Secret – Sharing

Motivating Problem

Motivating 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.

Motivating 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?

Motivating 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?

Motivating 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 left as an exercise to show that the minimal solution uses 462 locks and 252 keys per scientist.

Motivating 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 left as an exercise to show that the minimal solution uses 462 locks and 252 keys per scientist.
- This is impractical, and the numbers grow exponentially.

Threshold Schemes

Threshold Schemes

- We have some secret data D.

Threshold Schemes

- We have some secret data D.
- We wish to "break" this data in n pieces $D_1, \ldots, D_n$ such that:

Threshold Schemes

- We have some secret data D.
- We wish to "break" this data in n pieces $D_1, \ldots, D_n$ such that:
  - knowledge of k or more D_i pieces makes D easily computable.

Threshold Schemes

- We have some secret data D.
- We wish to "break" this data in n pieces $D_1, \ldots, D_n$ such that:
  - knowledge of k or more D_i pieces makes D easily computable.
  - knowledge of strictly less than k pieces leaves D completely undetermined (so all possible values are equally likely).

Threshold Schemes

- We have some secret data D.
- We wish to "break" this data in n pieces $D_1, \ldots, D_n$ such that:
  - knowledge of k or more D_i pieces makes D easily computable.
  - knowledge of strictly less than k pieces leaves D completely undetermined (so all possible values are equally likely).
- Such a scheme is called a (k, n) ***threshold scheme***.

Shamir's Threshold Scheme

Shamir's Threshold Scheme

- D is some element of a field $\mathbb{F}$.

Shamir's Threshold Scheme

- D is some element of a field $\mathbb{F}$.
- Pick a degree $k-1$ polynomial $q(x)$ from $\mathbb{F}[x]$ with constant term D.

Shamir's Threshold Scheme

- D is some element of a field $\mathbb{F}$.
- Pick a degree $k-1$ polynomial $q(x)$ from $\mathbb{F}[x]$ with constant term D.
- Set $D_i = q(i)$.

Shamir's Threshold Scheme

- D is some element of a field $\mathbb{F}$.
- Pick a degree $k-1$ polynomial $q(x)$ from $\mathbb{F}[x]$ with constant term D.
- Set $D_i = q(i)$.
- Given any k of these D_i values, we can use interpolation to find the coefficients of q, and then $D = q(0)$.

Shamir's Threshold Scheme

- D is some element of a field $\mathbb{F}$.
- Pick a degree $k-1$ polynomial $q(x)$ from $\mathbb{F}[x]$ with constant term D.
- Set $D_i = q(i)$.
- Given any k of these D_i values, we can use interpolation to find the coefficients of q, and then $D = q(0)$.
- Given $k-1$ of these D_i values, we can do nothing.

Blakley's Threshold Scheme

Blakley's Threshold Scheme

- Let $\mathbb{V}$ be a k-dimensional vector space over $GF(q)$ and let e be the k-dimensional vector $[1, 0, \ldots, 0]$.

Blakley's Threshold Scheme

- Let $\mathbb{V}$ be a k-dimensional vector space over $GF(q)$ and let e be the k-dimensional vector $[1, 0, \ldots, 0]$.
- Let g be the first coordinate axis and pick a $(k-1)$-dimensional flat H such that $g \cap H = P$.

Blakley's Threshold Scheme

- Let $\mathbb{V}$ be a k-dimensional vector space over $GF(q)$ and let e be the k-dimensional vector $[1, 0, \ldots, 0]$.
- Let g be the first coordinate axis and pick a $(k-1)$-dimensional flat H such that $g \cap H = P$.
- D is the first coordinate of P.

Blakley's Threshold Scheme

- Let $\mathbb{V}$ be a k-dimensional vector space over $GF(q)$ and let e be the k-dimensional vector $[1, 0, \ldots, 0]$.
- Let g be the first coordinate axis and pick a $(k-1)$-dimensional flat H such that $g \cap H = P$.
- D is the first coordinate of P.
- The pieces $D_1, \ldots, D_n$ are the first coordinates of points that are in general position with P – any k of them generate a $(k-1)$-dimensional flat. The other coordinates are public knowledge.

Blakley's Threshold Scheme

- Let $\mathbb{V}$ be a k-dimensional vector space over $GF(q)$ and let e be the k-dimensional vector $[1, 0, \ldots, 0]$.
- Let g be the first coordinate axis and pick a $(k-1)$-dimensional flat H such that $g \cap H = P$.
- D is the first coordinate of P.
- The pieces $D_1, \ldots, D_n$ are the first coordinates of points that are in general position with P – any k of them generate a $(k-1)$-dimensional flat. The other coordinates are public knowledge.
- Given any k of these D_i values we can generate H and hence D.

Blakley's Threshold Scheme

- Let $\mathbb{V}$ be a k-dimensional vector space over $GF(q)$ and let e be the k-dimensional vector $[1, 0, \ldots, 0]$.
- Let g be the first coordinate axis and pick a $(k-1)$-dimensional flat H such that $g \cap H = P$.
- D is the first coordinate of P.
- The pieces $D_1, \ldots, D_n$ are the first coordinates of points that are in general position with P – any k of them generate a $(k-1)$-dimensional flat. The other coordinates are public knowledge.
- Given any k of these D_i values we can generate H and hence D.
- Given $k-1$ of these D_i values we can do nothing as there is a hyperplane passing through all $k-1$ points and any given point on g.

Terminology

Terminology

- We have a ***secret*** K.

Terminology

- We have a ***secret*** K.
- We want to share K among a bunch of ***participants*** $\mathcal{P}$.

Terminology

- We have a ***secret*** K.
- We want to share K among a bunch of ***participants*** $\mathcal{P}$.
- Each participant is a p_i.

Terminology

- We have a ***secret*** K.
- We want to share K among a bunch of ***participants*** $\mathcal{P}$.
- Each participant is a p_i.
- A special person called the ***dealer*** D picks K.

Terminology

- We have a ***secret*** K.
- We want to share K among a bunch of ***participants*** $\mathcal{P}$.
- Each participant is a p_i.
- A special person called the ***dealer*** D picks K.
- We assume $D \notin \mathcal{P}$.

Terminology

- We have a ***secret*** K.
- We want to share K among a bunch of ***participants*** $\mathcal{P}$.
- Each participant is a p_i.
- A special person called the ***dealer*** D picks K.
- We assume $D \notin \mathcal{P}$.
- Each p_i gets a ***share*** S_{p_i}.

Terminology

- We have a ***secret*** K.
- We want to share K among a bunch of ***participants*** $\mathcal{P}$.
- Each participant is a p_i.
- A special person called the ***dealer*** D picks K.
- We assume $D \notin \mathcal{P}$.
- Each p_i gets a ***share*** S_{p_i}.
- The set of all shares is $\mathcal{S}$.

Access Structure

Access Structure

- We need to define more complex schemes than threshold schemes.

Access Structure

- We need to define more complex schemes than threshold schemes.
- We use an ***access structure*** Γ to do this.

Access Structure

- We need to define more complex schemes than threshold schemes.
- We use an ***access structure*** Γ to do this.
- $\Gamma \subseteq \wp(\mathcal{P})$.

