CS4501 Cryptographic Protocols
Lecture 5: Secret Sharing, $\mathbb{G}$, $\mathbb{F}$

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

Protecting Secrets

The guarantee provided by encryption is a strong one: it ensures that a corrupted party who knows the ciphertext cannot recover the plaintext.

For now, this is because the ciphertext can decrypt to *any* plaintext, but later in the semester we will show that this can be true even if the ciphertext can only be decrypted to exactly one plaintext (i.e. if the person who knows the ciphertext has total information about the message).

But ultimately, the security encryption relies on keeping a key secret.

Protecting Secrets

Suppose that we are trying to securely compute (for example) $f(x_1, x_2, x_3) = (y, y, y)$ where $y = (x_1 + x_2) \cdot x_3$. First we need to compute a $x_1 + x_2$, but this is neither an input nor an output. It can't be revealed to anybody. If it's encrypted, *who will keep the secret key?*

What if we had a way to lock up the data with many keys?

Challenge: we need to make sure that the data *can't* be unlocked unless at least one honest party participates.

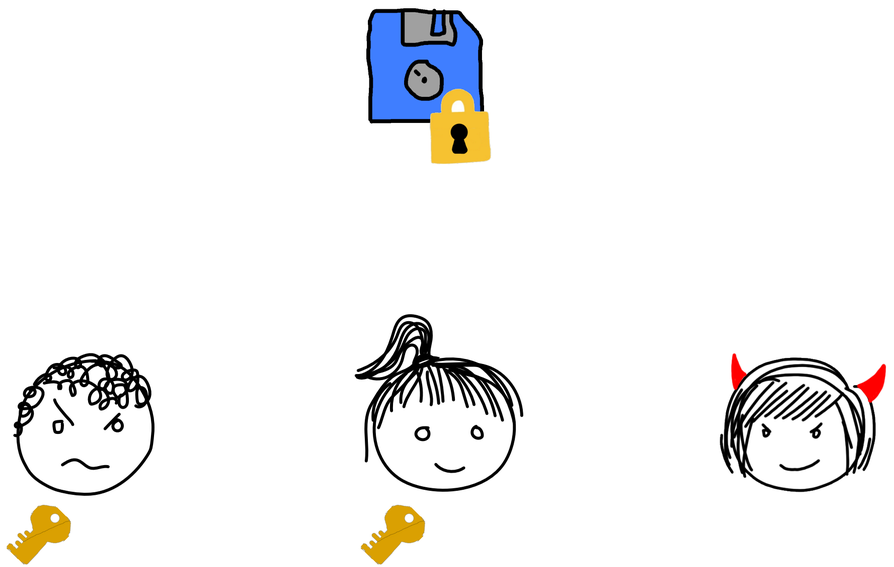
We also need to make sure that data *can* be unlocked when the honest parties agree that it should be, even if corrupted parties refuse to participate. (e.g. so that outputs can be revealed)

A Simple Solution

Suppose we have three parties, and we know at most one is corrupted (but not which).

Any two should be able to reveal the secret, but one by itself should not be able to.

We can imagine locking the data in a box. For every party P_i, there must be some lock for which P_i does not have a key, but the others (collectively) do.



A Simple Solution

Suppose we have three parties, and we know at most one is corrupted (but not which).

Any two should be able to reveal the secret, but one by itself should not be able to.

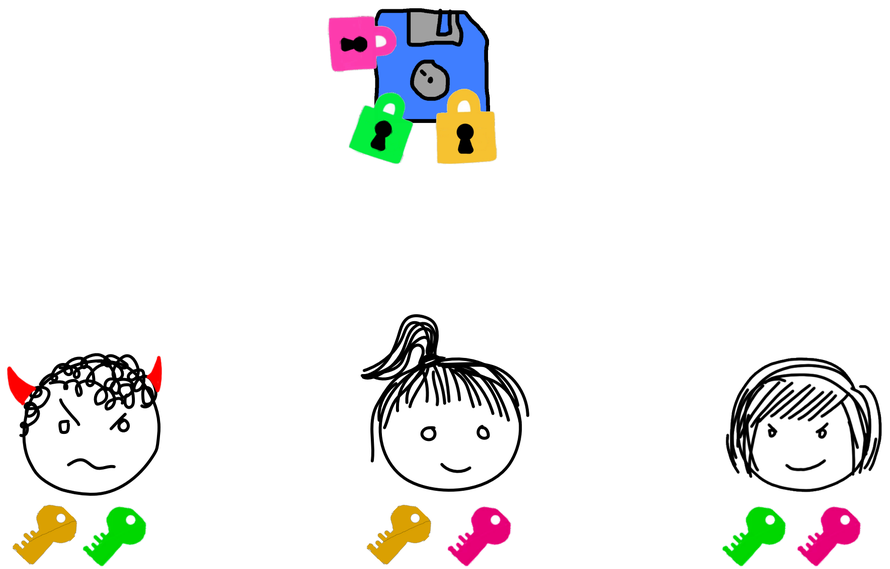
We can imagine locking the data in a box. For every party P_i, there must be some lock for which P_i does not have a key, but the others (collectively) do.

A Simple Solution

Suppose we have three parties, and we know at most one is corrupted (but not which).

Any two should be able to reveal the secret, but one by itself should not be able to.

We can imagine locking the data in a box. For every party P_i, there must be some lock for which P_i does not have a key, but the others (collectively) do.

