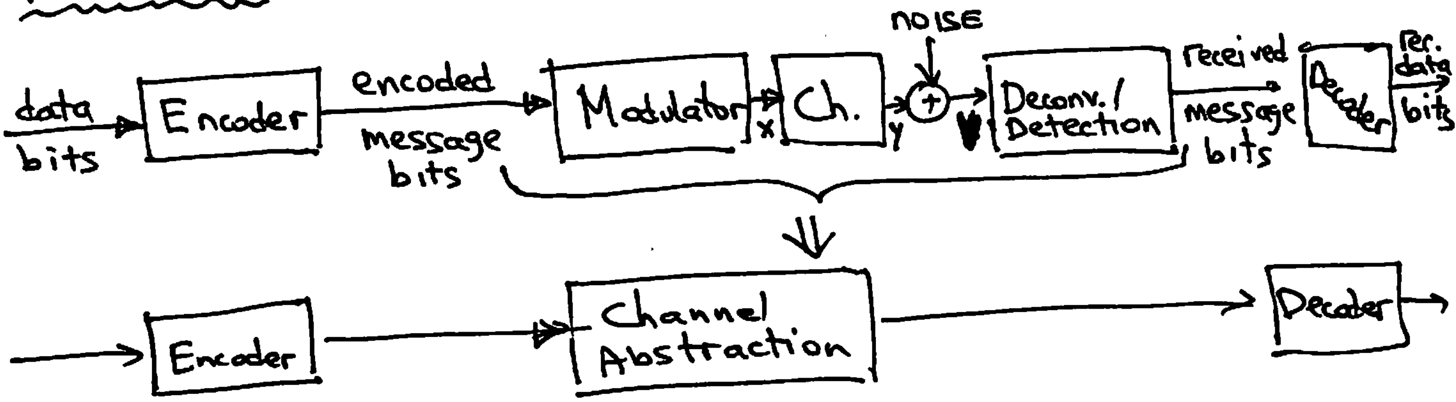
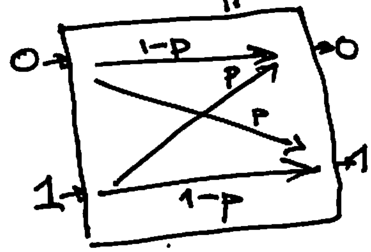
ERROR CORRECTION / DETECTION

LINEAR BLOCK CODES

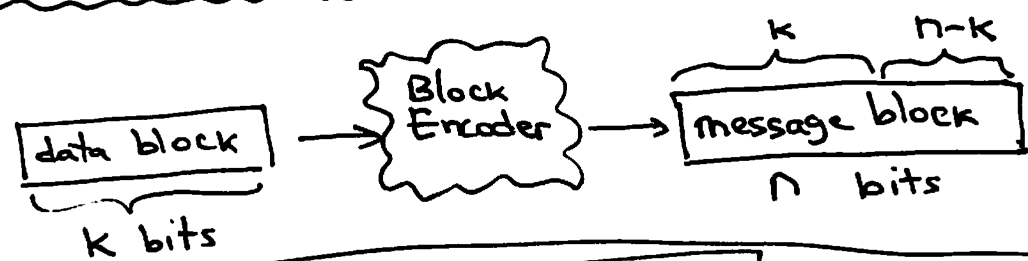
Motivation: look at the setup:

