(More) Secret Sharing, Polynomials, and Error Correcting Codes

Motivation:
Recall we’re finding ways to share a secret S among n people such that any k of them can reconstruct S, but any coalition of k – 1 of them have absolutely no information about what S is.

Galois Fields:
Recall that the Galois Field \( GF_q \) is the set of numbers \( \forall x \in \mathbb{Z} : \{0 \leq z \leq q \} \) together with the operations \( \cdot \) (mod q) and \( + \) (mod q). In this lecture, we will work with polynomials over \( GF_q \).

Definition: \( r \) is a root of a polynomial \( \iff P(r) = 0 \)

Recall from the previous lecture:

Theorem: Over any field \( F \), any degree n polynomial has at most n roots. (The proof was given by induction over n.)

Theorem: Given a field with points \( (a_1, b_1), \ldots, (a_n, b_n) \), there is a unique polynomial \( P \) of degree \( n-1 \) such that: \( P(x) : \forall i P(a_i) = b_i \)

Example: Consider a polynomial of degree 2 over \( GF_2 \), where:

\[
P(1) = 2 \quad (2) = 4 \quad P(3) = 2
\]

\[
\Delta_1(x) = \frac{x-2}{1-2} : \frac{x-3}{1-3} \quad \Delta_2(x) = \frac{x-1}{2-1} : \frac{x-3}{2-3} \quad \Delta_3(x) = \frac{x-1}{3-1} : \frac{x-2}{3-2}
\]

\[
P(x) = 2\Delta_1(x) + 4\Delta_2(x) + 2\Delta_3(x)
\]

\[
\Delta_1(x) = \frac{(x-2)(x-3)}{2}
\]

\[
2^{-1} \pmod{7} = 2 \cdot 4 \pmod{7} \equiv \pmod{7}
\]

Properties of Polynomials:

- A polynomial of degree \( n \) has \( \leq n \) roots.
- \( n \) points define a unique polynomial of degree \( n - 1 \).

Exercise: Consider \( n \) points in a finite field \( GF_q \). How many polynomials of degree \( n \) pass through these points? 1, 2, \( q, n, \infty \)???
Points

How many degree \( n - 1 \) polynomials.

\[
\begin{array}{c|c}
 n & 1 \\
n - 1 & q \\
\end{array}
\]

This is because there are exactly \( q \) choices for the value of the polynomial at the \( n \)-th point. For each such choice, there is exactly one polynomial of degree \( n - 1 \).

\[
\begin{array}{c|c}
 n - k & q^k \\
\end{array}
\]

Back to Secret Sharing:

Given \( n \) people, how do we construct a system where:

- Any subset of \( k \) out of \( n \) can reconstruct \( s \), the secret.
- Any subset of \( k - 1 \) out of \( n \) knows nothing about \( s \).

Let \( q \) be a prime larger than \( n \) and \( s \). We will work over \( GF_q \). Let \( P \) be a random polynomial of degree \( k - 1 \) such that \( P(0) = s \). We can pick \( P \) either by picking its coefficients (other than the constant term, which is \( s \)) to be random elements of \( GF_q \), or by picking its values at \( 1, \ldots, k - 1 \) to be random elements of \( GF_q \):

\[
P(1) = r_1 \quad P(2) = r_2 \quad \ldots \quad P(k-1) = r_{k-1}
\]

Both methods result in a random polynomial from the same set.

Now each person \( i \), for \( 1 \leq i \leq n \), gets \( P(i) \).

- Any \( k \) players know \( P(x) \) at \( k \) points therefore it is possible to interpolate and uncover the secret polynomial \( P(x) \), evaluate it at \( P(0) = s \) revealing the secret code \( s \) hidden by the polynomial.

- Any \( k - 1 \) players have no information about \( s \), since their \( k - 1 \) values are consistent with any of the \( q \) possibilities for \( P(0) \) (there is a unique polynomial of degree \( k - 1 \) that goes through the \( k - 1 \) given points and this chosen value at 0). Therefore they have no information about the secret \( s \).

Why must the modulus of the field be prime?

Consider:

\[
(Z_{15}, +, \cdot) \quad x^2 = 1 \quad (mod \ 15)
\]

1, 4, 11, 14 are roots of the polynomial! More than 2 values is not good. \( q \), the modulus of the field (in this case \( q = 15 \), must be prime.