Secret Sharing, Finite Groups and Fields, and Polynomials

Motivation:
Suppose we have a nuclear bomb code: $S$, that is broken down into 6 pieces $S_1, S_2, \ldots, S_6$, given to 6 people. Each person has part of the code.

We want break the code $S$ into pieces such that any 5 people can reconstruct the original code $S$, but 4 people cannot reconstruct any information about $S$ (not even one bit of $S$).

In general we’re trying to devise a scheme where there are $n$ people that share part of a “secret”, and that if $k$ people combine their parts of the secret, they will arrive at the original secret. However we want the safeguard such that if $k-1$ people combine their parts of the secret, they will know absolutely nothing about the secret.

Groups:
We’ll need to take with a little detour through the basics of abstract algebra. You will be introduced to 2 “algebraic structures” groups, and fields.

A group is a non-empty set $X = \{a, b, c, \ldots\}$ together with a binary operation $\cdot : X \times X \rightarrow X$, such that the following are satisfied:

1. Closure: $\forall a, b \in X \ a \cdot b \in X$
2. Associative Law: $\forall a, b, c \in X \ a \cdot (b \cdot c) = (a \cdot b) \cdot c$
3. Identity: $\exists e \in X : \forall a \in X \ e \cdot a = a \cdot e = a$
4. Inverse: $\forall a \in X \ \exists a^{-1} \in X : a \cdot a^{-1} = a^{-1} \cdot a = e$

A group is called a commutative group or Abelian group if it satisfies the condition that $\forall a, b \in X \ a \cdot b = b \cdot a$.

Example:
Consider the integers $\mathbb{Z}$ with the binary operation $\cdot$. This is a group, with identity $0$, and the inverse of $i \in \mathbb{Z}$ is $-i$.

Similarly, the real numbers $\mathbb{R}$ with the binary operation $\cdot$ forms a group. The identity is $0$, and the inverse of $x \in \mathbb{R}$ is $-x$.

Both of these groups are commutative.

Example:
Consider the group $\mathbb{Z}_n$ which is the set of integers $(\mod n)$ together with the operator additon $(\mod n)$.

One can see this group satisfies:

1. Closure
2. Associative: $a + ((b + c) \mod n)(\mod n) \equiv (a + b \mod n) + c \mod n$
3. Identity 0
4. Inverse $x^{-1} = n - x$

Is this group commutative?

$$(a + b) \mod n \equiv (b + a) \mod n$$

Yes!

Example:

Consider the group: $\mathbb{Z}_n - \{0\} = 1, 2, \ldots, n - 1$ together with the operator $\cdot (\mod n)$.

If $n$ is prime, this group satisfies:

1. Closure $a \neq 0(\mod n) \land b \neq 0(\mod n) \land a \cdot b \neq 0(\mod n)$
2. Associative
3. Identity 1 (n is prime!)
4. Inverse $a \neq 0(\mod n)$, $n$ (prime!), $gcd(a, n) = 1 \rightarrow a^{-1}$ exists.

Now, is this group commutative ($n$ is still prime)? In other words can we show the following?

$a \cdot b(\mod n) = b \cdot a(\mod n)$ Yes!

But what happens if $n$ is not prime?

(1) Our operation over the set $\mathbb{Z} - \{0\}$ is not closed. Consider the following:

$a \neq 0(\mod n) \land b \neq 0(\mod n)$

$a \cdot b(\mod n)$

$n = 6$

$a \equiv 2(\mod 6)$

$b \equiv 3(\mod 6)$

$a \cdot b \equiv 0(\mod 6)$

$6 \nmid 2$

$6 \nmid 3$ but

$6 \nmid 2 \cdot 3$

(4) We are not guaranteed an inverse for each member of the set $\mathbb{Z} - \{0\}$ as $\exists a : gcd(a, n) \neq 1$

Fields: A field $(X, +, \cdot)$ is a set $X$ together with 2 binary operations. A field must satisfy:

1. $(X, +)$ forms a commutative group, 0 is the identity.
2. $(X - \{0\}, \cdot)$ forms a commutative group, 1 the identity.
3. Distributive law: $a \cdot (b + c) = a \cdot b + a \cdot c$

Examples:
(\mathbb{Q}, +, \cdot)\) Rationals  
(\mathbb{Z}, +, \cdot)\) Integers, NOT a field! There is NO inverse \(a^{-1} \in \mathbb{Z}\) for multiplication.  
(\mathbb{R}, +, \cdot)\) Reals  
(\mathbb{C}, +, \cdot)\) Complex

However, these are infinite. How do we get to a finite field?  