Access Structure

- We need to define more complex schemes than threshold schemes.
- We use an ***access structure*** Γ to do this.
- $\Gamma \subseteq \wp(\mathcal{P})$.
- $\gamma \in \Gamma$ is known as an ***authorised subset*** and is allowed to compute K.

Access Structure

- We need to define more complex schemes than threshold schemes.
- We use an ***access structure*** Γ to do this.
- $\Gamma \subseteq \wp(\mathcal{P})$.
- $\gamma \in \Gamma$ is known as an ***authorised subset*** and is allowed to compute K.
- $\varpi \notin \Gamma$ is not allowed to compute K.

Access Structure

- We need to define more complex schemes than threshold schemes.
- We use an ***access structure*** Γ to do this.
- $\Gamma \subseteq \wp(\mathcal{P})$.
- $\gamma \in \Gamma$ is known as an ***authorised subset*** and is allowed to compute K.
- $\varpi \notin \Gamma$ is not allowed to compute K.
- Γ is ***monotone*** – $\gamma \in \Gamma \wedge \gamma \subseteq \xi \rightarrow \xi \in \Gamma$.

Access Structure

- We need to define more complex schemes than threshold schemes.
- We use an ***access structure*** Γ to do this.
- $\Gamma \subseteq \wp(\mathcal{P})$.
- $\gamma \in \Gamma$ is known as an ***authorised subset*** and is allowed to compute K.
- $\varpi \notin \Gamma$ is not allowed to compute K.
- Γ is ***monotone*** – $\gamma \in \Gamma \wedge \gamma \subseteq \xi \rightarrow \xi \in \Gamma$.
- A (k, n) threshold scheme has access structure $\Gamma = \{Y \subseteq \wp(P) \mid |Y| \geq k\}$.

Matroids

Matroids

- Given an access structure Γ, we can define a matroid M with groundset $\mathcal{P} \cup \{D\}$.

Matroids

- Given an access structure Γ, we can define a matroid M with groundset $\mathcal{P} \cup \{D\}$.
- As Γ is monotone, defining the ***minimal authorised subsets*** Γ_0 is sensible.

Matroids

- Given an access structure Γ, we can define a matroid M with groundset $\mathcal{P} \cup \{D\}$.
- As Γ is monotone, defining the ***minimal authorised subsets*** Γ_0 is sensible.
- The matroid on Γ is defined by:

Matroids

- Given an access structure Γ, we can define a matroid M with groundset $\mathcal{P} \cup \{D\}$.
- As Γ is monotone, defining the ***minimal authorised subsets*** Γ_0 is sensible.
- The matroid on Γ is defined by:

$$\Gamma_0 = \{A \subseteq \mathcal{P} \mid A \cup \{D\} \text{ is a circuit of } M\}$$

Matroids

- Given an access structure Γ, we can define a matroid M with groundset $\mathcal{P} \cup \{D\}$.
- As Γ is monotone, defining the ***minimal authorised subsets*** Γ_0 is sensible.
- The matroid on Γ is defined by:

$$\Gamma_0 = \{A \subseteq \mathcal{P} \mid A \cup \{D\} \text{ is a circuit of } M\}$$

- These matroids are **not** secret-sharing matroids.

Matroids

- Given an access structure Γ, we can define a matroid M with groundset $\mathcal{P} \cup \{D\}$.
- As Γ is monotone, defining the ***minimal authorised subsets*** Γ_0 is sensible.
- The matroid on Γ is defined by:

$$\Gamma_0 = \{A \subseteq \mathcal{P} \mid A \cup \{D\} \text{ is a circuit of } M\}$$

- These matroids are **not** secret-sharing matroids.
- These matroids have a lot to do with matroid ports, and an excluded minor characterisation was given by Seymour in 1976.

Perfect Secret Sharing

Perfect Secret Sharing

- A secret sharing scheme with access structure Γ is ***perfect*** if:

Perfect Secret Sharing

- A secret sharing scheme with access structure Γ is ***perfect*** if:
  - If $\gamma \in \Gamma$, then γ can compute K.

Perfect Secret Sharing

- A secret sharing scheme with access structure Γ is ***perfect*** if:
  - If $\gamma \in \Gamma$, then γ can compute K.
  - If $\gamma \notin \Gamma$, then γ can determine nothing at all about K (that is, given the information available to γ, no value of K is more likely than any other).

Perfect Secret Sharing

- A secret sharing scheme with access structure Γ is ***perfect*** if:
  - If $\gamma \in \Gamma$, then γ can compute K.
  - If $\gamma \notin \Gamma$, then γ can determine nothing at all about K (that is, given the information available to γ, no value of K is more likely than any other).
- Both threshold schemes introduced earlier are perfect.

Ideal Secret Sharing

Ideal Secret Sharing

- A perfect secret sharing scheme is ***ideal*** if:

Ideal Secret Sharing

- A perfect secret sharing scheme is ***ideal*** if:
  - The "length" of K is the same as the "length" of the shares.

Ideal Secret Sharing

- A perfect secret sharing scheme is ***ideal*** if:
  - The "length" of K is the same as the "length" of the shares.
- This is deliberately vague, though it can be formalised if one limits the origin of the secret.

Ideal Secret Sharing

- A perfect secret sharing scheme is ***ideal*** if:
  - The "length" of K is the same as the "length" of the shares.
- This is deliberately vague, though it can be formalised if one limits the origin of the secret.
- Both threshold schemes introduced earlier are ideal, as all fields elements have the same "length".

Secret Sharing Matrix – Definition

Secret Sharing Matrix – Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a finite matrix with entries from a finite set S such that $|S| > 1$.

Secret Sharing Matrix – Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a finite matrix with entries from a finite set S such that $|S| > 1$. For $i \in I$, $j \in J$, and $X \subseteq J - \{j\}$, let

$$n(i, j, X) = \left\{ a_{kj} \mid k \in I, a_{kx} = a_{ix} \text{ for all } x \in X \right\}.$$

Secret Sharing Matrix – Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a finite matrix with entries from a finite set S such that $|S| > 1$. For $i \in I$, $j \in J$, and $X \subseteq J - \{j\}$, let

$$n(i, j, X) = \left\{ a_{kj} \mid k \in I, a_{kx} = a_{ix} \text{ for all } x \in X \right\}.$$

Then A is a ***secret sharing matrix*** over S if for all $j \in J$ and all $X \subseteq J - \{j\}$, either $n(i, j, X) = S$ for all $i \in I$, or $|n(i, j, X)| = 1$ for all $i \in I$.