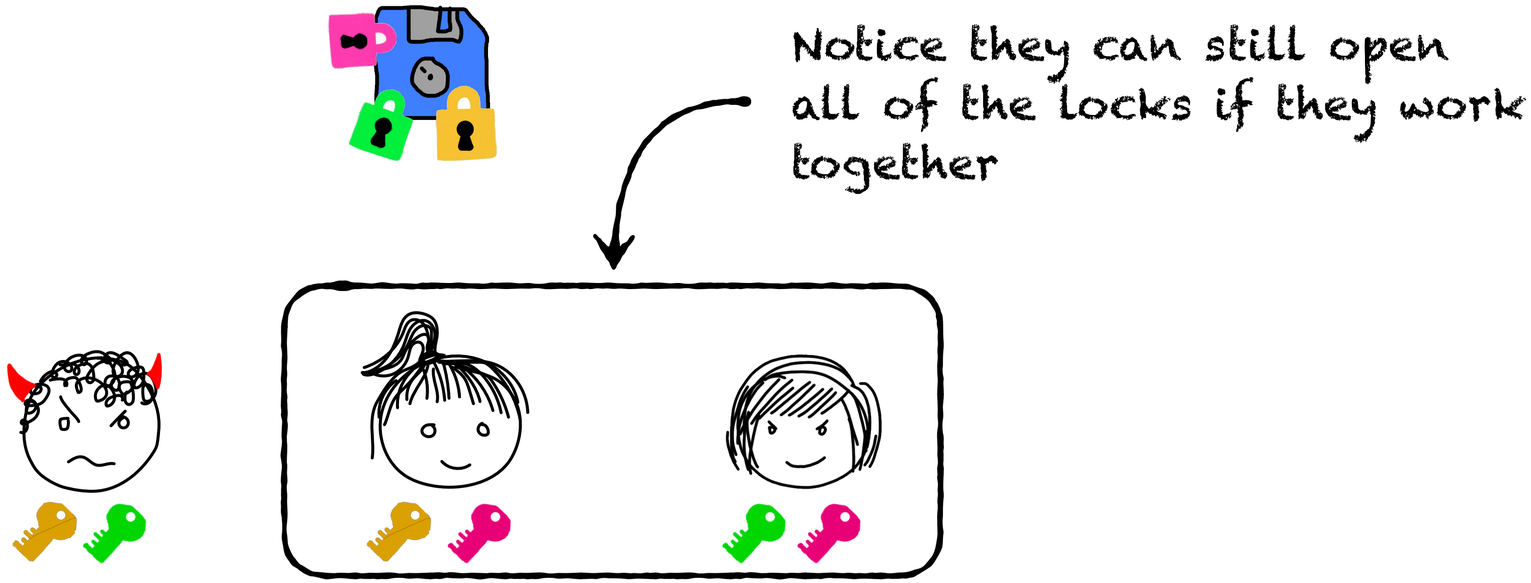


A Simple Solution

Suppose we have three parties, and we know at most one is corrupted (but not which).

Any two should be able to reveal the secret, but one by itself should not be able to.

We can imagine locking the data in a box. For every party P_i, there must be some lock for which P_i does not have a key, but the others (collectively) do.



Secret Sharing

1. Introduction

In [4], Liu considers the following problem:

> Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?

It is not hard to show that the minimal solution uses 462 locks and 252 keys per scientist. These numbers are clearly impractical, and they become exponentially worse when the number of scientists increases.

In this paper we generalize the problem to one in which the secret is some data D (e.g., the safe combina-

Somebody I know was recently asked to prove this “not hard minimal solution” on a quant trading firm hiring exam.

In 2002 Adi Shamir got a Turing award in part for proving that there is a better way if your secrets are numbers.

(Turing awards are very practical)

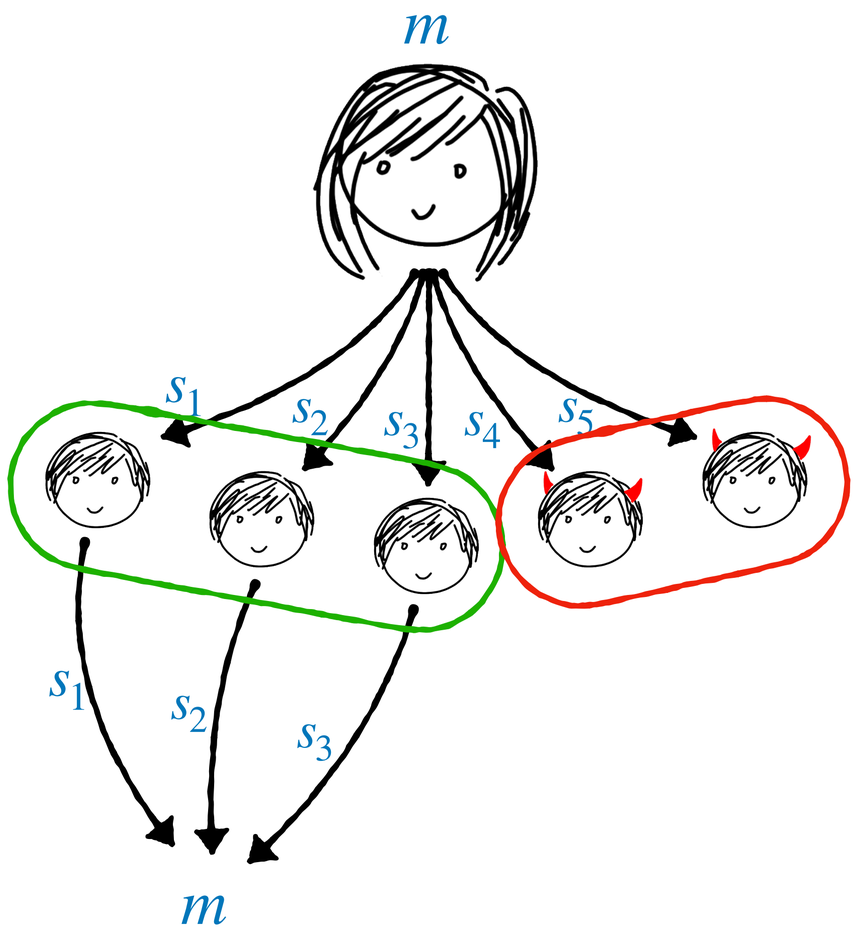
General Secret Sharing

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*.

