Matroids

Introduction to Model Theory
(Third hour)

December 16, 2021

Section 1

Closure operations

Closure operations

Definition

A *closure operation* on a set S is a map $\mathrm{cl}(-) : P(S) \to P(S)$ satisfying these identities:

(increasing) $X \subseteq \mathrm{cl}(X)$.

(monotone) $X \subseteq Y \implies \mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$

(idempotent) $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$.

Closed sets

Fix a closure operation $\mathrm{cl}(-)$ on S.

Definition

$X \subseteq S$ is *closed* if $\mathrm{cl}(X) = X$.

Fact

Let I be a set. Let X_i be closed for $i \in I$. Then $\bigcap_{i \in I} X_i$ is closed.

Fact

For any $X \subseteq S$,

- $\mathrm{cl}(X)$ *is closed.*
- $\mathrm{cl}(X)$ *is the smallest closed set containing X.*
- $\mathrm{cl}(X)$ *is the intersection of the closed sets containing X.*

Finitary closure operations

Definition

A closure operation on S is *finitary* if whenever $X \subseteq S$ and $a \in \mathrm{cl}(X)$, there is a finite subset $X_0 \subseteq X$ with $a \in \mathrm{cl}(X_0)$.

Idea

If a is in the closure of X, it's because of only finitely many elements of X.

Example

If $\langle A \rangle$ denotes the substructure of M generated by A, then $A \mapsto \langle A \rangle$ is a finitary closure operation on M.

Section 2

Matroids: definition and examples

The exchange property

A closure operation $\mathrm{cl}(-)$ on S satisfies the *exchange property* if:

Whenever $X \subseteq S$, $a, b \in S$, $a, b \notin \mathrm{cl}(X)$, *we have*

$$a \in \mathrm{cl}(X \cup \{b\}) \implies b \in \mathrm{cl}(X \cup \{a\}).$$

Definition

A *matroid* (or *pregeometry*) is a set with a finitary closure operation satisfying exchange.

Vector-space span

If $S \subseteq \mathbb{R}^n$, define

$$\mathrm{cl}(S) = \{a_1 v_1 + \cdots + a_n v_n : a_1, \ldots, a_n \in \mathbb{R};\ v_1, \ldots, v_n \in S\}.$$

Fact

This is a finitary closure operation satisfying exchange.

- If $v \in \mathrm{cl}(S \cup \{w\}) \setminus \mathrm{cl}(S)$, then
$$v = a_1 u_1 + \cdots + a_n u_n + bw$$
for some $u_1, \ldots, u_n \in S$, $a_1, \ldots, a_n, b \in \mathbb{R}$.
- $b \neq 0$, or else $v \in \mathrm{cl}(S)$.
- Then
$$w = b^{-1} v - b^{-1} a_1 u_1 - b^{-1} a_2 u_2 - \cdots - b^{-1} a_n u_n.$$

Graphs

Definition

A *graph* consists of

- A set V of *vertices*.
- A set E of *edges*.
- A map ϕ assigning to each edge $e \in E$ a set of one or two vertices.

An *edge from v_1 to v_2* is an edge e with $\phi(e) = \{v_1, v_2\}$.

- We allow loops—edges from v to v.
- We allow parallel edges—more than one edge from v to w.

Walks

If $a, b \in V$, a *walk* from a to b is a sequence

$$v_0, e_1, v_1, e_2, v_2, \ldots, e_n, v_n$$

where

- $v_0, v_1, v_2, \ldots, v_n \in V$.
- $e_1, e_2, \ldots, e_n \in E$.
- $v_0 = a$.
- $v_n = b$.
- e_i is an edge from v_{i-1} to v_i.

$$v_0 \xrightarrow{e_1} v_1 \xrightarrow{e_2} v_2 \xrightarrow{e_3} v_3$$

Span

Let S be a set of edges.