Secret Sharing Matrix – Example

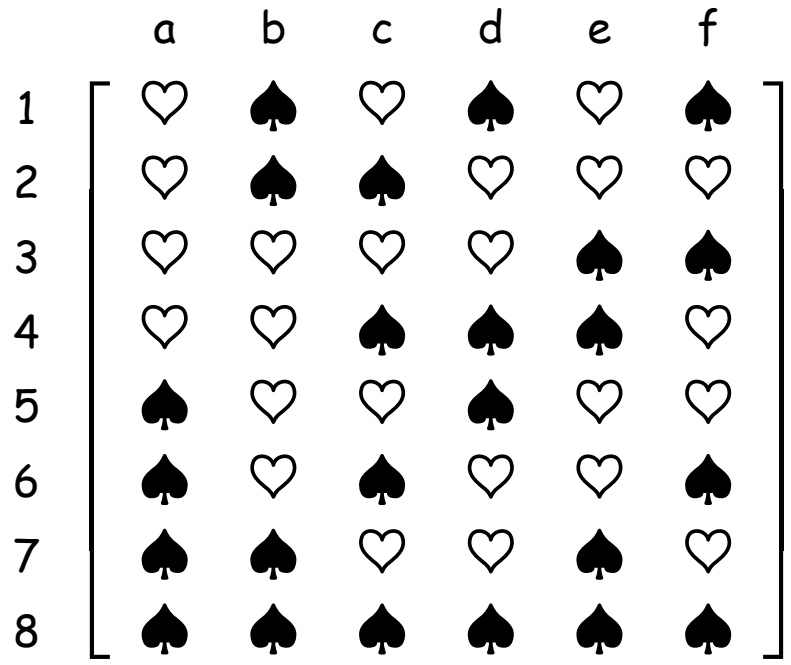
Secret Sharing Matrix – Example

This is a secret-sharing matrix with $S = \{♡, ♠\}$.

	a	b	c	d	e	f
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠

Secret Sharing Matrix – Example

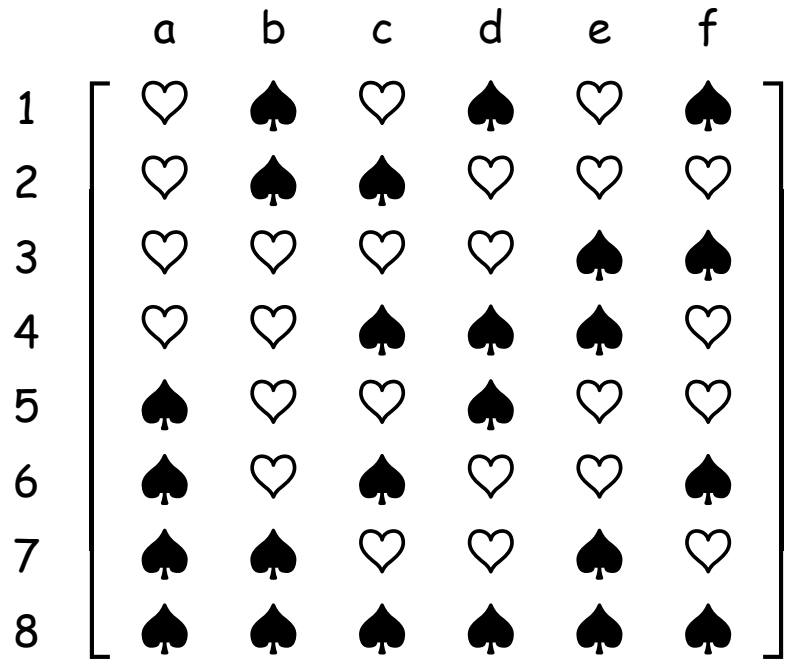
This is a secret-sharing matrix with $S = \{♡, ♠\}$.



Consider $j = d$ and $X = \{a, b\}$. Then $n(i, d, \{a, b\}) = \{♡, ♠\}$ for all i.

Secret Sharing Matrix – Example

This is a secret-sharing matrix with $S = \{\heartsuit, \spadesuit\}$.



Consider $j = d$ and $X = \{a, b\}$. Then $n(i, d, \{a, b\}) = \{\heartsuit, \spadesuit\}$ for all i.

Consider $j = d$ and $X = \{c, e\}$. Then $|n(i, d, \{c, e\})| = 1$ for all i.

Secret Sharing Matrix – Implementation

Secret Sharing Matrix – Implementation

- The secret sharing matrix A is assumed to be public knowledge.

Secret Sharing Matrix – Implementation

- The secret sharing matrix A is assumed to be public knowledge.
- Label the columns with $\mathcal{P} \cup \{D\}$.

Secret Sharing Matrix – Implementation

- The secret sharing matrix A is assumed to be public knowledge.
- Label the columns with $\mathcal{P} \cup \{D\}$.
- We can assume D is the first column.

Secret Sharing Matrix – Implementation

- The secret sharing matrix A is assumed to be public knowledge.
- Label the columns with $\mathcal{P} \cup \{D\}$.
- We can assume D is the first column.
- D picks row q uniformly at random from A.

Secret Sharing Matrix – Implementation

- The secret sharing matrix A is assumed to be public knowledge.
- Label the columns with $\mathcal{P} \cup \{D\}$.
- We can assume D is the first column.
- D picks row q uniformly at random from A.
- The secret is A_{q1}, and participant p_i gets share A_{qp_i}.

Secret Sharing Matrix – Implementation

- The secret sharing matrix A is assumed to be public knowledge.
- Label the columns with $\mathcal{P} \cup \{D\}$.
- We can assume D is the first column.
- D picks row q uniformly at random from A.
- The secret is A_{q1}, and participant p_i gets share A_{qp_i}.
- This gives an ideal secret sharing scheme with $\gamma \in \wp(\mathcal{P})$ being authorised if and only if $|n(i, 1, \gamma)| = 1$ for all i.

Secret Sharing Matrix – Example revisited

Secret Sharing Matrix – Example revisited

$A =$

	D	p_1	p_2	p_3	p_4	p_5
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠

Secret Sharing Matrix – Example revisited

$A =$

	D	p_1	p_2	p_3	p_4	p_5
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠

- D picks row 3, so the secret is ♡.

Secret Sharing Matrix – Example revisited

$A =$

	D	p_1	p_2	p_3	p_4	p_5
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠

- D picks row 3, so the secret is ♡.
- p_2 and p_4 get together, and can reduce the possible rows to 3 or 7, but the secret is still safe.

Secret Sharing Matrix – Example revisited

$A =$

	D	p_1	p_2	p_3	p_4	p_5
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠

- D picks row 3, so the secret is ♡.
- p_2 and p_4 get together, and can reduce the possible rows to 3 or 7, but the secret is still safe.
- They then torture p_1 and can now determine that the secret is ♡.

Matroids again

Matroids again

Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix.

Matroids again

Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix. Then $X \subseteq J$ ***spans*** $j \in J - X$ if $|n(i, j, X)| = 1$ for all $i \in I$,

Matroids again

Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix. Then $X \subseteq J$ ***spans*** $j \in J - X$ if $|n(i, j, X)| = 1$ for all $i \in I$, and $Y \subseteq J$ is ***independent*** if for all $j \in Y$, $Y - \{j\}$ does not span j.

Matroids again

Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix. Then $X \subseteq J$ ***spans*** $j \in J - X$ if $|n(i, j, X)| = 1$ for all $i \in I$, and $Y \subseteq J$ is ***independent*** if for all $j \in Y$, $Y - \{j\}$ does not span j.

Theorem

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix, and let $\mathcal{I}$ be its collection of independent sets.

