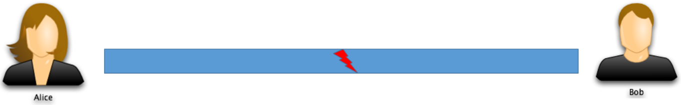
COL111: Discrete Mathematical Structures

Ragesh Jaiswal, CSE, IIT Delhi

Error Correcting Codes

Problem

Alice wants to send a sequence of integers $m_1, m_2, ..., m_n$ to Bob over a faulty communication channel that may *drop* at most k of the numbers sent by Alice. Assume that $\forall i, x_i \in \{0, 1, ..., q-1\}$ for some integer $q \geq n + k$. Suggest a method for Alice to communicate her message to Bob.



Problem

Alice wants to send a sequence of integers $m_1, m_2, ..., m_n$ to Bob over a faulty communication channel that may *drop* at most k of the numbers sent by Alice. Assume that $\forall i, x_i \in \{0, 1, ..., q-1\}$ for some integer $q \geq n + k$. Suggest a method for Alice to communicate her message to Bob.

- Let $n = 4, k = 2,\ q = 7$.
- Let $m_1 = 3,\ m_2 = 1,\ m_3 = 5,\ m_4 = 0$. So, Alice wants to send the message $3|1|5|0$.

- Let $n = 4, k = 2, q = 7$.
- Let $m_1 = 3,\ m_2 = 1,\ m_3 = 5,\ m_4 = 0$. So, Alice wants to send the message $3|1|5|0$.

- Idea using polynomials:
  - Claim 1: Alice can find the unique univariate polynomial $P(.)$ of degree $(n-1)$ with coefficients in $\{0, 1, ..., q-1\}$ s.t.
    - $P(1)\ (mod\ q) = m_1$,
    - $P(2)\ (mod\ q) = m_2$,
    - $P(3)\ (mod\ q) = m_3$,
    - $P(4)\ (mod\ q) = m_4$.

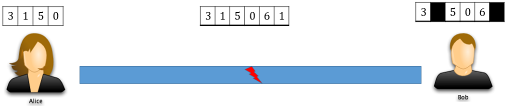
- Let $n = 4$, $k = 2$, $q = 7$.
- Let $m_1 = 3$, $m_2 = 1$, $m_3 = 5$, $m_4 = 0$. So, Alice wants to send the message $3|1|5|0$.

- Idea using polynomials:
  - Claim 1: Alice can find the unique univariate polynomial $P(.)$ of degree $(n-1)$ with coefficients in $\{0, 1, ..., q-1\}$ s.t.
    - $P(1) \ (mod\ q) = m_1$, $P(2) \ (mod\ q) = m_2$, $P(3) \ (mod\ q) = m_3$, $P(4) \ (mod\ q) = m_4$.
    - $P(x) = x^3 + 4x^2 + 5$ is such a polynomial.

- Let $n = 4$, $k = 2$, $q = 7$.
- Let $m_1 = 3$, $m_2 = 1$, $m_3 = 5$, $m_4 = 0$. So, Alice wants to send the message $3|1|5|0$.

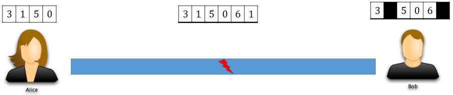
- Idea using polynomials:
  - Claim 1: Alice can find the unique univariate polynomial $P(.)$ of degree $(n-1)$ with coefficients in $\{0, 1, ..., q-1\}$ s.t.
    - $P(1) \ (mod\ q) = m_1$, $P(2) \ (mod\ q) = m_2$, $P(3) \ (mod\ q) = m_3$, $P(4) \ (mod\ q) = m_4$.
    - $P(x) = x^3 + 4x^2 + 5$ is such a polynomial.
  - Alice sends $P(1) \ (mod\ q)|P(2) \ (mod\ q)|P(3) \ (mod\ q)|P(4) \ (mod\ q)|P(5) \ (mod\ q)|P(6) \ (mod\ q)$ to Bob.
    - So, Alice sends $3|1|5|0|6|1$ to Bob.