- An edge e from v_1 to v_2 is *spanned* by S if there is a walk from v_1 to v_2 in S.
- The *span* of S is the set of edges spanned by S.

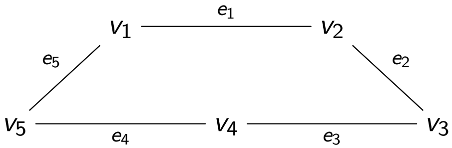
Fact

span$(-)$ *is a finitary closure operation.*

Cycles

A *cycle* is a sequence $v_1, e_1, v_2, e_2, v_2, \ldots, v_n, e_n$ where

- The v_i are distinct vertices.
- The e_i are distinct edges.
- e_i is an edge from v_i to v_{i+1}.
- e_n is an edge from v_n to v_1.
- $n \geq 1$.



Span and cycles

Fact

$e \in \text{span}(S)$ *iff at least one of the following holds:*

- $e \in S$
- *There is a cycle* C *with* $e \in C$ *and* $C \setminus \{e\} \subseteq S$.

Exchange

Fact

Let S be a set of edges. Let e_1, e_2 be two edges not in $\operatorname{span}(S)$. *Then*

$$e_1 \in \operatorname{span}(S \cup \{e_2\}) \implies e_2 \in \operatorname{span}(S \cup \{e_1\}).$$

Proof.

Let C be the cycle showing $e_1 \in \operatorname{span}(S \cup \{e_2\})$. Then $e_2 \in C$, or else $e_1 \in \operatorname{span}(S)$. Then C shows $e_2 \in \operatorname{span}(S \cup \{e_1\})$. □

Fact

If (V, E) is a graph, then there is a matroid on E where $\operatorname{cl}(S) = \operatorname{span}(S)$.

Section 3

Matroids: basic notions

Independent sets

Fix a matroid $(M, \mathrm{cl}(-))$.

Definition

A set $I \subseteq M$ is *independent* if $a \in I \implies a \notin \mathrm{cl}(I \setminus \{a\})$.

Fact

In $\mathbb{R}^n$, I is independent if it is linearly independent, i.e., for $a_1, \ldots, a_n \in \mathbb{R}$ and $v_1, \ldots, v_n \in I$,

$$a_1 v_1 + \cdots + a_n v_n = 0 \implies a_1 = a_2 = \cdots = a_n = 0.$$

Fact

In (V, E), a set $I \subseteq E$ is independent iff I contains no cycles, i.e., I is a "forest."

Spanning sets

Definition

A set $S \subseteq M$ is *spanning* if $\mathrm{cl}(S) = M$.

- In $\mathbb{R}^n$, a set S is spanning iff every vector in $\mathbb{R}^n$ is a linear combination of things in S.

Bases

Fix a matroid M.

Fact

The following are equivalent for $B \subseteq M$.

- *B is independent and spanning.*
- *B is maximal independent.*
- *B is minimal spanning.*

Definition

A *basis* is a set $B \subseteq M$ satisfying these properties.

- In $\mathbb{R}^n$, a basis is a vector space basis.
- In a graph $G = (V, E)$, a basis is a spanning tree or spanning forest.

Rank

Fact

Any matroid has a basis. Any two bases B_1, B_2 have the same cardinality.

Definition

The *rank* of M, written $r(M)$, is the cardinality of any basis.

Fact

1. *The rank of $\mathbb{R}^n$ is n.*
2. *The rank of a graph $G = (V, E)$ is the number of vertices minus the number of connected components.*

Rank of a set

Fact

If $S \subseteq M$,

- *There is a maximal independent subset $I \subseteq S$.*
- *If I_1, I_2 are two maximal independent subsets of S, then $|I_1| = |I_2|$.*

Definition

The *rank* of S, written $r(S)$, is the cardinality of any maximal independent subset.