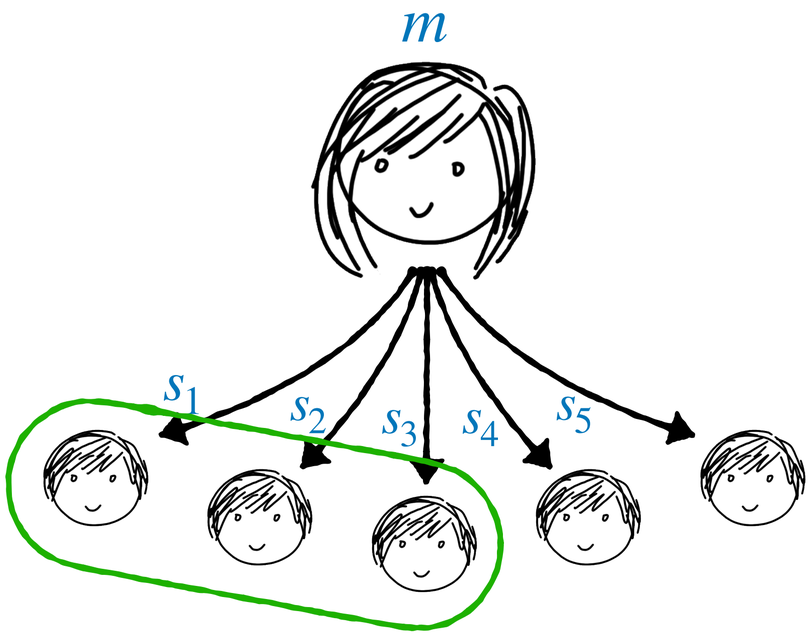


General Secret Sharing

For example:

- $n = 5$ with parties $\mathscr{P} = \{P_1, P_2, P_3, P_4, P_5\}$
- The following subsets can reconstruct:

  $X_1 = \{P_1, P_2, P_3\}$



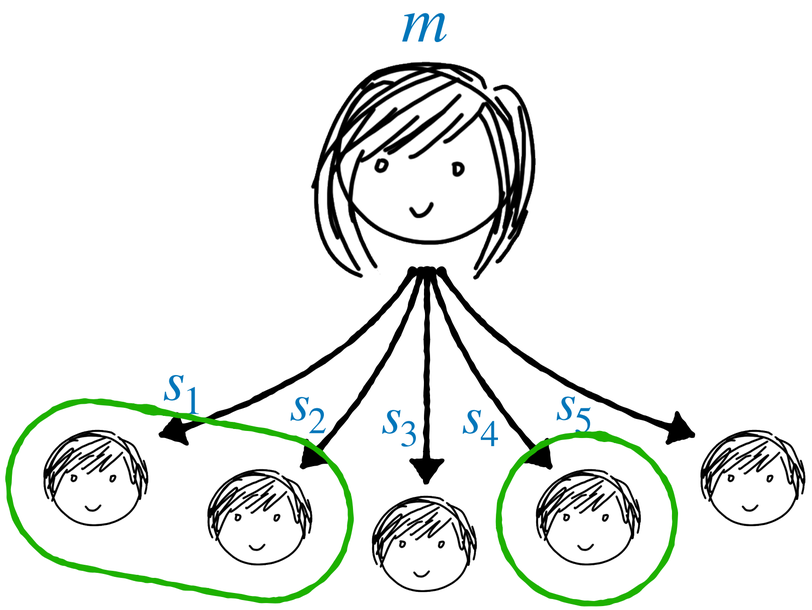
General Secret Sharing

For example:

- $n = 5$ with parties $\mathscr{P} = \{P_1, P_2, P_3, P_4, P_5\}$
- The following subsets can reconstruct:

  $X_1 = \{P_1, P_2, P_3\}$

  $X_2 = \{P_1, P_2, P_4\}$



General Secret Sharing

For example:

- $n = 5$ with parties $\mathscr{P} = \{P_1, P_2, P_3, P_4, P_5\}$
- The following subsets can reconstruct:

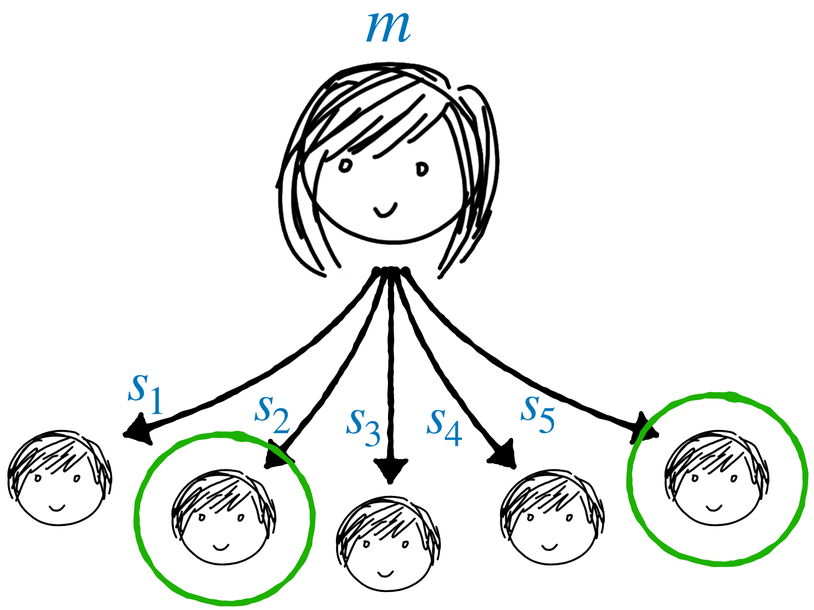
  $X_1 = \{P_1, P_2, P_3\}$

  $X_2 = \{P_1, P_2, P_4\}$

  $X_3 = \{P_2, P_5\}$

- The access structure is:

  $\Gamma = \{X \subseteq \mathscr{P} : \exists i \in [3] \text{ s.t. } X_i \subseteq X\}$



General Secret Sharing

For example:

- $n = 5$ with parties $\mathscr{P} = \{P_1, P_2, P_3, P_4, P_5\}$
- The following subsets can reconstruct:

