Matroids

↪ Abstract the notion of linear independence (Like groups abstract the notion of multiplication).

Def: A matroid is a pair $(E, \mathcal{I})$ where E is a set (of vectors or edges) and $\mathcal{I}$ is a collection of subsets of E s.t.

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

(I2) If $I \in \mathcal{I}$ and $J \subseteq I$, then $J \in \mathcal{I}$ (downward closure)

(I3) If $I_1, I_2 \in \mathcal{I}$ and $|I_1| > |I_2|$, $\exists e \in I_1 \setminus I_2$ s.t. $I_2 \cup \{e\} \in \mathcal{I}$ (augmentation / exchange).

Ex: Let $E = \{v_1, v_2, \ldots, v_m\}$ be a set of vectors (k=field) in k^n and let $\mathcal{I}$ be the set of independent subsets of E. Then $\mathcal{I}$ is a matroid:

to check (I3), if I_1, I_2 are both indep and I_1 has more vectors than I_2, then

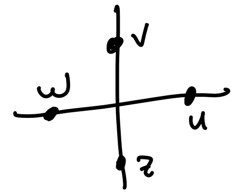
$$\dim(sp(I_1)) > \dim(sp(I_2))$$

So there is a vector $e \in I_1$ not in $sp(I_2)$. This can be added to I_2 to make a larger indep. set.

Such a matroid is called representable over k.

Ex: $E = \{u, v, w, z\}$:

$\mathcal{I} = \{\{u,v\}, \{v,w\}, \{w,z\}, \{z,u\}, \{u\}, \{v\}, \{w\}, \{z\}, \emptyset\}$

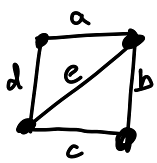


$\mathbb{R}^2$

$$\begin{pmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

Ex: $E = \{$edges of a graph $G\}$

$I = \{$subsets of E not containing a cycle$\}$

$G =$ 

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

$\mathcal{I} = \{\emptyset, a, b, c, d, ab, ac, ad, ae, bc, bd, be, cd, ce, de, abc, abd, abe, acd, ace, bcd, bde, cde\}$

This is called a <u>graphical</u> matroid.

Ex: A set of real numbers, algebraic independence

$\to$ <u>algebraic matroid</u> (algebraic dependence relation is a polynomial relation over $\mathbb{Z}$)

$E = \{2, \pi, \pi^2\}$ $\qquad$ $\mathcal{I} = \{\{2, \pi\}, \{2, \pi^2\}, \{2\}, \{\pi\}, \emptyset\}$

Not much known about these!

Def: A basis is a maximal independent set under $\subseteq$.

Def: A dependent set is a subset of E that is not in $\mathcal{I}$. A circuit is a minimal dependent set.

Lemma: In a finite matroid $M = (E, \mathcal{I})$, all bases have the same size.

Pf: If two bases B_1, B_2 have $|B_1| > |B_2|$, then by (I3), B_2 is contained in a larger independent set. Since B_2 is a basis, this is a contradiction. $\square$

⇝ In graphical matroids, bases are spanning forests.

Basis axioms for matroids: An alternative def:

Def: A matroid is a pair $(E, \mathcal{B})$ where X is a set and $\mathcal{B}$ is a set of subsets of X satisfying:

(B1) $\mathcal{B}$ is nonempty

(B2) Basis exchange: If $B_1 \neq B_2 \in \mathcal{B}$ are bases and $x \in B_1 \setminus B_2$, then $\exists y \in B_2$ s.t. $(B_1 - \{x\}) \cup \{y\} \in \mathcal{B}$.

Proof of equivalence (cryptomorphisms):

Let $M = (E, \mathcal{I})$ be a matroid as defined by (I1) - (I3), and let $\mathcal{B} = \{\text{maximal elts of } \mathcal{I}\}$. Then $\mathcal{B}$ is nonempty since $\emptyset \in \mathcal{I}$ (so $\mathcal{I}$ is nonempty). So (B1) holds.