**Finite Fields:** \((\mathbb{Z}_p, +, \cdot \mod p)\) where \(p\) is prime is a field. The fact that \((\mathbb{Z}_p, +, \cdot \mod p)\) are commutative groups was shown in the examples above, and the distributive law is easy to check.

The finite field \((\mathbb{Z}_p, +, \cdot \mod p)\) is also called a Galois Field, and denoted \(GF_p\), in honor of Evariste Galois (1811 - 32).

Fields are defined so that most of the standard properties we count on while adding and multiplying real numbers also hold over any field. For example the cancelation law:

\(ax = ay\) and \(a \neq 0\) implies that \(x = y\). We can cancel \(a\) from both sides because \(a^{-1}\) exists and so multiplying both sides by \(a^{-1}\), we get \(x = y\).

Since we can talk about multiplication and addition over a field, it makes sense to define polynomials over a field.

Consider a polynomial of degree \(d\):

\[P(x) = c_0 + c_1x + c_2x^2 + \cdots + c_dx^d\]  
over a field \(F\) where each \(c_i \in F\)

Recall that \(r \in F\) is a root of \(P(x)\) iff \(P(r) = 0\).

Let us prove that several familiar properties of polynomials continue to hold for polynomials over an arbitrary field \(F\):

1. A linear polynomial has at most 1 root, namely that of \(x \in F\): \(P(x) = 0\)
   
   Proof: \(P(x) = ax + b\) both \(a\) and \(b\) cannot be 0.
   
   Case \(a \neq 0\):  
   \[ax + b = 0 \iff ax = -b\]  
   \[\iff x = -b/a\]  
   Case \(a = 0\):  
   \[ax + b = 0 \iff b = 0\] Which is a contradiction!

2. Distinct linear polynomials (lines) agree (intersect) in at most one point:
   
   \[P_1(x) = a_1x + b_1\]  
   \[P_2(x) = a_2x + b_2\]  
   \[0 = P_1(x) - P_2 = a_1x + b_1 - (a_2x + b_2) = (a_1 - a_2)x + (b_1 - b_2)\]

Example:

Consider the two linear polynomials over \(GF_3\)

\[P(x) = 2x + 3\]  
\[P'(x) = 3x + 1\]

It is instructive to plot these two “lines” (they don’t look anything like lines in the plane), and to see that they intersect in the point \((2, 2)\).
**Theorem:** Over any field \( F \), any degree \( n \) polynomial has at most \( n \) roots.

The proof is by induction on \( n \), and is part of the next homework.

**Polynomial Interpolation:**

- 2 points determine a line of degree 1
- 3 points determine a unique degree 2 polynomial
- 
- \( \vdots \)
- \( n \) points determine a unique degree \( n-1 \) polynomial

**Theorem:** Consider \( F \), 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: \( P(a_i) = b_i \) for \( i = 1 \) to \( n \).

Proof: We shall show that there are polynomials, \( \Delta_i(x) \), of degree \( n-1 \), such that: \( \Delta_i(a_i) = 1 \), and for \( j \neq i \) \( \Delta_j(a_j) = 0 \). But then the polynomial \( P(x) = b_1\Delta_1(x) + b_2\Delta_2(x) + \cdots + b_n\Delta_n(x) \) has degree \( n-1 \), and satisfies the condition that \( P(a_i) = b_i \) for \( i = 1 \) to \( n \).

\[
\Delta_i(x) = \prod_{j\neq i} \frac{x-a_j}{a_i-a_j}
\]

Clearly the degree of this polynomial is \( n-1 \), and it is easy to check by direct substitution that \( \Delta(a_i) = 1 \), and for \( j \neq i \) \( \Delta_j(a_j) = 0 \).