  $X_1 = \{P_1, P_2, P_3\}$

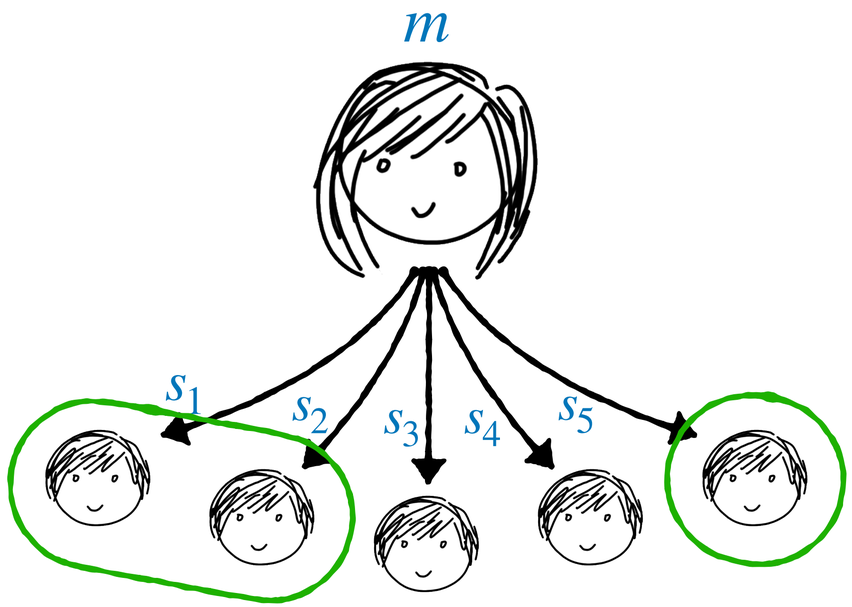
  $X_2 = \{P_1, P_2, P_4\}$

  $X_3 = \{P_2, P_5\}$

- The access structure is:

  $\Gamma = \{X \subseteq \mathscr{P} : \exists i \in [3] \text{ s.t. } X_i \subseteq X\}$

  For example, $\{P_1, P_2, P_5\} \in \Gamma$



General Secret Sharing

For example:

- $n = 5$ with parties $\mathscr{P} = \{P_1, P_2, P_3, P_4, P_5\}$
- The following subsets can reconstruct:

  $X_1 = \{P_1, P_2, P_3\}$

  $X_2 = \{P_1, P_2, P_4\}$

  $X_3 = \{P_2, P_5\}$

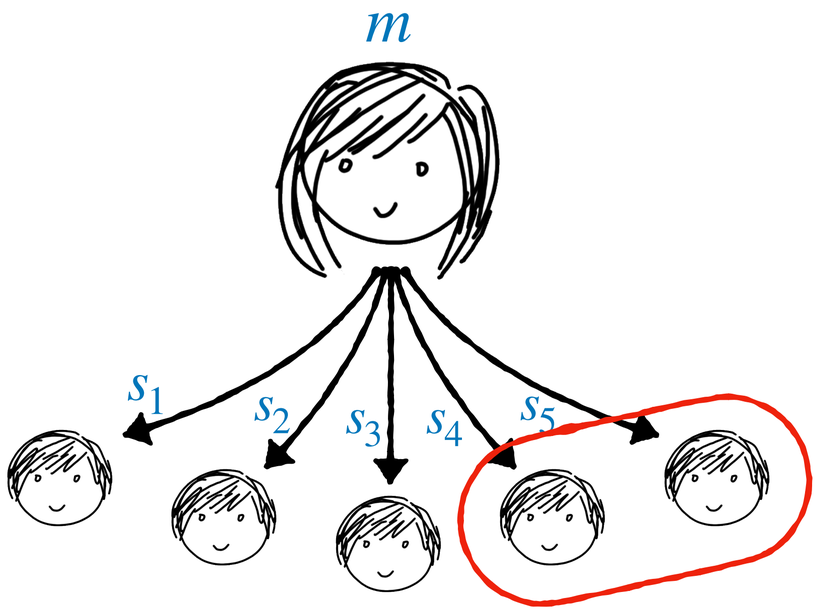
- The access structure is:

  $\Gamma = \{X \subseteq \mathscr{P} : \exists i \in [3] \text{ s.t. } X_i \subseteq X\}$

  For example, $\{P_1, P_2, P_5\} \in \Gamma$

- The forbidden structure is $\{X \subseteq \mathscr{P}\} \backslash \Gamma$.

  For example, $\{P_4, P_5\} \notin \Gamma$



This means set subtraction!

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 $\left\{s_{i_1}, \ldots, s_{i_k} : (s_1, \ldots, s_n) \leftarrow \mathsf{Share}(m_1)\right\} \equiv \left\{s_{i_1}, \ldots, s_{i_k} : (s_1, \ldots, s_n) \leftarrow \mathsf{Share}(m_2)\right\}$.

Note: this looks like the perfect secrecy definition for encryption! Alternatively we could write a privacy definition that looks like Shannon secrecy, and prove that it is implied by Definition 3, just as we did for encryption.

General Secret Sharing

Definition 3. Perfect Privacy for Secret Sharing

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

Note: this looks like the perfect secrecy definition for encryption! Alternatively we could write a privacy definition that looks like Shannon secrecy, and prove that it is implied by Definition 3, just as we did for encryption.

Note: Whereas we don't often explicitly use perfectly secret encryption schemes in practice anymore, the most commonly-used secret sharing schemes are indeed perfectly private!

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.

Question: Can we think of OTP as a special case of this?

Similarly: n-of-n additive sharing

- Consider $\mathscr{M} = \mathbb{Z}_\ell$ for some $\ell \in \mathbb{N}$.
- Share(m):
  1. Sample $s_1, \ldots, s_{n-1} \leftarrow \mathbb{Z}_\ell$.
  2. Compute $s_n := m - \sum_{i=1}^{n-1} s_i \bmod \ell$.
  3. Output $(s_1, \ldots, s_n)$.
- Recon($s_1, \ldots, s_n$):
  1. Output $\sum_{i=1}^{n} s_i \bmod \ell$.

Note: those of you who have taken algebra might notice these are really two special cases of the same general scheme…

Note: This is a threshold scheme for $t = n - 1$!

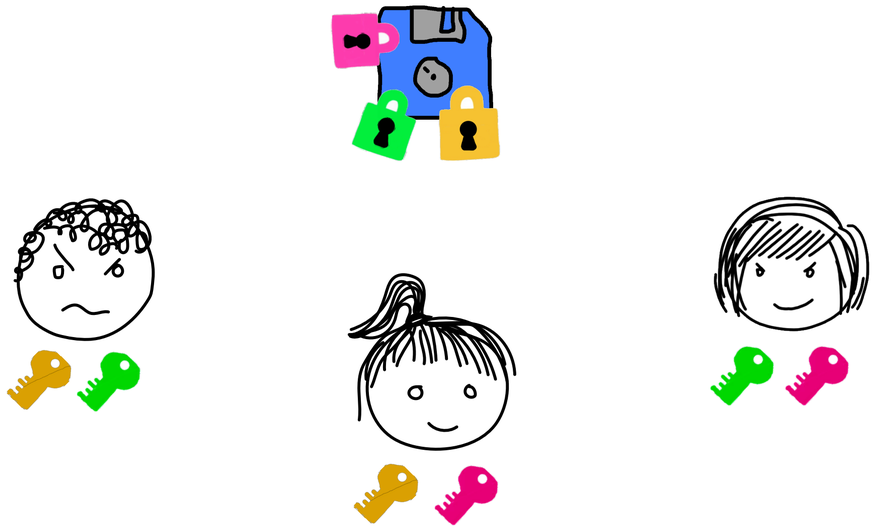
Slightly More General: Thresholds

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 $\Gamma = \{X \subseteq \mathscr{P} : |X| > t\}$.