For (B2), suppose $B_1 \neq B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$. Then $B_1 - \{x\}$ is still in $\mathcal{I}$ by (I2), and $|B_1 - \{x\}| < |B_2|$. So by (I3), $\exists y \in B_2$, $(B_1 - \{x\}) \cup \{y\} \in \mathcal{I}$.

Since all bases have the same size (prev Lemma), $(B_1 - \{x\}) \cup \{y\} \in \mathcal{B}$. So (B2) holds.

Converse: Let $M = (E, \mathcal{B})$ satisfy (B1) and (B2).

Let $\mathcal{I} = \{I \subseteq E : \exists B \in \mathcal{B},\ I \subseteq B\}$.

Then $\emptyset \in \mathcal{I}$ automatically, by (B1) so (I1) holds.

(I2) also holds by the def of $\mathcal{I}$.

For (I3), let $I_1, I_2 \in \mathcal{I}$ w/ $|I_1| < |I_2|$.

Assume for contradiction that for all $e \in I_2 \setminus I_1$, $I_1 \cup e \notin \mathcal{I}$.

Let B_1, B_2 be bases containing I_1, I_2 respectively, and among all choices of B_2 we choose one so that $|B_2 - (I_2 \cup B_1)|$ is minimal.

Note that
$$I_2 - B_1 = I_2 - I_1$$
for otherwise there would be $e \in I_2 - I_1$ with $e \in B_1$, and $I_1 \cup e \subseteq B_1$ would be independent, contradicting our assumption.

Now, suppose $B_2 - (I_2 \cup B_1)$ nonempty, let $x \in B_2 - (I_2 \cup B_1)$
Then by (B2), $\exists y \in B_1 \setminus B_2$ s.t.
$B_2 - x \cup y \in \mathcal{B}$. But then
$$|(B_2 - x \cup y) - (I_2 \cup B_1)| < |B_2 - (I_2 \cup B_1)|$$
contradicts minimality of B_2

$\Rightarrow B_2 - (I_2 \cup B_1) = \emptyset$. Thus $B_2 - B_1 = I_2 - B_1 = I_2 - I_1$.

Now suppose $B_2 - (I_1 \cup B_2)$ nonempty, let $x \in B_2 - (I_1 \cup B_2)$.
Then by (B2), $\exists y \in B_2 \setminus B_1$ s.t.
$B_0 := B_1 - x \cup y \in \mathcal{B}$. Then $I_1 \cup y \subseteq B_0 \Rightarrow I_1 \cup y \in \mathcal{I}$.
So $y \notin I_2$, but since $B_2 - B_1 = I_2 - I_1$ we do have $y \in I_2$, contradiction.

So $B_1 - (I_1 \cup B_2) = \emptyset$ so $B_1 - B_2 = I_1 - B_2 \subseteq I_1 - I_2$
But $|B_1 - B_2| = |B_2 - B_1| = |I_2 - I_1|$
$$\overset{\wedge|}{|I_1 - I_2|}$$
so $|I_1| \geq |I_2|$, $\rightarrow\leftarrow$. QED.

Circuit axioms

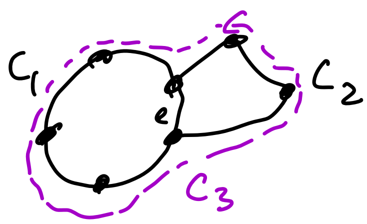
Another def. of matroid:

Def: A matroid is a pair $(E, \mathcal{C})$ where E is a finite set, $\mathcal{C}$ a collection of subsets of E called circuits, s.t.

(C1) $\emptyset \notin \mathcal{C}$,

(C2) If $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$ then $C_1 = C_2$

(C3) (Circuit elimination): If $C_1, C_2 \in \mathcal{C}$ and $e \in C_1 \cap C_2$, $\exists\ C_3 \in \mathcal{C}$ s.t. $C_3 \subseteq (C_1 \cup C_2) - e$.

Graphical: 

what does this mean for representable matroids?