- Let $n = 4, k = 2,\ q = 7$.
- Let $m_1 = 3,\ m_2 = 1,\ m_3 = 5,\ m_4 = 0$. So, Alice wants to send the message $3|1|5|0$.



- Idea using polynomials:
  - Claim 1: Alice can find the unique univariate polynomial $P(.)$ of degree $(n-1)$ with coefficients in $\{0, 1, ..., q-1\}$ s.t.
    - $P(1) \ (mod\ q) = m_1,\ P(2) \ (mod\ q) = m_2,\ P(3) \ (mod\ q) = m_3,\ P(4) \ (mod\ q) = m_4$.
    - $P(x) = x^3 + 4x^2 + 5$ is such a polynomial.
  - Alice sends $P(1) \ (mod\ q)|P(2) \ (mod\ q)|P(3) \ (mod\ q)|P(4) \ (mod\ q)|P(5) \ (mod\ q)|P(6) \ (mod\ q)$ to Bob.
    - So, Alice sends $3|1|5|0|6|1$ to Bob.
  - Claim 2: Even if any two messages are dropped, Bob can figure out the message that Alice wanted to communicate.

- Let $n = 4, k = 2, q = 7$.
- Let $m_1 = 3, m_2 = 1, m_3 = 5, m_4 = 0$. So, Alice wants to send the message 3|1|5|0.



- Idea using polynomials:
  - Claim 1: Alice can find the unique univariate polynomial $P(.)$ of degree $(n-1)$ with coefficients in $\{0, 1, ..., q-1\}$ s.t.
    - $P(1) \ (mod\ q) = m_1$, $P(2) \ (mod\ q) = m_2$, $P(3) \ (mod\ q) = m_3$, $P(4) \ (mod\ q) = m_4$.
    - $P(x) = x^3 + 4x^2 + 5$ is such a polynomial.
  - Alice sends $P(1) \ (mod\ q)|P(2) \ (mod\ q)|P(3) \ (mod\ q)|P(4) \ (mod\ q)|P(5) \ (mod\ q)|P(6) \ (mod\ q)$ to Bob.
    - So, Alice sends 3|1|5|0|6|1 to Bob.
  - Claim 2: Even if any two messages are dropped, Bob can figure out the message that Alice wanted to communicate.
    - In the above case, Bob finds the unique polynomial $Q(.)$ s.t. $Q(1) \ (mod\ q) = 3$, $Q(3) \ (mod\ q) = 5$, $Q(4) \ (mod\ q) = 0$, $Q(5) \ (mod\ q) = 6$ and then outputs $Q(1) \ (mod\ q)|Q(2) \ (mod\ q)|Q(3) \ (mod\ q)|Q(4) \ (mod\ q)$.

Polynomials

Properties of Polynomials

- A univariate (one variable) polynomial of degree d is of the form $p(x) = a_d x^{d-1} + a_{d-1} x^{d-1} + ... + a_0$, where x and *coefficients* a_i's are real numbers.
- A real number a is said to be a *root* of a polynomial $p(x)$ iff $p(a) = 0$.

Properties of Polynomials

- A univariate (one variable) polynomial of degree d is of the form $p(x) = a_d x^{d-1} + a_{d-1} x^{d-1} + ... + a_0$, where x and *coefficients* a_i's are real numbers.
- A real number a is said to be a *root* of a polynomial $p(x)$ iff $p(a) = 0$.

Theorem

A non-zero polynomial of degree d has at most d roots.

Properties of Polynomials

- A univariate (one variable) polynomial of degree d is of the form $p(x) = a_d x^{d-1} + a_{d-1} x^{d-1} + ... + a_0$, where x and *coefficients* a_i's are real numbers.
- A real number a is said to be a *root* of a polynomial $p(x)$ iff $p(a) = 0$.

