Lecture Review

Lecture 9: Polynomials, Secret Sharing, Error Detection

Most important fact: A degree \( d \) polynomial has at most \( d \) roots. As a consequence of this, if \( P \) is a degree \( d \) polynomial, then given \((x, P(x))\) for at least \( d + 1 \) values of \( x \), we can reconstruct \( P \).

Secret Sharing: To split a “secret” \( S \) into \( n \) parts such that any \( k \) of the parts can be used to re-construct the original secret, we choose a random degree \( k - 1 \) polynomial with constant term \( S \) and evaluate it at \( n \) randomly chosen non-zero points.

Lagrange Interpolation: Given \( d + 1 \) points, you can reconstruct the degree \( d \) polynomial using a technique called Lagrange Interpolation.

Lecture 10: Algebraic Structures

Groups: A group is a nonempty set \( G \) together with a binary operation \( \star \) such that the following three axioms hold:

1. Associativity: \( \forall x, y, z \in G, (x \star y) \star z = x \star (y \star z) \)
2. Identity: \( \exists e \in G \) such that \( \forall x \in G, e \star x = x = x \star e \)
3. Inverses: \( \forall x \in G, \exists x^{-1} \in G \) such that \( x \star x^{-1} = e = x^{-1} \star x \), where \( e \) is the identity from above

A group that also has the property that for all \( x, y \in G, x \star y = y \star x \) is called abelian.

Rings and Fields: Rings have two binary operations, usually written \( + \) and \( \ast \), such that \((R, +)\) is an abelian group and the distributive law holds. A Field is a ring where \( \ast \) is commutative and every non-zero element has a multiplicative inverse.

Secret Polynomials

Let’s say we want to share the number 251 between 5 people so that any 3 of them can recover it, but no 2 of them can. How can we do it?

Now suppose we are given the following pieces of data:

1. \( P(x) \in \mathbb{Z}_7[x] \)
2. \( \text{degree}(P) = 2 \)
3. \( P(1) = 1, P(3) = 6, P(4) = 4 \)

How do we re-construct \( P \)?
Permutation Groups

For any \( n \in \mathbb{N} \), let \( S_n \) be the set of all permutations of the set \( \{1, 2, \ldots, n\} \). \( S_n \) is called the permutation group on \( n \) letters. Prove the following about \( S_n \):

- \( S_n \) is a group
- \( |S_n| = n! \)
- If \( m \leq n \), then \( S_m \) is a subgroup of \( S_n \)

Group Problems (no pun intended!)

Please work on the following problems in groups of 3 people. When a problem is solved, make sure everybody in your group understands it, and then tell the TA.

Identify the Groups

For each of the following sets and operations, decide whether or not they form a group. For those that don’t, state which of the axioms they violate. For those that are, state what the identity element is and whether they are abelian (commutative) or not.

Notation: \( M_n(F) \) denotes the set of all \( n \times n \) matrices with entries from \( F \).

1. \((\mathbb{Z}_6, +)\)
2. \((\mathbb{Z}_6, \cdot)\)
3. \((\mathbb{Z}_{13}, \cdot)\)
4. \((\mathbb{Q} - \{0\}, \cdot)\)
5. \((M_2(\mathbb{R}), +)\) (matrix addition)
6. \((M_2(\mathbb{R}), \cdot)\) (matrix multiplication)
7. \((\mathbb{N}, \clubsuit)\), where \( a \clubsuit b = a^b \) (define \( 0^0 = 1 \))

Coping with a Lossy TA

As a group, your task is to send a message (a 3-digit number given to you by the TA) to another group, using your TA as the communication channel. You will be given 4 notecards on which to write pieces of information. Note you can put at most one \((x, P(x))\) pair on each card. Make sure to put the name of some group member on each of your message cards.

Unfortunately, your TA is a busy person and may “accidentally” drop one of your message packets. You can, however, be sure that at least 3 of your 4 messages will get through.

When you have your 4 notecards ready, call over the TA and he will swap yours with another randomly chosen group’s. Try to decode the other group’s message and let your TA know when you’re done.