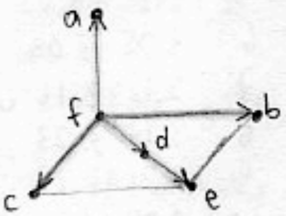
some motivating examples

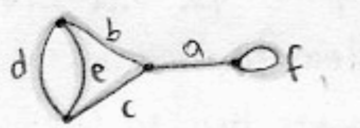
1. Linear algebra



$a = (1,0,0)$ $\quad$ $d = (0, \frac{1}{2}, \frac{1}{2})$
$b = (0,1,0)$ $\quad$ $e = (0,1,1)$
$c = (0,0,1)$ $\quad$ $f = (0,0,0)$

Goal: Choose a set of
lin. indep. vectors

2. Graph theory



Goal: Choose a set of edges
without forming cycles.

Q1. One of these vectors is not like the others. Which?
roads
Which?

f is useless:
one can never
choose it.

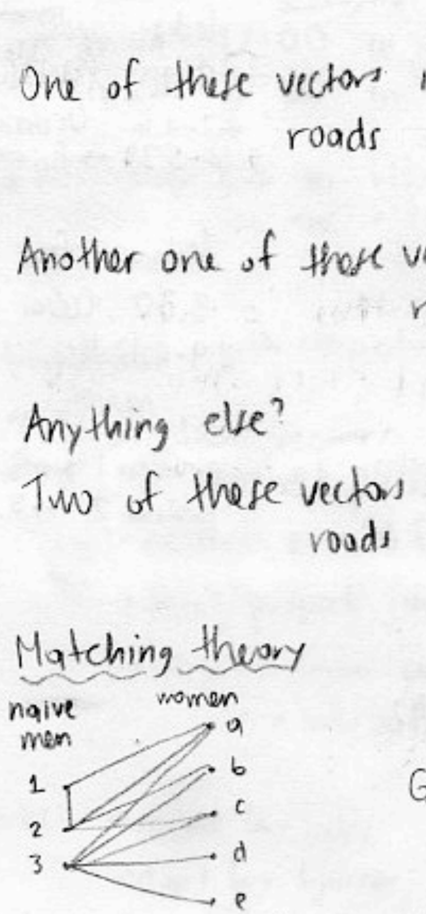
Q2 Another one of these vectors is not like the others. Which?
roads
Which?

a is essential:
one should always
choose it

Q3 Anything else?
Two of these vectors are not like the others. Which?
roads
Which?

d, e are "twins":
one can only
choose one of them

3. Matching theory



Goal: Choose a set of women
to propose to.
(No poligamy or same-sex marriage
in US and in Colombia.)

1. $\begin{pmatrix}\text{Independent sets}\\ \text{of vectors}\end{pmatrix}$

$$\boxed{\begin{array}{l}\emptyset\\ a, b, c, d, e\\ ab, ac, ad, ae, bc, bd, be, cd, ce\\ abc, abd, abe, acd, ace\end{array}}$$

(Do it.)

2. $\begin{pmatrix}\text{Independent sets}\\ \text{of edges}\end{pmatrix} \rightarrow$ the same ones.

(Exercise.)

3. $\begin{pmatrix}\text{Independent sets}\\ \text{of women}\end{pmatrix} \rightarrow$ the same ones.

(Exercise.)

Matroid theory studies "independence"; in particular 1, 2, 3.

Def. A matroid is a pair $(E, \mathcal{I})$ where

- E is a finite set
- $\mathcal{I}$ is a collection of subsets of E such that:

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $I \subset J$ and $J \in \mathcal{I}$, then $I \in \mathcal{I}$.

(I3) If $I, J \in \mathcal{I}$ and $|I| < |J|$, then there exists $j \in J - I$ such that $I \cup j \in \mathcal{I}$.

E = "ground set"

$\mathcal{I}$ = collection of "independent sets"

1 **Proposition.** Let E be a finite set of vectors in a vector space V, and let $\mathcal{I}$ be the collection of "linearly independent sets" in E. Then $(E, \mathcal{I})$ is a matroid.

Proof We need to check:

$(I1) \to$ trivial
$(I2) \to$ trivial
$(I3)$. Let $I = \{i_1, \ldots, i_a\}$. Suppose $I \cup j \notin \mathcal{I}$ for all $j \in J - I$.

I indep $\to$ eqn $c_1 i_1 + \cdots + c_a i_a + c j = 0 \quad c \neq 0$
$I \cup j$ dep

$$j = -\frac{c_1 i_1 + \cdots + c_a i_a}{c} \in \text{span } I$$

So $J \subseteq \text{span}(I) \Rightarrow \text{span}(J) \subseteq \text{span}(I)$
$\Rightarrow \dim(\text{span}(J)) \leq \dim(\text{span}(I)) \Rightarrow |J| \leq |I|$.
$\Rightarrow |J| \leq |I|$. $\Rightarrow\Leftarrow$ ■

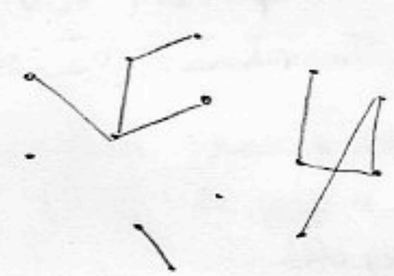
contradiction qed

vertices edges

2. **Proposition.** Let $G = (V, E)$ be a graph, and let $\mathcal{I}$ be the collection of edge sets forming no cycles.
Then $(E, \mathcal{I})$ is a matroid

Proof. $(I_1), (I_2)$ trivial

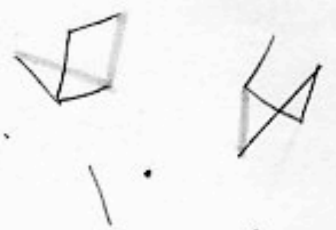
(I_3). Observation: If $I \subset E$ is independent, then the graph (V, I) has $|V| - |I|$ connected components. (Clear.)



(V, I)

Suppose $I \cup j \notin \mathcal{I}$ for all $j \in J - I$.

Then edge j forms a cycle with I $\Rightarrow$ Adding j doesn't connect components of (V, I)



$(V, I \cup J)$

$\Rightarrow (V, I \cup J)$ has $|V| - |I|$ components

$\Rightarrow (V, J)$ has $\geq |V| - |I|$ components

$\Rightarrow |V| - |J| \geq |V| - |I|$

$\Rightarrow |I| \leq |J|$ $\Rightarrow\Leftarrow$ ∎

3. **Proposition.** Let G be a bipartite graph with bipartition (D, E). Let $\mathcal{I}$ be the collection of subsets of E which can be matched to D. Then $(E, \mathcal{I})$ is a matroid.

Proof HW 1.

Two matroids are isomorphic if they are the same matroid, up to a relabelling of the ground set. (Like exs 1,2,3 from lecture 1.)

$(E, \mathcal{I}) \cong (E', \mathcal{I}')$ if there is a bijection between E and E' that induces a bijection between $\mathcal{I}$ and $\mathcal{I}'$.

We will often simply say that $(E, \mathcal{I})$ and $(E', \mathcal{I}')$ are the same matroid.

Def. Linear matroids are matroids of vector configurations. (Ex 1.)

Graphical matroids are matroids of graphs. (Ex 2.)

Transversal matroids are matroids of matching problems. (Ex. 3)

Def. A basis of a matroid is a maximal independent set.

↳ not contained in a larger indep. set

lecture 3
1/29/07

In example,

$\mathcal{B} = \{abc, abd, abe, acd, ace\}$

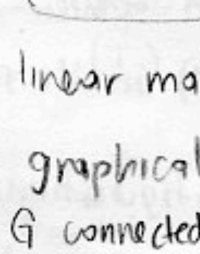
This is a shorter way of describing M, since

(indep. sets) = (subsets of bases)

Prop. All the bases of a matroid have the same size.

Proof. Suppose not; say $|B_1| < |B_2|$ are bases.
By (I3), $\exists\, b \in B_2$ s.t. $B_1 \cup b$ is independent.
But then B_1 wouldn't be max'l indep! ■

Cor. Every independent set is a subset of a basis.



Q. So why can this matching not be completed to a complete matching?
A. The matching cannot.
But $\{a,d\}$ can.

Ex. 1. For linear matroids, we expected this "by dimension".

Ex. 2. For graphical matroids.

G connected: "basis" = "spanning tree" (subgraph which · is connected · has no cycles · contains all vertices)

G general: "basis" = "spanning forest" (A sp. tree in each component.)

 It is not obvious that they should have the same size!

Ex 3. For transversal matroids, "bases" are called "transversals"

Given a set S

subsets $S_1, \dots, S_n$

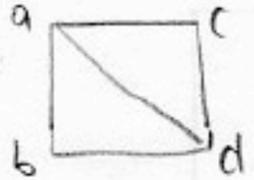
A transversal is a subset T of size n which can be labelled $T = \{a_1, \dots, a_n\}$ so that $a_i \in T_i$.

(In our example, $S = \{a, b, c, d, e, f\}$

$S_1 = \{a\}$ $S_2 = \{a, b, c\}$ $S_3 = \{a, b, c, d, e\}$

"Cultura general" in algebraic combinatorics.

How many spanning trees does a graph have?



Form a $V \times V$ matrix L: ("Laplacian")

Let $L_{v,v} = \deg(v)$

$L_{u,v} = -(\#\text{ edges from } u \text{ to } v)$

$$L = \begin{array}{c|cccc} & a & b & c & d \\ \hline a & 3 & -1 & -1 & -1 \\ b & -1 & 2 & 0 & -1 \\ c & -1 & 0 & 2 & -1 \\ d & -1 & -1 & -1 & 3 \end{array}$$

The eigenvalues of L are $0, \lambda_1, \lambda_2, \dots, \lambda_{v-1}$

Matrix-tree theorem (Kirchhoff)

The number of spanning trees of G is

$$\frac{1}{n} \lambda_1 \lambda_2 \cdots \lambda_{n-1}$$

It also equals any cofactor of L.

$$\begin{bmatrix} 3 & -1 & -1 & -1 \\ -1 & 2 & 0 & -1 \\ -1 & 0 & 2 & -1 \\ -1 & -1 & -1 & 3 \end{bmatrix}$$

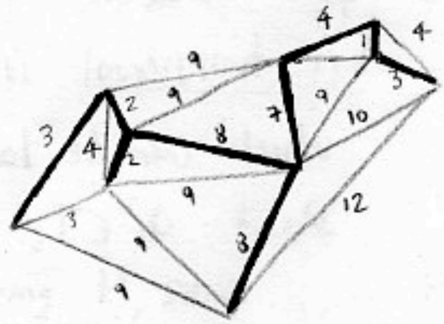
- Final project:
Understand this, and its generalization to linear matroids.

$$t(G) = (-1)^{3+3}(6-1+0-2+1+0)$$
$$= 8.$$

6

A "real-life" problem:

Given a graph $G=(V,E)$ and a weight on each edge $(w: E \to \mathbb{R}_{>0})$ find a minimum weight spanning tree of G.



One possible (but naive (ingenuo)) strategy:

(alg. voraz)

> **Greedy algorithm:**
> At each step, choose a cheapest edge that doesn't form a cycle.

Surprising fact: this works!

More generally:

Given: a matroid $M=(E,\mathcal{I})$

weights on the elements $w: E \to \mathbb{R}$

Problem: find a basis of minimum weight.

> **Greedy algorithm:** (Kruskal, 1956)
> - Start with $I=\emptyset$
> - Add to I a cheapest element e such that $I \cup e \in \mathcal{I}$.
> - Repeat until you have a basis.

> **Proposition.** Kruskal's algorithm works: For any weight function $w: E \to \mathbb{R}_{>0}$ it finds a basis of minimum weight.

Proof. Let Kruskal give $I = i_1 i_2 \dots i_n$ $\quad w(i_1) \leq \dots \leq w(i_n)$

let a min basis be $J = j_1 j_2 \dots j_n$ $\quad w(j_1) \leq \dots \leq w(j_n)$

Suppose $w(I) > w(J)$.

Let k be such that $w(i_k) > w(j_k)$.