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

Properties of Polynomials

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

Proof.

- Find a polynomial $p(x) = a_d x^d + a_{d-1} x^{d-1} + ... + a_0$ such that $p(x_i) = y_i$ for all i.
- This can be done by solving the following system:

$$\begin{pmatrix} x_1^d & x_1^{d-1} & \dots & x_1 & 1 \\ x_2^d & x_2^{d-1} & \dots & x_2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{d+1}^d & x_{d+1}^{d-1} & \dots & x_{d+1} & 1 \end{pmatrix} \times \begin{pmatrix} a_d \\ a_{d-1} \\ \vdots \\ a_0 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{d+1} \end{pmatrix}$$

Properties of Polynomials

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ $(x_i \neq x_j$ for $i \neq j)$, there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

Proof.

- Find a polynomial $p(x) = a_d x^d + a_{d-1} x^{d-1} + ... + a_0$ such that $p(x_i) = y_i$ for all i.
- This can be done by solving the following system:

$$\begin{pmatrix} x_1^d & x_1^{d-1} & \dots & x_1 & 1 \\ x_2^d & x_2^{d-1} & \dots & x_2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{d+1}^d & x_{d+1}^{d-1} & \dots & x_{d+1} & 1 \end{pmatrix} \times \begin{pmatrix} a_d \\ a_{d-1} \\ \vdots \\ a_0 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{d+1} \end{pmatrix}$$

- Is the above matrix invertible?

Properties of Polynomials

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

Proof.

- Find a polynomial $p(x) = a_d x^d + a_{d-1} x^{d-1} + ... + a_0$ such that $p(x_i) = y_i$ for all i.
- This can be done by solving the following system:

$$\begin{pmatrix} x_1^d & x_1^{d-1} & \dots & x_1 & 1 \\ x_2^d & x_2^{d-1} & \dots & x_2 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{d+1}^d & x_{d+1}^{d-1} & \dots & x_{d+1} & 1 \end{pmatrix} \times \begin{pmatrix} a_d \\ a_{d-1} \\ \vdots \\ a_0 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{d+1} \end{pmatrix}$$

- Is the above matrix invertible?
  - Yes, since the determinant $(= \prod_{i>j}(x_i - x_j))$ is non-zero as long as $x_1, x_2, ..., x_{d+1}$ are distinct.
- What about uniqueness?
  - Suppose there is another polynomial $q(x) \neq p(x)$ such that $\forall i, q(x_i) = y_i$. But then $r(x) = p(x) - q(x)$ is a degree d polynomial with $d+1$ roots.

$\square$

Properties of Polynomials

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- For all i define the polynomial $\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}$.
- Claim: The unique degree d polynomial in the above theorem is given by $p(x) = \sum_i y_i \cdot \Delta_i(x)$.

Properties of Polynomials

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- For all i define the polynomial $\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}$.
- Claim: The unique degree d polynomial in the above theorem is given by $p(x) = \sum_i y_i \cdot \Delta_i(x)$.
  - Suppose we are given $(1, 3), (2, 1), (3, 5), (4, 0)$, then the degree 3 polynomial that "fits" these pairs is given by:

$$
\begin{aligned}
p(x) \quad = \quad & \frac{3(x-2)(x-3)(x-4)}{(1-2)(1-3)(1-4)} + \frac{1(x-1)(x-3)(x-4)}{(2-1)(2-3)(2-4)} + \\
& \frac{5(x-1)(x-2)(x-4)}{(3-1)(3-2)(3-4)} + \frac{0(x-1)(x-2)(x-3)}{(4-1)(4-2)(4-3)}
\end{aligned}
$$

Properties of Polynomials

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- For all i define the polynomial $\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}$.
- Claim: The unique degree d polynomial in the above theorem is given by $p(x) = \sum_i y_i \cdot \Delta_i(x)$.
    - Suppose we are given $(1,3), (2,1), (3,5), (4,0)$, then the degree 3 polynomial that "fits" these pairs is given by:

$$p(x) = \frac{(x-2)(x-3)(x-4)}{-2} + \frac{(x-1)(x-3)(x-4)}{2} + \frac{5(x-1)(x-2)(x-4)}{-2}.$$

