recap

we're sending a message as points on a polynomial.

706981

7	0	6	9	8	1
1	2	3	4	5	6

corresponds with the 5-deg pol. that goes through $\{(1,7), (2,0), \ldots (6,1)\}$

call this polynomial $P(x)$.

what could go wrong?

① erasure errors (up to k erasures)

7	?	6	9	?	1
1		3	4		6

We need at least n points to decode $P(x)$ and get message back

send $n+k$ points so for $e \leq k$ erasures,

$n+k-e \geq n$ ✓

Bob: just interpolate with the points that come thru.

② general errors (up to k corruptions)

7	5	6	6	8	1
1	2	3	4	5	6

We need at least n ~~∧~~ points to decode $P(x)$ and get message back

CORRECT!

if Bob just interpolated with all the points he got, he would get a corrupted pol. b/c he doesn't know which points are bad.

how do we deal with this?

→

recap Berlekamp-Welch get back original pol. AND where the errors are!

Work in mod q (q large enough st. all characters you want to encode are unique)

Message: 2136

We know channel has 1 corruption.

Sender will find P(x) that goes thru (1,2), (2,1), (3,3), and (4,6) and sends P(1) ... P(6) thru the channel (6 = 4 + 2(1))

P(x) is still deg 3

Recipient gets all 6 packets but up to 1 is corrupted.

they know at least 5 (n+k) points are correct but don't know which ones

Error Locator Polynomial: $E(x) = (x-e_1)(x-e_2)\cdots(x-e_k)$ ← deg k polynomial

e_i = index of error.

Consider the expression $P(i)\,E(i) = r_i\,E(i)$, where r_i is the received val.

↳ if $P(i) = r_i$ so no corruption @ index i
this is true b/c same terms on both sides

↳ if $P(i) \neq r_i$ so index i WAS corrupted + there's error there
$E(i) = 0$ on both sides, $0 = 0$.

Idea! Set up system of $n+2k$ equations like above and solve.

recap

What are we solving for? coefficients of $Q(x)$ and $E(x)$

for an n-length message we wanna send...

Polynomial	Degree	# of Coefficients Unknown
$P(x)$	$n-1$	n
$E(x)$	k	$+\ k+1$ ← actually just k b/c in $(x-e_1)(x-e_2)\ldots$ the x^k coefficient will surely be 1.
$Q(x)$	$k+n-1$	$+\ k+n$
↑ $P(x)E(x)$	↑ multiplying pols = summing up degrees	$n+2k$

Write E + Q generally:

$$Q(x) = a_{k+n-1}x^{k+n-1} + a_{k+n}x^{k+n} + \ldots + a_1 x + a_0$$

$$E(x) = 1x^k + b_{k-1}x^{k-1} + \ldots b_1 x + b_0$$

Set up $Q(x) = E(x)$, for $1 \leq x \leq n+2k$.

After finding Q & E,

$P(x) = Q(x)/E(x)$

things to remember

- reason through why we need $n+2k$ points
- if you get multiple sol'ns for $Q(x)$ and $E(x)$, dividing the respective ones should still give the same $P(x)$
- erasure errors – simplest, just send more points
- deg of $P(x)$ is len(original_message) − 1
- the hypothetical polynomial that you get by interpolating over the received points in case of general errors is not relevant to us (the corrupt points will give us a bad polynomial so we do not want to consider it in any way) WE SOLVE FOR EVERYTHING WITH BERLEKAMP-WELCH.

Polynomial	Degree	Unknown Coefficients
$P(x)$	$n-1$	n
$E(x)$	k	$k+1$ ← one will always be 1
$Q(x)$	$k+n-1$	$k+n$
		$n+2k$

for when there is corruption

thanks for coming! help me help you → https://www.tinyurl.com/aishani-sp21-fb