Thm: If $(E, \mathcal{C})$ satisfies (C1)–(C3) and
$\mathcal{I} = \{I \subseteq E : I \text{ contains no member of } \mathcal{C}\}$
Then $(E, \mathcal{I})$ satisfies (I1)–(I3).
Conversely if $(E, \mathcal{I})$ is a matroid and $\mathcal{C}$ are the circuits, they satisfy (C1)–(C3).

Rank

Def: Let $X \subseteq E$ and $M = (E, \mathcal{I})$ a matroid.
Define $M|X = (X, \mathcal{I}|X)$ where $\mathcal{I}|X$ is $\{I \in \mathcal{I} : I \subseteq X\}$. This is a matroid, called the *restriction* of M to X.

Def: The *rank* of a matroid is the size of any (every) basis.
The *rank* of $X \subseteq E$, $rk(X)$, is the rank of $M|X$.

Rank Def of Matroid: A *matroid* is a finite set E along w/ a function $rk: \mathcal{P}(E) \to \mathbb{N}$ satisfying:

(R1) If $X \subseteq E$, $0 \leq rk(X) \leq |X|$.

(R2) If $X \subseteq Y \subseteq E$, $rk(X) \leq rk(Y)$

(R3) If $X, Y \subseteq E$, $rk(X \cup Y) + rk(X \cap Y) \leq rk(X) + rk(Y)$.

Note similarity to "upper semimodular" condition for posets.

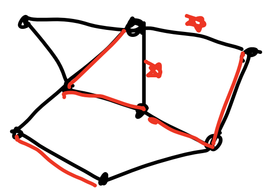
Recovering indep. sets from rank: $I \subseteq E$ indep iff $rk(I) = |I|$.

Closure

<u>Def</u>: If $M=(E,rk)$ is a matroid, define $cl: \mathcal{P}(E) \to \mathcal{P}(E)$ by
$$cl(X) = \{x \in E : rk(X \cup x) = rk(X)\}$$
(closure).

In representable matroids: $cl = sp$.

In graphical matroids: Closure means close up loops.



Both ✗'s are in closure of red set.

Closure axioms: (E, cl) is a matroid iff

(CL1) $X \subseteq cl(X)$ for all $X \subseteq E$

(CL2) If $X \subseteq Y$, $cl(X) \subseteq cl(Y)$

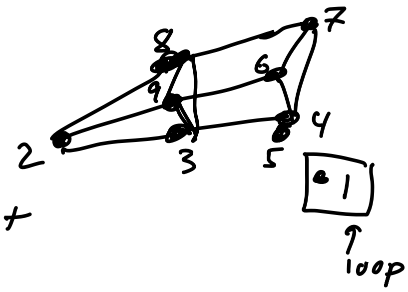
(CL3) $cl(cl(X)) = cl(X)$

(CL4) If $y \in cl(X \cup x) - cl(X)$, then $x \in cl(X \cup y)$.

<u>Def</u>: A flat is a set X s.t. $X = cl(X)$.

A hyperplane is a flat of rank $rk(M) - 1$.

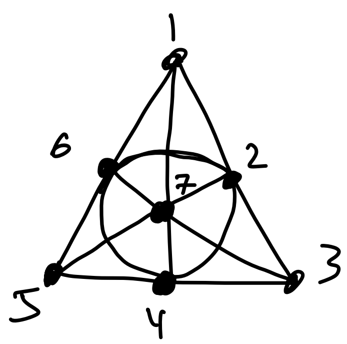
Drawing matroids of small rank:



For rank ≤ 4:

- Each elt of E is a point
- Loops (circuits of size 1) are on their own
- 2-elt circuits are doubled points
- 3-elt circuits are lines through 3 pts
- 4-elt circuits are planes

Ex: Fano matroid:



- All sets of 4 are dependent (all in same plane)
  $\Rightarrow$ rank 3 matroid
- All 7 lines are circuits

Bases: 124, 125, 126, 127, 134, ...

Hwk: Not graphical!