Rank in vector spaces and graphs

- If $V \subseteq \mathbb{R}^n$ is a linear subspace (a closed set), then $r(V)$ is the dimension of V.
- If $S \subseteq \mathbb{R}^n$ is arbitrary, then $r(S) = r(\mathrm{cl}(S))$.
  - This holds in any matroid.
- In a graph $G = (V, E)$, the rank of $S \subseteq E$ is the number of vertices in S minus the number of connected components (thinking of S as a subgraph).

Dependent sets and circuits

Definition

A *dependent set* is a set that is not independent.
A *circuit* is a minimal independent set.

Example

In a graph, a circuit is a cycle.

In $\mathbb{R}^n$, circuits aren't something very meaningful.

Dependent sets and circuits

Fact

1. *Any circuit is finite*
2. *Every dependent set contains a circuit.*
3. $a \in \mathrm{cl}(S)$ *iff at least one of the following holds:*
   - $a \in S$.
   - *There is a circuit* C *with* $a \in C$ *and* $C \setminus \{a\} \subseteq S$.

Loops

Let M be a matroid.

Definition

A *loop* is an element $x \in \mathrm{cl}(\varnothing)$.

- In $\mathbb{R}^n$, the zero vector is the unique loop.
- In a graph, a loop is an edge with the same start and end.
- In general, x is a loop if $\{x\}$ is a circuit.

Parallels

Definition

Two non-loop elements x, y are *parallel* if $x \in \mathrm{cl}(y)$.

Fact

This is an equivalence relation on non-loop elements.

- If $x \neq y$, then x and y are parallel iff $\{x, y\}$ is a circuit.
- In a graph, two edges are parallel if they have the same start and end.
- In $\mathbb{R}^n$, two vectors are parallel if they are geometrically parallel.

Simple matroids

Definition

A matroid M is *simple* if it has no circuits of size < 3.

Equivalently:

- There are no loops, and...
- If x and y are parallel, then $x = y$.

Simple matroids

Fact

Given any matroid M, we can form a simple matroid by throwing away loops and identifying parallel elements.

Fact

If M is a matroid and M' is the associated simple matroid, then M and M' have isomorphic lattices of closed sets.

Matroids are also called *pregeometries*, and simple matroids are called *geometries*.

Section 4

Finite matroids

In this section, all matroids are finite.

"Cryptomorphism"

- (Finite) matroids can be defined in many different ways.
- The different definitions appear unrelated...
- ...but are secretly equivalent.
- This phenomenon is called "*cryptomorphism*".

Definition via independent sets

Definition

A *matroid* is a finite set M and a family $\mathcal{I} \subseteq P(M)$ of "independent sets", satisfying the following axioms:

1. $\varnothing$ is independent.
2. A subset of an independent set is independent.
3. For any $X \subseteq M$, any two maximal independent subsets of X have the same cardinality.

Definition via bases

Definition

A *matroid* is a finite set M and a family $\mathcal{B} \subseteq P(M)$ of "bases", satisfying the following axioms:

1. There is at least one basis.
2. If B_1, B_2 are bases and $a \in B_2 \setminus B_1$, then there is $b \in B_1 \setminus B_2$ such that $B_1 \cup \{a\} \setminus \{b\}$ is a basis.

Definition via circuits

Definition

A *matroid* is a finite set M and a family $\mathcal{C} \subseteq P(M)$ of "circuits", satisfying the following axioms:

1. If C_1, C_2 are distinct circuits, then $C_1 \not\subseteq C_2$.
2. If C_1, C_2 are distinct circuits and $x \in C_1 \cap C_2$, then $C_1 \cup C_2 \setminus \{x\}$ contains a circuit.

Definition via rank functions

Definition

A *matroid* is a finite set M and a function $r : P(M) \to \mathbb{N}$ called the *rank function*, such that

1. $X \subseteq Y \implies r(X) \leq r(Y)$.
2. $0 \leq r(X) \leq |X|$.
3. $r(X \cup Y) \leq r(X) + r(Y) - r(X \cap Y)$.

