CS4501 Cryptographic Protocols
Lecture 6: $\mathbb{F}_p$, Interpolation, Linearity

https://jackdoerner.net/teaching/#2026/Spring/CS4501

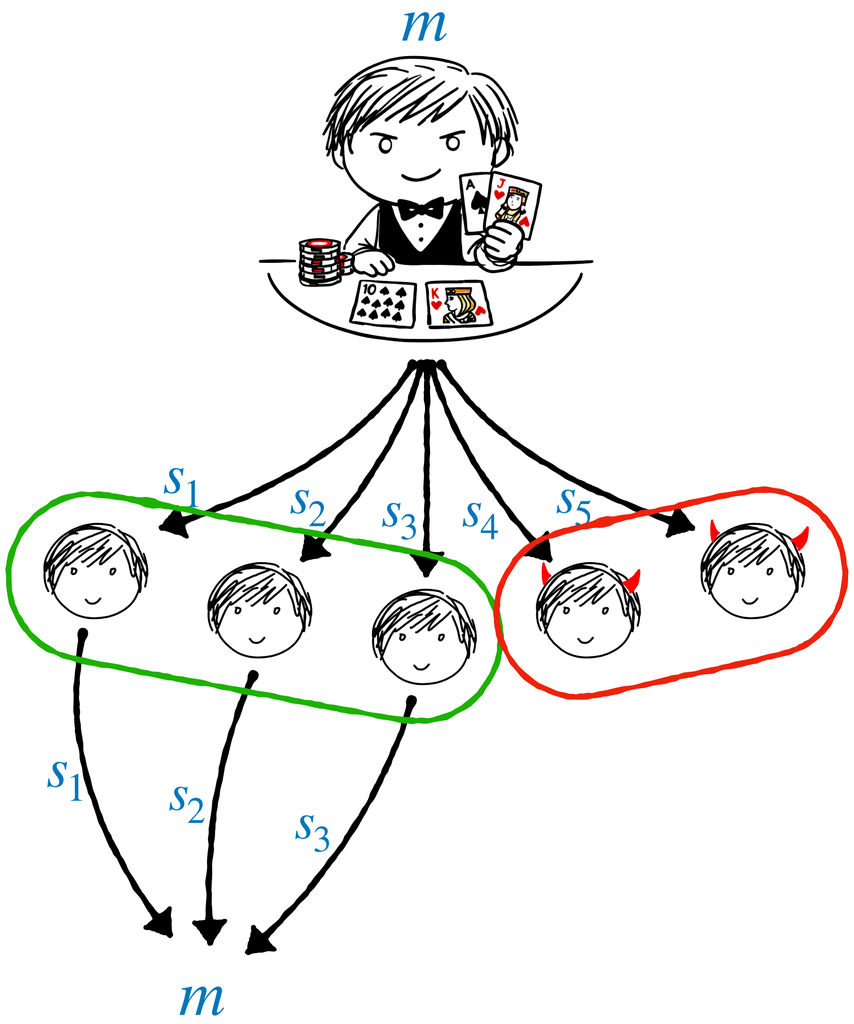
General Secret Sharing

The Setting:

- A dealer D holds a secret $m \in \mathcal{M}$.
- D wants to *share* m among n parties.
- D can communicate with each P_i over a private channel to send share s_i.
- *Authorized* subsets of parties can reconstruct m from their shares.

  The collection of all authorized sets is called the *access structure*, denoted Γ.
- *Unauthorized* subsets cannot learn any new information about m.

  The collection of all unauthorized sets is called the *forbidden structure*.



General Secret Sharing

Definition 1. Syntax for Secret Sharing

A *secret-sharing* scheme for access structure Γ over $\mathscr{P} = \{P_1, \ldots, P_n\}$ with message space $\mathscr{M}$ is a pair of algorithms $(\mathsf{Share}, \mathsf{Recon})$ such that:

- $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(m)$ samples n shares given a secret $m \in \mathscr{M}$.
- $m := \mathsf{Recon}\big((i_1, \ldots, i_k), \big(s_{i_1}, \ldots, s_{i_k}\big)\big)$ outputs the secret m if and only if it is given a set of shares $\big\{s_{i_1}, \ldots, s_{i_k}\big\}$ such that $\big\{P_{i_1}, \ldots, P_{i_k}\big\} \in \Gamma$.

Definition 2. Correctness for Secret Sharing

$\forall m \in \mathscr{M}$, if $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(m)$, then $\forall \{i_1, \ldots, i_k\} \subseteq [n]$ such that it $\big\{P_{i_1}, \ldots, P_{i_k}\big\} \in \Gamma$ it holds that $m = \mathsf{Recon}\big((i_1, \ldots, i_k), \big(s_{i_1}, \ldots, s_{i_k}\big)\big)$.

General Secret Sharing

Definition 2. Correctness for Secret Sharing

$\forall m \in \mathscr{M}$, if $(s_1, \ldots, s_n) \leftarrow \mathsf{Share}(m)$, then $\forall \{i_1, \ldots, i_k\} \subseteq [n]$ such that it $\left\{P_{i_1}, \ldots, P_{i_k}\right\} \in \Gamma$ it holds that $m = \mathsf{Recon}\left((i_1, \ldots, i_k), \left(s_{i_1}, \ldots, s_{i_k}\right)\right)$.

Definition 3. Perfect Privacy for Secret Sharing

$\forall m_1, m_2 \in \mathscr{M}$, $\forall \{i_1, \ldots, i_k\} \subseteq [n]$ such that it $\left\{P_{i_1}, \ldots, P_{i_k}\right\} \notin \Gamma$ it holds that $\left\{s_{i_1}, \ldots, s_{i_k} : (s_1, \ldots, s_n) \leftarrow \mathsf{Share}(m_1)\right\} \equiv \left\{s_{i_1}, \ldots, s_{i_k} : (s_1, \ldots, s_n) \leftarrow \mathsf{Share}(m_2)\right\}$.