$i_1 i_2 \dots i_{k-1}$, $j_1 \dots j_k$ indep $\Rightarrow i_1 i_2 \dots i_{k-1} j_r$ indep. for some $1 \leq r \leq k$

But $w(j_r) \leq w(j_k) < w(i_k)$

So greedy algorithm would have chosen j_r instead of i_k! ∎

In fact, matroids are the simplicial complexes where the greedy algorithm works.

Proposition. $M=(E,\mathcal{I})$ is a matroid if and only if

(I1) $\emptyset \in \mathcal{I}$

(I2) $I \subset J,\ J \in \mathcal{I} \Rightarrow I \in \mathcal{I}$

(I3') For any $w: E \to \mathbb{R}_{\geq 0}$, the greedy algorithm finds a set $I \in \mathcal{I}$ of minimum weight

(Def. A simplicial complex is an $(E,\mathcal{I})$ satisfying axiom (I2).)

Proof: $\Rightarrow$ ✓

$\Leftarrow$ Suppose $I, J \in \mathcal{I}$, $|I|<|J|$ don't satisfy exchange.

Consider the weighting:

$$w(e)=\begin{cases} 1 & e \in I \\ 2 & e \in J \quad e \notin I \\ N & e \in E \quad e \notin J \end{cases}$$

where N is huge. (Say $N > 2|E|$.)

- Greedy alg. will
  - choose all of I
  - not be able to choose any of J
  - choose the rest in $E-J$ $\Rightarrow$ weight $=|I|+N(r-|I|)$

- There is at least one basis containing J.

  It has weight $\leq 2|J|+N(r-|J|)$

$$< N + N(r-|J|)$$
$$= N(r-(|J|-1)) \leq N(r-|I|)$$

So greedy alg. did not choose a basis of min weight.

lecture 5
2/02/07

Prop. Let E be a finite set, and $\mathcal{B} \subset 2^E$.
Then $\mathcal{B}$ is the collection of bases of a matroid if and only if:

(B1) $\mathcal{B} \neq \emptyset$

(B2) If $A, B \in \mathcal{B}$ and $a \in A - B$, there exists $b \in B - A$ s.t. $A - a \cup b \in \mathcal{B}$.

Proof.

$\Rightarrow$ Let $\mathcal{B}$ be the collection of bases of $(E, \mathcal{I})$.

(B1): There are indep sets, so there are maxl ones.

(B2). Apply exchange axiom to $A - a$, B. $(|A-a| = |B| - 1)$

$\Leftarrow$ Let $\mathcal{B}$ satisfy (B1), (B2)

$\boxed{\text{Step 1}}$ The sets in $\mathcal{B}$ have the same size.

Proof: Take $B \in \mathcal{B}$ with $|B|$ minimal.

Goal: Every other $A \in \mathcal{B}$ has $|A| = |B|$

Induct on $|A-B|$

1a. Initial case $\quad |A-B| = 0 \Rightarrow A \subseteq B \overset{B \text{ min.}}{\Rightarrow} A = B \Rightarrow |A| = |B|$ ■

1b. Inductive step $\quad$ Sup true for $|A-B| = k-1$, prove it for $|A-B| = k$.

$|A-B| = k > 1 \Rightarrow$ Let $a \in A-B$

$\overset{(B2)}{\Rightarrow}$ Find $b \in B-A$ with $A-a \cup b \in \mathcal{B}$

Notice:

$|(A-a\cup b)-B| = |A-B| - 1$

By inductive assumption, $|A-a\cup b| = |B|$

$|A| = |B|$ ■

$\boxed{\text{Step 2}}$ Let $\mathcal{I} = \{ I \subseteq E : I \subseteq B \text{ for some } B \in \mathcal{B} \}$

Claim: $(E, \mathcal{I})$ is a matroid.

(I1): Let $B \in \mathcal{B}$. $\emptyset \subset B \Rightarrow \emptyset \in \mathcal{I}$

(I2): Suppose $I \subset J$, $J \in \mathcal{I} \Rightarrow J \subset B$ for a $B \in \mathcal{B}$

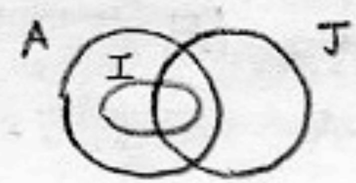
$\Rightarrow I \subset B \Rightarrow I \in \mathcal{I}$.

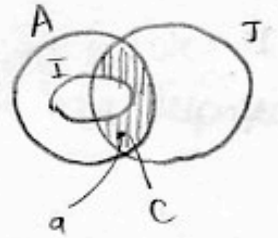
(I3): Given $\begin{pmatrix} I, J \in \mathcal{I} \\ |I| < |J| \end{pmatrix}$ need: $(\exists j \in J \text{ with } I \cup j \in \mathcal{I})$

<u>Proof</u>. Induct on $r - |J|$.

2a. initial case $r - |J| = 0$: J = basis.

Let A be a basis containing I.

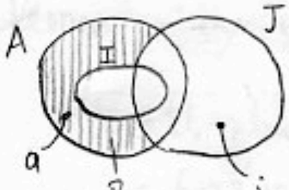


2a1 • 

If $C \neq \emptyset$

Let $a \in C$

- $I \cup a \subset A \Rightarrow I \cup a \in \mathcal{I}$
- $a \in J - I$ ■

2a2 • 

If $B \neq 0$

Let $a \in B$

Since $A, J \in \mathcal{B}$, $a \in A - J$

$\overset{(B2)}{\Rightarrow}$ Find $j \in J - A$ with $A - a \cup j \in \mathcal{B}$

- $I \cup j \subset A - a \cup j \Rightarrow I \cup j \in \mathcal{I}$
- $j \in J - I$ ■

2a3 • If $B = C = \emptyset$, 

$|J| > |I| = |A|$, contradicting Step 1.

2b Inductive step

Sup. true for $r - |J| = k-1$, show for $r - |J| = k$

Let $\begin{cases} I, J \in \mathcal{I} \\ |I| < |J| \end{cases}$ $\quad r - |J| = k$

Say $I \subset A$ $\quad J \subset B$ $\quad A, B \in \mathcal{B}$.

By the argument in initial case for I, B,

find $b \in B - I$ such that $I \cup b \in \mathcal{I}$.

2b1. Case 1: $b \in J \Rightarrow I \cup b \in \mathcal{I}$
$b \in J - I$ ✓ ■

2b2. Case 2: $b \notin J \Rightarrow I \cup b \in \mathcal{I}$
$J \cup b \subset B \Rightarrow J \cup b \in \mathcal{I}$

So $\begin{cases} I \cup b, J \cup b \in \mathcal{I} \\ |I \cup b| < |J \cup b| \end{cases}$ $\quad r - |J \cup b| = k-1$

Induction $\Rightarrow$ Find $c \in (J \cup b) - (I \cup b) \Rightarrow c \in J - I$
with $I \cup b \cup c \in \mathcal{I}$ $\quad I \cup c \in \mathcal{I}$ ■

Theorem/Definition.

A <u>matroid</u> $(E,\mathcal{B})$ consists of a finite ground set E and a collection $\mathcal{B} \subset 2^E$ of "bases" such that

(B1) $\mathcal{B} \neq \emptyset$

(B2) If $A, B \in \mathcal{B}$ and $a \in A-B$, there exists $b \in B-A$ with $A-a\cup b \in \mathcal{B}$.

We could have defined matroids in this equivalent way. (People do!)

$$\begin{tikzcd}
M=(E,\mathcal{I}) \arrow[rr] & & \mathcal{B}=\{\text{maxl. sets in } \mathcal{I}\} \arrow[d] \\
\mathcal{I}=\{\text{subsets of sets in } \mathcal{B}\} \arrow[u] & & M=(E,\mathcal{B}) \arrow[ll]
\end{tikzcd}$$

A slightly philosophical digression:

We have two axiom systems. 1. $(E, \mathcal{I}) \to (I1), (I2), (I3)$

2. $(E, \mathcal{B}) \to (B1), (B2)$

- Proving the equivalence of these two axiom systems was not easy. BUT.
- The real difficulty is coming up with good axiom systems.

Q. Is $(I1), (I2), (I3)$ a good axiom system for "independence"?

A. Definitely!

Evidence: (so far)
- It simultaneously applies to lin. alg., graph th., matching th., Dyck paths, ...
- It describes the simplicial complexes where the greedy algorithm works

⋮

Q Is $(B1), (B2)$ a good axiom system for "bases"?

A. Yes.
- It is "weak enough" that $(I1)-(I3) \Rightarrow (B1)-(B2)$
- It is "strong enough" that $(B1)-(B2) \Rightarrow (I1)-(I3)$.

⋮

lecture 6
2/05/07

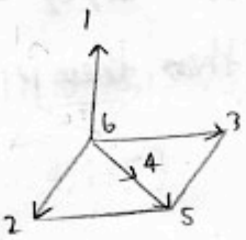
We have described matroids in terms of their $\begin{cases} \circ \text{ bases} \\ \circ \text{ independent sets} \end{cases}$

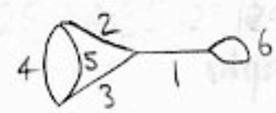
What about their dependent sets?

Remember our example matroid

$E = \{1, \ldots, 6\}$

$\mathcal{B} = \{123, 124, 125, 134, 135\}$





$\mathcal{I}$ was a long list

$\mathcal{B}$ was a more "economical" presentation.

Now

$\mathcal{D} = \{6, 16, 26, 36, 46, 56, 45, 234, 235, 245, 345, 126, \ldots\}$ too long!

Better to list just the minimal ones (by containment)

$\mathcal{C} = \{6, 45, 234, 235\}$ "circuits"

Def. A <u>circuit</u> of a matroid is a minimal dependent set.

Again, circuits completely describe the matroid.

$\mathcal{C}$ = circuits $\longrightarrow$ $\mathcal{D}$ = dependents = sets containing circuits

$\downarrow$

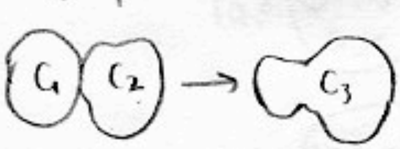
$\mathcal{I}$ = independents = not dependents.

So what are the key properties of circuits? (Circuit axioms?)

- non-triviality: (C1) $\emptyset$ is not a circuit.
- from big to small: (C2) A (proper) subset of a circuit is not a circuit
- from two circuits to...: (C3) If C_1, C_2 are circuits and $x \in C_1 \cap C_2$, then there is a circuit $C_3 \subseteq (C_1 \cup C_2) - x$.

$\downarrow$

graphs:



Theorem Let E be a finite set and $\mathcal{C} \subseteq 2^E$. Then $\mathcal{C}$ is the collection of circuits of a matroid if and only if it satisfies (C1), (C2), (C3).

Proof. "$\Rightarrow$"

Let $M = (E, \mathcal{I})$ be a matroid and $\mathcal{C}$ its collection of circuits. (minimal dependent sets)

(C1). $\emptyset$ is independent, so it's not a circuit. ✓

(C2). If $C_1 \subset C_2$ were circuits, C_2 wouldn't be minimal. ✓

(C3). Suppose not. Then $C_1 \cup C_2 - x$ is independent.

Take y in $C_1 - C_2$ $\quad (C_1 \not\subseteq C_2)$

Then $C_1 - y$ indep, $C_1 \cup C_2 - x$ indep $\qquad |C_1 - y| < |C_1 \cup C_2 - x|$

$\Rightarrow C_1 \cup a - y$ indep $\quad a \in C_2 \qquad |C_1 \cup a - y| < |C_1 \cup C_2 - x|$?

$\Rightarrow C_1 \cup a \cup b - y$ indep $\quad b \in C_2 \qquad |C_1 \cup a \cup b - y| < |C_1 \cup C_2 - x|$?

$\vdots$

This can only stop with $C_1 \cup C_2 - y$ indep.

But $\underset{\text{dep}}{C_2} \subseteq \underset{\text{indep}}{C_1 \cup C_2 - y}$

Today we'll see the first piece of evidence that the different points of view ($\mathcal{I}, \mathcal{B}, \mathcal{C}, \ldots$) are not isolated, they complement each other.

Theorem.

Let $M = (E, \mathcal{B})$ be a matroid. Let

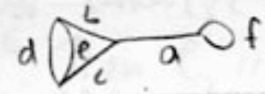
$$\mathcal{B}^* = \{ E - B \mid B \in \mathcal{B} \}$$

Then $M^* = (E, \mathcal{B}^*)$ is a matroid, called the <u>dual</u> of M.