Definition via closure operations

Definition

A *matroid* is a finite set M and a function $\mathrm{cl}(-) : P(M) \to P(M)$ such that

1. $X \subseteq \mathrm{cl}(X)$.
2. $X \subseteq Y \implies \mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$.
3. $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$.
4. If $a, b \notin \mathrm{cl}(X)$ and $a \in \mathrm{cl}(X \cup \{b\})$, then $b \in \mathrm{cl}(X \cup \{a\})$.

Duality

Let M be a (finite) matroid.

Definition

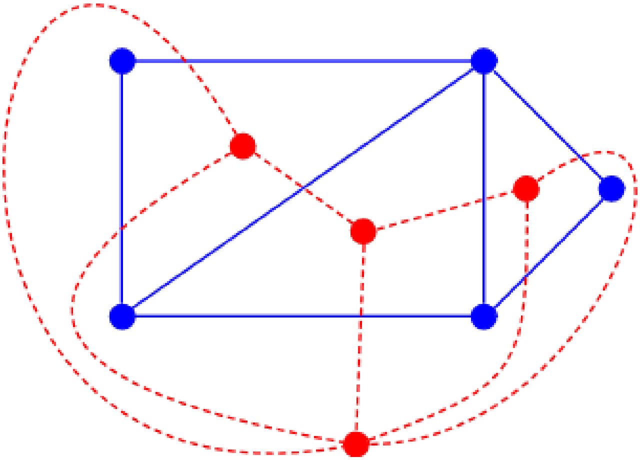
The *dual matroid* M' is characterized as follows:

- M' has the same underlying set as M.
- X is a basis of M' iff the complement $M \setminus X$ is a basis of M.

Fact

For matroids coming from planar graphs, this corresponds to taking the dual graph.

Duality



Greedy algorithms

Let M be a matroid and $f : M \to \mathbb{R}_{\geq 0}$ be a function.

Problem

Find an independent set $I \subseteq M$ maximizing $\sum_{x \in I} f(x)$.

Fact

The following "greedy algorithm" works:

- *Let $I_0 = \varnothing$.*
- *Once I_n is known...*
  - *Look at the set of $a \in M \setminus I_n$ such that $I_n \cup \{a\}$ is independent.*
  - *If empty, terminate and output I_n.*
  - *Otherwise, take a maximizing $f(a)$, let $I_{n+1} = I_n \cup \{a\}$.*

Also, this fact characterizes finite matroids (sort of).

Section 5

More examples of matroids

The uniform matroid

Let M be a set and n be finite. In the *uniform matroid of rank n on M*...

- A set $I \subseteq M$ is independent iff $|I| \leq n$.
- A set $B \subseteq M$ is a basis iff $|B| = n$.
- C is a circuit iff $|C| = n + 1$.
- $r(X) = \min(|X|, n)$.
- Closure is like so:

$$\mathrm{cl}(X) = \begin{cases} M & \text{if } |X| \geq n \\ X & \text{otherwise.} \end{cases}$$

Transversal matroids

Let X, Y be finite sets and $R \subseteq X \times Y$ be a relation.

- $X =$ people; $Y =$ jobs; $R(a, b)$ means person a can do job b.

Say $S \subseteq X$ is *independent* if there is an injection $f : S \to Y$ such that $R(a, f(a))$ holds for $a \in S$.

- We can assign each person in S a job in a non-overlapping, feasible way.

Fact

This defines a matroid structure on X.

Algebraic independence

Let L/K be an extension of fields.

Fact

There is a matroid on L where

- $a \in \mathrm{cl}(S)$ *if a is algebraic over the field generated by $K \cup S$.*
- $\{a_1, \ldots, a_n\}$ *is independent iff it is algebraically independent over K.*
- *The closed sets are the relatively algebraically closed subfields of L containing K.*
- *The rank of the matroid is the transcendence degree $\operatorname{tr.deg}(L/K)$.*

Algebraic closure in model theory

Let M be a structure.

