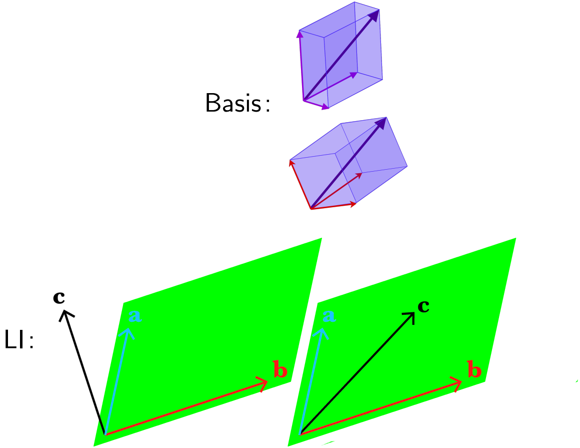
What are...cryptomorphisms?

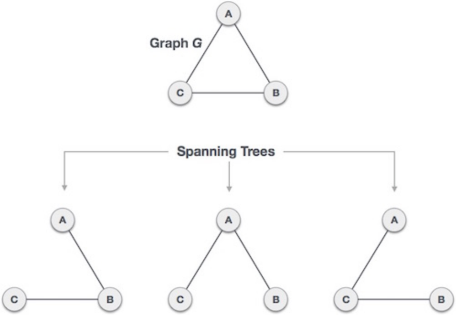
Or: Many definitions = good!

Cryptomorphisms



- Cryptomorphism = “equivalent and not straightforward way to define matroids”
- Example We have seen definitions via bases and linear independent (LI) sets
- Today A point of matroid theory is that there are many cryptomorphisms

Circuits



- Circuit = dependent (D=¬LI) set with all proper subsets being LI
- Circuits are the obstructions for sets to be bases
- Here is the definition of matroids using circuits:

Non-triviality	(C1)	$\emptyset \notin \mathcal{C}$;
Clutter	(C2)	if $C_1, C_2 \in \mathcal{C}$ and $C_1 \subseteq C_2$, then $C_1 = C_2$;
Circuit elimination	(C3)	if $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$, and $x \in C_1 \cap C_2$, then $C_3 \subseteq C_1 \cup C_2 - x$ for some $C_3 \in \mathcal{C}$.

Rank

$$\begin{bmatrix} 1 & 2 & 1 \\ -2 & -3 & 1 \\ 3 & 5 & 0 \end{bmatrix} \xrightarrow{2R_1+R_2 \to R_2} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 3 & 5 & 0 \end{bmatrix} \xrightarrow{-3R_1+R_3 \to R_3} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 0 & -1 & -3 \end{bmatrix}$$

$$\xrightarrow{R_2+R_3 \to R_3} \begin{bmatrix} 1 & 2 & 1 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{bmatrix} \xrightarrow{-2R_2+R_1 \to R_1} \begin{bmatrix} 1 & 0 & -5 \\ 0 & 1 & 3 \\ 0 & 0 & 0 \end{bmatrix}.$$

- Rank of $A \subset E$ = size of the largest LI subset of A
- Sets are LI $\Leftrightarrow$ full rank
- Here is the definition of matroids using the rank:

Theorem 2.15. *Let E be a finite set with an integer-valued function r defined on subsets of E. Then r is the rank function of a matroid if and only if for $A, B \subseteq E$:*

Normalization (r1) $0 \leq r(A) \leq |A|$;

Increasing (r2) *if $A \subseteq B$, then $r(A) \leq r(B)$;*

Semimodular (r3) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

For completeness: A formal statement

Cryptomorphisms are everywhere and matroids can be defined using...

(i) ...bases Seen

(ii) ...LI sets Seen

(iii) ...circuits Seen

(iv) ...cocircuits Skipped

(v) ...the rank function Seen

(vi) ...flats Next slide

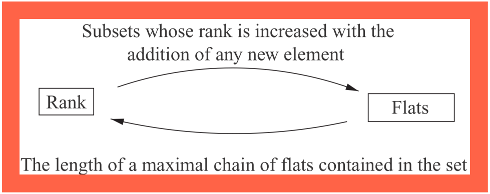
(vii) ...hyperplanes Next slide

(viii) ...closure operators Skipped

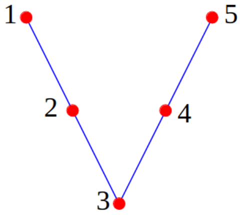
All of these have then interpretations in linear algebra, graph theory, geometry, combinatorics,... and all are equivalent

Flats

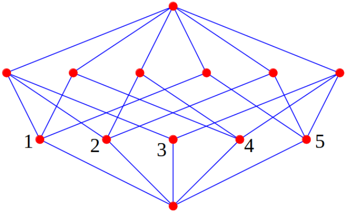
A quick definition:



5 point:



, flats:



- From geometry: flat = if you add anything new to a flat, its rank increases
- Hyperplanes = maximal flats that are not the entire matroid
- Example For an affine matroid (E is a subset of affine space and LI = usual LI) flats are the intersections of E with affine subspaces

Thank you for your attention!

I hope that was of some help.