Matroids again

Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix. Then $X \subseteq J$ ***spans*** $j \in J - X$ if $|n(i, j, X)| = 1$ for all $i \in I$, and $Y \subseteq J$ is ***independent*** if for all $j \in Y$, $Y - \{j\}$ does not span j.

Theorem

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix, and let $\mathcal{I}$ be its collection of independent sets. Then $M = (J, \mathcal{I})$ is a matroid with ground set J and independent sets $\mathcal{I}$.

Matroids again

Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix. Then $X \subseteq J$ ***spans*** $j \in J - X$ if $|n(i, j, X)| = 1$ for all $i \in I$, and $Y \subseteq J$ is ***independent*** if for all $j \in Y$, $Y - \{j\}$ does not span j.

Theorem

*Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix, and let $\mathcal{I}$ be its collection of independent sets. Then $M = (J, \mathcal{I})$ is a matroid with ground set J and independent sets $\mathcal{I}$. M is said to be a **secret sharing matroid**, and A is a secret sharing matrix for M.*

Matroids again

Definition

Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix. Then $X \subseteq J$ ***spans*** $j \in J - X$ if $|n(i, j, X)| = 1$ for all $i \in I$, and $Y \subseteq J$ is ***independent*** if for all $j \in Y$, $Y - \{j\}$ does not span j.

Theorem

*Let $A = [a_{ij} \mid i \in I, j \in J]$ be a secret sharing matrix, and let $\mathcal{I}$ be its collection of independent sets. Then $M = (J, \mathcal{I})$ is a matroid with ground set J and independent sets $\mathcal{I}$. M is said to be a **secret sharing matroid**, and A is a secret sharing matrix for M.*

- Using the earlier way to define a matroid, this definition applies to all ideal secret sharing schemes.

Secret Sharing Matroid – Example

Secret Sharing Matroid – Example

	D	p_1	p_2	p_3	p_4	p_5
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠

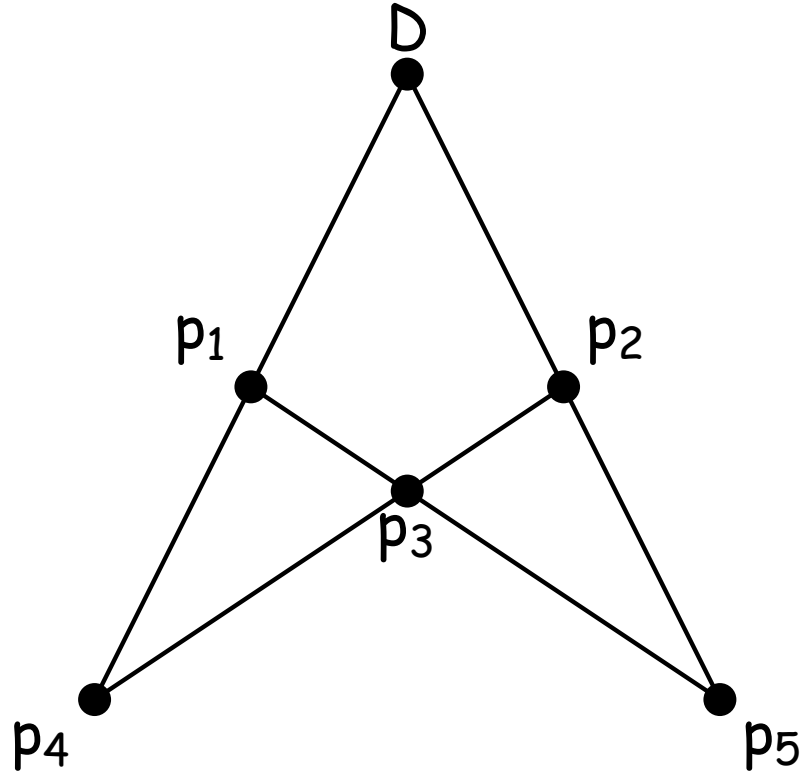
Secret Sharing Matroid – Example

	D	p_1	p_2	p_3	p_4	p_5
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠

This matrix is a secret sharing matrix for $M(K_4)$.

Secret Sharing Matroid – Example

	D	p_1	p_2	p_3	p_4	p_5
1	♡	♠	♡	♠	♡	♠
2	♡	♠	♠	♡	♡	♡
3	♡	♡	♡	♡	♠	♠
4	♡	♡	♠	♠	♠	♡
5	♠	♡	♡	♠	♡	♡
6	♠	♡	♠	♡	♡	♠
7	♠	♠	♡	♡	♠	♡
8	♠	♠	♠	♠	♠	♠



This matrix is a secret sharing matrix for $M(K_4)$.

Secret Sharing Matroids

Secret Sharing Matroids

There is a better way to define a secret sharing matroid, due to Seymour.

Secret Sharing Matroids

There is a better way to define a secret sharing matroid, due to Seymour.

Theorem

Let $A = [a_{ij} \mid i \in I, j \in J]$ *be a matrix with entries from some finite non-singleton set* S*, and let* M *be a matroid with ground set* J *and rank function* r.

Secret Sharing Matroids

There is a better way to define a secret sharing matroid, due to Seymour.

Theorem

Let $A = [a_{ij} \mid i \in I, j \in J]$ *be a matrix with entries from some finite non-singleton set* S*, and let* M *be a matroid with ground set* J *and rank function* r*. Then* A *is a secret sharing matrix for* M *if and only if for all* $X \subseteq J$*, the submatrix* $[a_{ij} \mid i \in I, j \in X]$ *has exactly* $|S|^{r(X)}$ *distinct rows.*

Secret Sharing Matroids

There is a better way to define a secret sharing matroid, due to Seymour.

Theorem

Let $A = [a_{ij} \mid i \in I, j \in J]$ *be a matrix with entries from some finite non-singleton set* S*, and let* M *be a matroid with ground set* J *and rank function* r*. Then* A *is a secret sharing matrix for* M *if and only if for all* $X \subseteq J$*, the submatrix* $[a_{ij} \mid i \in I, j \in X]$ *has exactly* $|S|^{r(X)}$ *distinct rows.*

From this theorem, we can safely disregard non-simple matroids.

Uniform Matroids

Uniform Matroids

- All uniform matroids are secret sharing.

Uniform Matroids

- All uniform matroids are secret sharing.
- For $U_{r,n}$, take $n - r$ mutually orthogonal latin r-hypercubes of order $|S|$.

Uniform Matroids

- All uniform matroids are secret sharing.
- For $U_{r,n}$, take $n - r$ mutually orthogonal latin r-hypercubes of order $|S|$.
- From these, we can construct a secret sharing matrix for $U_{r,n}$ over S.

Uniform Matroids

- All uniform matroids are secret sharing.
- For $U_{r,n}$, take $n - r$ mutually orthogonal latin r-hypercubes of order $|S|$.
- From these, we can construct a secret sharing matrix for $U_{r,n}$ over S.
- We take all possible $(n - r)$-tuples from S and assign them to the first $n - r$ columns of our matrix.