Definition 4. Threshold Secret Sharing

A $(t+1)$-of-n *threshold secret sharing* (TSS) scheme is any secret sharing scheme where the access structure comprises all subsets of parties of size greater than t. In other words, a secret sharing scheme with $\Gamma = \{X \subseteq \mathscr{P} : |X| > t\}$.

The Simplest Case: n-of-n XOR sharing

- Consider $\mathcal{M} = \{0,1\}^\ell$ for some $\ell \in \mathbb{N}$.
- Share(m):
  1. Sample $s_1, \ldots, s_{n-1} \leftarrow \{0,1\}^\ell$.
  2. Compute $s_n := m \oplus s_1 \oplus \ldots \oplus s_{n-1}$.
  3. Output $(s_1, \ldots, s_n)$.
- Recon($s_1, \ldots, s_n$):
  1. Output $s_1 \oplus \ldots \oplus s_n$.

Note: if $\exists i \in [n]$ such that $\mathcal{A}$ does not know s_i,
then $\mathcal{A}$ does not have any information about m.

Note: $\forall i \in [n], |s_i| = |m|$. So collectively we store $n \cdot \ell$ bits.

$(t+1)$-of-n from $(t+1)$-of-$(t+1)$

Let t be the maximum number of corruptions.

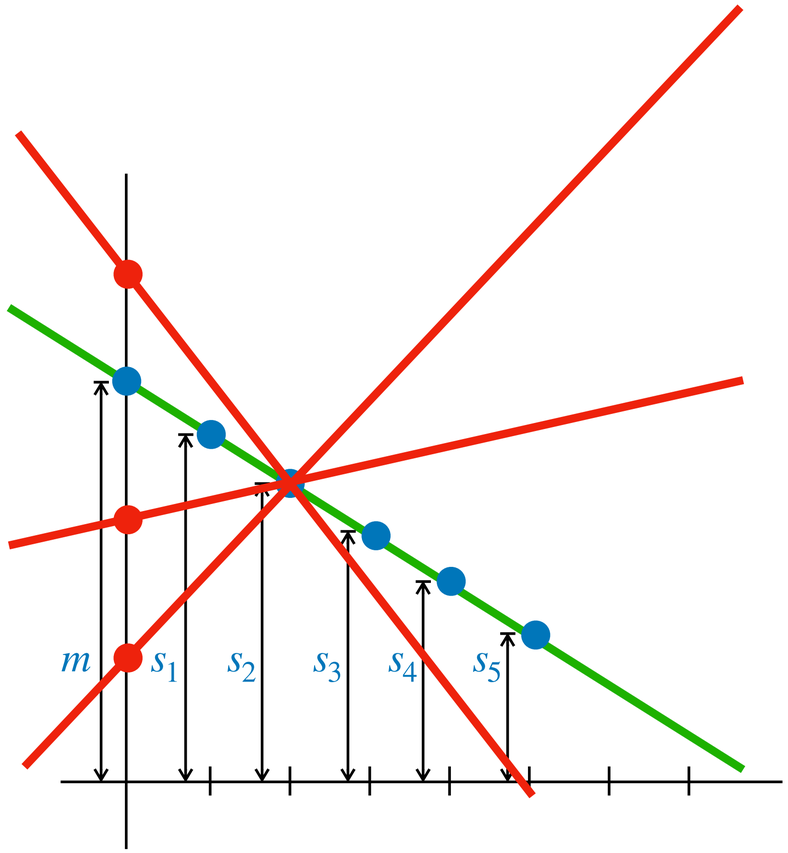
A Naïve Construction: for every size-$(t+1)$ subset of the parties, the Dealer secret-shares s to that subset using a $(t+1)$-of-$(t+1)$ secret sharing scheme.

Good News: correctness and privacy are trivially inherited.

Bad News: there are $\binom{n}{t+1}$ subsets. This is exponential when $t \approx n/2$.

2-of-n from Simple 2D Geometry

- Consider $\mathscr{M} = \mathbb{N}$
- Share(m):
  1. Find a random line that intersects the y-axis at m. I.e. let $f(x) = a \cdot x + m$ where a is random.
  2. Output $(s_1, \ldots, s_n)$ where $s_i = f(i) = i \cdot a + m$