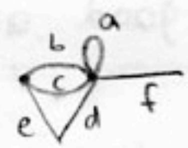
Ex

$E = \{a, b, c, d, e, f\}$

$\mathcal{B} = \{abc, abd, abe, acd, ace\}$



$\mathcal{B}^* = \{def, cef, cdf, bef, bdf\}$



Strategy of proof:

(Lemma on circuits) $\rightarrow$ (lemma on bases) $\rightarrow$ (theorem).

1. Lemma on circuits

If I is independent and $I \cup e$ is dependent, then there is a unique circuit in $I \cup e$, and it contains e.

<u>Proof</u>. $I \cup e$ contains a circuit C, and $C \not\subset I$ so $e \in C$.
Suppose C' is another one: $C' \subset I \cup e$, $e \in C'$
$(C3) \Rightarrow$ There is a circuit in $(C \cup C') - e \subseteq I$. ∎

<u>Note</u>. This is the "fundamental circuit of e with resp. to I"
It is denoted $C(e, I)$.

2. Lemma on bases

$(B2)^*$ Let $A, B \in \mathcal{B}$ and $b \in B-A$. Then there exists $a \in A-B$ such that $A-a\cup b \in \mathcal{B}$.

Proof.

A indep, $A \cup b$ dep $\Rightarrow$ Let $C = C(b,A)$

Idea: The only real dependence in $A\cup b$ is C.

So $A-a\cup b$ is a basis if and only if $a \in C(b,A)$ $(a \neq b)$

(You break that dependence)

Need $a \in A-B$, $a \in C$. Since B indep, C dep $\Rightarrow \exists\, a \in C-B$. ∎

3. Proof of theorem

Check $\mathcal{B}^*$ satisfies (B1), (B2). (B1) is obvious.

(B2) Let $B^* = E-B$.

Let $A^*, B^* \in \mathcal{B}^*$ $a \in A^*-B^*$

$\Rightarrow A, B \in \mathcal{B}$ $a \in B-A$

Use $(B2)^* \Rightarrow$ Find $b \in A-B$ such that $A-b\cup a \in \mathcal{B}$.

$\Rightarrow b \in B^*-A^*$ has $(A-b\cup a)^* \in \mathcal{B}^*$

$A^*-a\cup b \in \mathcal{B}^*$ ∎

Remark. $\boxed{(E,\mathcal{B}) \text{ is a matroid} \iff \mathcal{B} \text{ satisfies } (B1), (B2)^*.}$

Proof. Exercise. (Hint: Use matroid duality)

Or see Oxley, Corollary 2.1.5.

lecture
2/9/07

<u>Today</u>: Duality for linear matroids.

First:

<u>The matroid of a subspace</u>

Let V be a k-dim subspace of $\mathbb{R}^n$, with a fixed system of coordinates. By HW 1, Problem 1, there is a matroid $M(V)$, such that

If the rows of a $k \times n$ matrix A span V the columns of A have matroid $M(V)$.

<u>Goal</u>. Describe $M(V)$ intrinsically, without reference to A.

Say $k=3$, $n=5$.

$$A = \begin{array}{c} \\ 3 \\ \\ \end{array}\!\!\begin{array}{c} \begin{bmatrix} | & | & | & | & | \\ c_1 & c_2 & c_3 & c_4 & c_5 \\ | & | & | & | & | \end{bmatrix} \\ 5 \end{array} \qquad \text{rowspace}(A) = V$$

Note: $\left(\begin{array}{c} c_1, c_3, c_4 \text{ is} \\ \text{a basis} \end{array}\right) \iff \begin{bmatrix} | & & | & | & \\ c_1 & 0 & c_3 & c_4 & 0 \\ | & & | & | & \end{bmatrix} = A_{134}$ has col. rank 3

$$\iff \dim(\text{rowspace } A_{134}) = 3$$

Consider the projection

$$\pi_{134} : \mathbb{R}^5 \longrightarrow X_{134} = \{(*,0,*,*,0)\}$$
$$(x_1, \ldots, x_5) \longmapsto (x_1, 0, x_3, x_4, 0)$$

Then

$$\text{rowspace } A_{134} = \pi_{134}(V)$$

So $\begin{pmatrix} c_1, c_3, c_4 \\ \text{basis} \end{pmatrix} \Longleftrightarrow \dim(\pi_{134}(V)) = 3 \Longleftrightarrow \pi_{134}|_V : V \to X_{134}$ is bijective

$$\Longleftrightarrow V \cap \ker \pi_{134} = \emptyset \Longleftrightarrow V \cap X_{25} = \emptyset$$

$$\Longleftrightarrow V + X_{25} = \mathbb{R}^5$$

So: **Prop.** The bases of the matroid $M(V)$ are the subsets S for which $V \cap X_{E-S} = \emptyset$

Theorem. "Orthogonal complements are matroid duals"

If M is the matroid of a subspace V of $\mathbb{R}^n$, then M^* is the matroid of the orthogonal complement $V^\perp$.

Note This also holds over any field.

Corollary.
The dual of a linear matroid is linear.

Proof of Theorem.

$(S \text{ is a basis of } M(V^\perp))$

$\Longleftrightarrow V^\perp \cap X_{E-S} = 0$

$\Longleftrightarrow V^\perp \cap X_S^{\perp} = 0$

$\Longleftrightarrow (V + X_S)^\perp = 0$

$\Longleftrightarrow V + X_S = \mathbb{R}^n$

$\Longleftrightarrow V \cap X_S = \emptyset$

$\Longleftrightarrow ((E-S) \text{ is a basis of } M(V))$

Lemma:
$U^\perp \cap V^\perp = (U+V)^\perp$
Proof: Exercise.

Therefore
$M(V^\perp) = M(V)^*$ ∎

<u>Note</u> A "generic" k-plane and $(n-k)$-plane have empty intersection.

So a "generic" k-plane V has every k-set S as a basis, giving the uniform matroid $U_{n,k}$.

The matroid $M(V)$ "measures" how special the position of V is with respect to the coordinate axes and the subspaces determined by them.

Today: Duality for graphs

vertices → points
edges → continuous curves

Def. A planar graph is one that can be drawn in the plane, so that no edges intersect (except possibly at their endpoints)

Def A plane graph is one already drawn in the plane.

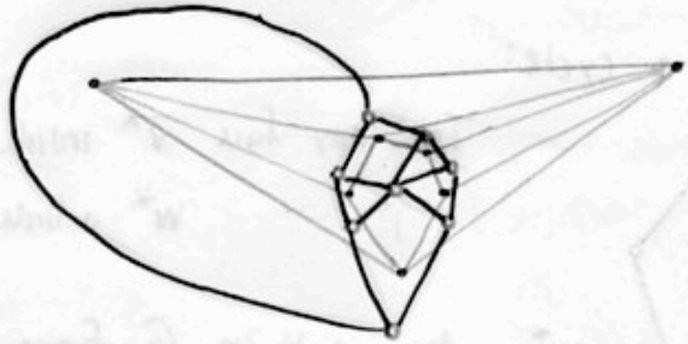
Note: A plane graph G divides the plane into regions, called the "faces" of the graph.

Define the dual plane graph G^*:

- draw a vertex f^* of G^* in each face f of G
- then, for each edge e in G, common to faces f and g, draw an edge e^* in G^* joining f^* and g^*, which crosses only edge e.

Observation. Suppose G is connected
If G^* is a dual for G,
then G is a dual for G^*: $\boxed{G^{**} = G}$

Ex.



$G \to G^*$

$V \leftrightarrow F^*$
$E \leftrightarrow E^*$
$F \leftrightarrow V^*$

Theorem. "Graph duality is matroid duality"
If G is a connected plane graph and G^* is dual to it, then $M(G^*) = M(G)^*$

Proof.

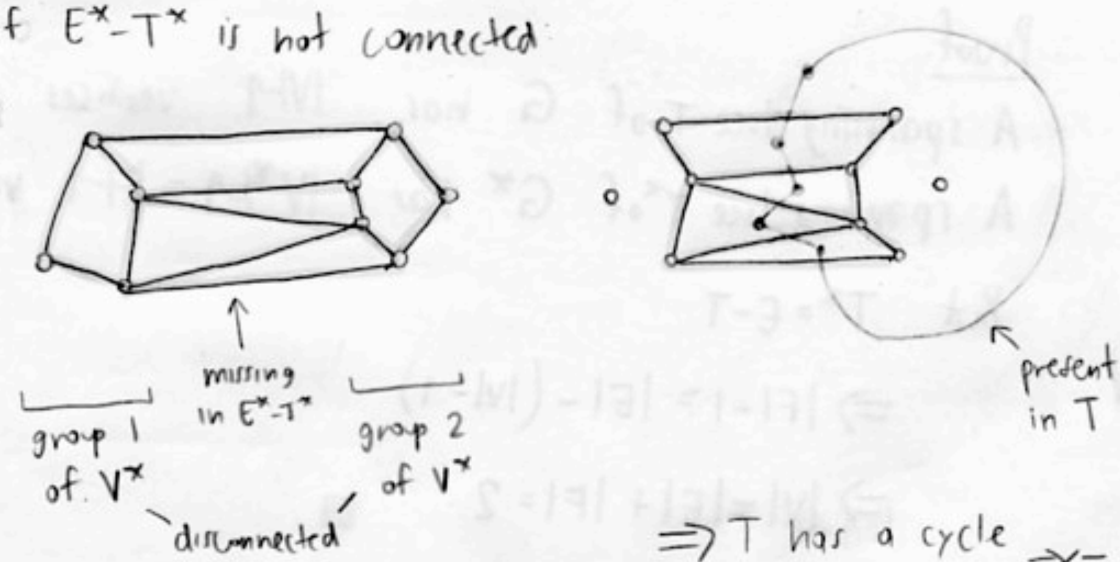
Need: (T spanning tree on G) $\Longleftrightarrow$ ($E^* - T^*$ spanning tree on G^*)

By duality, it suffices to show "$\Rightarrow$" (and then apply it to $T \to E^* - T^*$, $G \to G^*$)

"$\Rightarrow$" A spanning tree is a connected, cycle-free subgraph using all the vertices. Suppose not:

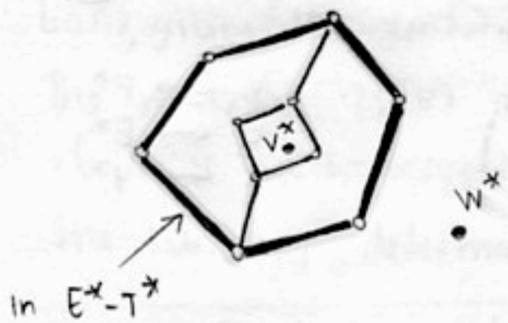
- If $E^* - T^*$ is not connected

G^*



$\Rightarrow T$ has a cycle $\Rightarrow\!\!\times\!\!\Leftarrow$

∘ If $E^* - T^*$ has a cycle:



Take any face v^* inside the cycle
w^* outside the cycle

Any path in G from v to w would need to cross the cycle
$\Rightarrow$ would need an edge e such that $e^* \in E^* - T^*$
$\Rightarrow e \notin T$

So v and w are disconnected in T
$\Rightarrow \Leftarrow$

∎

> Corollary (Euler)
>
> For a connected plane graph,
> $$|V| - |E| + |F| = 2.$$

Proof.

A spanning tree T of G has $|V|-1$ vertices

A spanning tree T^* of G^* has $|V^*|-1 = |F|-1$ vertices

But $T^* = E - T$

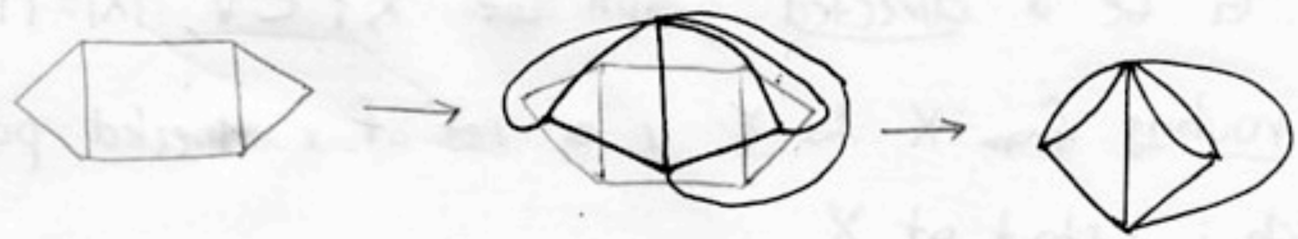
$$\Rightarrow |F| - 1 = |E| - (|V| - 1)$$

$$\Rightarrow |V| - |E| + |F| = 2.$$ ∎

Observation.