Definition

If $\phi(x)$ is an $L(M)$-formula, then $\phi(M)$ denotes $\{a \in M : M \models \phi(a)\}$.
Such sets are called *M-definable sets*.
If $A \subseteq M$, an A-definable set is a set of the form $\phi(M)$, where $\phi(x)$ is an $L(A)$-formula.

Algebraic closure in model theory

Let M be a structure.

Definition

For $A \subseteq M$, the *algebraic closure* of A, written $\mathrm{acl}(A)$, is the union of all finite A-definable sets $X \subseteq M$.
We say b is *algebraic* over A if $b \in \mathrm{acl}(A)$.

Fact

$\mathrm{acl}(-)$ *is a finitary closure operator.*

Algebraic closure in model theory

Fact

In RCF, ACF, and many other theories of fields (like $\mathbb{Q}_p$), b is algebraic over A iff b is field-theoretically algebraic over A.

In these theories, $\mathrm{acl}(-)$ satisfies exchange, so it defines a matroid.

Algebraic closure in model theory

Let T be an L-theory.

Definition

T is *strongly minimal* if for any model M and M-definable set $X \subseteq M$, either X is finite or X is cofinite ($M \setminus X$ is finite).

ACF is strongly minimal.

Definition

If $L \supseteq \{\leq\}$, we say T is *o-minimal* if for any model M and M-definable set $X \subseteq M$, X is a finite union of intervals.

RCF and DLO are o-minimal.

Fact

In a strongly minimal or o-minimal theory, $\mathrm{acl}(-)$ *satisfies exchange, and defines a matroid.*

Section 6

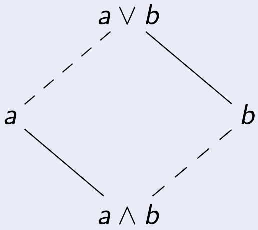
Modular matroids

Review: modular lattices

Definition

A lattice $(M, \leq)$ is *modular* if for any $a, b \in M$, there is an isomorphism

$$f : [a \wedge b, a] \to [b, a \vee b]$$
$$f(x) = x \vee b$$
$$f^{-1}(y) = y \wedge a$$



Modularity

Fact

The following properties are equivalent in a matroid M:

1. *If X, Y are finite-rank closed sets, then*
$$r(X \cup Y) = r(X) + r(Y) - r(X \cap Y).$$
2. *The lattice of finite-rank closed sets is modular.*
3. *The lattice of closed sets is modular.*

A matroid M is *modular* if these conditions hold.

Vector spaces

Example

$\mathbb{R}^n$ is a modular matroid, because

$$\dim(V + W) = \dim(V) + \dim(W) - \dim(V \cap W)$$

for linear subspaces $V, W \subseteq \mathbb{R}^n$.

Matroids and modular lattices

Let $(L, \wedge, \vee, 0)$ be a modular lattice with minimum 0.

Definition

An *atom* is a minimal non-zero element.

Definition

A modular lattice L is *atomistic* if every element has the form $x_1 \vee \cdots \vee x_n$ for some $n \geq 0$ and some atoms $x_1, \ldots, x_n$.

Fact

1. *If M is a modular matroid, the lattice of finite-rank closed sets is an atomistic modular lattice.*
2. *Atomistic modular lattices correspond exactly to modular simple matroids.*

Decomposition of modular matroids

Fact

Let M be a modular simple matroid. For $x, y \in M$, define $x \sim y$ if $\{x, y\}$ is closed.

1. $\sim$ *is an equivalence relation.*
2. M *is a direct sum* $M_1 + M_2 + \cdots$ *of the equivalence classes.*

Fact

This amounts to decomposing the corresponding lattice as a product:

$$L \cong L_1 \times L_2 \times \cdots \times L_n.$$

(at least when there are finitely many components).