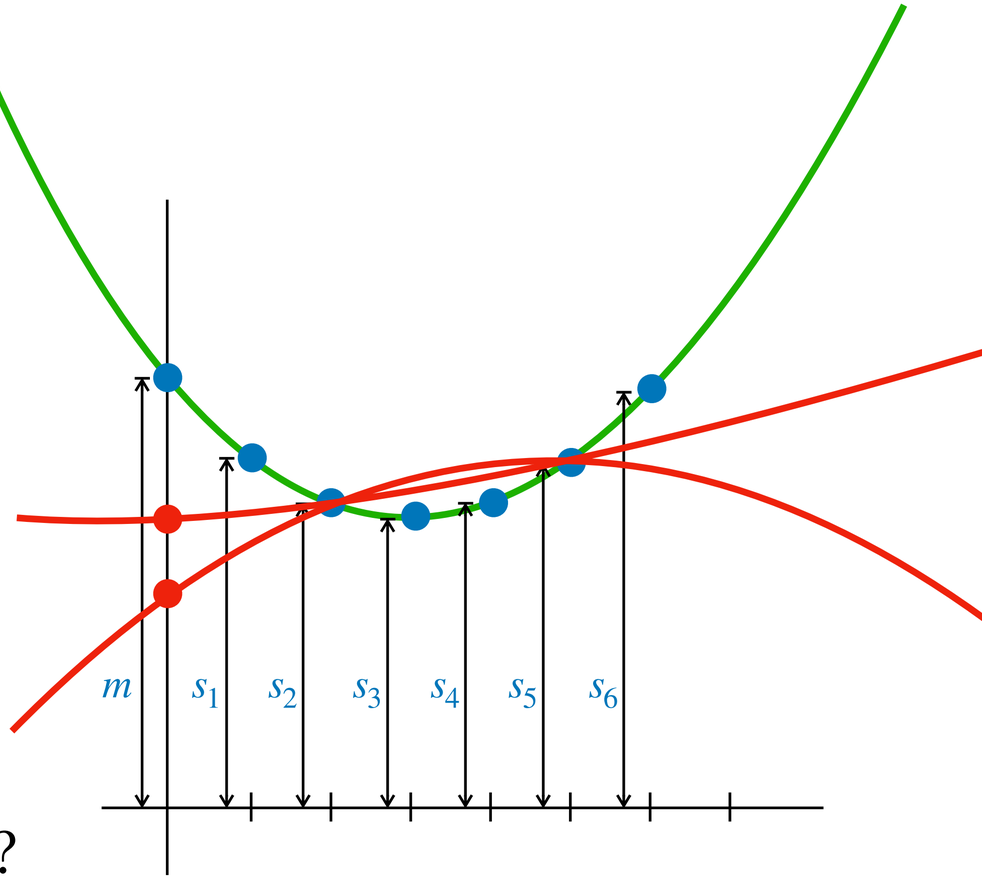


- Recon($(i, j), (s_i, s_j)$):
  1. Compute the slope $a := \dfrac{s_j - s_i}{j - i}$.
  2. Output the y-intercept $s_i - i \cdot a$.

Correctness: Every pair of shares completely determines m.
Security: Every single share is independent of m.

3-of-n from Simple 2D Geometry

- Consider $\mathscr{M} = \mathbb{N}$
- Share(m):
  1. Find a random parabola f that intersects the y-axis at $f(0) = m$.
  2. Output $(s_1, \ldots, s_n)$ where $s_i = f(i)\ \forall i \in [n]$.
- Recon($(i, j, k), (s_i, s_j, s_k)$):
  3. Interpolate $f(0)$.



Problem: how do we ensure all the shares are integers?

Deeper Problem: how do we choose a parabola "randomly." There are infinitely many parabolae and the uniform distribution is not well-defined over infinite domains.

3-of-n from Simple 2D Geometry

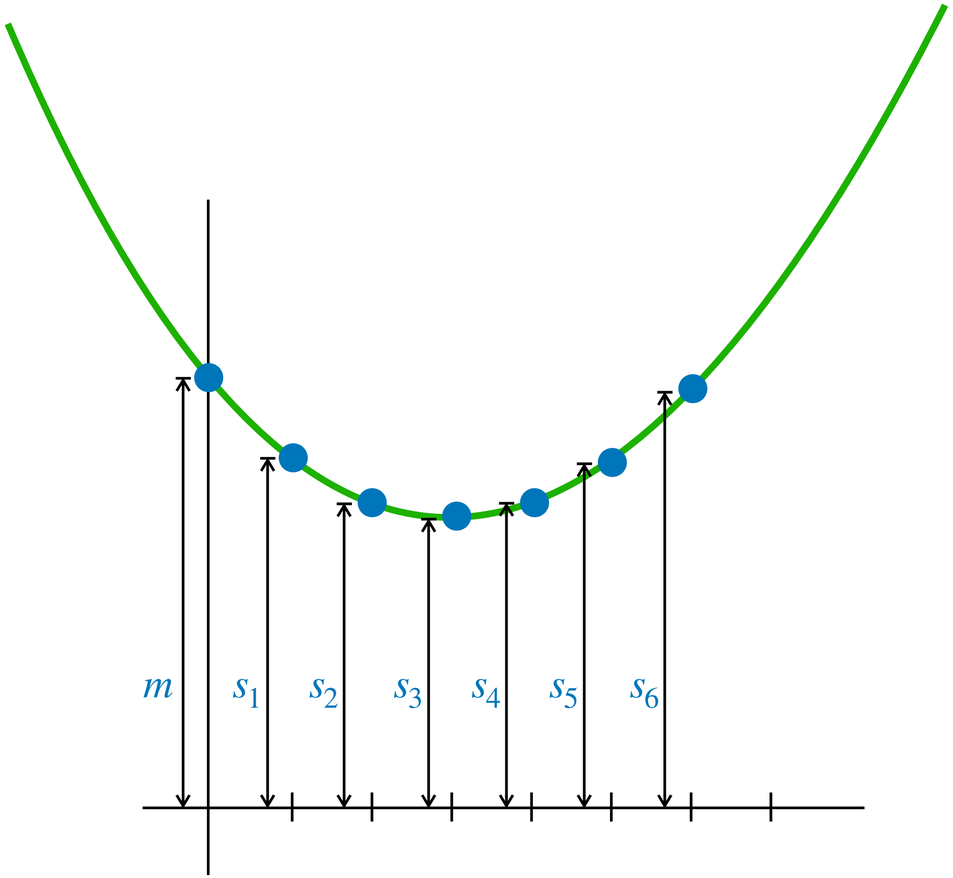
To fix this problem, we need to be able to compute polynomials over some finite domain.

This will guarantee that uniform distributions are well defined, and that shares can be encoded efficiently.

$\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$ don't work: they're all infinite.

We need a domain that supports addition and multiplication, and the inverses of those operations.

In order to identify such a domain, we have to introduce some ideas from abstract algebra.



We can Categorize by Axioms

Let $\mathbb{G}$ be a set and $\star : \mathbb{G} \times \mathbb{G} \to \mathbb{G}$ be a binary operation such that $\mathbb{G}$ is closed under $\star$.

Definition 5: $(\mathbb{G}, \star)$ is a *group* if and only if all of the following axioms hold:

1. Associativity: $\forall a, b, c \in \mathbb{G},\ a \star (b \star c) = (a \star b) \star c$.
2. Identity: there exists an identity element i such that $\forall a \in \mathbb{G}$ we have $i \star a = a \star i = a$.
3. Inverses: $\forall a \in \mathbb{G}\ \exists b \in \mathbb{G}$ such that $a \star b = i$.

