Wednesday 2/13

Independent Sets, Bases, and Circuits

Recall that a **(matroid) independence system** $\mathscr{I}$ is a family of subsets of E such that

$$\emptyset \in \mathscr{I}; \tag{1a}$$

$$\text{if } I \in \mathscr{I} \text{ and } I' \subseteq I, \text{ then } I' \in \mathscr{I}; \tag{1b}$$

$$\text{if } I, J \in \mathscr{I} \text{ and } |I| < |J|, \text{ then there exists } x \in J \setminus I \text{ such that } I \cup x \in \mathscr{B} \tag{1c}$$

and that a **(matroid) basis system** $\mathscr{B}$ is a family of subsets of E such that, for all $B, B' \in \mathscr{B}$,

$$|B| = |B'|; \tag{2a}$$

$$\text{for all } e \in B \setminus B', \text{ there exists } e' \in B' \setminus B \text{ such that } B \setminus e \cup e' \in \mathscr{B}, \tag{2b}$$

$$\text{for all } e \in B \setminus B', \text{ there exists } e' \in B' \setminus B \text{ such that } B' \setminus e' \cup e \in \mathscr{B}. \tag{2c}$$

(Homework: (2a) and (2b) $\iff$ (2a) and (2c).)

If G is a graph with edge set E and $M = M(G)$ is its graphic matroid, then

$$\mathscr{I} = \{A \subseteq E \mid A \text{ is acyclic}\},$$
$$\mathscr{B} = \{A \subseteq E \mid A \text{ is a spanning forest of } G\}.$$

If S is a set of vectors and $M = M(S)$ is the corresponding linear matroid, then

$$\mathscr{I} = \{A \subseteq S \mid A \text{ is linearly independent}\},$$
$$\mathscr{B} = \{A \subseteq S \mid A \text{ is a basis for span}(S)\}.$$

Proposition 1. *Let E be a finite set.*

1. *If $\mathscr{I}$ is an independence system on E, then $\mathscr{B} = \{$maximal elements of $\mathscr{I}\}$ is a basis system.*
2. *If $\mathscr{B}$ is a basis system, then $\mathscr{I} = \bigcup_{B \in \mathscr{B}} 2^B$ is an independence system.*
3. *These constructions are mutual inverses.*

(Proof: Exercise.)

We already have seen that an independence system on E is equivalent to a matroid rank function. So Proposition 1 asserts that a basis system provides the same structure on E. Bases turn out to be especially convenient for describing the standard operations on matroids that we'll see soon.

One last way of defining a matroid (there are many more!):

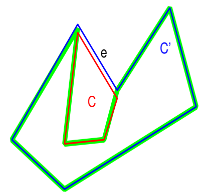
Definition 1. A **(matroid) circuit system** $\mathscr{C}$ on E is a family of subsets of E such that, for all $C, C' \in \mathscr{C}$,

$$C \not\subseteq C'; \quad \text{and} \tag{3a}$$

$$\text{for all } e \in C \cap C', \; C \cup C' \setminus e \text{ contains an element of } \mathscr{C}. \tag{3b}$$

In a linear matroid, the circuits are the minimal dependent sets of vectors. Indeed, if C, C' are such sets and $e \in C \cap C'$, then we can find two expressions for e as nontrivial linear combinations of vectors in C and in C', and equating these expressions and eliminating e shows that $C \cup C' \setminus e$ is dependent, hence contains a circuit.

In a graph, if two cycles C, C' meet in an edge $e = xy$, then $C \setminus e$ and $C' \setminus e$ are paths between x and y, so concatenating them forms a closed path, which must contain some cycle.



Proposition 2. *Let E be a finite set.*

(1) *If $\mathscr{I}$ is an independence system on E, then*
$$\{C \notin \mathscr{I} \mid C' \in \mathscr{I} \ \forall C' \subsetneq C\}$$
is a circuit system.
(2) *If $\mathscr{C}$ is a circuit system, then*
$$\{I \mid C \not\subseteq I \ \forall C \in \mathscr{C}\}$$
is an independence system.
(3) *These constructions are mutual inverses.*

So we have yet another equivalent way of defining a matroid.

Operations on Matroids

Some ways of constructing new matroids from old ones include *duality*, *direct sums*, and *deletion and contraction*. But first, a couple of pieces of terminology.

Definition 2. Let M be a matroid and V a vector space over a field $\mathbb{F}$. A set of vectors $S \subset V$ **represents M over $\mathbb{F}$** if the linear matroid $M(S)$ associated with S is isomorphic to M.