Our example earlier was a 2-of-3 TSS scheme.

Can we generalize it?



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

Naïvely, we can envision the following solution to achieve an arbitrary threshold among n parties. Let t be the maximum number of corruptions.

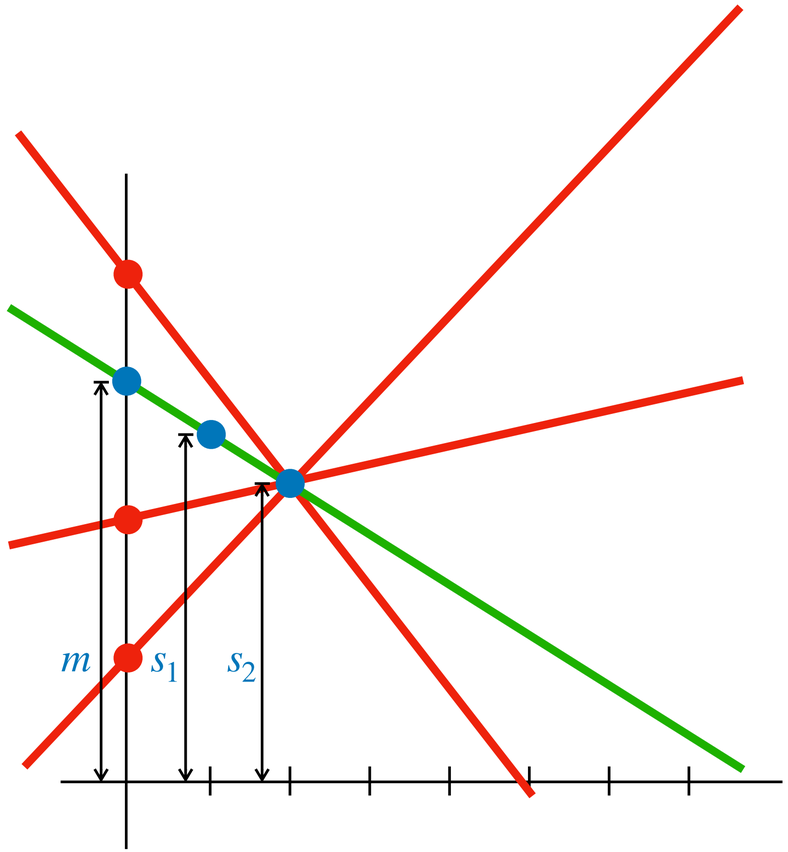
- For every size-$(t+1)$ subset of the parties, the Dealer secret-shares s to the parties in that subset using a $(t+1)$-of-$(t+1)$ secret sharing scheme.
- By the correctness of the $(t+1)$-of-$(t+1)$ secret-sharing scheme, every set of $t+1$ parties can reconstruct. So our new scheme is also correct.
- By the privacy of the $(t+1)$-of-$(t+1)$ secret-sharing scheme, and the fact that all of the sharings distributed by the dealer are completely independent, the entire set of shares known to any set of t parties has a distribution that is independent of the message that is shared. So our new scheme is private.

Bad News: there are $\binom{n}{t+1}$ subsets. When $t \approx n/2$ we have $\binom{n}{t+1} \in \Omega\left(\frac{2^n}{\sqrt{n}}\right)$.

Can we do better?

2-of-2 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, s_2) where $s_1 = f(1) = a + m$ and $s_2 = f(2) = 2a + m$.
- Recon(s_1, s_2):
  1. Compute $a := \dfrac{s_2 - s_1}{2 - 1} = s_2 - s_1$.
  2. Output $s_1 - a$.

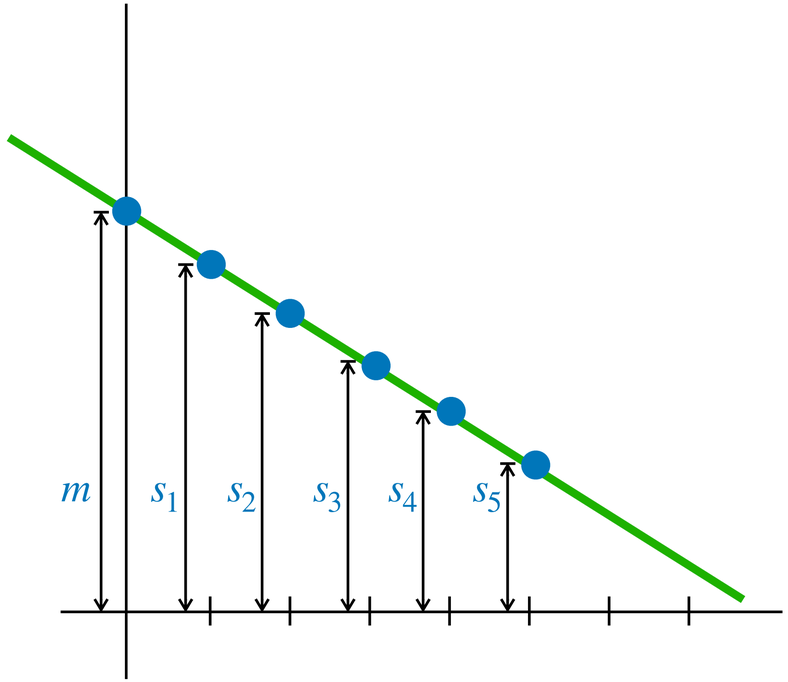


Correctness: follows from high-school geometry :)

Privacy Intuition: for any s_2 and any m there is a line going through $(2,s_2)$ and $(0,m)$.