Definition 6: $(\mathbb{G}, \star)$ is a *commutative (a.k.a. abelian) group* if it is a group, and:

4. Commutativity: $\forall a, b \in \mathbb{G}$ we have $a \star b = b \star a$.

Definition 7: the *order* of $(\mathbb{G}, \star)$ is the size of $\mathbb{G}$.

If a mathematical statement relies only on group axioms, it holds for *any* group.

Finite Groups (by Example)

Consider $(\mathbb{Z}_m, +)$ where $+$ is interpreted as addition modulo m.

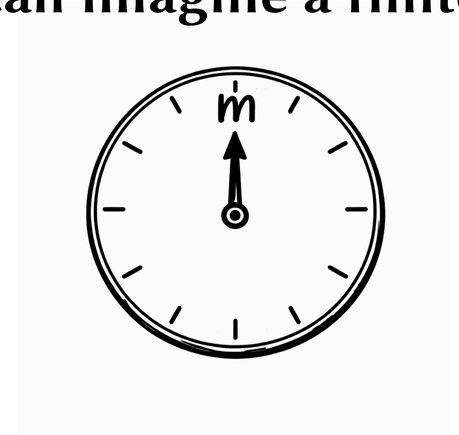
Closure: holds because the range of $\bmod m$ is $[0, m-1] = \mathbb{Z}_m$.

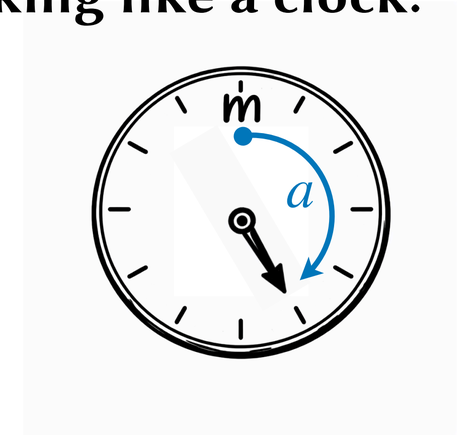
Associativity, Identity, Commutativity: the same as integer $+$ on $\mathbb{Z}$. Identity element is 0.

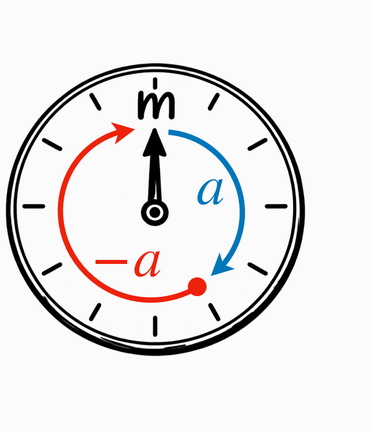
Inverses: Because $0 + 0 = 0$, the additive inverse of 0 is itself.
Notice that $m \bmod m = 0$. The additive inverse of $a \in \mathbb{Z}_m$ is a number $b \in \mathbb{Z}_m$ such that $(a + b) \bmod m = m \bmod m = 0$. Does $b \in \mathbb{Z}_m$ always exist? **Yes.**

We will refer to the additive inverse of a as "$-a$". Note that maybe $|a| \neq |-a|$!

You can imagine a finite group working like a clock:







We can Categorize by Axioms

Let $\mathbb{F}$ be a set and $+ : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ and $\cdot : \mathbb{F} \times \mathbb{F} \to \mathbb{F}$ be binary operations under which $\mathbb{F}$ is closed.

Definition 8: $(\mathbb{F}, +, \cdot)$ is a *field* if and only if all of the following conditions hold:

1. $(\mathbb{F}, +)$ is a commutative group. Let the additive identity be denoted 0.
2. $(\mathbb{F} \setminus \{0\}, \cdot)$ is a commutative group. Let the multiplicative identity be denoted 1.
3. Distributivity: $\forall a, b, c \in \mathbb{F}$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$.

Question: is $(\mathbb{Z}_4, +, \cdot)$ a field (ops are modular)? **No.** 2 has no multiplicative inverse.
is $(\mathbb{Z}_5, +, \cdot)$ a field (ops are modular)? **Yes.**

$$(1 \cdot 1) \bmod 5 = 1$$
$$(2 \cdot 3) \bmod 5 = 6 \bmod 5 = 1$$
$$(3 \cdot 2) \bmod 5 = 6 \bmod 5 = 1$$
$$(4 \cdot 4) \bmod 5 = 16 \bmod 5 = 1$$

Next Question: for what values of m is $(\mathbb{Z}_m, +, \cdot)$ a field?

(Chalkboard Proof)

A Few Notes

Notation: $\mathbb{F}_p$ denotes a field of order p, and $\mathbb{F}_p[x]$ denotes the set of all polynomials in the variable x with coefficients in $\mathbb{F}_p$. Unless otherwise specified, the operations for any field are denoted $+$ and $\cdot$.

