HP'$

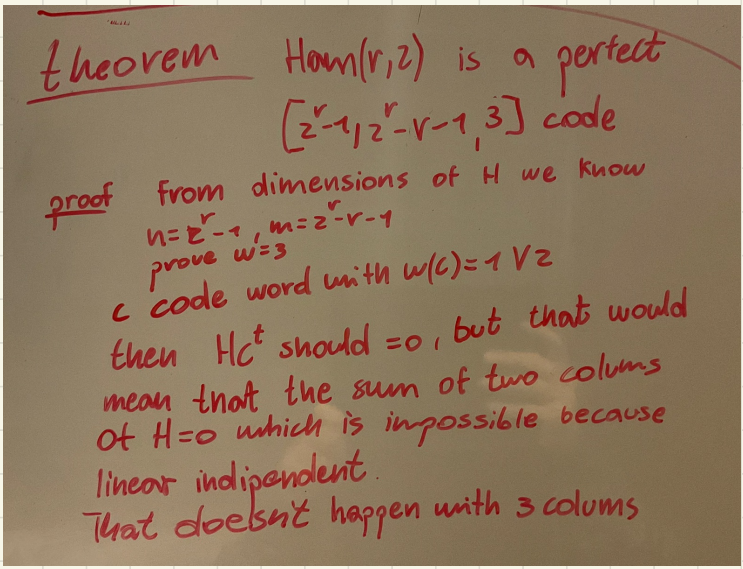
This implies that if G' is the generator matrix for the second code

then $G'(H')^T = G'(HP)^T = (G'P^T)H^T$ so $G'P^T$ is a generator matrix for the first code

Now P^T is also a permutation matrix $\rightarrow$ G and G' generate equivalent code

theorem Ham(r,2) is a perfect $[2^r-1, 2^r-r-1, 3]$-code

proof : ~~Non~~ capita capita!



Algorithm Decoding HC

we recieve r, G and H are in standard position

1) calculate syndrome $s=Hr^t$
2) if $s=0 \rightarrow$ r is the original code word and the message are the first 2^r-r-1 bits
3) if $s\neq 0 \rightarrow$ suppose an error has occured. The position of the error is the position of the column of H equal to s.

we can generalize binary HC over arbitrary fields.

Must take care in creation of parity check matrix because elements must be linearly indipendent

if we use $v \in \mathbb{F}_q^r \setminus \{0\}$ then we cannot use kv $(k \in \mathbb{F}_q \setminus \{1,0\})$.

for each ray of vectors have to pick one representative in H.

example: r=2 q=3

$$H:=\begin{pmatrix}1&1&1&0\\2&1&0&1\end{pmatrix} \Rightarrow G:=\begin{pmatrix}1&0&2&1\\0&1&2&2\end{pmatrix}$$ Ham(2,3) is a $[4,2,3]$-code

cannot pick $\binom{2}{2}$ because $2\binom{1}{1}$
but $\binom{1}{2}$ yes bcz $\binom{1}{0}+2\binom{0}{1}$

example : r=2 q=5

$$H:=\begin{pmatrix}1&1&1&1&1&0\\4&3&2&1&0&1\end{pmatrix} \Rightarrow G:=\begin{pmatrix}1&0&0&0&4&1\\0&1&0&0&4&2\\0&0&1&0&4&3\\0&0&0&1&4&4\end{pmatrix}$$ Ham(2,5) $[6,4,3]$-code

theorem Ham(r,q) is a perfect $\left[\frac{q^r-1}{q-1}, \frac{q^r-1}{q-1}-r, 3\right]$-code over $\mathbb{F}_q$

Hamming codes are infite, there are other which are not

The ternary Golay code

consider the field $\mathbb{F}_3$ and take the matrix

$$S_5 := \begin{pmatrix} 0&1&2&2&1 \\ 1&2&2&1&0 \\ 2&2&1&0&1 \\ 2&1&0&1&2 \\ 1&0&1&2&2 \end{pmatrix}$$

the ternary Golay code $Gol(11,3)$ is a $[11,6]$-code over $\mathbb{F}_3$ with generator matrix

$$G := \begin{pmatrix} 1&0&0&0&0&0&1&1&1&1&1 \\ 0& & & & & & & & & & \\ 0& & & & & & & & & & \\ 0& & & Id_5 & & & & S_5 & & & \\ 0& & & & & & & & & & \\ 0& & & & & & & & & & \end{pmatrix}$$

and parity check matrix

$$H := \begin{pmatrix} 2&0&2&1&1&2&1&0&0&0&0 \\ 2&2&0&2&1&1&0&1&0&0&0 \\ 2&1&2&0&2&1&0&0&1&0&0 \\ 2&1&1&2&0&2&0&0&0&1&0 \\ 2&2&1&1&2&0&0&0&0&0&1 \end{pmatrix}$$

The ternary Golay code is a perfect 2 error correcting code

proof:

can be computed that $GG^T = \begin{pmatrix} 0&0&0&0&0&0&0&0&0&0&0 \\ 0&2&0&0&0&0&1&1&1&1&1 \\ 0&0&2&0&0&0&1&2&2&1&1 \\ 0&0&0&2&0&0&1&1&2&2&1 \\ 0&0&0&0&2&0&1&1&1&2&2 \\ 0&0&0&0&0&2&1&2&1&1&2 \\ 0&1&1&1&1&1&2&0&0&0&0 \\ 0&1&2&1&1&2&0&2&0&0&0 \\ 0&1&2&2&1&1&0&0&2&0&0 \\ 0&1&1&2&2&1&0&0&0&2&0 \\ 0&1&1&1&2&2&0&0&0&0&2 \end{pmatrix}$

if $x := x_1 \cdots x_6$ message word xG is a code word, hence

$\forall x \in \mathbb{F}_3 \quad x^2 \in \{0,1\}$

$$xG \cdot xG = xG(xG)^T = xGG^T x^T = \left(2 \sum_{i=2}^{6} x_i \right)^2 = 2 \left(4 \sum x_i \right)^2 = 2 \left(\sum x_i \right)^2 \Rightarrow \text{either } 2 \cdot 0 \text{ or } 2 \cdot 1, \text{ so } \neq 1$$

(single value, sum of digits $\Rightarrow$ weight mod 3; multiply scalar $\times 2$; multiply again for x^T; do it for rows and columns)

The weight then cannot be 1, 4, 7 or 10.