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 $a := \dfrac{s_j - s_i}{j - i}$.
  2. Output $s_i - i \cdot a$.

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

3-of-n from Simple 2D Geometry

We want to make it so that 3 points are needed to reconstruct…

Claim: 3 points define a unique polynomial of degree ≤ 2

Proof:

- Let $(x_1, y_1), (x_2, y_2), (x_3, y_3)$ be points such that $x_1 \neq x_2 \neq x_3$.
- Suppose that both $f(x) = a_1 \cdot x^2 + b_1 \cdot x + c_1$ and $g(x) = a_2 \cdot x^2 + b_2 \cdot x + c_2$ pass through all three points. That is, $f(x_i) = g(x_i) = y_i \quad \forall i \in [3]$.
- Let $h(x) = f(x) - g(x)$. Note that $\deg(f) \leq 2 \wedge \deg(g) \leq 2 \implies \deg(h) \leq 2$.
- We also know that $h(x_i) = f(x_i) - g(x_i) = 0 \quad \forall i \in [3]$.
- This gives us two possible cases:
  1. $h(x) = 0 \ \forall x \implies f(x) = g(x) \ \forall x$
  2. $0 < \deg(h) \leq 2$ but h has 3 roots, which is a contradiction! ∎

$(t+1)$-of-n from Simple 2D Geometry

We want to make it so that $t+1$ points are needed to reconstruct...

Theorem 1: $t+1$ points define a unique polynomial of degree $\leq t$

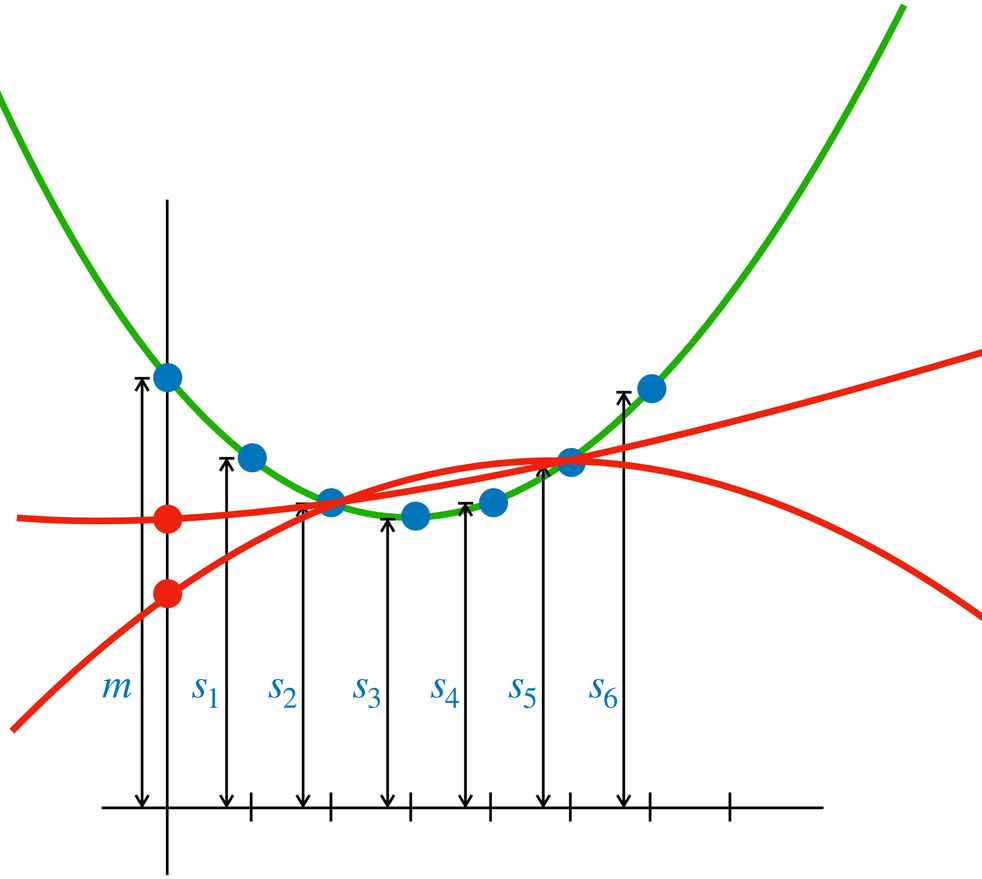
Proof:

- Let $(x_i, y_i)\ \forall i \in [t+1]$ be points such that $x_i \neq x_j\ \forall i, j \in [t+1]$.
- Suppose that both $f(x)$ and $g(x)$ are polynomials of degree $\leq t$ that pass through all $t+1$ points. That is, $f(x_i) = g(x_i) = y_i \quad \forall i \in [t+1]$.
- Let $h(x) = f(x) - g(x)$. Note that $\deg(f) \leq t \wedge \deg(g) \leq t \implies \deg(h) \leq t$.
- We also know that $h(x_i) = f(x_i) - g(x_i) = 0 \quad \forall i \in [t+1]$.
- This gives us two possible cases:
  1. $h(x) = 0\ \forall x \implies f(x) = g(x)\ \forall x$
  2. $0 < \deg(h) \leq t$ but h has $t+1$ roots, which is a contradiction! ∎

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($(i, j, k), (s_i, s_j, s_k)$):
  1. Recover the coefficients of f.
  2. Output $f(0)$.

we call this "interpolation"