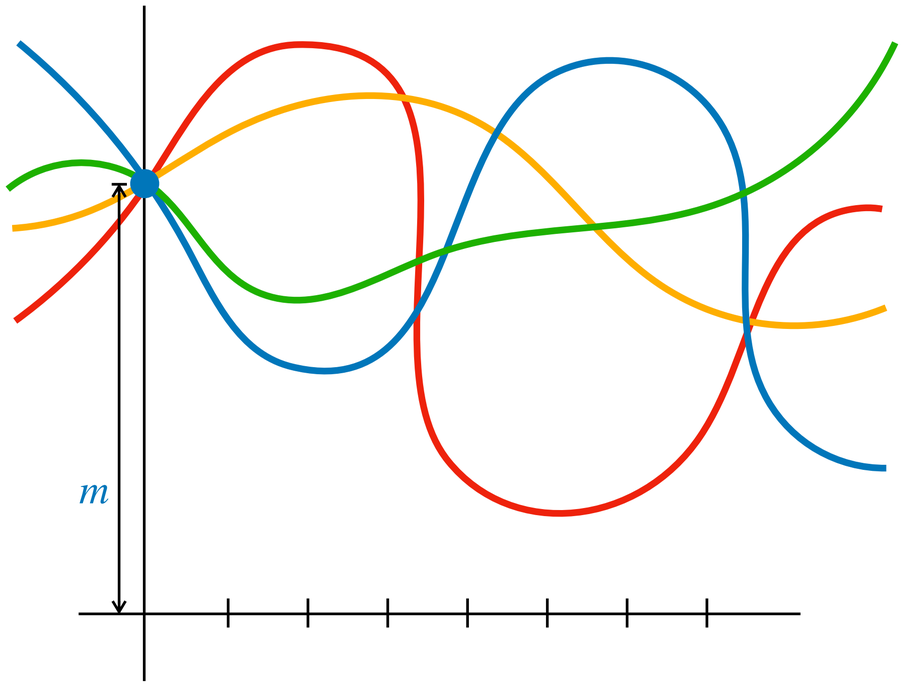
Note 1: for the rest of the semester I will use $\mathbb{F}_p$ and $\mathbb{Z}_p$ interchangeably if and only if p is prime. $\mathbb{Z}_m$ for some non-prime m is a *commutative ring*, which is like a field except that it lacks multiplicative inverses.

Note 2: is possible to construct a field of order p^k for any prime p and any $k \in \mathbb{N}$, but if $k \neq 1$ then the operations supported the field are *not* integer addition and multiplication. Nevertheless, anything you prove from field axioms holds for such fields!

Note 3: don't forget about groups! We will have more to say about them later in the course when we start introducing assumptions.

Polynomials over $\mathbb{F}_p$

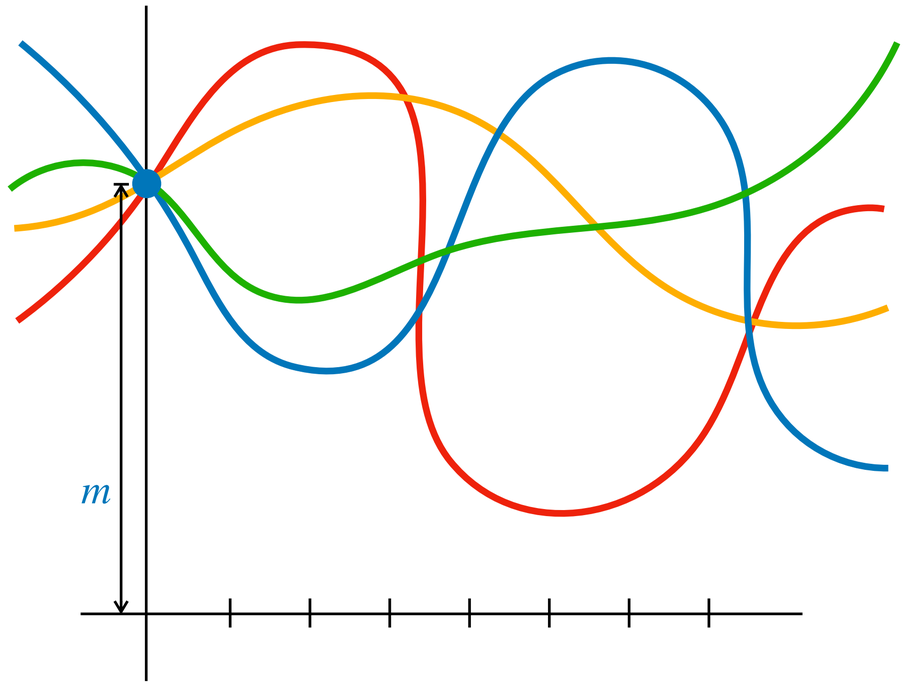
- Let $0 \leq t < p$ where p is a prime.
- Let $\mathscr{P}_{p,t,m} = \{f \in \mathbb{F}_p[x] : \deg(f) \leq t \wedge f(0) = m\}$.
- Every $f \in \mathscr{P}_{p,t,m}$ is of the form
  $f(x) = m + a_1 \cdot x + a_2 \cdot x^2 + \ldots + a_t \cdot x^t$.
  where $a_1, \ldots, a_t \in \mathbb{F}_p$.
- Thus $|\mathscr{P}_{p,t,m}| = |\mathbb{F}_p|^t = p^t$.



$t+1$ Points Determine $f \in \mathscr{P}_{p,t,m}$

- Last class we proved **Lecture 5, Theorem 1**: any set of $t+1$ points $(x_1, y_1), \ldots, (x_{t+1}, y_{t+1})$ with pairwise distinct x-coordinates define a unique polynomial.
- We only used field axioms in that proof, so it holds for $\mathbb{F}_p[x]$ too.

Corollary 1: let $x_1, \ldots, x_t \in \mathbb{F}_p \setminus \{0\}$ be pairwise distinct and let $y_1, \ldots, y_t \in \mathbb{F}_p$ and $m \in \mathbb{F}_p$. There exists exactly one $f \in \mathscr{P}_{p,t,m}$ such that $f(x_i) = y_i \ \forall i \in [t]$.