Uniform Matroids

- All uniform matroids are secret sharing.
- For $U_{r,n}$, take $n - r$ mutually orthogonal latin r-hypercubes of order $|S|$.
- From these, we can construct a secret sharing matrix for $U_{r,n}$ over S.
- We take all possible $(n - r)$-tuples from S and assign them to the first $n - r$ columns of our matrix.
- These definition a coordinate system on our latin hypercubes, and we fill in the matrix in the natural way.

Uniform Matroids

- All uniform matroids are secret sharing.
- For $U_{r,n}$, take $n - r$ mutually orthogonal latin r-hypercubes of order $|S|$.
- From these, we can construct a secret sharing matrix for $U_{r,n}$ over S.
- We take all possible $(n - r)$-tuples from S and assign them to the first $n - r$ columns of our matrix.
- These definition a coordinate system on our latin hypercubes, and we fill in the matrix in the natural way.
- This also shows that secret sharing matrices are not unique.

$U_{2,4}$ part a

$U_{2,4}$ part a

We wish to construct a secret sharing matrix for $U_{2,4}$ over the set $S = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$.

$U_{2,4}$ part a

We wish to construct a secret sharing matrix for $U_{2,4}$ over the set $S = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$. We need two mutually orthogonal latin squares of order four:

$U_{2,4}$ part a

We wish to construct a secret sharing matrix for $U_{2,4}$ over the set $S = \{♠, ♡, ♣, ♢\}$. We need two mutually orthogonal latin squares of order four:

	♣	♠	♢	♡
♣	♣	♠	♢	♡
♠	♠	♣	♡	♢
♢	♢	♡	♣	♠
♡	♡	♢	♠	♣

	♣	♠	♢	♡
♣	♣	♢	♡	♠
♠	♠	♡	♢	♣
♢	♢	♣	♠	♡
♡	♡	♠	♣	♢

$U_{2,4}$ part a

We wish to construct a secret sharing matrix for $U_{2,4}$ over the set $S = \{\spadesuit, \heartsuit, \clubsuit, \diamondsuit\}$. We need two mutually orthogonal latin squares of order four:

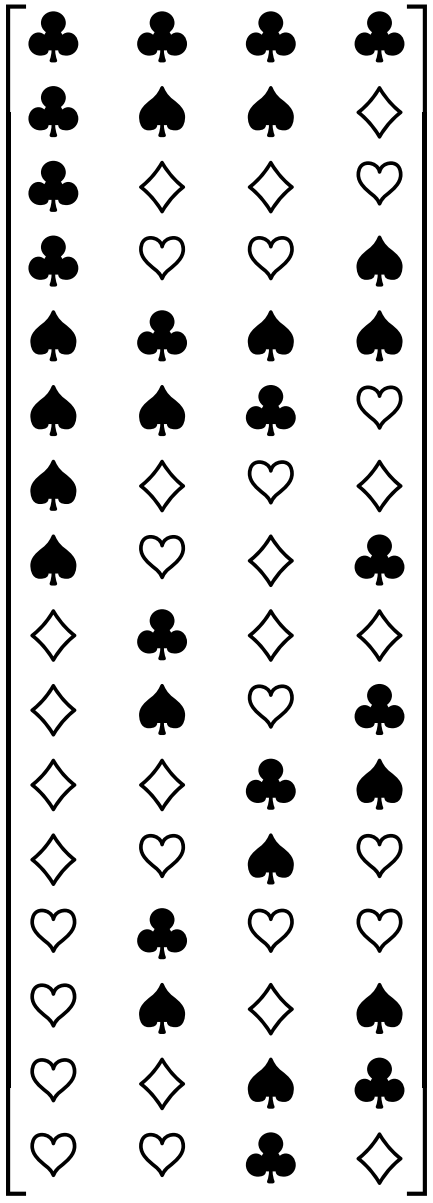
	♣	♠	♢	♡
♣	♣	♠	♢	♡
♠	♠	♣	♡	♢
♢	♢	♡	♣	♠
♡	♡	♢	♠	♣

	♣	♠	♢	♡
♣	♣	♢	♡	♠
♠	♠	♡	♢	♣
♢	♢	♣	♠	♡
♡	♡	♠	♣	♢

From this, we can construct a secret sharing matrix.

$U_{2,4}$ part b

$U_{2,4}$ part b



Representable Matroids

Representable Matroids

- All matroids representable over a finite field are secret sharing.

Representable Matroids

- All matroids representable over a finite field are secret sharing.
- Take a matrix representation of the matroid and construct the rowspace.

Representable Matroids

- All matroids representable over a finite field are secret sharing.
- Take a matrix representation of the matroid and construct the rowspace.
- When viewed as a matrix, the rowspace is a secret sharing matrix.

$M(K_4)$

$M(K_4)$

Take a $GF(2)$-representation
of $M(K_4)$:

$M(K_4)$

Take a $GF(2)$-representation of $M(K_4)$:

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$M(K_4)$

Take a GF(2)-representation of $M(K_4)$:

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

The rowspace of M is:

$M(K_4)$

Take a $GF(2)$-representation of $M(K_4)$:

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

The rowspace of M is:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$M(K_4)$

Take a $GF(2)$-representation of $M(K_4)$:

$$M = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

This is the example from earlier.

The rowspace of M is:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Vamos

Vamos

- The Vamos matroid is not secret sharing.

Vamos

- The Vamos matroid is not secret sharing.
- This was shown by Seymour in 1992, and some other people since.

Vamos

- The Vamos matroid is not secret sharing.
- This was shown by Seymour in 1992, and some other people since.
- His proof uses graph theory tricks, and isn't applicable to other matroids.

Partitions

Partitions

Definition

Let Ω be a set. A family ϖ of nonempty sets is a ***partition*** of Ω if the union of the elements of ϖ is equal to Ω and the elements of ϖ are pairwise disjoint.

Partitions

Definition

Let Ω be a set. A family ϖ of nonempty sets is a ***partition*** of Ω if the union of the elements of ϖ is equal to Ω and the elements of ϖ are pairwise disjoint. Elements of ϖ are called the ***blocks*** of the partition.

Partitions

Definition

Let Ω be a set. A family ϖ of nonempty sets is a ***partition*** of Ω if the union of the elements of ϖ is equal to Ω and the elements of ϖ are pairwise disjoint. Elements of ϖ are called the ***blocks*** of the partition.

Definition

Let Ω be a set, and let ϖ and ϖ' be two partitions of Ω. If every member of ϖ' is a subset of some element of ϖ, then ϖ' is a ***refinement*** of ϖ, denoted $\varpi' \leq \varpi$.

Partitions

Definition

Let Ω be a set. A family ϖ of nonempty sets is a ***partition*** of Ω if the union of the elements of ϖ is equal to Ω and the elements of ϖ are pairwise disjoint. Elements of ϖ are called the ***blocks*** of the partition.