The weight of code word xG is always at least the weight of x, because the first 6 symbols of xG are x

if x has weight 1, xG has weight at least 5 because all rows of G have $w \geq 4$.

Suppose x has weight 2, then xG has weight bigger than 4.

Take two rows G_i and G_j and look at the quotients of the last 5 entries

$G_{i7}/G_{j7} \cdots G_{i11}/G_{j11}$. there are at least 3 different quotients

Every linear combination will have at least 2 non zero symbols in the last 5 digits, so wait at least 4, hence 5 or more

can do the same if x weight 3 using last 3 digits.

Prove perfectness with sphere packing boundary

$$\sum_{i=0}^{2} \binom{11}{i} 2^i = 1 + 2\binom{11}{1} + 4\binom{11}{2} = 1 + 22 + 220 = 243 = 3^5 = 3^{11-6} \quad \checkmark$$

Binary Golay codes

$$B := \begin{pmatrix} 1&1&0&1&1&1&0&0&0&1&0&1 \\ 1&0&1&1&1&0&0&0&1&0&1&1 \\ 0&1&1&1&0&0&0&1&0&1&1&1 \\ 1&1&1&0&0&0&1&0&1&1&0&1 \\ 1&1&0&0&0&1&0&1&1&0&1&1 \\ 1&0&0&0&1&0&1&1&0&1&1&1 \\ 0&0&0&1&0&1&1&0&1&1&1&1 \\ 0&0&1&0&1&1&0&1&1&1&0&1 \\ 0&1&0&1&1&0&1&1&1&0&0&1 \\ 1&0&1&1&0&1&1&1&0&0&0&1 \\ 0&1&1&0&1&1&1&1&0&0&0&1 \\ 1&1&1&1&1&1&1&1&1&1&1&0 \end{pmatrix}$$

12×12, symmetric, the rows are cyclic permutations of each other

$B^2 = Id_{12}$

The extended Golay code $Gol(24,12)$ is a binary code with generator matrix $G := Id_{12} | B$

B is its own inverse so $B | Id_{12}$ is a parity check matrix, G is also one

Its minimal weight is 8

proof: first prove that weight of a random word is multiple of 4

$GG^T = 0$ since G^T is parity check matrix $\Rightarrow$ inproduct of two code words is zero.

This means that the number of entries where both 1 are even (otherwise would have >0).

Suppose now that x and y are two code words of which weight is multiple of 4, then

$w(x+y) = w(x) + w(y) - 2(\text{num of common 1's})$

this is still multiple of 4 because all its terms are

Notice that all rows of G have weight 8 or 12, so every code word has weight $4K$, $K \in \mathbb{N}$.

Now prove no word can have weight 4

suppose $xG = [x \; xb]$ is code word with weight 4.

Since $B | Id_{12}$ is also a generator matrix, there exists an y such that

$$xG = x \underbrace{xB} = y[B | Id_{12}] = [\underbrace{yB} \; y] = [x \; y]$$

therefore either x or y must have weight ≤ 2. If it's the case for x we know xG is the sum of at most two rows of G and can never have weight $=4$. For $w(y) \leq 2$ we do the same

Since $d=8$ we are able to correct all error vectors with weight <4

Take $H:=G$, suppose we have error vector e with weight at most 3.

Split the vector in two parts of lenght 12 $e:=[e_1, e_2]$

the syndrome is then $s:= Ge^t = e_1^t + Be_2^t$

$w(e)<4$ so either e_1 or e_2 have weight <2

suppose $w(e_2)$ at most 1, then the syndrome s consists of either a word of weight at most 3 (if $e_2=0$) or a row B with at most two digits changed. If $w(e_1)$ at most 1 we can do the same but using the syndrome. $t= [B|d_{12}]e^t = Be_1^t + e_2^t = Bs$

algorithm decoding extended binary Golay code

we recieve r

1) Compute syndrome $s= Gr^t$
2) if $w(s)\leq 3$ then $e:=[s,0]$ stop
3) if $w(s+B_i)<3$ then $e:=[s+B_i, \delta_i]$ $\delta_i \rightarrow$ vector with only zeroes except the ith one. stop
4) Compute $t:= Bs$ — have to try with each row, we find the right i
5) if $w(t)\leq 3 \longrightarrow e:=[0,t]$ stop
6) if $w(t+B_i)<3 \longrightarrow e:=[\delta_i, t+B_i]$, stop
7) if e not determined, retransmission

The binary Golay code $[23,12]$ has the same generator matrix as $Gol[24,12]$ except for the last column which is omitted.

The minimal weight is 7.

$Gol[23,12]$ is a perfect $[23,4^{12},7]$ code

to decode it we use the same algorithm

We add one bit so that $w(r_1)$ or $w(r_0)$ is odd (we call it r')

FUNDAMENTAL THEOREMS

1) evers perfect linear code over $\mathbb{F}_q$ symbols (q prime power) has the parameters of a repetition code a Hamming or Golay code $(Gol(23,2), Gol(11,3))$

2) evers perfect linear code over $\mathbb{F}_q$ is a repetition, a Hamming or a Golay code