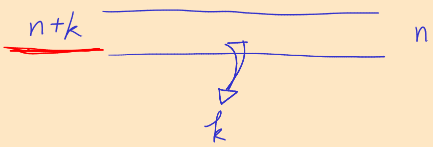
Erasures



k = 2

1 2 3
1 2 3
1 2 3

n(k+1)

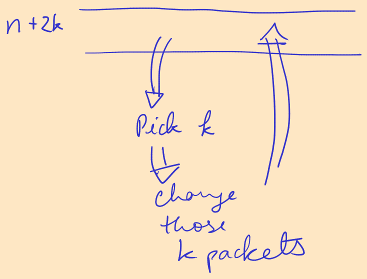
deg n−1 poly

n pts ⟶ get deg n-1 poly

4 5 3

deg 2 poly (0, 4), ~~(1, 5)~~, (2, 3)
(4, —), ~~(5, —)~~

Corruption



n

n+k k

① Which packets corrupted

② How those packets "

deg (n+k−1)

n+2k

5 Errors, Error-Correcting Codes, and Intro to Counting

Computer Science Mentors 70

Mar 01 - Mar 05
Spring 2021

Amogh Gupta, Sylvia Jin, Aekus Bhathal, Abinav Routhu, Debayan Bandyopadhyay

Roast us here: `https://tinyurl.com/csm70-feedback20`

1 Erasures

1. Sylvia would like to send a secure message to Amogh over a channel of size n. This means Sylvia can send at most n packets at a time across the channel. However, the channel is not very reliable.

   Assume the channel behaves as follows: of the first batch of n packets, it corrupts none; of the second batch of n packets, it corrupts exactly 1; of the third batch of n, it corrupts exactly 2; and so on, until for the $(n+1)^{\text{th}}$ batch of n packets (and thereafter), it corrupts all of them.

   Suppose we use error correcting codes for each batch of packets in order to recover the original messages which were sent through the channel. What is the maximum size message (in terms of packets) that we can send? Your final answer should be a closed-form expression, but keeping it as a summation is also acceptable.

   Assume n is even.

m_k = # of packets of info

$m_k + 2k = n$

$\Rightarrow m_k = n - 2k$

$k = \frac{n}{2}$

$k = n$

$2k = 2n$

$m_k + 2k = n$

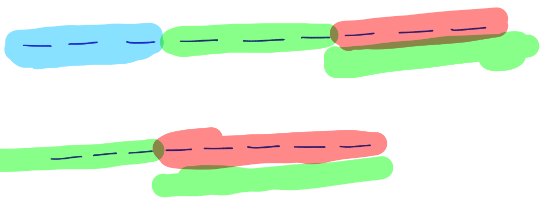
$m_k + n = n$

$\Rightarrow m_k = 0$

Total # of packets $= \sum_{k=0}^{n/2} m_k = \sum_{k=0}^{n/2} (n-2k)$

$\sum_{i=0}^{n} i = \frac{n(n+1)}{2}$

$= \sum_{k=0}^{n/2} n + 2\sum_{k=0}^{n/2} k$



$= \left(\frac{n}{2}+1\right)n + \overset{1}{\cancel{2}}\frac{(n/2)(n/2+1)}{\underset{1}{\cancel{2}}}$

$= \frac{n^2}{4} + \frac{n}{2}$

2 Errors/Corruptions

1. Leanne is playing Among Us with 9 of her other friends.

   (a) Leanne wishes to send a message to her friends to tell her friends the room code, such that if all 9 of her friends join together, they can determine the room code. What kind of scheme could Leanne use?

   Polynomials

   11

   $\underbrace{(1, p(1)),\ (2, p(2)),\ \dots,\ (9, p(9))}_{}$

   10 pts $\underbrace{p(0)}_{}$ = room code

   mod p

   (b) There are two imposters, who are working together to not get caught. Leanne is not an imposter, and she wishes to send a message to her friends to confirm this fact with her friends. She uses the same scheme as in part (a), where her message is 0 if Leanne is not an imposter and 1 if Leanne is an imposter. How could the two imposters work together to make Leanne seem like an imposter?

   $p(0)$ = message

   $p(1)$ $p(2)$ $p(3)$ $p(i)$ $p(9)$

   imp

   $0, 1, 2, \dots, i-1, i+1, \dots, 9$

   $q(0) = 1$ $q(1) = p(1)$ $q(2) = p(2)$ $q(i) \neq p(i)$ $q(9) = p(9)$

   (c) Leanne now knows that the imposters will do what they did in part (b). How should Leanne change her scheme to make sure that the message is sent correctly and $\underbrace{\text{determine at least one imposter?}}_{}$

   9

   $k = 2$

   $n + 2 \cdot 2 = 9$

   $\Rightarrow n = 5$

   deg-4 poly

   $p(0)$ = message $1, 2, 3, \dots, 9$

   $E(x) = (x-4)(x-5)$

2. In this problem, we explore why we need $n + 2k$ points to correct for k general errors. Suppose Alice is trying to send a message of length n to Bob, but she knows that if she sends a message, k packets will be corrupted. Alice knows that by Berlekamp-Welch, she should send $n + 2k$ packets to ensure that the message can be decoded. By considering an adversary, Eve, who can corrupt k packets of her choice, show that $n + 2k$ is the minimal number of packets to send to be able to decode the message; in other words, if Alice sends fewer than $n + 2k$ packets, then the message could potentially not be decoded.

n packets P deg $n-1$

corruptions

$P(1)\ P(2) \ldots P(n)\ P(n+1) \cdots P(n+2k)$

Alice

$(1, P(1))$

$(2, P(2))$

$\vdots$

$(i, P(i))$

$\vdots$

$(n+2k, P(n+2k))$

Choose k msg

$\downarrow$

change them

Bob

$(1, r_1)$

$(2, r_2)$

$\vdots$

(i, r_i)