Different embeddings of G may give different dual graphs G^*

G_1



G_1^*

G_2

G_2^*

(G_1^* has a vertex of degree 6, G_2^* doesn't.)

But $M(G_1^*) \cong M(G_2^*)$.

A good project:

(1) How are the different duals of G related?

(2) When is $M(G) \cong M(H)$?

Duality for transversal matroids

Let G be a directed graph. Let $X, Y \subset V$, $|X| = |Y| = r$

A routing from X to Y is a set of r directed paths which:
- start at X
- end at Y
- have no vertices in common. (A path may consist of a single vertex)

Ex:

$\bullet = X$

$\circ = Y$

$r = 4$

Theorem. (Mason, 1972) Let $G = (V, E)$ be a digraph and let $B_0 \subseteq V$. Let

$$L(G, B_0) = \{X \subset V \mid \text{there is a routing from } X \text{ to } B_0\}$$

Then $L(G, B_0)$ is the collection of bases of a matroid.

(in hw 3)

Such a matroid is called "cotransversal" or "strict gammoid".

Theorem (Ingleton–Piff, 1973)
Cotransversal matroids are precisely the duals of transversal matroids.

Sketch of a proof: (F. Ardila, "Transversal and cotransversal...", 2006)

1 ◦ Transversal matroids are linear $\to$ represented by $V \subset \mathbb{R}^n$

2 ◦ Cotransversal matroids are linear $\to$ represented by $W \subset \mathbb{R}^n$

3 ◦ (The Vs appearing in 1) and (the Ws appearing in 2) are orthogonal complements of each other. $\boxtimes$

Project:

- Understand this proof.
- Investigate the different linear reps. of transv, cotransv matroids.

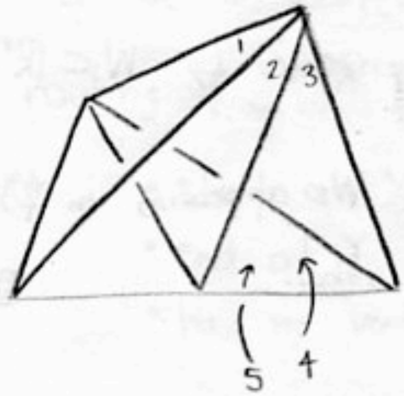
Goal for the next week(s):

Define and study:

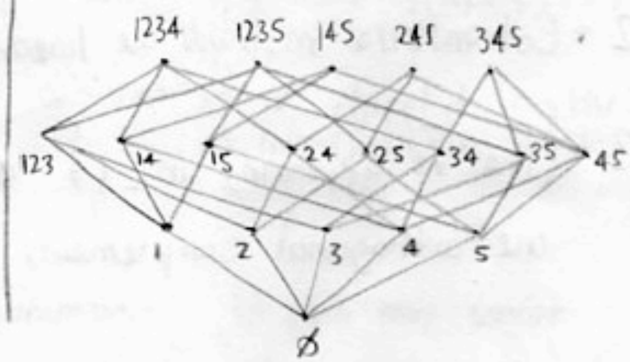
rank $\to$ closure $\to$ lattice of flats

Let's motivate this with hyperplane arrangements.

A hyperplane arrangement:



Its intersection poset:



Elements of P_A: Intersections of hyperplanes of A.

Order in P_A: $x \leq y$ in P_A if $x \supseteq y$.

This is a partially ordered set:

- A set P
- A partial order $\leq$ such that
  - $a \leq a$
  - $a \leq b$ and $b \leq a$ imply $a = b$
  - $a \leq b$ and $b \leq c$ imply $a \leq c$

(Ex: $a<b$, $A \subset B$, $a|b$, ...)

Note
For $a \neq b$, we could have:
- $a<b$,
- $a>b$, or
- neither.

Question.
How much does L_A (a combinatorial object) tell us about A (a geometric object)?
Ex. # regions? # bounded regions? topology?

Answer.
A lot!
Yes. Yes. Yes.

Next goal: Generalize and study this construction:
$(M \text{ matroid}) \to (L_M$ "lattice of flats")

lecture 13
2/19/07

Rank ("Dimension" for matroids)

Let M be a matroid on E.

> **Def.** The rank function $r: 2^E \to \mathbb{N}$ is
>
> $r(X) = \max\{|I| : I \subseteq X,\ I \in \mathcal{I}\}$
>
> $=$ size of any "basis" of A $\longrightarrow$ [Recall: (HW 2) $(A, \mathcal{I}_A)$ is pure

> **Def.** The rank of M is $r(M) = r(E)$.

Some key properties:

(R1) $0 \le r(X) \le |X|$ for all X

(R2) $r(X) \le r(Y)$ for all $X \subseteq Y$

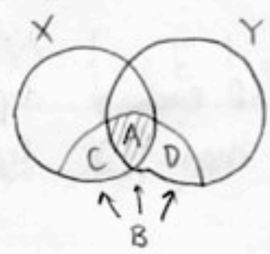
(R1), (R2) $\to$ trivial

(R3) $r(X \cup Y) + r(X \cap Y) \le r(X) + r(Y)$ for all X, Y.

Proof of (R3):

Let A be a basis of $X \cap Y$

A is independent in $X \cup Y$ so extend it to a basis $B \supseteq A$ of $X \cup Y$



$r(X \cup Y) = |B| = |A| + |C| + |D|$

$r(X \cap Y) = |A|$

$r(X) \geq |A| + |C|$ since $A \cup C \in \mathcal{I}$, $A \cup C \subseteq X$

$r(Y) \geq |A| + |D|$ since $A \cup D \in \mathcal{I}$, $A \cup D \subseteq Y$

These "key properties" are strong enough:

> **Theorem.**
> A function $r: 2^E \to \mathbb{N}$ is the rank function of a matroid on E if and only if it satisfies (R1), (R2), (R3).

$\Rightarrow$ Done

$\Leftarrow$ Given r, say

$$I \in \mathcal{I} \iff r(I) = |I|.$$

Using (R1)–(R3), one proves:

- $(E, \mathcal{I})$ is a matroid
- Its rank function is r.

Details omitted – do it yourself or see Oxley.

But the key step is this:

> **Lemma.** Let $X, Y \subset E$.
> If $r(X \cup y) = r(X)$ for all $y \in Y$
> then $r(X \cup Y) = r(X)$.

$\rightarrow$ If each y dep. on X then Y dep. on X.

Proof: Induct on $|Y|$.

$|Y| = 0, 1 \rightarrow$ trivial.

Suppose true for $|Y| = n-1$.

Let $|Y| = n$. Write $Y = \underbrace{Y'}_{\substack{n-1 \\ \text{elts}}} \cup \underbrace{y}_{\text{elt}}$

$r(X\cup y') = r(X)$ for $y'\in Y' \Rightarrow \underline{r(X\cup Y') = r(X)}$ by induction hyp.

$\underline{r(X\cup y) = r(X)}$ also.

Now:

$$\begin{aligned} r(X\cup Y) &= r(X\cup Y'\cup y) \\ &= r((X\cup Y')\cup(X\cup y)) \\ &\le r(X\cup Y') + r(X\cup y) - r((X\cup Y')\cap(X\cup y)) \qquad (R3) \\ &= r(X) + r(X) - r(X) \\ &= r(X) \end{aligned}$$

But $r(X\cup Y) \geq r(X)$ by (R2) $\Rightarrow r(X\cup Y) = r(X)$. ☒

$\boxed{\text{Closure}}$ ("Span" for matroids)

Let M be a matroid on E.

> <u>Def</u> The <u>closure</u> <u>operator</u> $cl: 2^E \to 2^E$ is
> $cl(X) = \{x\in E \mid r(X\cup x) = r(X)\}$

examples:
- topological closure
- span
- generated subgroup
- Convex hull
- algebraic closure

↑

Key properties:

(CL1) For all X, $X \subseteq cl(X)$.

(CL2) For all $X\subseteq Y$, $cl(X) \subseteq cl(Y)$

(CL3) For all X, $cl(cl(X)) = cl(X)$

} defining properties of an "abstract closure operator"

(CL4) For all $X\subseteq E$, $x\in E$,

if $\begin{pmatrix} y\notin cl(X) \\ y\in cl(X\cup x)\end{pmatrix}$ then $x\in cl(X\cup y)$.

} "exchange property"

Proof:

(CL1) is trivial.

(CL2). Let $X \subseteq Y$. Want: $cl(X) \subseteq cl(Y)$

Let $x \in cl(X) \Rightarrow r(X \cup x) = r(X)$.

Let B be a basis of X

$\Rightarrow$ basis of $X \cup x$ also. (so $B \cup x$ is dependent)

Extend B to a basis C of $Y \cup x$.

C doesn't contain x (because $B \cup x$ is dependent), so $C \subseteq Y$.

$$\Rightarrow r(Y) \geq |C| = r(Y \cup x)$$

$$\Rightarrow r(Y) = r(Y \cup x) \quad \Rightarrow x \in cl(Y).$$

(CL3) We know $X \subseteq cl(X) \Rightarrow cl(X) \subseteq cl(cl(X))$

Suppose $x \in cl(cl(X))$

$$r(cl(X) \cup x) = r(cl(X)) = r(X)$$

But

$$cl(X) \cup x \supseteq X \cup x \supseteq X$$

so also

$$r(X \cup x) = r(X) \Rightarrow x \in cl(X)$$

<u>Lemma</u>

$\boxed{r(cl(X)) = r(X)}$

<u>Proof</u>.

$r(X \cup x) = r(X) \quad x \in cl(X)$

$\Downarrow$ lemma

$r(X \cup cl(X)) = r(X)$

$r(cl(X)) = r(X)$

(CL4) let $y \in cl(X \cup x) \Rightarrow r(X \cup x \cup y) = r(X \cup x)$

$y \notin cl(X) \Rightarrow r(X \cup y) \neq r(X)$

$r(X \cup y) = r(X) + 1$

$$\Rightarrow r(X \cup x \cup y) = r(X \cup x)$$
$$\leq r(X) + 1 = r(X \cup y)$$

$$\Rightarrow x \in cl(X \cup y)$$

<u>Lemma</u>. $X \subset E, x \in E$

$\boxed{r(X \cup x) = r(X) \text{ or } r(X) + 1}$

<u>Proof</u>

B basis of X

$\Downarrow$

B or $B \cup x$ basis of $X \cup x$.

$\boxed{\text{Theorem. A function } cl: 2^E \to 2^E \text{ is the closure operator of a matroid on } E \text{ if and only if it satisfies (CL1)–(CL4).}}$

In other words: $\boxed{\text{We can think of a matroid as a closure operator satisfying the exchange property.}}$

$\Rightarrow$ Done

$\Leftarrow$ Given cl, define

$$I \in \mathcal{I} \iff x \notin cl(I-x) \text{ for all } x \in I.$$

Using (CL1) - (CL4), one proves:

- $(E, \mathcal{I})$ is a matroid
- cl is its closure operator.

Key lemma. If $X \in \mathcal{I}$ and $X \cup x \notin \mathcal{I}$ (with $\mathcal{I}$ as above) then $x \in cl(X)$.

Details omitted. ∎

Parenthesis. (A possible project)

- A closure operator satisfying ((CL4): exchange property) is a matroid. It captures the combinatorial essence of independence.
- A closure operator satisfying ((CL4'): antiexchange property) is a convex geometry. It captures the combinatorial essence of convexity. Ex: cl = "convex hull"

$\boxed{\text{(CL4'): If } \begin{pmatrix} y \in cl(X \cup x) \\ y \notin cl(X) \end{pmatrix} \text{ then } x \notin cl(X \cup y).}$

$\boxed{\text{Flats}}$ ("Closed sets" for matroids)

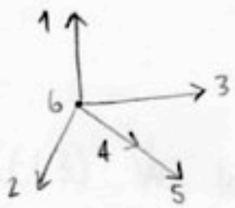
Let M be a matroid on E.

