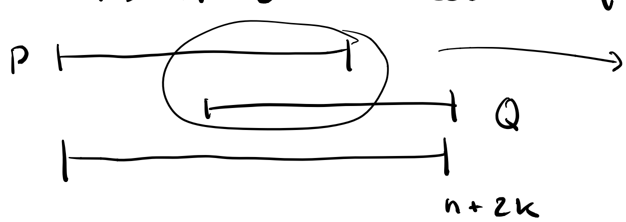
ECCs and the BW Algorithm:

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



overlap must be $\geq n$
$\Rightarrow P = Q$.

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

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

← 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:

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

← all of these equalities hold!

⇓ this is a linear system in coefficients

$$\left.\begin{aligned} P(1)E(1) &= a_1 E(1) \\ P(2)E(2) &= a_2 E(2) \\ &\vdots \\ \underbrace{P(m)E(m)}_{n+k \text{ variables}} &= \underbrace{a_m E(m)}_{k \text{ variables}} \end{aligned}\right] n+2k \text{ equations}$$

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? $n + k_e + 2k_c$

(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?

$n=1$: $P(x)$ has degree 0 $\Rightarrow$ $\underline{P(x) = c}$

$P(1) = 2 = P(3)$

$\Rightarrow P(x) = 2$

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).

(a) $0 \leq p < \frac{1}{2}$.

(b) $m = \dfrac{n}{1-2p}$.

$$m = \underset{\substack{\uparrow \\ \text{message length}}}{\underline{n}} + 2\underset{\substack{\uparrow \\ \text{\# of corrupt packets}}}{\underline{k}}$$

$$= n + 2(pm)$$

$$(1-2p)m = n$$

$$m = \frac{n}{1-2p}$$

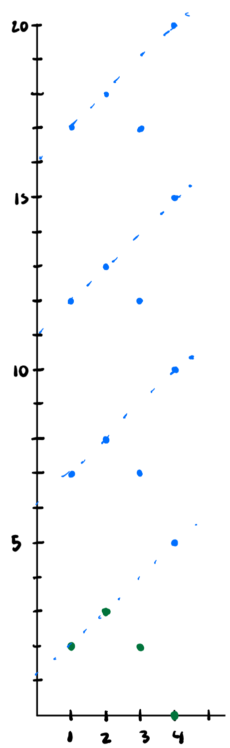
3. Let $P(x)$ be a degree 1 polynomial over $GF(5)$ and suppose we are told that

$$P(1) \equiv 2, \; P(2) \equiv 3, \; P(3) \equiv 2, \; P(4) \equiv 0.$$

Furthermore, we are told that exactly one of the above values is wrong. Find the wrong value and compute $P(0)$.

3 is wrong

$P(0) = 1.$



$P(x) = x + 1$

$P(0) = 1$

$\deg(P) = 1,$

$P(1) \equiv 2$

$P(2) \equiv 3$

$P(3) \equiv 2$

$P(4) \equiv 0$

$GF(5)$

$k = 1$

$n = 2$

$E(x) = x + a_0$

$P(x)E(x) = a_1 x^2 + a_2 x + a_3$

4. 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, $\Phi^{-1}(.95) \approx 2.58$)

$$m \geq n + 2E \quad , \quad X_i = \begin{cases} 1 & i \text{ is corrupted} \\ 0 & \text{c.w.} \end{cases}$$

$$E = \sum_{i=1}^{m} X_i \qquad \mathbb{E}[X_i] = p$$

$$\text{Var}(X_i) = p(1-p)$$

$$\frac{E - mp}{\sqrt{mp(1-p)}} \sim \mathcal{N}(0,1) \text{ by CLT.}$$

$$E \leq \frac{m-n}{2} \iff$$

$$\mathbb{P}\left[\frac{E - mp}{\sqrt{mp(1-p)}} \leq \frac{m - 2mp - n}{2\sqrt{mp(1-p)}}\right] \geq .95$$

$$\Rightarrow \quad \frac{(1-2p)m - n}{2\sqrt{mp(1-p)}} \geq \Phi^{-1}(.95)$$