Friday 2/8/08

Geometric Lattices and Matroids

Warning: If \( A \) is a set and \( e \) isn’t, then I am going to abuse notation by writing \( A \cup e \) and \( A \setminus e \) instead of \( A \cup \{e\} \) and \( A \setminus \{e\} \), when no confusion can arise.

Recall that a matroid closure operator on a finite set \( E \) is a map \( A \mapsto \tilde{A} \) on subsets \( A \subseteq E \) satisfying

\[
\begin{align*}
(1a) & \quad A \subseteq \tilde{A} = \overline{A}; \\
(1b) & \quad A \subseteq B \implies \tilde{A} \subseteq \tilde{B}; \\
(1c) & \quad e \notin \tilde{A}, e \in A \cup f \implies f \in \overline{A \cup e} \quad \text{(the exchange condition).}
\end{align*}
\]

A matroid \( M \) is then a set \( (E, M) \) together with a matroid closure operator. A closed subset of \( M \) (i.e., a set that is its own closure) is called a flat of \( M \). The matroid is called simple if \( \emptyset \) and all singleton sets are closed.

**Theorem 1.** 1. Let \( M \) be a simple matroid with finite ground set \( E \). Let \( L(M) \) be the poset of flats of \( M \), ordered by inclusion. Then \( L(M) \) is a geometric lattice, under the operations \( A \cap B = A \cap B, A \cup B = \overline{A \cup e} \).

2. Let \( L \) be a geometric lattice and let \( E \) be its set of atoms. Then the function \( \tilde{A} = \{e \in E \mid e \leq \bigvee A\} \) is a matroid closure operator on \( E \).

**Proof.** For assertion (1), we start by showing that \( L(M) \) is a lattice. The intersection of flats is a flat (an easy exercise), so the operation \( A \cap B = A \cap B \) makes \( L(M) \) into a meet-semilattice. It’s bounded (with \( \emptyset = \emptyset \) and \( 1 = E \)), so it’s a lattice by [1/25/08, Prop. 2]. Meanwhile, \( \overline{A \cup e} \) is the meet of all flats containing both \( A \) and \( B \).

By definition of a simple matroid, the singleton subsets of \( E \) are atoms in \( L(M) \). Every flat is the join of the atoms corresponding to its elements, so \( L(M) \) is atomic. The next step is to show that \( L(M) \) is semimodular.

Claim: If \( F \in L(M) \) and \( e \in E \setminus F \), then \( F \preceq F \cup \{e\} \).

Indeed, if \( F \preceq F' \subseteq F \cup \{e\} = \overline{F \cup \{e\}} \), then for any \( f \in F' \setminus F \), we have \( e \in F \cup \{f\} \subseteq F' \) by \( \Box \), so \( F' = F \cup \{e\} \), proving the claim.

On the other hand, if \( F \preceq F' \) then \( F' = F \cup \{e\} \) for any atom \( e \in F' \setminus F \). So we have exactly characterized the covering relations in \( L(M) \). It follows that \( L \) is ranked, with rank function

\[
r(F) = \min \{|B| : B \subseteq E, F = \bigvee B\}.
\]

(Such a set \( B \) is called a basis of \( F \).)

We now need to show that \( r \) satisfies the submodular inequality. Let \( F, F' \) be flats and let \( G = F \cap F' \). Let \( G \preceq G \cup \{e_1\} \preceq G \cup \{e_1\} \cup \{e_2\} \preceq \cdots \preceq G \cup \{e_1\} \cup \cdots \cup \{e_p\} = \overline{F} \)

\[
\begin{align*}
&G \preceq G \cup \{e_1\} \preceq G \cup \{e_1\} \cup \{e_2\} \preceq \cdots \preceq G \cup \{e_1\} \cup \cdots \cup \{e_q\} = F',
\end{align*}
\]

be maximal chains, so that

\[
(2) \quad r(F) - r(G) = p \quad \text{and} \quad r(F') - r(G) = q.
\]

But then \( G \cup \{e_1, \ldots, e_p, e_1', \ldots, e_q'\} = F \cup F' \), so

\[
F \preceq F \cup \{e_1\} \preceq \cdots \preceq F \cup \{e_1\} \cup \cdots \cup \{e_q'\} = F \cup F',
\]

where each \( \leq \) is either \( \preceq \) or \( = \). So \( r(F \cup F') - r(G) \leq p + q \), which when combined with \( \Box \) implies submodularity.
For assertion (2), it is easy to check that $A \mapsto \tilde{A}$ is a closure operator, and that $\tilde{A} = A$ for $|A| \leq 1$. So the only nontrivial part is to establish (1c).

Note that if $L$ is semimodular, $e \in L$ is an atom, and $x \not\preceq e$, then $x \vee e \succeq e$ (because $r(x \vee e) - r(x) \leq r(e) - r(x \wedge e) = 1 - 0 = 1$).