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- For all i define the polynomial $\Delta_i(x) = \frac{\prod_{j \neq i}(x - x_j)}{\prod_{j \neq i}(x_i - x_j)}$.
- Claim: The unique degree d polynomial in the above theorem is given by $p(x) = \sum_i y_i \cdot \Delta_i(x)$.
- This method of "fitting" a polynomial is known as *Lagrange interpolation*.

Properties of Polynomials

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- Do both the above theorems hold when the variable x and all coefficients are restricted to be real numbers?

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- Do both the above theorems hold when the variable x and all coefficients are restricted to be real numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be complex numbers?

Properties of Polynomials

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- Do both the above theorems hold when the variable x and all coefficients are restricted to be real numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be complex numbers? Yes.

Properties of Polynomials

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- Do both the above theorems hold when the variable x and all coefficients are restricted to be real numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be complex numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be rational numbers?

Properties of Polynomials

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- Do both the above theorems hold when the variable x and all coefficients are restricted to be real numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be complex numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be rational numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be integers?

Properties of Polynomials

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) = y_i$ for $1 \leq i \leq d+1$.

- Do both the above theorems hold when the variable x and all coefficients are restricted to be real numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be complex numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be rational numbers? Yes.
- Do both the above theorems hold when the variable x and all coefficients are restricted to be integers? No.

Properties of Polynomials

- Let $q > 1$ be some prime number.
- Consider polynomials where the variable x and coefficients can only take values from the set $\{0, ..., q-1\}$.
- All arithmetic operations are performed modulo q.

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) \pmod q = y_i$ for $1 \leq i \leq d+1$.

- Do the above theorems hold?

- Let $q > 1$ be some prime number.
- Consider polynomials where the variable x and coefficients can only take values from the set $\{0, ..., q-1\}$.
- All arithmetic operations are performed modulo q.

Theorem

A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) \pmod{q} = y_i$ for $1 \leq i \leq d+1$.

- Do the above theorems hold? Yes.
- Where did we use the fact that q is a prime number?

Properties of Polynomials

- Let $q > 1$ be some prime number.
- Consider polynomials where the variable x and coefficients can only take values from the set $\{0, ..., q-1\}$.
- All arithmetic operations are performed modulo q.

Theorem

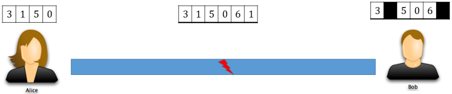
A non-zero polynomial of degree d has at most d roots.

Theorem

Given $(d+1)$ pairs $(x_1, y_1), (x_2, y_2), ..., (x_{d+1}, y_{d+1})$ ($x_i \neq x_j$ for $i \neq j$), there is a unique polynomial $p(x)$ of degree d such that $p(x_i) \pmod q = y_i$ for $1 \leq i \leq d+1$.

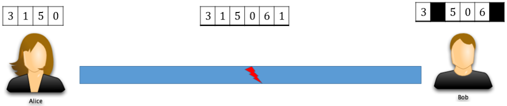
- Do the above theorems hold? Yes.
- Where did we use the fact that q is a prime number?
- The set $\{0, 1, ..., q-1\}$ for prime q along with addition and multiplication modulo q is something known as a *Finite Field*. This is useful in a lot of areas of computer science.

- Let $n = 4, k = 2, q = 7$.
- Let $m_1 = 3$, $m_2 = 1$, $m_3 = 5$, $m_4 = 0$. So, Alice wants to send the message $3|1|5|0$.



