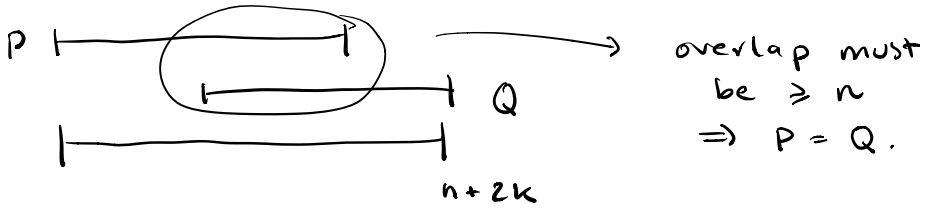
ECCs and the BW Algorithm:

Goal: Send info reliably using redundancy.

- Suppose we want to send a message of length n.
- Idea: embed info in a polynomial w/ degree $\leq n-1$ and send $(1, P(1)), \ldots, (m, P(m))$
  - ↳ Can send arbitrarily many packets
  - ↳ Robust against random errors.
- Erasure errors: easier to deal with.
  - ↳ If we know a channel will erase k packets at random, send $m = n+k$ to make up the lost packets.
  - ↳ Reconstruction is just interpolation.
- Corruption errors: more involved.
  - ↳ If we know a channel will corrupt k packets at random, send $m = n+2k$.
  - ↳ Use BW to reconstruct.
- Why $n+2k$?
  - ↳ To be able to decode, we need there to be exactly one polynomial going through $m-k$ points of degree $\leq n-1$.
  - ↳ $m \geq n+2k$ forces uniqueness



- **Berlekamp-Welch (BW):** (let $m = n + 2k$)
  - Suppose the received message is $a_1, \dots, a_m$
  - Consider

$$\begin{aligned} P(1) &= a_1 \\ P(2) &= a_2 \\ &\vdots \\ P(m) &= a_m \end{aligned}$$

$\leftarrow$ k of these equalities don't hold!

  - Let E be a degree k polynomial w/ leading coefficient 1 such that

$$E(x) = 0 \iff x \text{ was corrupted}$$

  - Multiply by $E(i)$ on both sides:

$$\begin{aligned} P(1)E(1) &= a_1 E(1) \\ P(2)E(2) &= a_2 E(2) \\ &\vdots \\ P(m)E(m) &= a_m E(m) \end{aligned}$$

$\leftarrow$ all of these equalities hold!

$\Downarrow$ this is a linear system in coefficients

$$\begin{aligned} P(1)E(1) &= a_1 E(1) \\ P(2)E(2) &= a_2 E(2) \\ &\vdots \\ P(m)E(m) &= a_m E(m) \end{aligned}$$

$n+2k$ equations

$P(m)E(m)$: $n+k$ variables; $a_m E(m)$: k variables

(1.) Alice wants to send a message of length n to Bob across a channel that erases k_e packets and corrupts k_c packets. She works over GF(7).

(a) How many packets must Alice send?

(b) Suppose $n=1$, $k_e=0$, and $k_c=1$, and Alice sends the packets $(1, 2)$, $(2, 4)$, $(3, 2)$. What message was she trying to send?

(2.) Let $0 \leq p \leq 1$ be a real number and suppose Alice sends a message across a channel that behaves as follows: if Alice sends m packets, pm of them are corrupted (rounding down if necessary)

(a) For what values of p is decoding possible?

(b) If Alice wants to send a message of length n, how many packets must she send (assume p is in the range such that decoding is possible).

(3.) Suppose now Alice sends a message across a channel that corrupts each packet independently with probability $p < \frac{1}{2}$. If Alice wants to send a message of length n (where n is large), how many packets must she send to ensure that Bob can decode the message with probability $> .95$? (Hint: CLT, $\Phi^{-1}(.95) \approx 2.58$)