Definition

Let Ω be a set, and let ϖ and ϖ' be two partitions of Ω. If every member of ϖ' is a subset of some element of ϖ, then ϖ' is a ***refinement*** of ϖ, denoted $\varpi' \leq \varpi$. We say that ϖ' is ***finer*** than ϖ and that ϖ is ***coarser*** than ϖ'.

p-representable matroids

p-representable matroids

Definition

Let a and b be two partitions of a set X. Then the ***meet*** of a and b, denoted $a \wedge b$, has blocks defined by

p-representable matroids

Definition

Let $\mathfrak{a}$ and $\mathfrak{b}$ be two partitions of a set X. Then the ***meet*** of $\mathfrak{a}$ and $\mathfrak{b}$, denoted $\mathfrak{a} \wedge \mathfrak{b}$, has blocks defined by

$$\{\alpha \cap \beta \mid \alpha \text{ is a block of } \mathfrak{a}, \beta \text{ is a block of } \mathfrak{b}\}.$$

p-representable matroids

Definition

Let α and β be two partitions of a set X. Then the ***meet*** of α and β, denoted $\alpha \wedge \beta$, has blocks defined by

$$\{\alpha \cap \beta \mid \alpha \text{ is a block of } \alpha, \beta \text{ is a block of } \beta\}.$$

Definition

Let $M = (E, r)$ be a matroid with rank function r, and let $d \geq 2$ be an integer. M is ***p-representable*** of degree d if there exists a finite set Ω of cardinality $d^{r(M)}$ and partitions ϖ_i of Ω, $i \in E$, such that for every $F \subseteq E$ the meet-partition $\varpi_F = \bigwedge_{i \in F} \varpi_i$ has $d^{r(F)}$ blocks all of the same cardinality.

p-representable matroids – example

p-representable matroids – example

Let $\Omega = \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \vartheta\}$. Then the following partitions of Ω give a p-representation of $M(K_4)$.

p-representable matroids – example

Let $\Omega = \{\alpha, \beta, \gamma, \delta, \varepsilon, \zeta, \eta, \vartheta\}$. Then the following partitions of Ω give a p-representation of $M(K_4)$.

$\varpi_D = \{\{\alpha, \beta, \gamma, \delta\}, \{\varepsilon, \zeta, \eta, \vartheta\}\}$

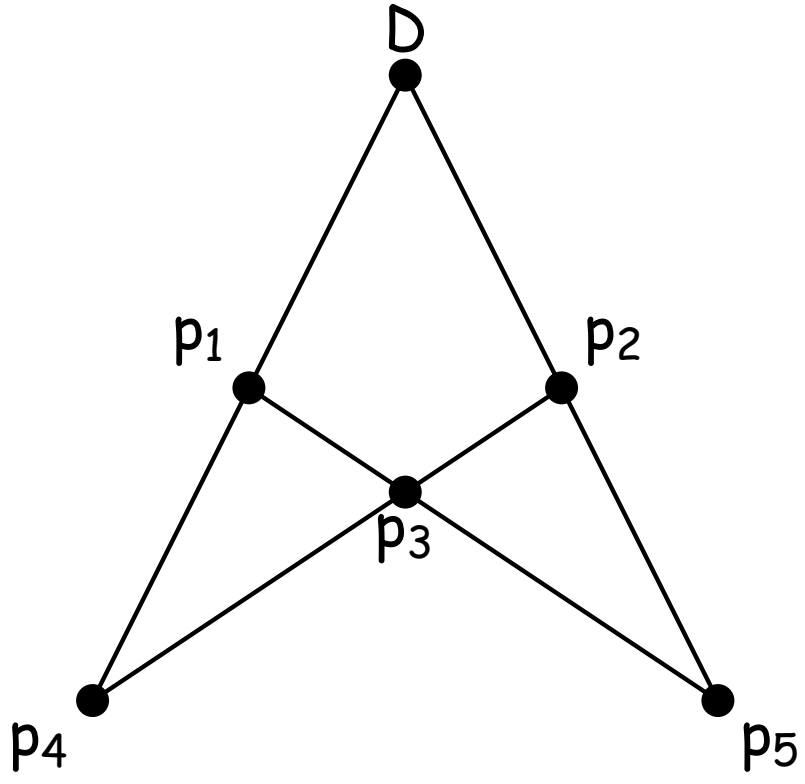
$\varpi_{p_1} = \{\{\alpha, \beta, \eta, \vartheta\}, \{\gamma, \delta, \varepsilon, \zeta\}\}$

$\varpi_{p_2} = \{\{\alpha, \gamma, \varepsilon, \eta\}, \{\beta, \delta, \zeta, \vartheta\}\}$

$\varpi_{p_3} = \{\{\alpha, \delta, \varepsilon, \vartheta\}, \{\beta, \gamma, \zeta, \eta\}\}$

$\varpi_{p_4} = \{\{\alpha, \beta, \varepsilon, \zeta\}, \{\gamma, \delta, \eta, \vartheta\}\}$

$\varpi_{p_5} = \{\{\alpha, \gamma, \zeta, \vartheta\}, \{\beta, \delta, \varepsilon, \eta\}\}$



Groups

Groups

- p-representable matroids are the same as secret sharing matroids.

Groups

- p-representable matroids are the same as secret sharing matroids.
- For a proof of this, see Welsh (2011).

Groups

- p-representable matroids are the same as secret sharing matroids.
- For a proof of this, see Welsh (2011).
- Partitions are unwieldy, but we can apply group theory to p-representable matroids.

Groups

- p-representable matroids are the same as secret sharing matroids.
- For a proof of this, see Welsh (2011).
- Partitions are unwieldy, but we can apply group theory to p-representable matroids.

Definition

A p-representation of a rank-r matroid M is ***group-induced*** if there is a group G and functions, f_i, $i \in E$, from G^r to G, such that the blocks of ϖ_i are $\{(g_1, \ldots, g_r) \in G^r \mid f_i(g_1, \ldots, g_r) = g\}$, for all $g \in G$, giving a p-representation of M that is equivalent to the original p-representation.

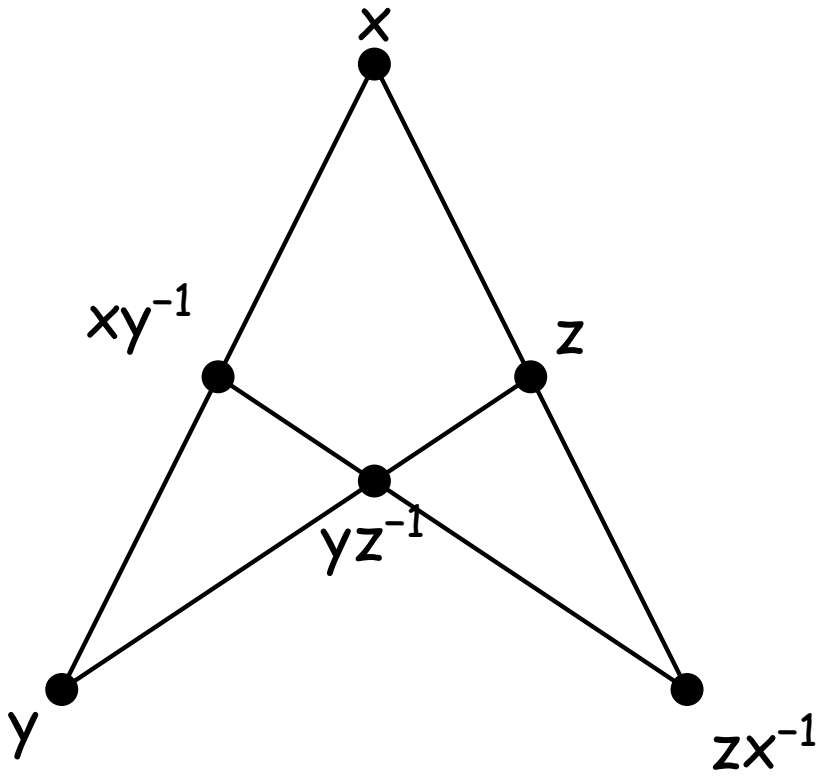
Groups – example

Groups – example

The following is a group-induced p-representation of $M(K_4)$.

