Lagrange Interpolation, Secret Sharing, Errors

Computer Science Mentors 70

Prepared by: Aishani Sil, Austin Lei, Agnibho Roy, Debayan Bandyopadhyay, Abinav Routhu

1 Lagrange Interpolation

1. In this question, we want to demonstrate the intuition behind the Lagrange interpolation technique.

   Let $p(x)$ be a polynomial of degree 2 over GF(7). Suppose $p(1) = 2$, $p(2) = 1$ and $p(3) = 4$. We would like to find the coefficient representation for p.

   (a) Suppose we had polynomials, p_1, p_2, and p_3, of degree 2 satisfying the following properties:

   $$\begin{aligned} p_1(1) = 1, \quad p_1(2) = 0, \quad p_1(3) = 0 \\ p_2(1) = 0, \quad p_2(2) = 1, \quad p_2(3) = 0 \\ p_3(1) = 0, \quad p_3(2) = 0, \quad p_3(3) = 1 \end{aligned}$$

   How can we express p in terms of $p_1,\ p_2$, and p_3?

   (b) Now let's actually find the coefficient representation of p_1. To start off with, show that p_1 must have the form $c(x-2)(x-3)$ for some constant $c \in GF(7)$.

   (c) What is the value of c? What is the coefficient representation of p_1?

   (d) Now find p_2 and p_3 using the same method.

   (e) Using what we've done so far, find p

   (f) Do you see how this relates to CRT?

2. Suppose that P and Q are degree n polynomials such that $P(1) = Q(1), \cdots, P(n+1) = Q(n+1)$. Show that $P = Q$.

3. Let p be a degree 2 polynomial and q be another degree 2 polynomial in GF(7). Both of them go through the points (1, 2), (2, 1), and (3, 4). Find p and q.

2 Secret Sharing

1. (SU19 MT2) A group of 23 officials are voting on whether to pass a law. All the officials need to vote in favor of the law for it to pass. To make the voting fair, they want to use an anonymous secret-sharing scheme, such that other members of the group cannot see what an official voted for (unless the vote is unanimous, which makes determining this trivial). Suppose there is a third party who will pick a degree d polynomial $P(x)$ in $GF(23)$, give each official a point $(i, P(i))$, and be able to confirm if a guessed polynomial is correct or not (but not reveal the polynomial itself).

   (a) What should degree d be for this scheme? Why?

   (b) If official i wants to vote in favor of the law, what must they do?

   (c) If official i wants to vote against the law, what must they do?

   (d) Explain why $P(x)$ can be recovered with a unanimous vote, and cannot be recovered otherwise.

(e) Explain why this scheme is anonymous.

2. **Graphs and Channels**
Let's say that we want to encode graphs as polynomials and send it over a channel somehow. Let's say that each graph is labelled by nodes $0 \ldots n-1$, we transfer points along a channel by sending points that maps each point to their degree in mod n. Answer the following questions:

   (a) Find the polynomial that encodes a k_n complete graph. Is this polynomial unique to this type of graph? In other words, is every k_n polynomial represented by this polynomial?

   (b) Find the polynomial that encodes a $k_{\frac{n}{2},\frac{n}{2}}$ bipartite graph

   (c) Lets say that this channel is lossy and k packets get corrupted. Is there a way to recover the original graph if we have corrupted packets?

3 Errors

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?

(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?

(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 determine at least one imposter?

(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? Which packet(s) were corrupted?

3. **Wonky Channels Potpourri**

We want to send a total of kn packets over a channel, but the channel can only handle n packets every use. Assume $k < n$ and n to be even. Based on the given behavior of the channels, answer the following questions.

(a) Consider the channel to erase l packets every time the channel is used to transfer information. How many reliable packets of information can we send if we can send kn packets?

(b) Consider the channel to improve over time. It starts at 1 packet erased, and then 2, so on and so forth until k packets erased. How many reliable packets of information can we send if we can send kn packets?

(c) Consider the channel to improve over time. It starts at 1 packet corrupted, and then 2, so on and so forth until k packets corrupted. How many reliable packets of information can we send if we can send kn packets?