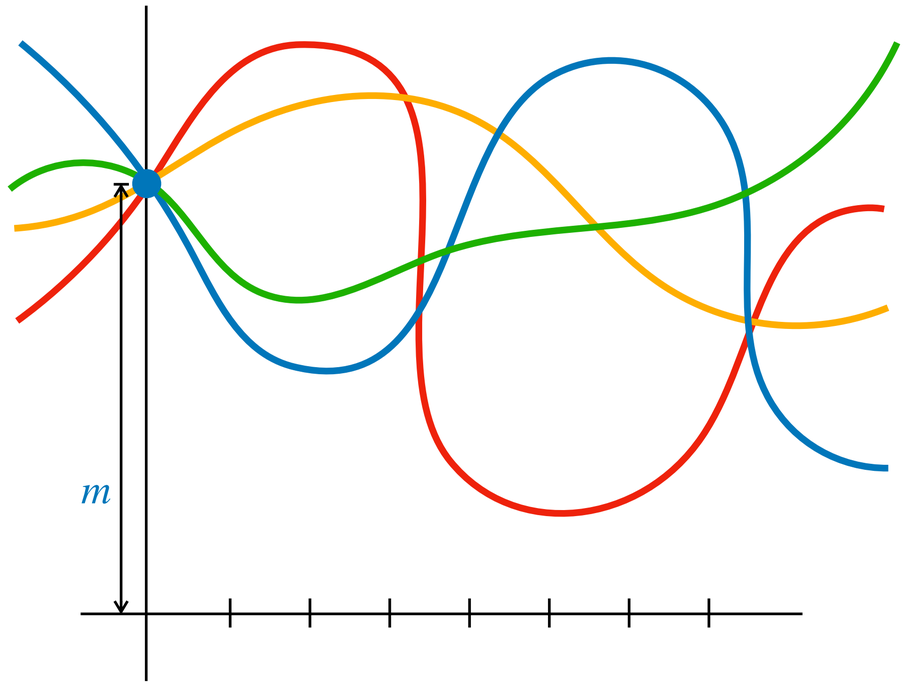


$t+1$ Points Determine $f \in \mathscr{P}_{p,t,m}$

Corollary 1: let $x_1, \ldots, x_t \in \mathbb{F}_p \setminus \{0\}$ be pairwise distinct and let $y_1, \ldots, y_t \in \mathbb{F}_p$ and $m \in \mathbb{F}_p$. There exists exactly one $f \in \mathscr{P}_{p,t,m}$ such that $f(x_i) = y_i \ \forall i \in [t]$.

Corollary 2: let $x_1, \ldots, x_t \in \mathbb{F}_p \setminus \{0\}$ be pairwise distinct and let $y_1, \ldots, y_t \in \mathbb{F}_p$. For every $m \in \mathbb{F}_p$,

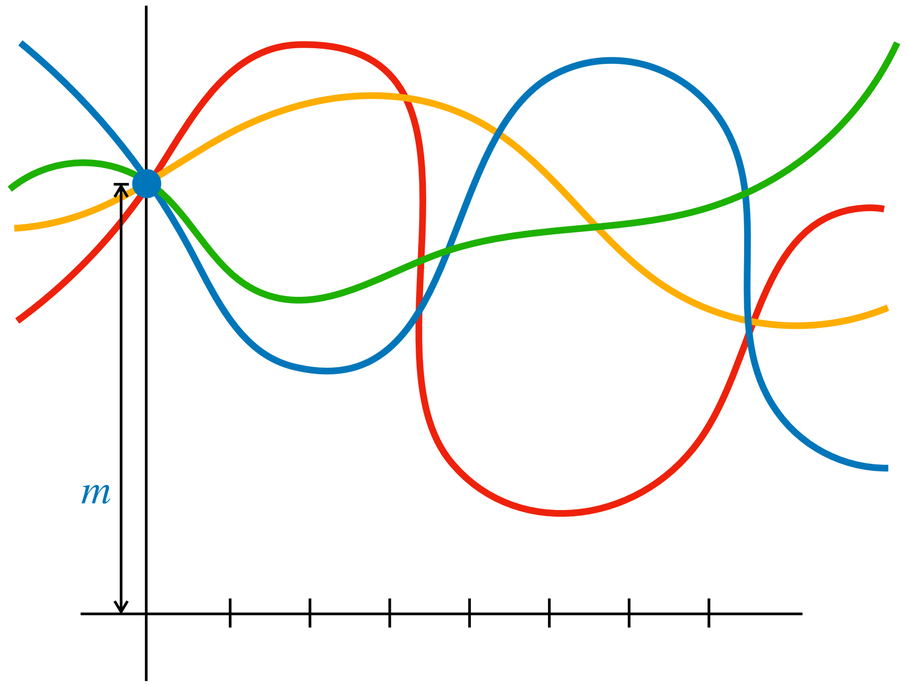
$$\Pr\left[\bigwedge_{i\in[t]} f(x_i) = y_i : f \leftarrow \mathscr{P}_{p,t,m}\right] = \frac{1}{|\mathscr{P}_{p,t,m}|} = p^{-t}.$$



t Points Leak Nothing About $f(0)$

Corollary 2: let $x_1, \ldots, x_t \in \mathbb{F}_p \setminus \{0\}$ be pairwise distinct and let $y_1, \ldots, y_t \in \mathbb{F}_p$. For every $m \in \mathbb{F}_p$,

$$\Pr\left[\bigwedge_{i\in[t]} f(x_i) = y_i : f \leftarrow \mathscr{P}_{p,t,m}\right] = \frac{1}{|\mathscr{P}_{p,t,m}|} = p^{-t}.$$



Corollary 3: let $x_1, \ldots, x_t \in \mathbb{F}_p \setminus \{0\}$ be pairwise distinct. For every $m \in \mathbb{F}_p$,

$$\left(f(x_1), \ldots, f(x_t) : f \leftarrow \mathscr{P}_{p,t,m}\right) \equiv (y_1, \ldots y_t) \leftarrow \mathbb{F}_p^t,$$