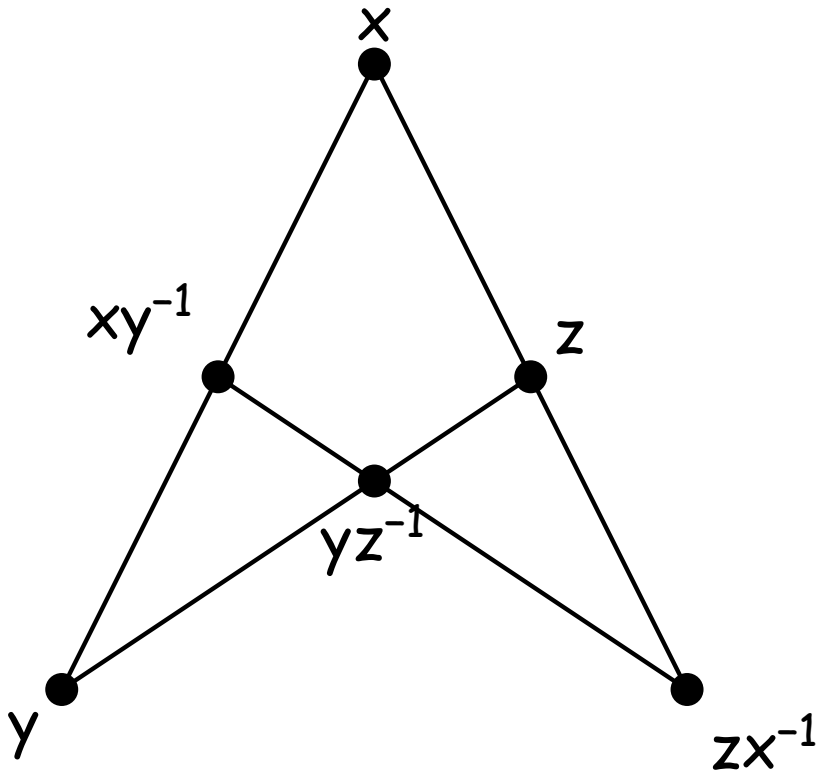
Groups – example

The following is a group-induced p-representation of $M(K_4)$.



Groups – example

The following is a group-induced p-representation of $M(K_4)$.



All p-representations of $M(K_4)$ arise from groups, and they are all equivalent to the one given here.

More on group-induced p-representations

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.
- If G is a group that defines a p-representation of the non-Fano, then G is abelian and has odd order.

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.
- If G is a group that defines a p-representation of the non-Fano, then G is abelian and has odd order.
- Every matroid representable over a prime field has a group-induced p-representation.

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.
- If G is a group that defines a p-representation of the non-Fano, then G is abelian and has odd order.
- Every matroid representable over a prime field has a group-induced p-representation. Construction.

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.
- If G is a group that defines a p-representation of the non-Fano, then G is abelian and has odd order.
- Every matroid representable over a prime field has a group-induced p-representation. Construction.
- All graphic matroids have a group-induced p-representation.

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.
- If G is a group that defines a p-representation of the non-Fano, then G is abelian and has odd order.
- Every matroid representable over a prime field has a group-induced p-representation. Construction.
- All graphic matroids have a group-induced p-representation. Construction.

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.
- If G is a group that defines a p-representation of the non-Fano, then G is abelian and has odd order.
- Every matroid representable over a prime field has a group-induced p-representation. Construction.
- All graphic matroids have a group-induced p-representation. Construction.
- F_7^+ has no group-induced p-representation.

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.
- If G is a group that defines a p-representation of the non-Fano, then G is abelian and has odd order.
- Every matroid representable over a prime field has a group-induced p-representation. Construction.
- All graphic matroids have a group-induced p-representation. Construction.
- F_7^+ has no group-induced p-representation.
- O_7 has non-equivalent p-representations.

More on group-induced p-representations

- If G is a group that defines a p-representation of the Fano, then G is a power of $\mathbb{Z}_2$.
- If G is a group that defines a p-representation of the non-Fano, then G is abelian and has odd order.
- Every matroid representable over a prime field has a group-induced p-representation. Construction.
- All graphic matroids have a group-induced p-representation. Construction.
- F_7^+ has no group-induced p-representation.
- O_7 has non-equivalent p-representations.
- Given a group function, it is very hard to tell if this function gives the correct number of solutions to define a block of a p-representation.

Almost Affine Codes

Almost Affine Codes

- Let F be a finite set of size $q \geq 2$.

Almost Affine Codes

- Let F be a finite set of size $q \geq 2$.
- Consider F^S, the set of all mappings from $S \stackrel{\text{def}}{=} \{1, \ldots, n\}$ into F.

Almost Affine Codes

- Let F be a finite set of size $q \geq 2$.
- Consider F^S, the set of all mappings from $S \stackrel{\text{def}}{=} \{1, \ldots, n\}$ into F.
- For any subset $X \subseteq S$, let $\rho_X^S : F^S \to F^X$ be the mapping induced by the inclusion mapping $X \hookrightarrow S$.

Almost Affine Codes

- Let F be a finite set of size $q \geq 2$.
- Consider F^S, the set of all mappings from $S \stackrel{\text{def}}{=} \{1, \ldots, n\}$ into F.
- For any subset $X \subseteq S$, let $\rho_X^S : F^S \to F^X$ be the mapping induced by the inclusion mapping $X \hookrightarrow S$.
- A q-ary ***code*** of length n is a non-empty subset of F^S.

Almost Affine Codes

- Let F be a finite set of size $q \geq 2$.
- Consider F^S, the set of all mappings from $S \stackrel{\text{def}}{=} \{1, \ldots, n\}$ into F.
- For any subset $X \subseteq S$, let $\rho_X^S : F^S \to F^X$ be the mapping induced by the inclusion mapping $X \hookrightarrow S$.
- A q-ary ***code*** of length n is a non-empty subset of F^S.
- The image $\rho_X^S(\mathcal{C})$ of a code $\mathcal{C}$ under ρ_X^S will be denoted by $\mathcal{C}_X$.

Almost Affine Codes

- Let F be a finite set of size $q \geq 2$.
- Consider F^S, the set of all mappings from $S \stackrel{\text{def}}{=} \{1, \ldots, n\}$ into F.
- For any subset $X \subseteq S$, let $\rho_X^S : F^S \to F^X$ be the mapping induced by the inclusion mapping $X \hookrightarrow S$.
- A q-ary ***code*** of length n is a non-empty subset of F^S.
- The image $\rho_X^S(\mathcal{C})$ of a code $\mathcal{C}$ under ρ_X^S will be denoted by $\mathcal{C}_X$.
- We say that $\mathcal{C}_X$ is the ***projection*** of $\mathcal{C}$ into the coordinate space F^X.