$\boxed{\text{Def. A \underline{flat} of M is a set } F \subseteq E \text{ such that } cl(F) = F.}$

In other words, $r(F \cup x) = r(F) + 1$ for all $x \notin F$.

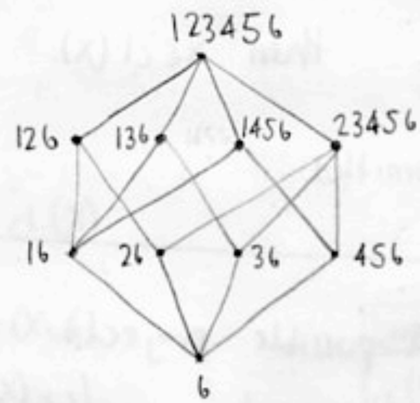
Ex If M is represented by a vector configuration,

(flats) $\longleftrightarrow$ (spanned subspaces)



Flats: 6
16, 26, 36, 456
126, 136, 1456, 23456
123456

We can order the flats by containment:



Conjunto parcialmente ordenado (poset)

Def A partially ordered set (poset) $(P, \leq)$ is a set P with a binary relation "$\leq$" such that
- $a \leq a$
- $a \leq b$ and $b \leq a \Rightarrow a = b$
- $a \leq b$ and $b \leq c \Rightarrow a \leq c$

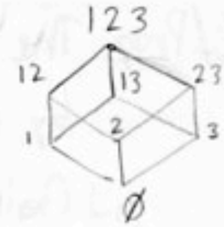
For $a \neq b$, one can have
- $a < b$,
- $a > b$, or
- neither.

Examples of posets:

① 2^S = subsets of a set S

$A \le B$ means $A \subseteq B$

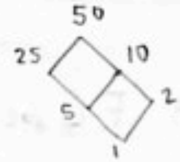
$2^{[3]}$:



② D_n = divisors of n

$a \le b$ means $a \mid b$

D_{50}:



③ $P = \mathbb{Z}$

$a \le b$ means $a \le b$

④ L_M = flats of M

$A \le B$ means $A \subseteq B$

$\left(\begin{array}{l}\text{Say } a \text{ \underline{covers} } b \\ \text{Write } a \gtrdot b\end{array}\right)$ if $\left(\begin{array}{l}\cdot\ a > b, \text{ and} \\ \cdot\ \text{there is no } c \text{ such that } a > c > b\end{array}\right)$

Draw P by putting
- a dot for each elt. of P
- an edge for each cover relation $a \gtrdot b$.

Def A poset P is a lattice if every pair of elements a, b has a least upper bound $a \vee b$ and a greatest lower bound $a \wedge b$.

LUB: $(a \le a \vee b), (b \le a \vee b)$, and $\left(\begin{array}{l} a \le c \\ b \le c \end{array} \Rightarrow a \vee b \le c\right)$

GLB: $(a \ge a \wedge b), (b \ge a \wedge b)$, and $\left(\begin{array}{l} a \ge c \\ b \ge c \end{array} \Rightarrow a \wedge b \ge c\right)$

Show ①, ②, ③ are lattices, is not.

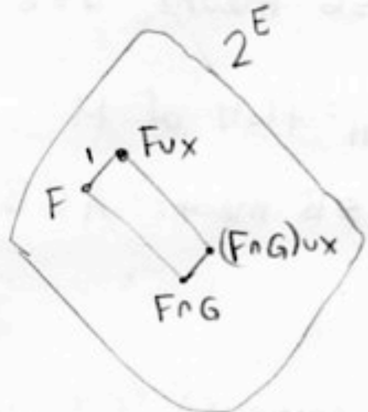
Def/Prop. The poset of flats of a matroid M ordered by containment is a lattice.
Call it the "<u>lattice of flats</u>" L_M.

<u>Proof.</u> Let F, G be flats.

∘ $F \wedge G = F \cap G$:

- $F \cap G \subseteq F$, $F \cap G \subseteq G$. If $H \subseteq F$, $H \subseteq G$ then $H \subseteq F \cap G$.

- $F \cap G$ is a flat:
  Let $x \notin F \cap G \Rightarrow x \notin F$ or $x \notin G$.
  Say $x \notin F$.
  $$r(F) + r((F\cap G) \cup x) \geq r(F \cup x) + r(F \cap G) = r(F) + 1 + r(F \cap G)$$
  So $r((F \cap G)\cup x) \geq r(F \cap G) + 1$.



∘ $F \vee G = cl(F \cup G)$

- $cl(F \cup G) \supseteq F \cup G \supseteq F, G$ (CL1). If $H \supseteq F$, $H \supseteq G$ then $H \supseteq F \cup G$
  $\Rightarrow$ (CL2) $cl(H) \supseteq cl(F \cup G)$
  $\Rightarrow$ (CL3) $H \supseteq cl(F \cup G)$ ▨

Def. A poset is <u>graded</u> if there exists a rank function $r : P \to \mathbb{Z}$ such that
- ∘ If x is minimal, then $r(x) = 0$.
- ∘ If y covers x, then $r(y) = r(x) + 1$.

In other words, P "has floors"

Prop. L_M is graded.

Proof. The rank on L_M is the rank on M.

- Note: $cl(\emptyset) = \{loops\}$ is the unique minl element of L_M, and it has rank 0.

- Suppose $F \lessdot G$.

Let $x \in G - F$. Then $F \subsetneq F \cup x \subseteq G \Rightarrow \underset{F}{\underset{\shortparallel}{cl(F)}} \subsetneq cl(F \cup x) \subseteq \underset{G}{\underset{\shortparallel}{cl(G)}}$

But

$r(cl(F\cup x)) = r(F \cup x) = r(F)+1 > r(cl(F))$

so

$cl(F \cup x) = G \rightarrow r(G) = r(F)+1$ ∎

Prop L_M is "submodular":

$r(x) + r(y) \geq r(x \vee y) + r(x \wedge y)$

for all $x, y \in L_M$

Proof:

$r(F) + r(G) \geq r(F \cup G) + r(F \cap G) = r(cl(F \cup G)) + r(F \cap G) = r(F \vee G) + r(F \wedge G)$ ∎

Prop. L_M is "atomic":

Every element is a join of elements of rank 1.

Proof: Let $F \in L_M$. For each $f \in F$, $cl(f) \subset F$. So

$$F = \bigcup_{f \in F} f \subseteq \bigcup_{f \in F} cl(f) \subseteq F$$

So $F = \bigcup_{f \in F} cl(f) \Rightarrow F = cl\left(\bigcup_{f \in F} cl(f)\right) = \bigvee_{f \in F} \overset{\text{rank } 1}{\overset{\downarrow}{cl(f)}}$ ∎

Notes.

- In a lattice, any finite set $a, b, c, \ldots$ has a "meet" $a \wedge b \wedge c \wedge \ldots$ (a greatest lower bound) and a "join" $a \vee b \vee c \vee \ldots$ (a least upper bound)

- In L_M,
  $F \wedge G \wedge \ldots = F \cap G \cap \ldots$
  $F \vee G \vee \ldots = cl(F \cup G \cup \ldots)$

Def. A finite lattice is *geometric* if it is semimodular and atomic.

(note: semimodular $\to$ graded)

> **Theorem** A lattice is geometric if and only if it is the lattice of flats of a matroid.

$\Leftarrow$: done

$\Rightarrow$: Let $\mathcal{L}$ be geometric.

Let E be the set of atoms. (If $E=\emptyset$, $\mathcal{L}=\mathcal{L}(U_{0,0})$)

Define

$$r: 2^E \to \mathbb{Z}$$

$$r(\{e_1,\dots,e_k\}) = r_{\mathcal{L}}(e_1 \vee \dots \vee e_k)$$

Claim: (1) (E,r) is a matroid

(2) Its lattice of flats is $\mathcal{L}$.

Proof of (1):

Check that r satisfies the local rank axioms:

(R1)' $r(\emptyset)=0$

Clear since $r(\emptyset) = r_{\mathcal{L}}(\hat{0})$

(R2)' $r(A\cup a) - r(A) = 0$ or 1.

Let $\bigvee_{\alpha\in A} \alpha = x \Rightarrow r(A\cup a) - r(A) = r_{\mathcal{L}}(x \vee a) - r_{\mathcal{L}}(x)$

$\mathcal{L}$ semimodular $\Rightarrow r_{\mathcal{L}}(a) + r_{\mathcal{L}}(x) \geq r_{\mathcal{L}}(x\vee a) + r_{\mathcal{L}}(x \wedge a)$

$$r_{\mathcal{L}}(x\vee a) - r_{\mathcal{L}}(x) \leq r_{\mathcal{L}}(a) - r_{\mathcal{L}}(\underbrace{x\wedge a}_{\leq a})$$

$$\underset{\text{clear}}{0 \leq} r_{\mathcal{L}}(x\vee a) - r_{\mathcal{L}}(x) \leq \underbrace{1 - (0 \text{ or } 1)}_{\leq 1}$$

(R3)' If $r(A)=r(A\cup a)=r(A\cup b)$ then $r(A)=r(A\cup a\cup b)$.

Let $\bigvee_{\alpha\in A}\alpha = x$.

Then $r_{\mathcal{L}}(x)=r_{\mathcal{L}}(x\vee a)=r_{\mathcal{L}}(x\vee b)$

Since $x\le x\vee a \Rightarrow x=x\vee a$ $\Rightarrow x\vee a\vee b = x\vee b = x$

$x\le x\vee b \Rightarrow x=x\vee b$

$\Rightarrow r_{\mathcal{L}}(x\vee a\vee b)=r_{\mathcal{L}}(x)$

$\Rightarrow r(A\cup a\cup b)=r(A)$. ☒

So $\mathcal{L}$ geometric $\to (E,r)$ is a matroid M.

Now I need to show "it is the right matroid" — that is:

(2) Claim: $\mathcal{L}=\mathcal{L}_M$.

<u>Proof</u>. We show that this is an isomorphism of posets:

$$\varphi:\mathcal{L}\longrightarrow\mathcal{L}_M$$

$$x\longmapsto\{\text{atoms } a\le x\}$$

Need to check: ⓐ φ is a bijection on the sets $\mathcal{L}$, $\mathcal{L}_M$

ⓑ φ preserves order: $x\underset{\mathcal{L}}{\le} y \iff \varphi(x)\underset{\mathcal{L}_M}{\le}\varphi(y)$

Note: $\mathcal{L}$ is atomic, so $x=\bigvee_{\substack{\text{atoms}\\ a\le x}} a = \bigvee_{a\in\varphi(x)} a$

ⓐ • φ is well-defined:

Let $F=\{\text{atoms } a \text{ such that } a\le x\}$. Need: F flat.

Suppose not: $r_M(F\cup b)=r_M(F)$ for $b\in E$, $b\notin F$.

$\Rightarrow r_{\mathcal{L}}(x\vee b)=r_{\mathcal{L}}(x) \underset{\text{semimod}}{\Rightarrow} r_{\mathcal{L}}(x\wedge b)=r_{\mathcal{L}}(b)=1$

$\Rightarrow x\wedge b=b\Rightarrow b\le x\Rightarrow b\in F$.

• φ is injective:

Suppose $\varphi(x)=\varphi(y)$. Then

$$x = \bigvee_{\substack{\text{atoms}\\ \alpha\le x}} \alpha = \bigvee_{\substack{\text{atoms}\\ \alpha\le y}} \alpha = y.$$

• φ is surjective:

Let F be a flat of M.

Let $x = \bigvee_{\alpha\in F} \alpha$. Claim: $F=\varphi(x)$.

$\subseteq$: $a\in F \Rightarrow x=\bigvee_{\alpha\in F}\alpha \geq a \Rightarrow a\in\varphi(x)$

$\supseteq$: $a\in\varphi(x) \Rightarrow a\le x = \bigvee_{\alpha\in F}\alpha \Rightarrow \bigvee_{\alpha\in F}\alpha = \left(\bigvee_{\alpha\in F}\alpha\right)\vee a$

$$\Rightarrow r_{\mathcal{L}}\Big(\bigvee_{\alpha\in F}\alpha\Big) = r_{\mathcal{L}}\Big(\bigvee_{\alpha\in F\cup a}\alpha\Big) \Rightarrow r_M(F)=r_M(F\cup a).$$

Since F is a flat, $a\in F$.