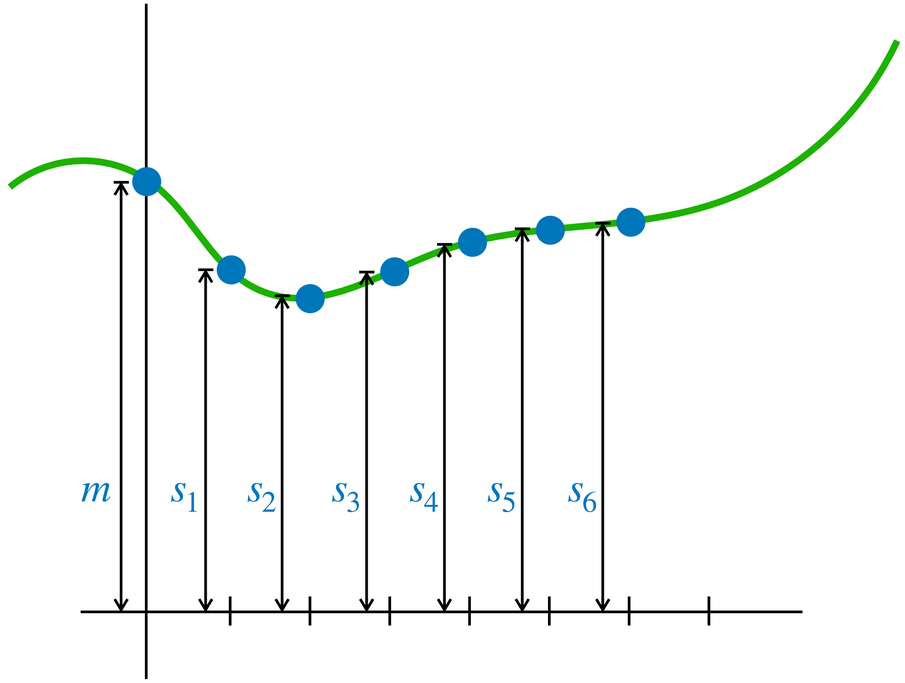
or in other words, the distribution of $y_1, \ldots, y_t \in \mathbb{F}_p$ is independent of m.

Note: this is like Shannon Secrecy.

Finally, $(t+1)$-of-n Shamir Sharing over $\mathbb{F}_p$

- Let $0 \leq t < n < p$ where t is the corruption limit, n is the number of parties, p is a prime, and let $\mathscr{M} = \mathbb{F}_p$
- $\mathsf{Share}_{p,n,t}(m)$:
  1. Sample $f \leftarrow \mathscr{P}_{p,t,m}$ uniformly (by sampling the coefficients of f uniformly from $\mathbb{F}_p$).
  2. Output $(s_1, \ldots, s_n)$ where $s_i = f(i)\ \forall i \in [n]$.
- $\mathsf{Recon}_{p,n,t}\big((i_1, \ldots, i_{t+1}), (s_{i_1}, \ldots, s_{i_{t+1}})\big)$:
  1. Interpolate $f(0) \in \mathbb{F}_p$.

How to do this, in general?

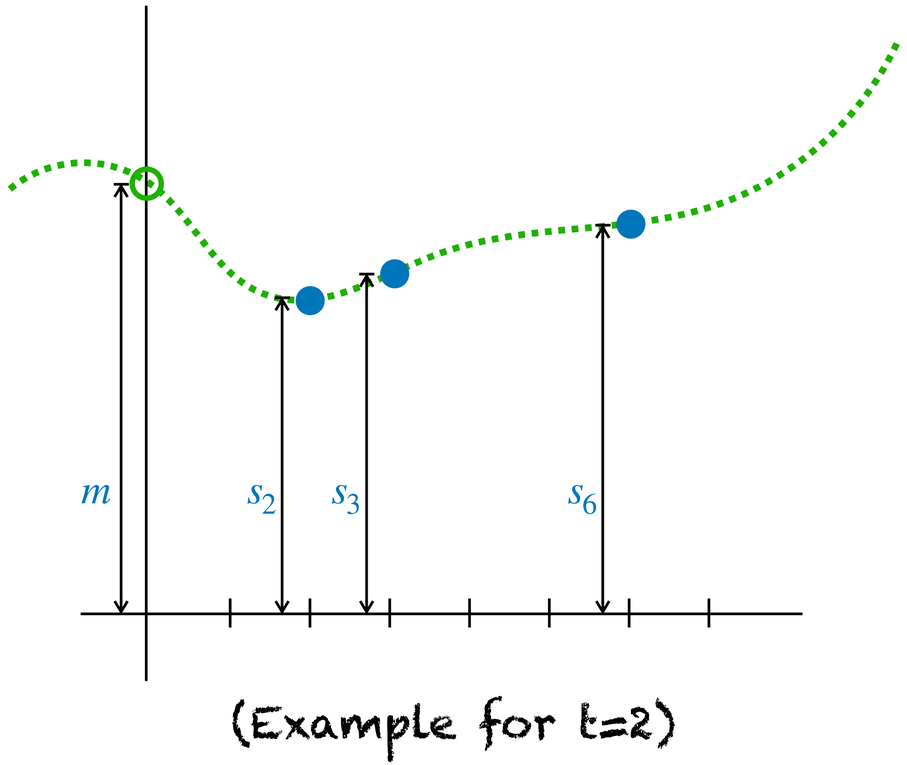


Interpolation: the Problem

- **Given:** pairwise distinct $(i_1, \ldots, i_{t+1}) \in \mathbb{F}_p^{t+1}$ and $\left(s_{i_1}, \ldots, s_{i_{t+1}}\right) \in \mathbb{F}_p^{t+1}$.
- **Find:** $f(x) = m + a_1 \cdot x + \ldots a_t \cdot x^t$ satisfying:

$$f(i_1) = m + a_1 \cdot i_1 + \ldots a_t \cdot i_1^t = s_{i_1}$$
$$f(i_2) = m + a_1 \cdot i_2 + \ldots a_t \cdot i_2^t = s_{i_2}$$
$$\ldots$$
$$f(i_{t+1}) = m + a_1 \cdot i_{t+1} + \ldots a_t \cdot i_{t+1}^t = s_{i_{t+1}}$$

This is a linear system with $t + 1$ equations and $t + 1$ variables, so...