A **regular** matroid is one that is representable over every field. (For instance, we will see that graphic matroids are regular.) For some matroids, the choice of field matters. For example, every uniform matroid is representable over every infinite field, but $U_k(n)$ can be represented over $\mathbb{F}_q$ if and only if $k \leq q^n - 1$ (so that there are enough nonzero vectors in $\mathbb{F}_q^n$), although this condition is not sufficient. (For example, $U_2(4)$ is not representable over $\mathbb{F}_2$.) Some matroids are not representable over *any* field; the smallest such has a ground set of size 9.

Definition 3. Let M be a matroid with basis system $\mathscr{B}$. The *dual matroid* M^* (or $M^\perp$) has basis system
$$\mathscr{B}^* = \{E \setminus B \mid B \in \mathscr{B}\}.$$

Note that (2a) is clearly invariant under complementation, and complementation swaps (2b) and (2c). Also, it is clear that $M^{**} = M$.

What does this mean in the linear setting? Let $S = \{v_1, \dots, v_n\} \subset \mathbb{F}^r$, and let $M = M(S)$. We may as well assume that S spans $\mathbb{F}^r$. That is, $r \leq n$, and the $r \times n$ matrix X with columns v_i has full rank r. Let Y be any $(n-r) \times n$ matrix with
$$\operatorname{rowspace}(Y) = \operatorname{nullspace}(X).$$
That is, the rows of Y span the orthogonal complement of $\operatorname{rowspace}(X)$ according to the standard inner product. Then the columns of Y represent M^*. To see this, first, note that $\operatorname{rank}(Y) = \dim \operatorname{nullspace}(X) = n - r$, and second, check that a set of columns of Y spans its column space if and only if the complementary set of columns of X has full rank.

Example 1. Let $S = \{v_1, \dots, v_5\}$ be the set of column vectors of the following matrix:
$$X = \begin{bmatrix} 1 & 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

Notice that X has full rank (it's in row-echelon form, after all), so it represents a matroid of rank 3 on 5 elements. We could take Y to be the matrix

$$Y = \begin{bmatrix} 0 & 0 & -2 & 1 & 0 \\ 1 & 1 & -1 & 0 & 0 \end{bmatrix}.$$

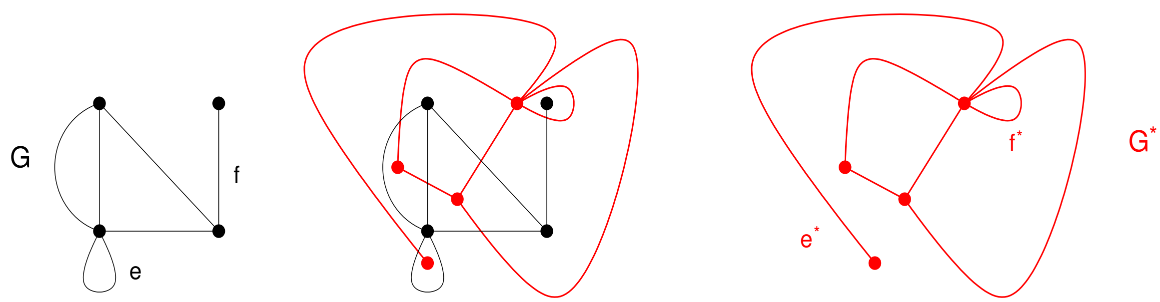
Then Y has rank 2. Call its columns $\{v_1^*, \dots, v_5^*\}$; then the pairs of columns that span its column space are

$$\{v_1^*, v_3^*\},\ \{v_1^*, v_4^*\},\ \{v_2^*, v_3^*\},\ \{v_2^*, v_4^*\},\ \{v_3^*, v_4^*\},$$

whose (unstarred) complements are precisely those triples of columns of X that span *its* column space.

In particular, every basis of M contains v_5, which corresponds to the fact that no basis of M^* contains v_5^*.

Example 2. Let G be a connected *planar* graph, i.e., one that can be drawn in the plane with no crossing edges. The **planar dual** is the graph G^* whose vertices are the regions into which G divides the plane, with two vertices of G^* joined by an edge e^* if the corresponding faces of G are separated by an edge e of G. (So e^* is drawn *across* e in the construction.)



Some facts to check about planar duality:

- $A \subset E$ is acyclic if and only if $E^* \setminus A^*$ is connected.
- $A \subset E$ is connected if and only if $E^* \setminus A^*$ is acyclic.
- G^{**} is naturally isomorphic to G.
- e is a loop (bridge) if and only if e^* is a bridge (loop).

Definition 4. Let M be a matroid on E. A **loop** is an element of E that does not belongs to any basis of M. A **coloop** is an element of E that belongs to every basis of M.

In a linear matroid, a loop is a copy of the zero vector, while a coloop is a vector that is not in the span of all the other vectors.