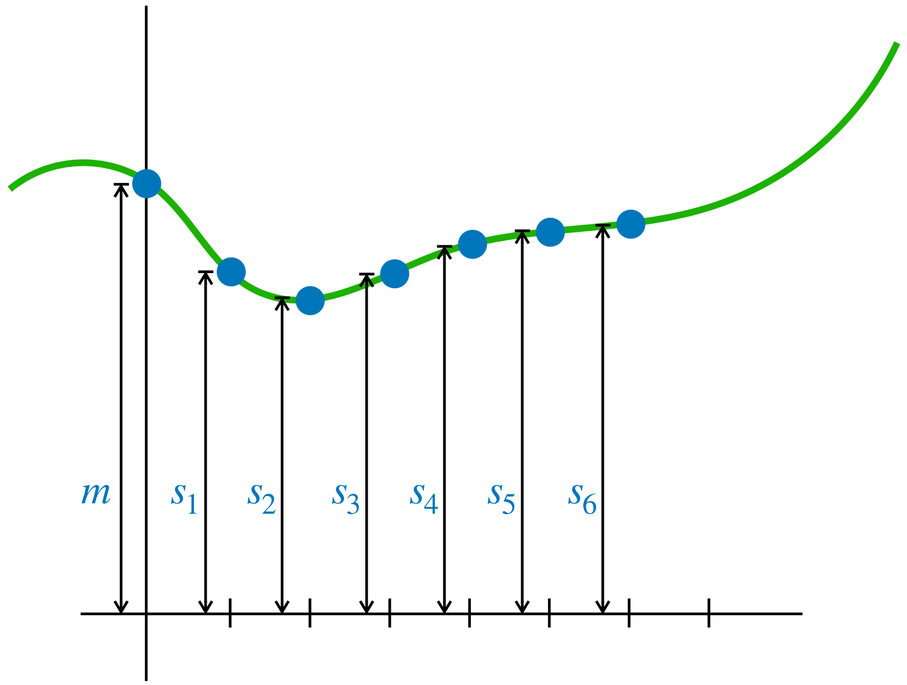


Correctness: from uniqueness of parabola.

Privacy Intuition: for any s_i, s_j and any m there is a (unique) parabola going through (i, s_i), (j, s_j), and $(0, m)$.

Finally, $(t+1)$-of-n Shamir Sharing

- Consider $\mathscr{M} = \mathbb{N}$
- Share(m):
  1. Find a random polynomial f of degree t 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$\left((i_1, \ldots, i_{t+1}), \left(s_{i_1}, \ldots, s_{i_{t+1}}\right)\right)$:
  1. Interpolate $f(0)$.



Correctness: from uniqueness of degree-t polynomial.

Privacy Intuition: for any collection of t points and any m there is a (unique) degree-t polynomial going through those points and $(0,m)$.

There is one huge problem! Can you see it?

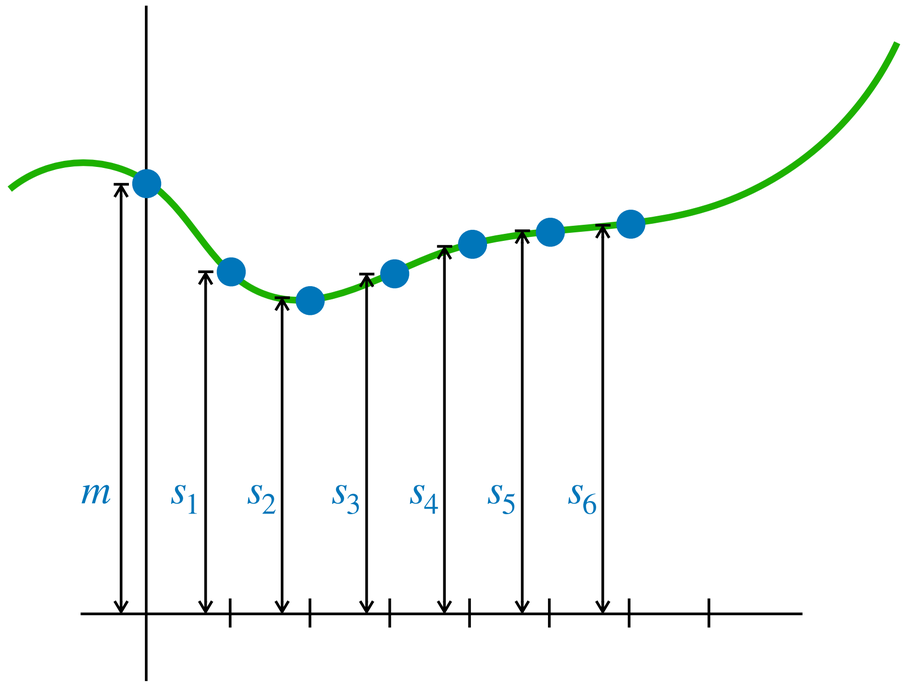
- How can we sample a polynomial "randomly?"
- Uniform distributions are not well-defined on countably infinite sets such as $\mathbb{N}$ and $\mathbb{Z}$!
- Suppose that set S is countably infinite. If the probability of every specific element being sampled is exactly 0, then

$$\sum_{s \in S} \Pr[x = s : x \leftarrow S] = 0$$

and if the probability of every specific element being sampled is nonzero, then

$$\sum_{s \in S} \Pr[x = s : x \leftarrow S] = \infty$$

In both cases, we contradict the law of total probability.



There is one huge problem! Can you see it?

- We need to work over a finite domain.
- We need to have at least $n + 1$ distinct x-coordinates.
  Can we work modulo $n + 1$?
- No! Suppose again that we want a 2-of-3 scheme.
  Here is the reconstruction algorithm again. Remember,
  we're working in $\mathbb{Z}_4$. How do we define division modulo 4?
- Suppose $j - i = 2$ and $s_j - s_i = 1$.
  Real number division won't work because $\frac{1}{2} \notin \mathbb{Z}_4$.
- What if we define division as "the inverse of multiplication modulo 4." We call this *modular multiplicative inverse.*
  Is there any number in $\mathbb{Z}_4$ that you can multiply by 2 to get 1?

Recon$((i, j), (s_i, s_j))$:

1. Compute $a := \dfrac{s_j - s_i}{j - i}$.
2. Output $s_i - i \cdot a$.

$(0 \cdot 2) \bmod 4 = 0$

$(1 \cdot 2) \bmod 4 = 2$

$(2 \cdot 2) \bmod 4 = 0$

$(3 \cdot 2) \bmod 4 = 2$

It would help us to understand what kind of finite domains support interpolation.

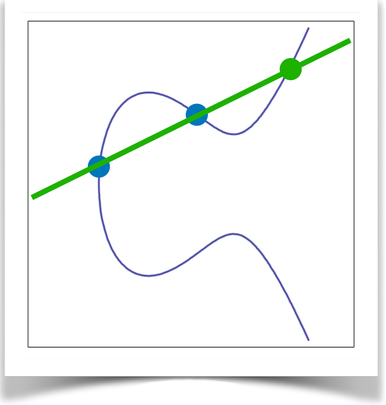
It's time to learn about algebraic structures!