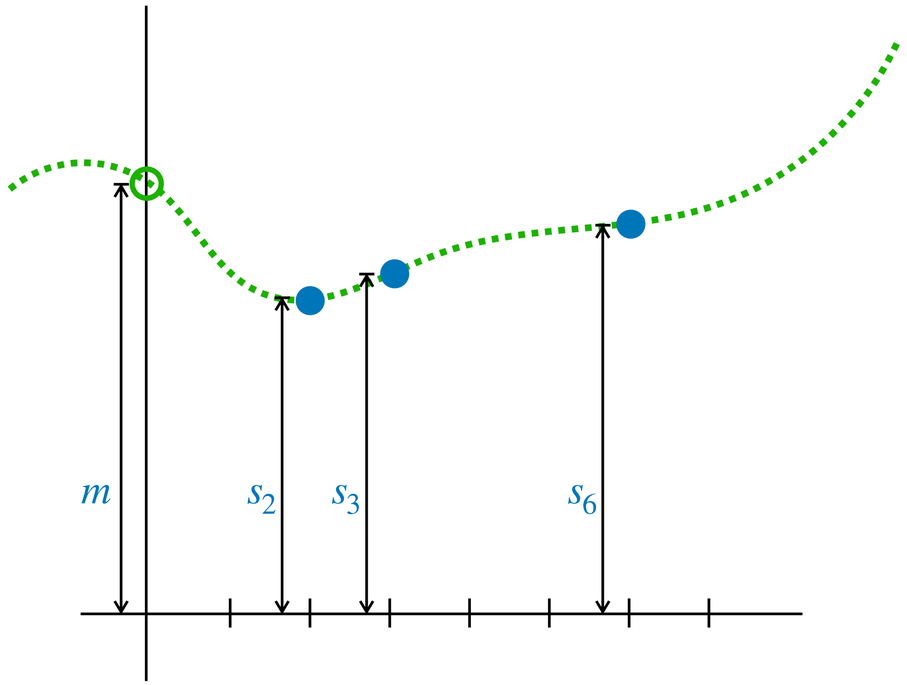
Interpolation: the Problem

- **Given:** pairwise distinct $(i_1, \ldots, i_{t+1}) \in \mathbb{F}_p^{t+1}$
  and $\left(s_{i_1}, \ldots, s_{i_{t+1}}\right) \in \mathbb{F}_p^{t+1}$.
- **Find:** $f(x) = m + a_1 \cdot x + \ldots a_t \cdot x^t$ satisfying:

$$\begin{bmatrix} 1 & i_1 & \cdots & i_1^t \\ \vdots & \vdots & \ddots & \vdots \\ 1 & i_{t+1} & \cdots & i_{t+1}^t \end{bmatrix} \begin{bmatrix} m \\ a_1 \\ \vdots \\ a_t \end{bmatrix} = \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{t+1} \end{bmatrix}$$

This is called a Vandermonde Matrix

It has determinant $\prod_{0 \le j < k \le t+1} (i_k - i_j) \neq 0$, therefore...



(Example for t=2)

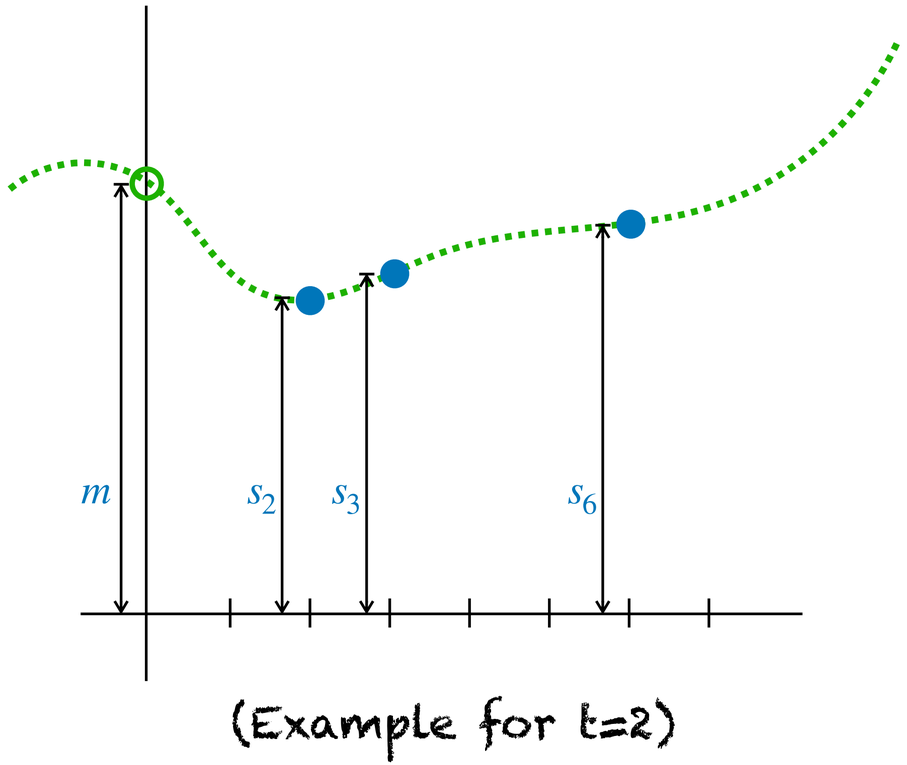
Interpolation: the Problem

- **Given:** pairwise distinct $(i_1, \ldots, i_{t+1}) \in \mathbb{F}_p^{t+1}$
  and $\left(s_{i_1}, \ldots, s_{i_{t+1}}\right) \in \mathbb{F}_p^{t+1}$.
- **Find:** $f(x) = m + a_1 \cdot x + \ldots a_t \cdot x^t$ satisfying:

$$\begin{bmatrix} m \\ a_1 \\ \vdots \\ a_t \end{bmatrix} = \begin{bmatrix} 1 & i_1 & \cdots & i_1^t \\ \vdots & \vdots & \ddots & \vdots \\ 1 & i_{t+1} & \cdots & i_{t+1}^t \end{bmatrix}^{-1} \begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_{t+1} \end{bmatrix}$$

... it is always invertible.

Let's turn this into an *interpolation* algorithm for directly recovering any point on the polynomial!



CS4501 Cryptographic Protocols
Lecture 6: $\mathbb{F}_p$, Interpolation, Linearity

https://jackdoerner.net/teaching/#2026/Spring/CS4501