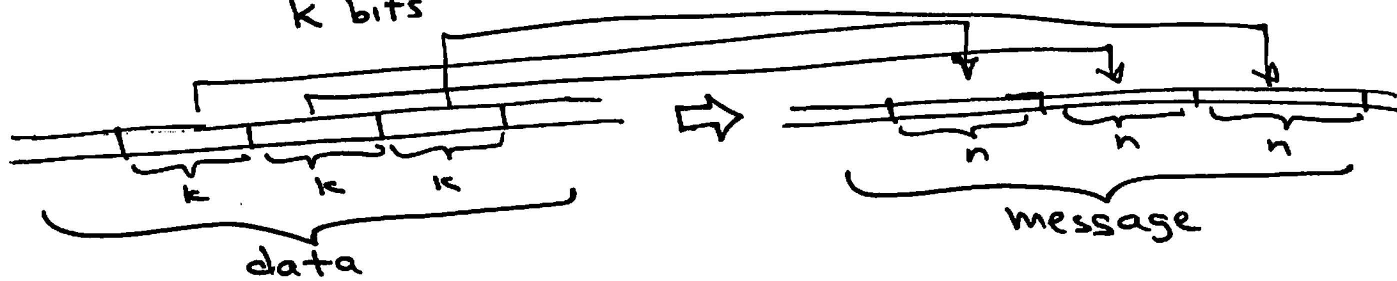




BSC
Binary
Symmetric
channel

Further simplification: block coding





Tool for working with blocks / BSC : Hamming distance

Ex. HD("00001", "10000") = ?
HD("00001", "000") = ?

Comparing rates:

msg. block length: $n_1 = 10$ ‖ vs. ‖ msg.: $n_2 = 11$

data block length: $k_1 = 7$ ‖ ‖ data: $k_2 = 8$

$7/10 < 8/11$: (n_2, k_2) is faster

Comparing probabilities:

data block length: $k_1 = 10$ ‖ vs. ‖ data: $k_2 = 15$

$\mathbb{P}$(error in the block): $P_1 = 10^{-7}$ ‖ ‖ $\mathbb{P}$(err): $P_2 = 10^{-9}$

$\underbrace{10 \quad 10 \quad 10}_{30}$ ‖ ‖ $\underbrace{15 \quad 15}_{30}$

$\mathbb{P}(\text{err}) = 1 - (1-10^{-7})^3 \approx 3 \cdot 10^{-7}$ ‖ vs. ‖ $\mathbb{P}(\text{err}) = 1-(1-10^{-9})^2 \approx 2 \cdot 10^{-9}$

$\Uparrow$ better in $\mathbb{P}$(error)

$\mathbb{F}_2$ arithmetic:

addition:

+	0	1
0	0	1
1	1	0

multiplication:

·	0	1
0	0	0
1	0	1

$x + x = 0$, ALWAYS

BLOCK CODE = A SET OF MESSAGES OF GIVEN LENGTH

LINEAR BLOCK CODE : INVARIANT TO $\mathbb{F}_2$-POINTWISE ADDITION

Ex.: {"110", "000"} : IS this A LINEAR CODE?

Ex.: WHAT IS THE MINIMAL LINEAR CODE CONTAINING "0101" AND "0001"?

Ex.: HOW MANY ELEMENTS IN A LINEAR CODE?

"RECTANGULAR" CODE

Ex.: $k=4$

d_1	d_2	d_3	d_4

data word

d_1	d_2	p_1
d_3	d_4	p_2
p_3	p_4	

d_1	d_2	d_3	d_4	p_1	p_2	p_3	p_4

$$\left.\begin{aligned} p_1 &= d_1+d_2 \\ p_2 &= d_3+d_4 \\ p_3 &= d_1+d_3 \\ p_4 &= d_2+d_4 \end{aligned}\right\} \text{ALL IN } \mathbb{F}_2$$

If $p \ll 1$ then $\mathbb{P}(\text{err. in 4-bit data}) \approx 28p^2$

Compare to REPLICATION (by 2):

$$\mathbb{P}(\text{err. in 4-bit data}) \approx 4p$$

Ex.: $k=6$

d_1	d_2	d_3	d_4	d_5	d_6

d_1	d_2	d_3	p_1
d_4	d_5	d_6	p_2
p_3	p_4	p_5	

$\longrightarrow n = 11$

$\mathbb{P}(\text{error transmitting 6-bit data}) \approx ?$

(assuming $p \lll 1$)

HAMMING CODES

STEP 1: SELECT $m > 1$ (INTEGER) FOR $(2^m-1, 2^m-1-m, 3)$ CODE

STEP 2: COMPILE A (2^m-1)-by-m TABLE, ROWS OF WHICH FORM BINARY REPRESENTATIONS OF NUMBERS $1, 2, \dots 2^m-1$

FOR $m=2$:

0	1
1	0
1	1

FOR $m=3$:

0	0	1
0	1	0
0	1	1
1	0	0
1	0	1
1	1	0
1	1	1

STEP 3: ASSOCIATE EVERY ROW WITH A SINGLE "1" ENTRY WITH A PARITY BIT (TOTAL OF m PARITY BITS). THE REST OF THE ROWS ARA ASSOCIATED WITH THE DATA BITS.