(b) φ preserves order:

• $x\underset{\mathcal{L}}{\leq} y \Rightarrow \{\text{atoms} \le x\} \subseteq \{\text{atoms}\le y\} \Rightarrow \varphi(x) \underset{\mathcal{L}_M}{\leq} \varphi(y)$

• $\varphi(x) \underset{\mathcal{L}_M}{\leq} \varphi(y) \Rightarrow x = \bigvee_{a\in\varphi(x)} a \underset{\mathcal{L}}{\leq} \bigvee_{a\in\varphi(y)} a = y$ ∎

∎

So we have

$$\text{matroids} \longrightarrow \text{geometric lattices}$$

$$M \longmapsto \mathcal{L}_M$$

How much information do we lose?

- We lose loops
- We lose parallel elements

We don't lose anything else! (Follows from the proof.)

<u>Def</u> A matroid is <u>simple</u> if it has no loops and no parallel elements.

<u>Theorem.</u>
This correspondence is bijective:

$$\text{simple matroids} \longleftrightarrow \text{geometric lattices}$$

<u>note</u>:
matroid = "(combinatorial) pregeometry"
simple matroid = "(combinatorial) geometry"

Also, there is a canonical way to go:

$$\text{matroid} \longrightarrow \text{simple matroid}$$

- delete loops
- keep 1 element of each parallel class.

Prop. Geometric lattices are coatomic: every flat of corank k is the meet of some k coatoms.

Proof.

coatoms of $\mathcal{L}_M$ = flats of M of rank $r(M)-1$

= "hyperplanes"

= maximal non-spanning sets of M.

Induct on k. $k=1$ obvious.

Let X be a flat with $r(X) = r-k$.

Let $y \notin X$, and $Y = \mathrm{cl}(X \cup y) \Rightarrow r(Y) = r-k+1$. and $Y \gtrdot X$ in $\mathcal{L}_M$.

So $Y = H_1 \cap \dots \cap H_{k-1}$.

- If $E-y$ is not spanning, let $H_k = E-y$.
- If $E-y$ is spanning, we have $\underset{\text{non-span.}}{\underset{\uparrow}{X}} \subset \underset{\text{span.}}{\underset{\uparrow}{E-y}}$, so let

$X \subset H_k \subset E-y$ with H_k maximal non-spanning.

Either way,

$$\begin{matrix} X \subset Y \\ X \subset H_k \end{matrix} \rightarrow X \subset \underset{\text{in } \mathcal{L}_M}{\underset{\uparrow}{(Y \cap H_k)}} \subset Y$$

But $X \lessdot Y$ and $\underset{\text{no } y}{\underset{\uparrow}{Y \cap H_k}} \neq \underset{\text{yes } y}{\underset{\uparrow}{Y}} \Rightarrow X = Y \cap H_k$. ▨

vector spaces $\to$ subspaces

groups $\to$ subgroups

matroids $\to$ submatroids?

Ojo

pg. 41 $\downarrow$ pg. 40

lecture 19
3/7/07

$\boxed{\text{minors}}$ (the matroids "living inside" a matroid)

Let M be a matroid on E.

Let $T \subseteq E$.

Def. The <u>deletion</u> of T from M (or <u>restriction</u> to $E-T$ of M) is the matroid $M \setminus T = M|(E-T)$ with

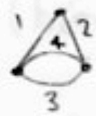
- Ground set: $E-T$
- Rank: $r_{M\setminus T}(X) = r(X)$ $(X \subseteq E-T)$

Def. The <u>contraction</u> of T from M is the matroid M/T with

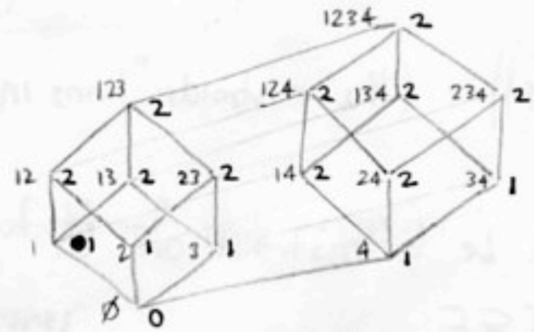
- Ground set: $E-T$
- Rank: $r_{M/T}(X) = r_M(X \cup T) - r_M(T)$ $(X \subseteq E-T)$

Recall:

One way to think about a matroid is through its rank function.

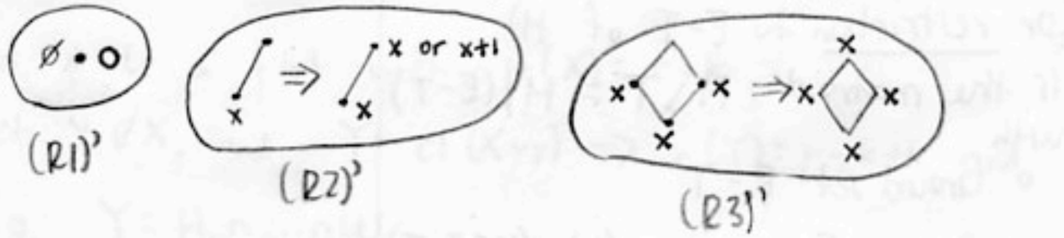
Ex. $G =$ 

$\mathcal{B} = 12, 13, 14, 23, 24$

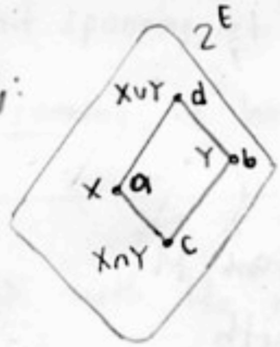


$r : 2^E \to \mathbb{Z}$

A rank function is a labelling of 2^E such that:



Note: Submodularity:

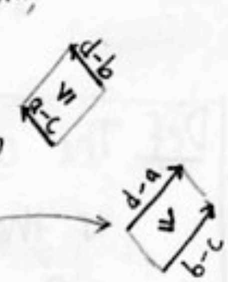


In any parallelogram,

$a + b \geq c + d$

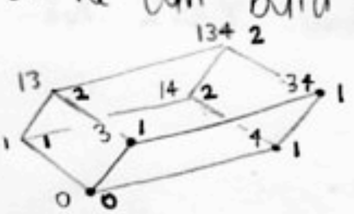
$a - c \geq d - b$

$b - c \geq d - a$

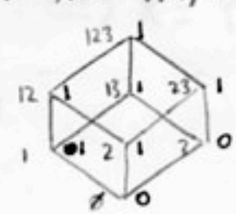


"Subcubes" also have these properties.

So we can build more matroids in this way:



M\2

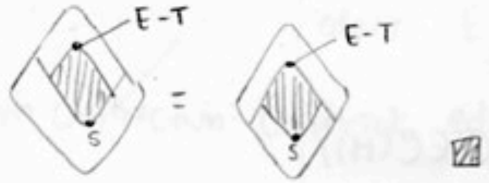


M/4

Prop. Let $S, T \subseteq E$, $S \cap T = \emptyset$. Then

- $(M \setminus S) \setminus T = M \setminus (S \cup T) = (M \setminus T) \setminus S$
- $(M/S)/T = M/(S \cup T) = (M/T)/S$
- $(M/S) \setminus T = (M \setminus T)/S$

Pf. By picture. For example, the third is



So deletion and contraction commute:

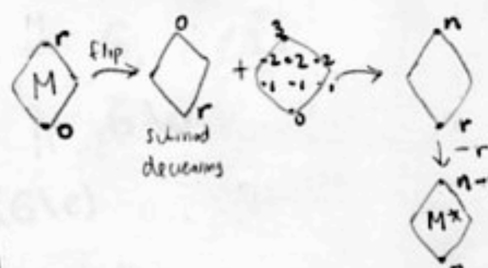
$$M/2\setminus 59/6/7\setminus 8 = M/267\setminus 589$$

Def. A <u>minor</u> of M is a matroid of the form $M/S\setminus T$ for $S, T \subset E$, $S \cap T = \emptyset$

lecture 20
3/9/07

By the way:

Prop.
$r_{M^*}(X) = |X| - r_M + r_M(E-X)$



Prop. Deletion and contraction are dual:

$$(M/T)^* = M^* \setminus T$$
$$(M \setminus T)^* = M^*/T$$

Pf: You. (HW 4)

Prop. $\mathcal{I}(M \setminus T) = \{I \subseteq E-T : I \in \mathcal{I}(M)\}$ → indeps. disjoint with T

$\mathcal{I}(M/T) = \{I \subseteq E-T : I \cup B_T \in \mathcal{I}(M)\}$ → indeps. containing a basis for T

where B_T is (any) fixed basis of T.

Pf.

$X \in \mathcal{I}(M \setminus T) \iff r_{M \setminus T}(X) = |X| \iff r_M(X) = |X| \iff X \in \mathcal{I}(M)$

$X \in \mathcal{I}(M/T) \iff r_{M/T}(X) = |X| \iff r_M(X \cup T) - r_M(T) = |X|$

$\iff r_M(X \cup B_T) = |B_T| + |X| \iff X \cup B_T \in \mathcal{I}(M)$

Prop.

$\mathcal{C}(M \setminus T) = \{C \subseteq E - T : C \in \mathcal{C}(M)\}$

$\mathcal{C}(M/T) =$ minimal sets in $\{C - T : C \in \mathcal{C}(M)\}$

$cl_{M \setminus T}(X) = cl_M(X) - T$

$cl_{M/T}(X) = cl_M(X \cup T) - T$

$\mathcal{L}_{M \setminus T} =$ complicated

$\mathcal{L}_{M/T} =$ interval $[cl(T), 1]$ of $\mathcal{L}_M$

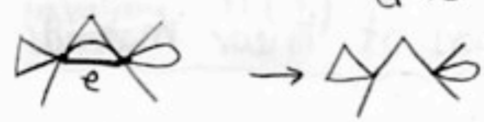
etc.

Minors of graphical matroids:

Let $G=(V,E)$

Let $e \in E$.

G G\e

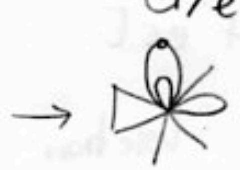


Graph deletion: Delete edge e

vertices: V

edges: $E \setminus e$

G/e



Graph contraction: Contract edge $e = i_1 i_2$

vertices: $(V - \{i_1, i_2\}) \cup i$

edges: ab if $ab \in E$ $a,b \neq i_1, i_2$

ai if $ai_1 \in E$ or $ai_2 \in E$

Prop. "Graph minors are matroid minors"

$$M(G \setminus e) = M(G) \setminus e$$

$$M(G/e) = M(G)/e$$

Pf For $e \notin I$

I indep in $M(G)\setminus e \iff I$ indep in $M(G)$, $e \notin I$

$\iff I$ has no circs. in G, $e \notin I$

$\iff I$ has no circs. in $G \setminus e$

$\iff I$ indep in $M(G \setminus e)$.

I indep in $M(G)/e \iff I \cup e$ indep in $M(G)$

(Sup e not a loop.) $\iff I \cup e$ has no circs in G

$\iff I$ has no circs in G/e

$\iff I$ indep in $M(G/e)$ ☒

Corollary.

Every minor of a graphical matroid is graphical.

Minors of linear matroids

Let E be a vector configuration in a vector space V.

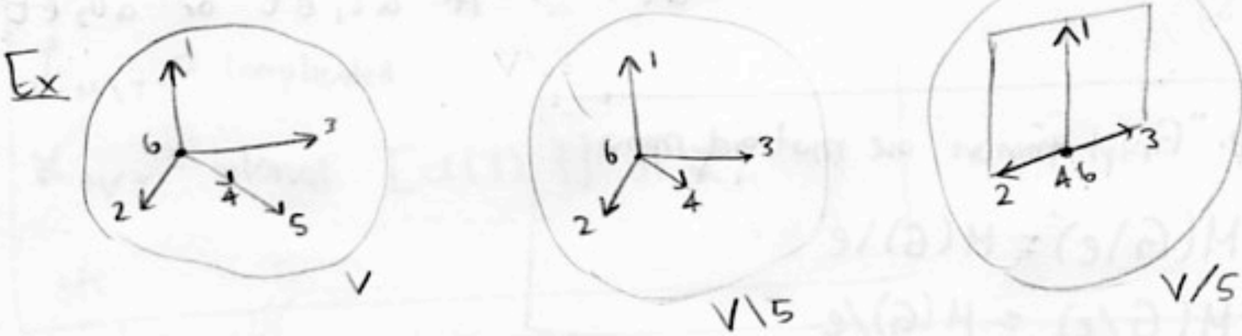
Let $e \in E$.