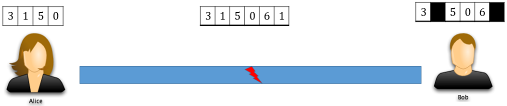
- Idea using polynomials:
  - Claim 1: Alice can find the unique univariate polynomial $P(.)$ of degree $(n-1)$ with coefficients in $\{0, 1, ..., q-1\}$ s.t.
    - $P(1) \ (mod\ q) = m_1$, $P(2) \ (mod\ q) = m_2$, $P(3) \ (mod\ q) = m_3$, $P(4) \ (mod\ q) = m_4$.
    - $P(x) = x^3 + 4x^2 + 5$ is such a polynomial.
  - Alice sends $P(1) \ (mod\ q)|P(2) \ (mod\ q)|P(3) \ (mod\ q)|P(4) \ (mod\ q)|P(5) \ (mod\ q)|P(6) \ (mod\ q)$ to Bob.
    - So, Alice sends $3|1|5|0|6|1$ to Bob.
  - Claim 2: Even if any two messages are dropped, Bob can figure out the message that Alice wanted to communicate.
    - In the above case, Bob finds the unique polynomial $Q(.)$ s.t. $Q(1) \ (mod\ q) = 3$, $Q(3) \ (mod\ q) = 5$, $Q(4) \ (mod\ q) = 0$, $Q(5) \ (mod\ q) = 6$ and then outputs $Q(1) \ (mod\ q)|Q(2) \ (mod\ q)|Q(3) \ (mod\ q)|Q(4) \ (mod\ q)$.

- Let $n = 4, k = 2,\ q = 7$.
- Let $m_1 = 3,\ m_2 = 1,\ m_3 = 5,\ m_4 = 0$. So, Alice wants to send the message $3|1|5|0$.



- Use Lagrange interpolation to determine the polynomial that Alice uses.
  - We know $P(1)\ (mod\ 7) = 3, P(2)\ (mod\ 7) = 1, P(3)\ (mod\ 7) = 5, P(4)\ (mod\ 7) = 0$.
  - $Q(x) = \frac{3\cdot(x-2)(x-3)(x-4)}{-6} + \frac{1\cdot(x-1)(x-3)(x-4)}{2} + \frac{5\cdot(x-1)(x-2)(x-4)}{-2}$
  - $Q(x) \equiv 3 \cdot (x-2)(x-3)(x-4) + 4 \cdot (x-1)(x-3)(x-4) + 1 \cdot (x-1)(x-2)(x-4)\ (mod\ 7)$.
  - $Q(x) \equiv (x^3 + 4x^2 + 5)\ (mod\ 7)$.
  - So, $P(x) = x^3 + 4x^2 + 5$.

- Let $n = 4, k = 2, q = 7$.
- Let $m_1 = 3,\ m_2 = 1,\ m_3 = 5,\ m_4 = 0$. So, Alice wants to send the message $3|1|5|0$.



- Use Lagrange interpolation to determine the polynomial that Alice uses.
- Use Lagrange interpolation to determine the polynomial that Bob reconstructs.

Secret Sharing

Secret Sharing

- Suppose there is a super secret key s and this key may be used to fire Nuclear missiles.
- You cannot entrust any single person with this key.
- Ideally, you would want to split this key s into n parts and give each part to a responsible person with the following two properties:
  - If any k (or more) people get together, then they can reconstruct the key s.
  - Less than k people cannot reconstruct s using their shares.

Secret Sharing

- Suppose there is a super secret key s and this key may be used to fire Nuclear missiles.
- You cannot entrust any single person with this key.
- Ideally, you would want to split this key s into n parts and give each part to a responsible person with the following two properties:
  - If any k (or more) people get together, then they can reconstruct the key s.
  - Less than k people cannot reconstruct s using their shares.
- Idea using (finite field) polynomials:
  - Pick a large prime $q >> s, n$.
  - Pick a random polynomial of degree $(k-1)$ such that $P(0) \ (mod \ q) = s$ and give $P(1) \ (mod \ q), P(2) \ (mod \ q), ..., P(n) \ (mod \ q)$ as shares to n people.

End