ERROR CORRECTION, COUNTABILITY 5

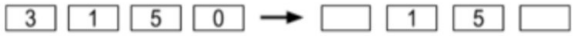
COMPUTER SCIENCE MENTORS 70

October 1 - 5, 2018

1 Erasure Errors

1.1 Introduction

We want to send n packets and we know that k packets could get lost. We use a polynomial under GF(q).



How many more points does Alice need to send to account for k possible errors? __
What degree will the resulting polynomial be? ___
How large should q be if Alice is sending n packets with k erasure errors, where each packet is a integer between 0 and m?

What would happen if Alice instead sends $n + k - 1$ points? Why will Bob be unable to recover the message?

1.2 Questions

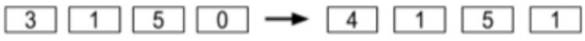
1. Suppose $A = 1$, $B = 2$, $C = 3$, $D = 4$, and $E = 5$. Assume we want to send a message for which the information is contained in 3 packets. Recover the lost part of the message, or explain why it cannot be done.
   1. C_AA
   2. CE_ _

2. Suppose we want to send n packets, and we know $p = 20\%$ of the packets will be erased. How many extra packets should we send? What happens if p increases (say to 90%)?

2 General Errors (Berlekamp and Welch)

2.1 Introduction

Now instead of losing packets, we know that k packets are corrupted. Furthermore, we do not know which k packets are changed. Instead of sending k additional packets, we will send an additional $2k$. This ensures that we have at least $n + k$ un-corrupted points and can uniquely determine the original polynomial.



Solomon-Reed Codes

1. Identical to erasure errors: Alice creates $n - 1$ degree polynomial $P(x)$.

$$P(x) = p_0 + p_1 x + \ldots + p_{n-1} x^{n-1}$$

2. Alice sends $P(1), \ldots, P(n + 2k)$

3. Bob receives $R(1), \ldots, R(n + 2k)$

For how many points does $R(x) = P(x)$?

True or false: $P(x)$ is the unique degree $n - 1$ polynomial that goes through at least $n + k$ of the received points.

Berlekamp Welch
How do we find the original polynomial $P(x)$? Suppose that $m_1, \ldots, m_k$ are the corrupted packets. Let $E(x) = (x - m_1) \ldots (x - m_k)$. Then $P(i) * E(i) = r_i * E(i)$ for any i greater than 1 and less than $n + 2k$. Why?

Let $Q(i) = P(i)E(i)$. So we have $Q(i) = P(i)E(i) = r_i * E(i)$ where $1 \leq i \leq 2k + n$.
What degree is $Q(i)$?

How many coefficients do we need to describe $Q(i)$?

What degree is $P(i)$?

How many unknown coefficients do we need to describe $E(i)$?

We can write $Q(i) = r_i E(i)$ for every i that is $1 \leq i \leq 2k + n$.
How many equations do we have? How many unknowns?

Once we have the above described equations, how do we determine what $P(i)$ is?

2.2 Questions

1. (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 $P(x)$.

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

2. You want to send a super secret message consisting of 10 packets to the space station through some astronauts. You are afraid that some malicious spy people are going to tell the wrong message and make the space station go spiraling out of orbit. Assuming that up to 5 of the astronauts are malicious, design a scheme so that the group of astronauts (including the malicious ones) still find the correct message that you want to send. You can send any number of astronauts, but try to make the number that you have to send as small as possible. Astronauts can only carry one packet with them.

3 Countability

3.1 Introduction

(a.) Cardinality is defined as the number of elements in a set. We define a set as countably infinite if it has the same cardinality as the natural numbers (or any countable set).
(b.) We can prove a set is countable by finding a bijection between the set and any countable set. A few classic examples are the hotel argument to show that $\mathbb{Z}^+$ is countable, and the spiral argument to show that the $\mathbb{Q}$ is countable, both included in your notes.
(c.) To prove a set is uncountable, we can either find a bijection between it and an uncountable set or use the Cantor Diagonalization proof, included in your notes.

3.2 Questions

1. **True/False**
   (a) Every infinite subset of a countable set is countable
   (b) If A and B are both countable, then $A \times B$ is countable
   (c) If A_i is countable, then $A_1 \times A_2 \times A_3 .... \times A_N$ for N finite is countable.
   (d) If A_i is countable, then $A_1 \times A_2 \times A_3 ...$ a countably infinite number of times is countable.
   (e) Every infinite set that contains an uncountable set is uncountable.
2. Are these sets countably infinite/uncountably infinite/finite? If finite, what is the order of the set?
   (a) Finite bit strings of length n.
   (b) All finite bit strings of length 1 to n.
   (c) All finite bit strings
   (d) All infinite bit strings
   (e) All finite or infinite bit strings.
3. Find a bijection between N and the set of all integers congruent to $1 \mod n$, for a fixed n.

4. Are the power sets S of a countably infinite set are finite, countably infinite, or uncountably infinite? Provide a proof for your answer.