Accordingly, suppose that $e \notin \tilde{A}$ but $e \in \overline{A \cup f}$. Let $x = \bigvee A \in L$. Then

$$x < x \vee f$$

and

$$x < x \vee e \leq x \vee f$$

which implies that $x \vee f = x \vee e$, and in particular $f \leq x \vee e = \overline{A \cup e}$, proving that $A \mapsto \tilde{A}$ is a matroid closure operator.

In view of this bijection, we can describe a matroid on ground set $E$ by the function $A \mapsto r(\tilde{A})$, where $r$ is the rank function of the associated geometric lattice. It is standard to abuse notation by calling this function $r$ also. Formally:

**Definition 1.** A matroid rank function on $E$ is a function $r : 2^E \to \mathbb{N}$ satisfying

\begin{align*}
(3a) & \quad r(A) \leq |A|; \quad \text{and} \\
(3b) & \quad r(A) + r(B) \geq r(A \cap B) + r(A \cup B)
\end{align*}

for all $A, B \subseteq E$.

**Example 1.** Let $n = |E|$ and $0 \leq k \leq E$, and define

$$r(A) = \min(k, |A|).$$

This clearly satisfies (3a) and (3b). The corresponding matroid is called the **uniform matroid** $U_k(n)$, and has closure operator

$$\tilde{A} = \begin{cases} A & \text{if } |A| < k, \\ E & \text{if } |A| \geq k. \end{cases}$$

So the flats of $M$ of the sets of cardinality $< k$, as well as (of course) $E$ itself. Therefore, the lattice of flats looks like a Boolean algebra $B_n$ that has been truncated at the $k^{th}$ rank. For $n = 3$ and $k = 2$, this lattice is $M_5$; for $n = 4$ and $k = 3$, it is the following:

If $S$ is a set of $n$ points in general position in $\mathbb{F}^k$, then the corresponding matroid is isomorphic to $U_k(n)$. This sentence is tautological, in the sense that it can be taken as a definition of “general position”. Indeed, if $\mathbb{F}$ is infinite and the points are chosen randomly (in some reasonable analytic or measure-theoretic sense), then $L(S)$ will be isomorphic to $U_k(n)$ with probability 1. On the other hand, $\mathbb{F}$ must be sufficiently large (in terms of $n$) in order for $\mathbb{F}^k$ to have $n$ points in general position.

As for “isomorphic”, here’s a precise definition.

**Definition 2.** Let $M, M'$ be matroids on ground sets $E, E'$ respectively. We say that $M$ and $M'$ are **isomorphic**, written $M \cong M'$, if there is a bijection $f : E \to E'$ meeting any (hence all) of the following conditions:

1. There is a lattice isomorphism $L(M) \cong L(M')$;
2. $r(A) = r(f(A))$ for all $A \subseteq E$. (Here $f(A) = \{f(a) \mid a \in A\}$.)
3. $\overline{f(A)} = f(\overline{A})$ for all $A \subseteq E$.

In general, every equivalent definition of “matroid” (and there are several more coming) will induce a corresponding equivalent notion of “isomorphic”. 
One important application of matroids is in graph theory. Let $G$ be a finite graph with vertices $V$ and edges $E$. For convenience, we’ll write $e = xy$ to mean “$e$ is an edge with endpoints $x, y$”; this should not be taken to exclude the possibility that $e$ is a loop (i.e., $x = y$) or that some other edge might have the same pair of endpoints.

**Definition 3.** For each subset $A \subseteq E$, the corresponding *induced subgraph* of $G$ is the graph $G|_A$ with vertices $V$ and edges $A$. The *graphic matroid* or *complete connectivity matroid* $M(G)$ on $E$ is defined by the closure operator

$$
\hat{A} = \{ e = xy \in E \mid x, y \text{ belong to the same component of } G|_A \}. \tag{4}
$$

Equivalently, $e = xy \in \hat{A}$ if there is a path between $x, e$ consisting of edges in $A$ (for short, an $A$-path). For example, in the following graph, $14 \in \hat{A}$ because $\{12, 24\} \subseteq A$.

**Proposition 2.** The operator $A \mapsto \hat{A}$ defined by (4) is a matroid closure operator.

*Proof.* It is easy to check that $A \subseteq \hat{A}$ for all $A$, and that $A \subseteq B \implies \hat{A} \subseteq \hat{B}$. If $e = xy \in \hat{A}$, then $x, y$ can be joined by an $A$-path $P$, and each edge in $P$ can be replaced with an $A$-path, giving an $A$-path between $x$ and $y$.

Finally, suppose $e = xy \notin \hat{A}$ but $e \in A \cup f$. Let $P$ be an $(A \cup f)$-path; in particular, $f \in P$. Then $P \cup f$ is a cycle, from which deleting $f$ produces an $(A \cup e)$-path between the endpoints of $f$. 

\[\square\]