$(n+2k, r_{n+2k})$

$r_i = P(i) \quad \forall i$

$\exists i: r_i \neq P(i)$ ($\exists$ upto k such i)

$Q(1) \equiv E(1)P(1) \equiv E(1)r_1 \pmod p$

$Q(2) \equiv E(2)P(2) \equiv E(2)r_2 \pmod p$

$Q(i) \equiv E(i)P(i) \equiv E(i)r_i \pmod p$

$\vdots$

$E(n+2k)P(n+2k) \equiv E(n+2k)r_{n+2k} \pmod p$

deg $P = n-1$

$$\frac{Q(x) \leftarrow n+k}{E(x)} = P(x)$$

$\uparrow k$

$e_i \neq 0 \Rightarrow$ Packet i is good.

$n+2k$ vars

$n+2k$ congruences

$n = 3$

$a_0 + a_1 x + a_2 x^2 \equiv r_1 \pmod p$

$a_0 + a_1 + a_2 \equiv r_1 \pmod p$

$a_0 + 2a_1 + 4a_2 \equiv r_2 \pmod p$

$a_0 + 3a_1 + 9a_2 \equiv r_3 \pmod p$

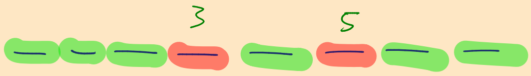
n out of $n+2k$

$E(x)$ deg k poly with leading coeff is 1

$(x-e_1)(x-e_2)\cdots(x-e_k)$

Packet i corr $\Rightarrow$ $\underline{e_i = 0}$

☆



$n = 4$

$P(x)$ $P'(x)$

$(1, 2, 3, 4, 0)$

deg 2 $\quad P(x)$

3 Berlekamp-Welch

(a) Alice sends Bob a message of length 3 on the Galois Field of 5 (modular space of mod 5). Bob receives the following message: (3, 2, 1, 1, 1). Assuming that Alice is sending messages using the proper general error message sending scheme, set up the linear equations that, when solved, give you the $Q(x)$ and $E(x)$ needed to find the original $P(x)$.

1 general error.

$$Q(x) = a_0 + a_1x + a_2x^2 + a_3x^3$$
$$E(x) = (x - e_1)$$
$$a_0 \equiv 1(-e_1) \mod 5$$
$$a_0 + a_1 + a_2 + a_3 \equiv 3(1 - e_1) \mod 5$$
$$a_0 + 2a_1 + 4a_2 + 3a_3 \equiv 2(2 - e_1) \mod 5$$
$$\vdots$$

$e_1 = 3 \qquad x = 3$

$a_0 = 2$

$a_1 = 3$

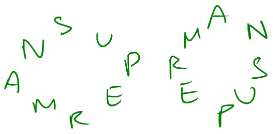
$a_2 = 3$

$a_3 = 1$

(b) What is the encoded message that Alice actually sent? Which packet(s) were corrupted?

4 SUPERmutations

2. How many ways are there to arrange the letters of the word "SUPERMAN"...



   (a) ...on a straight line? $8!$ USPERNAM

   (b) ...on a straight line, such that "SUPER" occurs as a substring?
   $4!$ MSUPERNA SUPERNAM UPERNAMS

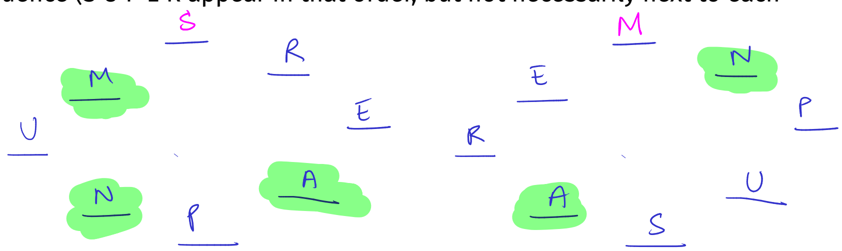
   (c) ...on a circle? Note: If we arrange elements on a circle, all permutations that are "shifts" are equivalent (i.e. SUPERMAN and UPERMANS). $7!$ $\qquad 8!/8 = 7!$

   (d) ...on a circle, such that "SUPER" occurs as a substring? Reminder: SUPER can occur anywhere on the circle!
   $3!$

3. Now how many ways are there to arrange the letters of the word "SUPERMAN"...

   (a) ...on a straight line, such that "SUPER" occurs as a subsequence (S U P E R appear in that order, but not necessarily next to each other)?
   $\underline{S}\ \underline{N}\ \underline{U}\ \underline{M}\ \underline{A}\ \underline{P}\ \underline{E}\ \underline{R}$ $\qquad \binom{8}{3} \cdot 3! \cdot 1 = \binom{8}{3} \cdot 3!$ $\qquad$ SMUPNERA SUPEMANR $\qquad$ SPUERMAN

   (b) ...on a circle, such that "SUPER" occurs as a subsequence (S U P E R appear in that order, but not necessarily next to each other)?
   $$\binom{7}{3} \cdot 3! \cdot 2 = 420$$
   $$\binom{7}{2} \cdot 2! \cdot 5 \cdot 2 = 420$$



4. How many 5-digit sequences have the digits in ...

(a) strictly increasing order?

12345

35789

~~35879~~

~~35 889~~

0 1 2 3 4 5 6 7 8 9

04568

$\boxed{\binom{10}{5}}$

(b) non-decreasing order?

12345

35789

35879

35889

5 stars

9 bars

(10 bins)

$\binom{14}{9}$

$\binom{10+5-1}{10-1}$

$\binom{10+5-1}{5}$