CS 70 ## 33 LECTURE 13

ERROR CORRECTION

why $n+2k$ for the general case?

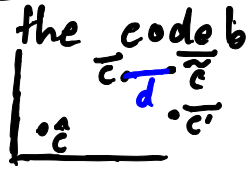
ERASURE We used an identical scheme because we don't care about secrecy.

GENERAL Same thing, with more redundancy. Our algorithm needed $n+2k$ unknowns: nth coeff. in $Q(x)$, and k coeff. in $E(x)$. We know this works, but why?

DISTANCE

Look at the codebook:

message	m	m'	$\widetilde{m}$	← need gaps
codeword	$\vec{c}$	$\vec{c'}$	$\widetilde{\vec{c}}$	← each is $n+2k$



← some things are closer together

Hamming Distance: $d(\vec{s}, \vec{r}) = \sum_{j=1}^{L} 1(r[j] != s[j])$

indicator function

By changing d elements in $\vec{s}$, we arrive at $\vec{r}$. However, the adversary just needs to confuse the decoder. Say $d=5$. Then say the adversary changes $k=4$. Was it $\vec{s}$, changed by 4, or $\vec{r}$, changed by 1?

This means $d=5$ cannot protect against 4 changes or 3 changes. But, if only 2 corrections can be made, it must've been $\vec{s}$. So, we can protect against $\lfloor d/2 \rfloor$ errors if d is odd & $d/2-1$ if d is even.

SYSTEMATIC CODES

$\vec{c} = [\vec{m} \quad \overrightarrow{\text{extra}}]^T$ min. distance $= \min_{\vec{c}, \vec{c'}} d(\vec{c}, \vec{c'})$

$\vec{c} = [x2 \quad x4]^T$ can min. distance = 6? no!

min. distance $\leq 1 +$ extra length

For our polynomials, $\lfloor (2k+1)/2 \rfloor = k$, the number of corruptions we can handle.

Counting

Probability theory happens to rely on counting & number theory. Say you had a 100-sided die, and you win on prime #s. How likely? Clearly, this has to do w/how many primes ≤ 100.

You learned multiplication as the area of a rectangle, counting squares. How many permutations are there of n distinct objects?

$n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = n!$

Sahai's joke of the day: in English, "no choice" & "one choice" are the same. How many ways to arrange k objects? $n(n-1)\ldots(n-k+1) = \prod_{j=0}^{n-k+1} (n-j) = \frac{n!}{(n-k)!}$

Division

30 squares, 6 per row. How many rows? $30/6 = 5$

This is counting "equivalence classes" when every class is of the same size.

Can we think of $n!/(n-k)!$ in this way? We know $n!$ is arranging everything. $(n-k)!$ is then the # of ways to arrange the rest.

★ How many ways to pick, not arrange, k objects? If order doesn't matter, there's probably division.

$(n!/(n-k)!)/k! = n!/k!(n-k)! = n$ choose $k = \binom{n}{k}$