Projective geometries

Definition

A *d-dimensional projective geometry* is an indecomposable modular simple matroid of rank $d+1$.

Fact

A 0-dimensional projective geometry is a single point.

Fact

A 1-dimensional projective geometry is a uniform matroid of rank 2 on a set of three or more points.

Projective planes

Definition

A *projective plane* is a set M of *points*, and a set $L \subseteq P(M)$ of *lines*, satisfying the axioms:

- For any two distinct points x, y, there is a unique line containing x and y.
- For any two lines ℓ_1, ℓ_2, there is a unique point in the intersection $\ell_1 \cap \ell_2$.
- Every line has at least three points, and every point is on at least three lines.

Fact

1. *A projective plane determines a 2-dimensional projective geometry in which the closed sets are $\varnothing$, M, the singletons (points), and the lines.*
2. *2-dimensional projective geometries are the same thing as projective planes.*

The real projective plane

- Define a formal symbol P_ℓ for lines $\ell \subseteq \mathbb{R}^2$ so that

$$P_{\ell_1} = P_{\ell_2} \iff \ell_1 \parallel \ell_2.$$

- Let $\ell_\infty = \{P_\ell : \ell \text{ is a line in } \mathbb{R}^2\}$.
- For ℓ a line in $\mathbb{R}^2$, let $\overline{\ell}$ be $\ell \cup \{P_\ell\}$.

Idea

P_ℓ is a "point at infinity."

Definition

The *real projective plane* has

- Points are elements of $\mathbb{R}^2 \cup \ell_\infty$.
- Lines are ℓ_∞ and the $\overline{\ell}$ for $\ell \subseteq \mathbb{R}^2$.

The real projective plane

Fact

The real projective plane is the simple matroid associated with $\mathbb{R}^3$.

Definition

A *skew field* is a structure $(K, +, \cdot)$ satisfying all the field axioms except possibly $xy = yx$.

Example: the quaternions.

Fact

If K *is a skew field, there is a natural modular matroid structure on* K^n *generalizing the one on* $\mathbb{R}^n$. *When* $n = 3$, *this gives a projective plane.*

Projective 3-spaces

Definition

A projective 3-space is a set M of "points", a set $L \subseteq P(M)$ of "lines", and a set $\Pi \subseteq P(M)$ of "planes", such that

- Any two points determine a line.
- Any two lines on a plane intersect in a point.
- Any two lines through a point determine a plane.
- Any two planes intersect in a line.
- [Various non-degeneracy axioms]

Duality

Given a projective plane P, we can build a *dual* projective plane P' where

- Points in P' correspond to lines in P.
- Lines in P correspond to points in P'.
- If x, ℓ are a point and a line in P, and x', ℓ' are the corresponding line and point in P', then

$$x \in \ell \iff \ell' \in x'.$$

Fact

The real projective plane is isomorphic to its dual.

Duality

Fact

Let $(L, \leq)$ be an atomistic modular lattice of length $n < \infty$. Then the dual lattice $(L, \geq)$ is an atomistic modular lattice of length n.

Fact

Given a modular simple matroid M, there is a "dual" modular simple matroid M' whose lattice of closed sets is dual to the lattice of closed sets in M.

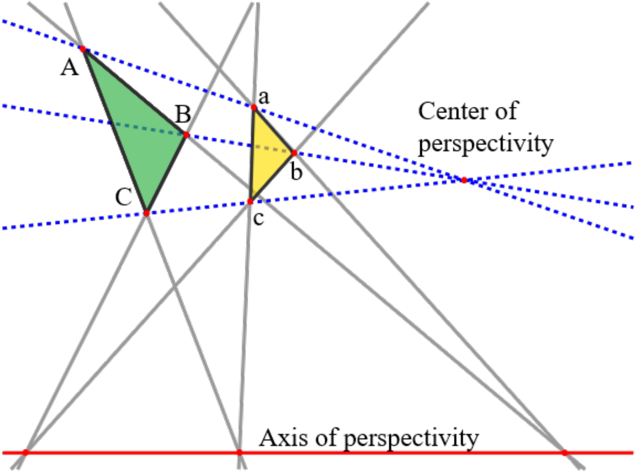
Remark

Points in M' correspond to hyperplanes in M (closed sets of rank one less than the rank of M).