Deletion: vector config: $E-e$ in V

Contraction: Let $\pi : V \to e^{\perp}$ be the orthogonal projection

vector config: $\pi(E-e)$ in $e^{\perp}$.

Ex



lecture 21
3/12/07

Prop. "Vector config minors are matroid minors"

$M(V\backslash e) = M(V)\backslash e$

$M(V/e) = M(V)/e$

Pf. For $e \notin I$:

I independent in $M(V)\backslash e \Leftrightarrow I$ lin indep $\Leftrightarrow I$ indep in $M(V\backslash e)$

I indep in $M(V)/e \iff I \cup e$ indep in $M(V)$

$\iff$ no lin. eqn involving I, e

?

I indep in $M(V/e) \iff$ no lin eqn involving $\pi(I)$

lin eqn in $I, e \Rightarrow \underbrace{c_1 v_1 + \dots + c_k v_k}_{I} + ce = 0$

$$\Rightarrow \pi(c_1 v_1 + \dots + c_k v_k + ce) = 0$$

$$\Rightarrow c_1 \pi(v_1) + \dots + c_k \pi(v_k) = 0$$

lin eqn in $\pi(I) \Rightarrow c_1 \pi(v_1) + \dots + c_k \pi(v_k) = 0$

$$\Rightarrow \pi(c_1 v_1 + \dots + c_k v_k) = 0 \qquad \ker \pi = \text{multiples of } e$$

$$\Rightarrow c_1 v_1 + \dots + c_k v_k = ce$$

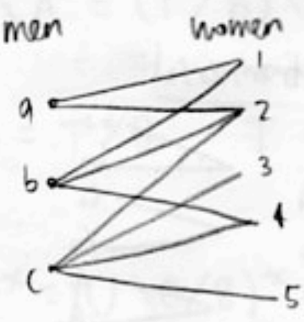
$\blacksquare$

Corollary

Every minor of a linear matroid is linear.

Minors of transversal matroids

Is every minor of a transversal matroid transversal?

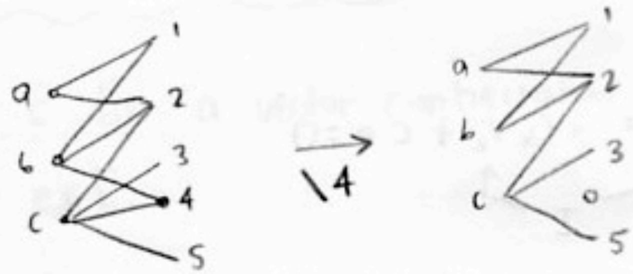


bases: maxl sets of women who can marry simultaneously.

Deletion of e

Bases not containing e → e decides not to get married

→ erase e from the graph.



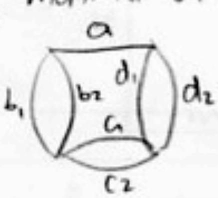
Contraction of e

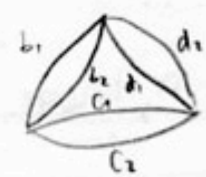
Bases containing e → e demands to get married.

→ what to do to the graph?

who did e marry?

A transversal matroid with a non-transversal contraction:

Let $G =$ 

$G/a =$ 

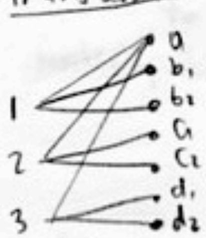
$M = M(G)$

$$\mathcal{C} = \left\{ \begin{matrix} b_1b_2,\ c_1c_2,\ d_1d_2, \\ ab_i\ c_j\ d_k \end{matrix} \right\}$$

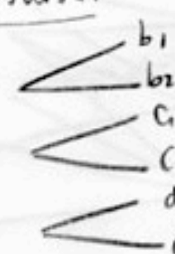
M/a

$$\mathcal{C}(M/a) = \left\{ \begin{matrix} b_1b_2,\ c_1c_2,\ d_1d_2, \\ b_i\ c_j\ d_k \end{matrix} \right\}$$

transversal:



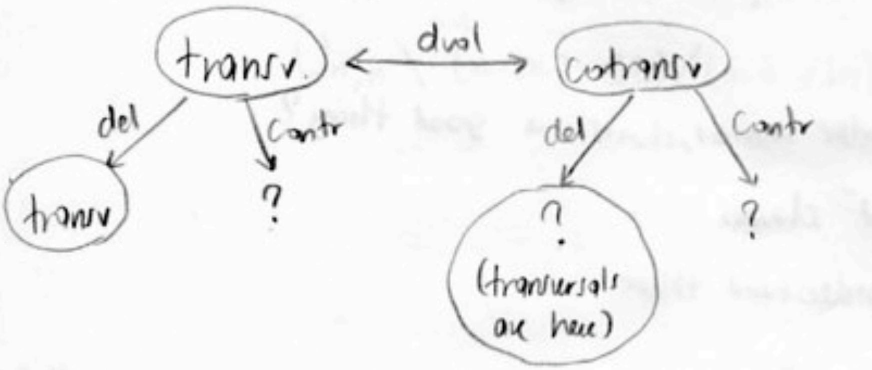
non-transversal:

must have 

→ $b_i c_j d_k$?

- Graphical matroids are closed under minors, duality.
- Linear matroids are closed under minors, duality.
-

Want to expand transversals to a class closed under minors, duality.



- $\text{transv} = (\text{cotransv})^*$
- $\text{del}(\text{transv}) = \text{transv}$
- $\text{transv} \subset \text{del}(\text{cotransv})$

<u>Def</u> A gammoid is a contraction of a transversal.

> <u>Prop</u> Gammoids are closed under minors, duality.
> They are the minimal such class containing transversal matroids.

<u>Proof</u>. Let M be a gammoid on E.

<u>Contr</u>: $M/A = (\underset{\substack{\uparrow \\ \text{transv. mat.}}}{T}/B)/A = T/(A \cup B) = \text{gammoid}.$

<u>del</u>: $M \setminus A = (T/B)\setminus A = \overbrace{(T \setminus A)}^{\text{transv.}} / B = \text{gammoid}$

<u>dual</u>: $M = T/B \quad T \text{ transv} \Rightarrow T = \underset{\substack{\uparrow \\ \text{cotransv}}}{U} \setminus C \Rightarrow M = U \setminus C / B$

$M^* = (U \setminus C / B)^* = \underbrace{U^*}_{\text{transv.}} \setminus C / B \quad \blacksquare$

lecture 22
3/14/07

Last time we saw:

	closed under minors	closed under duals
Graphical matroids	Y	N
Linear matroids	Y	Y
Transversal matroids	N	N
Gammoids	Y	Y

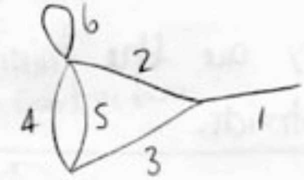
Q Why is being closed under minors, duals a good thing?

A ∘ These are "well-behaved" classes.

∘ We can use this to understand them.

$\boxed{\text{Q. How can you tell if a matroid is graphical?}}$

∘ If Y, you could find the graph.

$\mathcal{C} = \{234, 235, 45, 6\} \longrightarrow$ 

∘ If N, what? Could this

$$C = \{1279, 1289, 13456, 1789, 2346, 2567, 2789\}$$

be the set of circuits of a graphical matroid?

No, because

$$\mathcal{C}(M \setminus 3456) = \{1279, 1289, 1789, 2789\}$$

$$\mathcal{C}(M \setminus 3456/9) = \{127, 128, 178, 278\}$$

$$M \setminus 3456/9 \cong U_{2,4}$$

which is not graphical.

Ex. $U_{m,n}$ not graphical except $U_{0,n}, U_{1,n}, U_{n-1,n}, U_{n-2,n}$

Pf. $U_{r,s} \setminus e \cong U_{r-1,s}$

$U_{r,s} / e \cong U_{r-1,s-1}$

So $U_{m,n} \setminus (n-m-2 \text{ elements}) \cong U_{m,m+2}$

$U_{m,n} \setminus (n-m-2 \text{ elts}) / (m-2 \text{ elts}) \cong U_{2,4}$ not graphical for $n \geq m+2$, $m \geq 2$

Other non-graphical matroids: $M(K_5)^*, M(K_{3,3})^*$

F_7 = "Fano matroid", F_7^*

go to next page

Theorem (Tutte, 1959)

A matroid is graphical $\Leftrightarrow$ It has no minor isomorphic to $U_{2,4}, M(K_5)^*, M(K_{3,3})^*, F_7, F_7^*$

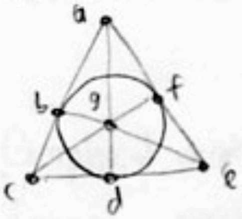
Proof: Difficult, intricate. (Chapter 13 of Oxley.)

Project?

So: There are 5 obstructions to being graphical.

"forbidden minors"

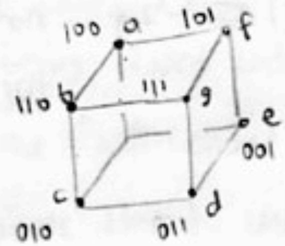
The Fano matroid F_7



$C = \{abc, cde, efa, agd, bge, cgf, bcd\}$

Why is it a matroid?

$\mathbb{F} = GF(2) = \{0,1\}$ $\quad V = \mathbb{F}^3$ $\quad E = \mathbb{F}^3 - 000$



$\boxed{\text{Prop. } F_7 \text{ is not representable over } \mathbb{R}}$ (as vectors in $\mathbb{R}^3$)

Pf. Sup it is.

We can assume $a=(100)$, $c=(010)$, $e=(001)$, $g=(xyz)$ $\qquad x,y,z \neq 0$

$$d = *(100) + *(xyz) \longrightarrow d = (0, ry, rz) \qquad r \neq 0$$
$$= *(010) + *(001)$$

$$\longrightarrow f = (sx, 0, sz) \qquad s \neq 0$$

$$\longrightarrow b = (tx, ty, 0) \qquad t \neq 0$$

Now $\alpha d + \beta f + \gamma b = 0 \Rightarrow x(\beta s + \gamma t) = 0$

$\alpha, \beta, \gamma \neq 0$ $\qquad y(\alpha r + \gamma t) = 0$

$\qquad z(\alpha r + \beta s) = 0$

$$\Rightarrow 2\alpha r = 0 \quad 2\beta s = 0 \quad 2\gamma t = 0 \Rightarrow 2 = 0 \quad \blacksquare$$

$\boxed{\text{Corollary } F_7^* \text{ is not representable over } \mathbb{R}}$

Linearity / representability

Theorem. (Tutte, 58) A matroid is representable over $GF(2)$ $\iff$ it contains no $U_{2,4}$ minor.

Theorem (Bixby, 79) (Seymour, 79) A matroid is rep. over $GF(3)$ $\iff$ no $U_{2,5}, U_{3,5}, F_7, F_7^*$

Theorem (Tutte 58) A matroid is rep. over any field $\iff$ no $U_{2,4}, F_7, F_7^*$

Conjecture (Rota, 71) Rep. over $GF(q)$ is characterized by a finite list of excluded minors, for any $q = p^\alpha$. ← still open

Theorem (Geelen, Gerards, Kapoor 00) Seven excluded minors for $GF(4)$.

"Fear it may fail for $q \geq 5$"

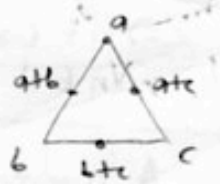
Theorem (Lazarson 1958) Infinitely many excluded minors for $\mathbb{R}$, or any $\mathbb{F}$ with $\operatorname{char} \mathbb{F} = 0$.

Open. In which $GF(q)$ can you represent $U_{r,n}$?

Non-linear matroids

We saw $F_7 =$  is not rep. in char >2

Now $F_7^- =$  is not rep. in char 2:



Prop $F_7 \oplus F_7^-$ is not linear.