Anyone who has taken MATH 3354 or MATH 4652 can take a nap now.

I will be simplifying heavily in the next part.

Abstract Algebra

- Think about your favorite number systems (i.e. sets of numbers): $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C}$
- We say that a set S is *closed* under some binary operator $\star$ if $x \in S \land y \in S \implies x \star y \in S$.
- $\mathbb{N}, \mathbb{Z}, \mathbb{R}, \mathbb{Q}, \mathbb{C},$ and $\mathbb{Z}_4$ are all closed under the operations $+$ and $\cdot$.
- Notice, however, that inverses aren't guaranteed by closure. $\mathbb{N}$ does not have additive inverses! $\mathbb{Z}_4$ doesn't have multiplicative inverses! So some of these behave slightly differently...
- We can add and multiply other kinds of things: for example, *matrices*, *real-valued functions*, *polynomials*. Are they closed? Do they have inverses? Unlike the others, matrix multiplication isn't commutative! So we have another slightly different kind of thing...
- We can also define other kinds of closed sets with binary operators. Consider the set of 2D points on this *elliptic curve:*
  - If we choose any two points with distinct x-coordinates, and draw a line between them, that line touches a third point.
  - It turns out the set of points on an elliptic curve is closed under this operation, and inverses exist too! It behaves just like addition.



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 $\mathbb{G}$.

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 $a \star b = b \star a$

Question: is $(\mathbb{Z}, +)$ a group? **Yes.**
is $(\mathbb{Z}, \cdot)$ a group? **No.** 2 has no inverse.
is $(\mathbb{R}, \cdot)$ a group? **No.** 0 has no inverse.
is $(\mathbb{R}^*, \cdot)$ a group, where $\mathbb{R}^* = \mathbb{R} \backslash \{0\}$? **Yes.**

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 $a \star b = b \star a$

Question: is $(M_{n\times m}(\mathbb{R}), +)$ a group, where $M_{n\times m}(\mathbb{R})$ is the set of all $n \times m$ matrices over $\mathbb{R}$? **Yes.**

is $(M_{n\times n}(\mathbb{R}), \cdot)$ a group? **No.** Some elements are non-invertible.

is $(GL_n(\mathbb{R}), \cdot)$ a group, where $GL_n(\mathbb{R}) = \{x \in M_{n\times n}(\mathbb{R}) : \det(x) \neq 0\}$? **Yes.** But not commutative.

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 $a \star b = b \star a$

Out of Scope: we can also build groups from *polynomials*.
we can build groups from *geometry* and *topology*.
the set of *bijective functions* is a group under the *composition* operator $\circ$.

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.

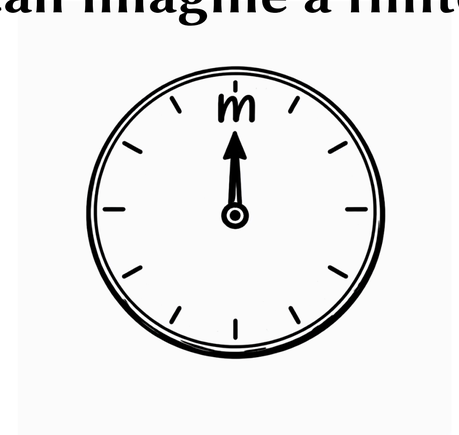
Closure: holds because the range of $\bmod m$ is $[0, m-1] = \mathbb{Z}_m$.

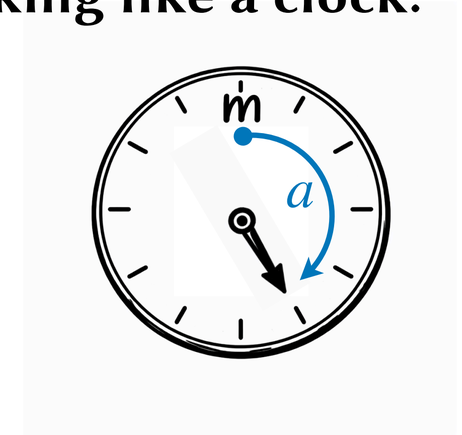
Associativity, Identity, Commutativity: the same as integer $+$ on $\mathbb{Z}$. Identity element is 0.

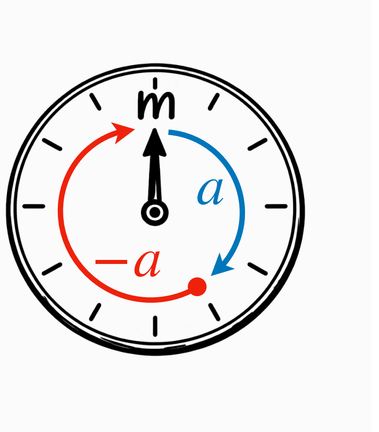
Inverses: Because $0 + 0 = 0$, the additive inverse of 0 is itself.
Notice that $m \bmod m = 0$. The additive inverse of $a \in \mathbb{Z}_m$ is a number $b \in \mathbb{Z}_m$ such that $(a + b) \bmod m = m \bmod m = 0$. Does $b \in \mathbb{Z}_m$ always exist? **Yes.**

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:







Let's Look Again at What We Need

Recon$((i,j),(s_i,s_j))$:

1. Compute $a := \dfrac{s_j - s_i}{j - i}$.
2. Output $s_i - i \cdot a$.

1. Structure with addition, multiplication, finite order.
2. Additive inverses

Let's Look Again at What We Need

Recon$((i,j),(s_i,s_j))$:

1. Compute $a := \dfrac{s_j - s_i}{j - i}$.
2. Output $s_i - i \cdot a$.

1. Structure with addition, multiplication, finite order.
2. Additive inverses
3. Multiplicative inverses

Since we require distinct x-coordinates, to reconstruct, we don't need a multiplicative inverse for 0.

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 $(\mathbb{Z}, +, \cdot)$ a field? **No.** 2 has no multiplicative inverse.
is $(\mathbb{R}, +, \cdot)$ a field? **Yes.**
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 Time: When is $\mathbb{Z}_m$ a Field?

CS4501 Cryptographic Protocols
Lecture 5: Secret Sharing, $\mathbb{G}$, $\mathbb{F}$

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