Theory@UCLA Week 2 – presented by Nakul Khambhati

1) Lagrange interp (+ secret sharing) — 15ish mins
   → any finite field stuff ??
2) Codes: pose the problem: XOR repetition ⇔ compare rate (n,k) correcting capability distance?
   → illustrate Hamming code,
   introduce generator & parity check matrix
   use lin alg to "prove" its props like rate, distance, etc.

   generalize to general (linear?) codes...

(Maybe reverse the order)

7 6 5 4 ... 2 0

0 1 1

= 6

–	0	1	0	0	1	0	1
0	~~1~~	~~2~~	3	~~4~~	5	6	7
000	001	010	011	100	101	110	111

→

–	0	1	0	0	1	1	1
0	~~1~~	~~2~~	3	~~4~~	5	6	7

decoding rule:

check if parity bits are ok → identify ones that aren't
in binary, then spell out the error pos!

} abstractify using matrices

↳ 3B1B visual to illustrate this

↳ lin alg (I need to learn this!)

① 0101 → 0100101

(work this out later)

$$(0101)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

(1x4) 4x7

for some reason, row vector. can take transpose and get column.

$= [\quad\quad\quad]$

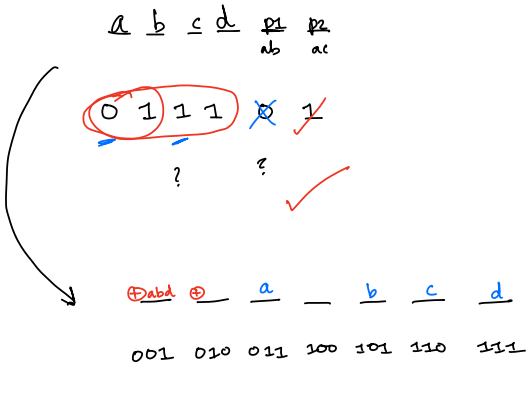
(1x7)

(parity check is just all 7 non zero 3 bit columns)

Can this in an order that's intuitive.
ideally.

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

binary counting (or reverse).



gen:

how does one generalize this though?

$$(a\ b\ c\ d)\begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

4×7

why is distance 3 though?

why does this count in binary??

Prop

eggs to generalize

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

1 2 3 4 5 6 7

3×7

7×1

can verify $H \cdot G = 0$

?? need to take some transposes.

Prop] Why?

gen matrix: Ex: 2.16. (web-coding-book)

Q] Some linear prop?

like determinant and invertible stuff?

2.3.5 linear code d = min # of lin ind cols of H.

↓ use this to prove generalized Hamming code has dist 3
∴ error correcti...

capabiliv