Pf. If it was rep over $\mathbb{F}$, then

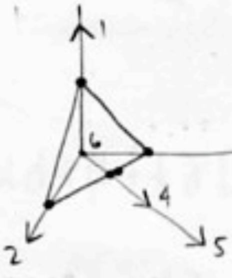
- the restriction F_7 is rep over $\mathbb{F}$ $\rightarrow$ char $\mathbb{F} = 2$
- the restriction F_7^- is rep. over $\mathbb{F}$ $\rightarrow$ char $\mathbb{F} > 2$. ∎

An aside:

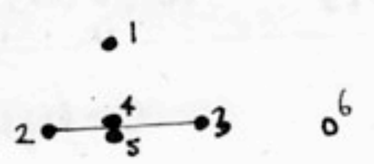
$v_1, \dots, v_n \in \mathbb{F}^d$ are affinely indep $\Leftrightarrow$ $a_1 v_1 + \dots + a_n v_n = 0$ for some $a_i \in \mathbb{F}$, not all 0, s.t. $a_1 + \dots + a_n = 0$

$\Leftrightarrow$
- 2 on a point
- 3 on a line
- 4 on a plane
- ⋮

Idea:



$\longrightarrow$



$C = \{6, 45, 234, 235\}$

Prop A loopless matroid is linear $\iff$ it is the affine matroid of some point configuration.

Pf affine matroid of $v_1, \dots, v_n \in \mathbb{F}^d$ $\cong$ linear matroid of $(1,v_1), \dots, (1,v_n) \in \mathbb{F}^{d+1}$

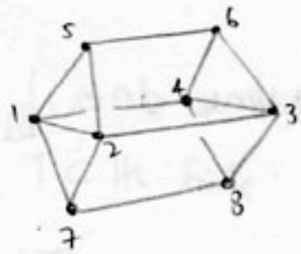
$$\begin{array}{l} \sum_i a_i v_i = 0 \\ \sum_i a_i = 0 \end{array} \iff \sum_i a_i (1, v_i) = (\Sigma a_i, \Sigma a_i v_i) = 0$$

$\blacksquare$

So now we can use what we know about projective geometry.

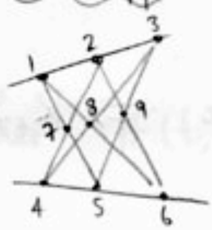
Non-linear matroids

Vamos



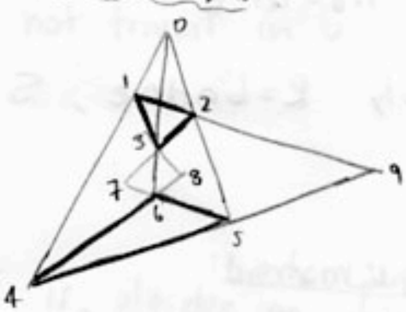
C: 1456, 2356, 1478, 2378, every 5

non-Pappus



C: 123, 456, 157, ... every 4

non-Desargues



C: 014, 025, 129, ... every 4

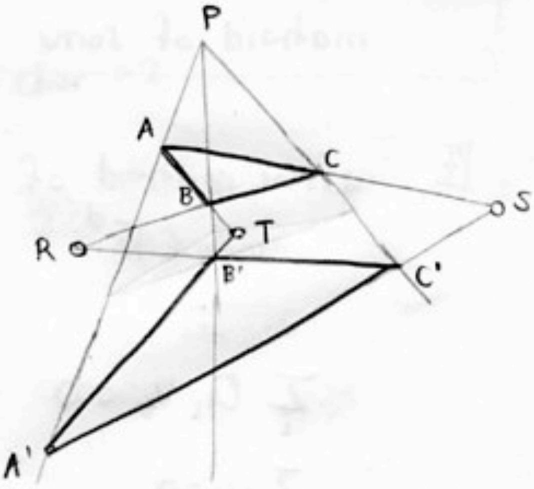
These are matroids, but not representable (from proj geom)

Desargues's Theorem

If triangle ABC, $A'B'C'$ are perspective from a point P, then the points

$R = BC \cap B'C'$, $S = AC \cap A'C'$, $T = AB \cap A'B'$

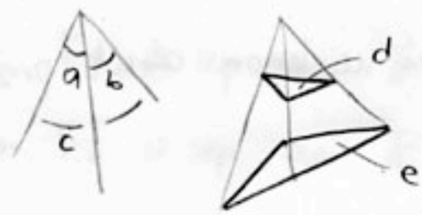
are collinear.



Proof.

Prove it in 3-D.

Label the planes



Then $AB = a \cap d$, $A'B' = a \cap e$ $\rightarrow$ $T = a \cap d \cap e$

Similarly $R = b \cap d \cap e$, $S = c \cap d \cap e$ $\Rightarrow$ R, S, T on line $d \cap e$. ▨

Desargues matroid:

The affine matroid of $A, B, C, A', B', C', P, R, S, T$

(Exercise: This is $M(K_5)$.)

non-Desargues matroid:

The same matroid, except the circuit R, S, T is erased.

(Exercise: This is a matroid.)

Algebraic matroids

$\mathbb{F}$ - field

$\mathbb{K}$ - extension field (so $\mathbb{F}$ is a subfield of $\mathbb{K}$)

Ex: $\mathbb{F} = \mathbb{R}$ $\quad \mathbb{K} = \mathbb{C}$

$\mathbb{F} = \mathbb{C}$ $\quad \mathbb{K} = \mathbb{C}(x,y,z)$ - rat'l fns in x, y, z.

$u \in \mathbb{K}$ is <u>algebraic</u> over $\mathbb{F}$ if there is $P(x) \in \mathbb{F}[x]$ with $P(u) = 0$.
<u>transcendental</u> otherwise.

$u, t_1, \ldots, t_n \in \mathbb{K}$

u is <u>alg. dep</u> on $t_1, \ldots, t_n$ over $\mathbb{F}$ if there is

$P(u, t_1, \ldots, t_n) = 0$ for P with coeffs in $\mathbb{F}$
not trivial in u

(i.e. u is algebraic over $\mathbb{F}(t_1, \ldots, t_n)$)

$T \subset \mathbb{K}$ finite

T <u>alg. dep.</u> over $\mathbb{F}$ if some $t \in T$ is alg. dep. on $T - t$

<u>alg. indep.</u> otherwise

<u>Theorem</u> Let $\mathbb{K}$ be an extension field of $\mathbb{F}$ and let E be a finite subset of $\mathbb{K}$. Then the alg. ind. subsets of E are the indep. sets of a matroid.

<u>Def</u> A matroid is <u>algebraic</u> if it comes from this construction.

<u>Ex.</u> $\mathbb{F} = \mathbb{C}$

$\mathbb{K} = \mathbb{C}(x,y,z)$

$a = z \quad b = (y+z)^2 \quad c = xy + xz \quad d = x \quad e = 1/x \quad f = 1+i$

Ex $\mathbb{F} = \mathbb{R}$

$\mathbb{K} = \mathbb{C}$

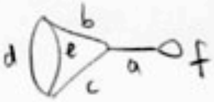
$a = \sqrt{2} \quad b = 1+i \quad c = 1 \quad d = \sqrt[7]{5+\sqrt{2}}$

Ex $\mathbb{F} = \mathbb{Q}$

$\mathbb{K} = \mathbb{R}$

$a = \sqrt{2} \quad b = \sqrt[3]{3} \quad c = e \quad d = e + \pi$

1. $de - 1 = 0$
   $f - (1+i) = 0$ $\longrightarrow$ Same as our good old friend:
   $bd^2 - c^2 = 0$
   $c^2e^2 - b = 0$
   no more



2. all loops! ($\mathbb{C}$ = algebraic closure of $\mathbb{R}$)
3. a,b loops
   c indep
   d – open! not known whether $e+\pi$ is algebraic.

Ex. from last time:

$a = r \quad b = s^2 \quad c = xs \quad d = x \quad e = 1/x^2 \quad f = 1+i$

$r = wz \quad s = y + wz$

Circs: f
d, e
b, c, d
b, c, e

Algebraic matroids are matroids:

$\mathbb{F}$ field
$\mathbb{K}$ field extension
$E \subset \mathbb{K}$ finite

The closure of this matroid would be $cl: 2^E \to 2^E$:

$$cl(A) = \{x \in E \mid x \text{ is alg. dep. on } A \text{ over } \mathbb{F}\}$$

Let's prove this is a matroid closure.

(CL1) $A \subseteq cl(A)$

coeffs in $\mathbb{F}(A)$

$a \in A \to$ is a root of $x - a = 0$

(CL2) $A \subseteq B \Rightarrow cl(A) \subseteq cl(B)$

$x \in cl(A) \longrightarrow P(x) = 0$ with coeffs in $\mathbb{F}(A) \Rightarrow$ in $\mathbb{F}(B)$.

(CL3) $cl(cl(A)) = cl(A)$

wait.

(CL4) If $a \notin cl(A)$ and $a \in cl(A \cup b)$
then $b \in cl(A \cup a)$.

$a \in cl(A \cup b) \to P(a) = 0$ P with coeffs in $\mathbb{F}(A \cup b)$

- This is a polynomial equation in $A \cup a \cup b$ with coeffs in $\mathbb{F}$
- It involves b (or else $a \in cl(A)$)

$\to Q(b) = 0$ Q with coeffs in $\mathbb{F}(A \cup a)$.

(CL3):

Note. $\mathbb{F} \subset \mathbb{K}$ field extension
$\Rightarrow \mathbb{K}$ is a vector space over $\mathbb{F}$
$[\mathbb{K} : \mathbb{F}]$ = dim of this = "degree" of extension

<u>Lemma</u>. x alg. dep. on $a_1 \dots a_k$ over $\mathbb{F}$
$\Longleftrightarrow [\mathbb{F}(a_1, \dots, a_k, x) : \mathbb{F}(a_1, \dots, a_k)]$ is finite

<u>Proof</u>.
$\Leftarrow$ If alg. dep.

$$\sum_{i=1}^{n} P_i(a_1, \dots, a_k) x^i = 0$$

then $1, x, \dots, x^{n-1}, x^n$ are linearly dependent, and one can check $1, x, \dots, x^{n-1}$ generate $\mathbb{F}(a_1, \dots, a_k, x)$ as a $\mathbb{F}(a_1, \dots, a_k)$-vector space.

$\Rightarrow$ If there is no alg. dependence, then

$1, x, x^2, \dots$

are linearly independent. ∎

<u>Lemma</u>. $\mathbb{F} \subset \mathbb{K} \subset \mathbb{L}$ field extensions

$$\Rightarrow [\mathbb{L}:\mathbb{F}] = [\mathbb{L}:\mathbb{K}]\cdot[\mathbb{K}:\mathbb{F}]$$

<u>Proof</u>. x_i basis of $\mathbb{L}$ over $\mathbb{K}$

y_j basis of $\mathbb{K}$ over $\mathbb{F}$

$\Rightarrow x_i y_j$ basis of $\mathbb{L}$ over $\mathbb{F}$.

(CL3): $\mathrm{cl}(\mathrm{cl}(A)) = \mathrm{cl}(A)$

- $\supseteq$ clear
- $\subseteq$ Let $a \in \mathrm{cl}(\mathrm{cl}(A))$

$\Rightarrow a$ dep on $\mathrm{cl}(A)$

$\Rightarrow [\mathbb{F}(\mathrm{cl}(A), a) : \mathbb{F}(\mathrm{cl}(A))]$ finite

$$\begin{tikzcd}
 & \mathbb{F}(\mathrm{cl}\,A, a) \arrow[dl, dash] \arrow[dr, dash, "\text{finite}"] & \\
\mathbb{F}(A,a) \arrow[dr, dash] & & \mathbb{F}(\mathrm{cl}(A)) \arrow[dl, dash, "\text{finite}"] \\
 & \mathbb{F}(A) &
\end{tikzcd}$$

finite $\rightarrow$ since adding each $a \in \mathrm{cl}(A)$ gives a finite degree

$\Rightarrow [\mathbb{F}(\mathrm{cl}(A), a) : \mathbb{F}(A)]$ finite

$\Rightarrow [\mathbb{F}(\mathrm{cl}A, a) : \mathbb{F}(A,a)] \cdot \underbrace{[\mathbb{F}(A,a) : \mathbb{F}(A)]}_{\text{finite}}$ finite

$\downarrow$

$a \in \mathrm{cl}A$ ∎