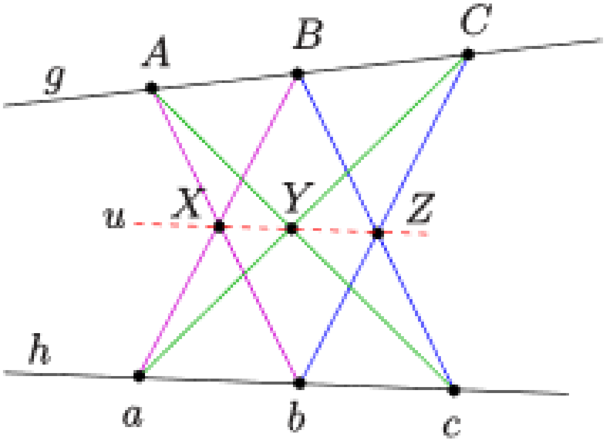
Remark

This duality is unrelated to the duality for finite matroids.

Desargues's theorem



Pappus's theorem



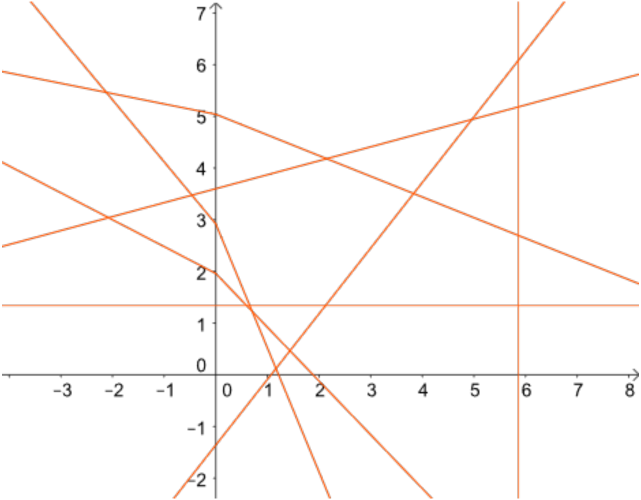
Projective planes

Fact

Let P be a projective plane.

- *P comes from a skew field iff P satisfies Desargues's theorem.*
- *P comes from a field iff P satisfies Desargues's theorem and Pappus's theorem.*
- *If P is a Desarguesian projective plane, then the corresponding skew field is determined up to isomorphism.*
- *There are non-Desarguesian projective planes.*

Non-desarguesian planes



Higher dimensional projective geometries

Fact

If $n > 2$, then any n-dimensional projective geometry comes from a skew field.

Desargues's theorem is automatic.

Modularity in model theory

Conjecture (Trichotomy conjecture, FALSE)

Let M be a model of a strongly minimal theory. Consider the simple matroid associated with $(M, \mathrm{acl}(-))$. Then one of three things happens:

1. *The matroid is trivial ($\mathrm{cl}(X) = X$).*
2. *The matroid is a projective geometry* usually infinite rank *over a skew field* or an affine geometry.
3. *M defines an algebraically closed field.*

1. If $(M, \mathrm{acl}(-))$ is modular, then (1) or (2) must happen.
   - This happens when M is ω-categorical.
2. Hrushovski found a counterexample to the trichotomy conjecture.
3. The trichotomy conjecture is true in the context of "Zariski geometries."
4. For o-minimal theories, the trichotomy conjecture is (essentially) true.