Almost Affine Codes

- Let F be a finite set of size $q \geq 2$.
- Consider F^S, the set of all mappings from $S \stackrel{\text{def}}{=} \{1, \ldots, n\}$ into F.
- For any subset $X \subseteq S$, let $\rho_X^S : F^S \to F^X$ be the mapping induced by the inclusion mapping $X \hookrightarrow S$.
- A q-ary ***code*** of length n is a non-empty subset of F^S.
- The image $\rho_X^S(\mathcal{C})$ of a code $\mathcal{C}$ under ρ_X^S will be denoted by $\mathcal{C}_X$.
- We say that $\mathcal{C}_X$ is the ***projection*** of $\mathcal{C}$ into the coordinate space F^X.
- A code $\mathcal{C} \subseteq F^S$ is called ***almost affine*** if it satisfies the condition $r(X) \stackrel{\text{def}}{=} \log_q(|\mathcal{C}_X| \in \mathbb{Z}^+ \cup \{0\}$ for all $X \subseteq S$.

Multilinear Codes

Multilinear Codes

- Let F be a m-dimensional vector space over $GF(q)$ and let $\mathcal{C}$ be a linear subspace of the nm-dimensional vector space F^n.

Multilinear Codes

- Let F be a m-dimensional vector space over $GF(q)$ and let $\mathcal{C}$ be a linear subspace of the nm-dimensional vector space F^n.
- Then $\mathcal{C}$ is an almost affine code of length n over F if and only if for all subsets $X \subseteq \{1, \ldots, n\}$ the dimension of the vector space $\mathcal{C}_X$ is divisible by m.

Multilinear Codes

- Let F be a m-dimensional vector space over $GF(q)$ and let $\mathcal{C}$ be a linear subspace of the nm-dimensional vector space F^n.
- Then $\mathcal{C}$ is an almost affine code of length n over F if and only if for all subsets $X \subseteq \{1, \ldots, n\}$ the dimension of the vector space $\mathcal{C}_X$ is divisible by m.
- These codes are known as ***multilinear codes***.

Matroids from codes

Matroids from codes

- Let $\mathcal{C} \subseteq \mathsf{F}^{\mathsf{S}}$ be an almost affine code, and let $\wp(\mathsf{S})$ be the power set of S.

Matroids from codes

- Let $\mathcal{C} \subseteq \mathsf{F}^{\mathsf{S}}$ be an almost affine code, and let $\wp(\mathsf{S})$ be the power set of S.
- Let $\mathsf{r}(\mathsf{X})$ be defined as before:

Matroids from codes

- Let $\mathcal{C} \subseteq \mathsf{F}^{\mathsf{S}}$ be an almost affine code, and let $\wp(\mathsf{S})$ be the power set of S.
- Let $\mathsf{r}(\mathsf{X})$ be defined as before:
  $\mathsf{r}(\mathsf{X}) \stackrel{\text{def}}{=} \log_q(|\mathcal{C}_{\mathsf{X}}| \in \mathbb{Z}^+ \cup \{0\}$ for $\mathsf{X} \subseteq \mathsf{S}$.

Matroids from codes

- Let $\mathcal{C} \subseteq \mathsf{F}^{\mathsf{S}}$ be an almost affine code, and let $\wp(\mathsf{S})$ be the power set of S.
- Let $\mathsf{r}(\mathsf{X})$ be defined as before:
  $\mathsf{r}(\mathsf{X}) \stackrel{\text{def}}{=} \log_q(|\mathcal{C}_{\mathsf{X}}| \in \mathbb{Z}^+ \cup \{0\}$ for $\mathsf{X} \subseteq \mathsf{S}$.
- Then $\mathsf{r}(\mathsf{X})$ is the rank function of a matroid $\mathsf{M}(\mathcal{C})$ with S as its ground set.

Matroids from codes

- Let $\mathcal{C} \subseteq F^S$ be an almost affine code, and let $\wp(S)$ be the power set of S.
- Let $r(X)$ be defined as before:
  $r(X) \stackrel{\text{def}}{=} \log_q(|\mathcal{C}_X| \in \mathbb{Z}^+ \cup \{0\}$ for $X \subseteq S$.
- Then $r(X)$ is the rank function of a matroid $M(\mathcal{C})$ with S as its ground set.
- A matroid M is said to be ***almost affinely representable*** if an almost affine code $\mathcal{C}$ exists such that $M = M(\mathcal{C})$.

Matroids from codes

- Let $\mathcal{C} \subseteq F^S$ be an almost affine code, and let $\wp(S)$ be the power set of S.
- Let $r(X)$ be defined as before:
  $r(X) \stackrel{\text{def}}{=} \log_q(|\mathcal{C}_X| \in \mathbb{Z}^+ \cup \{0\}$ for $X \subseteq S$.
- Then $r(X)$ is the rank function of a matroid $M(\mathcal{C})$ with S as its ground set.
- A matroid M is said to be ***almost affinely representable*** if an almost affine code $\mathcal{C}$ exists such that $M = M(\mathcal{C})$.
- If $\mathcal{C}$ is equivalent to a multilinear code, then M is said to be ***multilinearly representable***.

Multilinear Matroid Example

Multilinear Matroid Example

Let $F = GF(3)^2$. Then the rowspace of this matrix is an almost affine code of length 9 over F.

Multilinear Matroid Example

Let $F = GF(3)^2$. Then the rowspace of this matrix is an almost affine code of length 9 over F.

$$\begin{bmatrix} 10 & 10 & 00 & 10 & 00 & 10 & 10 & 10 & 00 \\ 01 & 01 & 00 & 01 & 00 & 01 & 01 & 01 & 00 \\ 00 & 00 & 00 & 10 & 10 & 21 & 01 & 10 & 10 \\ 00 & 00 & 00 & 02 & 01 & 20 & 12 & 02 & 01 \\ 00 & 10 & 10 & 01 & 00 & 01 & 00 & 11 & 10 \\ 00 & 01 & 01 & 21 & 00 & 21 & 00 & 10 & 01 \end{bmatrix}$$

Multilinear Matroid Example

Let $F = GF(3)^2$. Then the rowspace of this matrix is an almost affine code of length 9 over F.

$$\begin{bmatrix} 10 & 10 & 00 & 10 & 00 & 10 & 10 & 10 & 00 \\ 01 & 01 & 00 & 01 & 00 & 01 & 01 & 01 & 00 \\ 00 & 00 & 00 & 10 & 10 & 21 & 01 & 10 & 10 \\ 00 & 00 & 00 & 02 & 01 & 20 & 12 & 02 & 01 \\ 00 & 10 & 10 & 01 & 00 & 01 & 00 & 11 & 10 \\ 00 & 01 & 01 & 21 & 00 & 21 & 00 & 10 & 01 \end{bmatrix}$$

The matroid of this code is the non-Pappus matroid, showing that representable matroids are a proper subclass of secret sharing matroids.