FOR $m=2$:

0	1	p_1
1	0	p_2
1	1	d_1

FOR $m=3$:

0	0	1	p_1
0	1	0	p_2
0	1	1	d_1
1	0	0	p_3
1	0	1	d_2
1	1	0	d_3
1	1	1	d_4

STEP 4: DEFINE THE ENCODER: EACH PARITY BIT IS THE $\mathbb{F}_2$-SUM OF THOSE DATA BITS WHICH HAVE "1" IN THE CORRESPONDING COLUMN

FOR $m=2$:
$$p_1 = d_1$$
$$p_2 = d_1$$

FOR $m=3$:
$$p_1 = d_1 + d_2 + d_4$$
$$p_2 = d_1 + d_3 + d_4$$
$$p_3 = d_2 + d_3 + d_4$$

STEP 5: DEFINE THE DECODER: FOR EACH <u>COLUMN</u> OF THE TABLE, COMPUTE THE SUM OF OF THOSE BITS WHICH CORRESPOND TO A ROW WITH A "1". ~~IN THEIR ROW~~

IF <u>NO BIT ERROR</u> THEN ALL SUMS ARE 0.

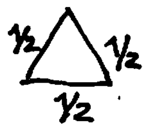
IF <u>ONE BIT ERROR</u>, THE SUMS DEFINE THE 3-BIT BINARY REPRESENTATION OF THE CORRUPTED BIT'S INDEX

OPTIMALITY OF HAMMING CODES:

H.C. : m EXTRA BITS TO CORRECT ANY SINGLE ERROR TRANSMITTING $2^m - 1 - m$ BITS

THEOREM: m EXTRA BITS <u>CANNOT</u> CORRECT EVERY SINGLE ERROR TRANSMITTING $2^m - m$ BITS!

PROOF: <u>VOLUME</u>!

Ex. IS IT POSSIBLE TO PLACE 3 TRIANGLES 

INSIDE 

?

(NO INTERSECTIONS ALLOWED)

SOLUTION: "AREA" CALCULATIONS : $\frac{\sqrt{3}}{8}$ VS. $\frac{1}{2}$

PROOF OF OPTIMALITY: SURROUND EACH CODE WORD WITH THE RESULTS OF 1-BIT ERRORS IN ITS TRANSMISSION. $\longrightarrow$ GET A $n+1$ -ELEMENT SET FOR A TOTAL OF 2^k CODE WORDS, THIS YIELDS $(n+1)2^k$ ELEMENTS. HENCE

$$2^n \geq (n+1)2^k \quad \text{, OR, SINCE } m = n-k$$

$$2^m \geq m+k+1 \text{ , i.e.}$$

$$\boxed{k < 2^m - m}$$

Ex. HOW MANY BITS IN A HAMMING CODE WORD WITH 4 PARITY BITS ?

INSIGHT: "LINEAR" CODES ARE DEFINED BY LINEAR EQUATIONS

Ex.:

$$\left.\begin{aligned} p_3 + d_2 + d_3 + d_4 &= 0 \\ p_2 + d_1 + d_3 + d_4 &= 0 \\ p_1 + d_1 + d_2 + d_4 &= 0 \end{aligned}\right\} \begin{array}{l} \mathbb{F}_2\text{-equations} \\ \text{FOR HAMMING} \\ \text{WITH 3 PARITY } \cancel{\text{CODES}} \text{ BITS} \end{array}$$

"DECODING" BECOMES "SOLVING SYSTEMS OF LINEAR EQUATIONS"