18.997 Topics in Combinatorial Optimization	9 March 2004

Matroids

Lecturer: Michel X. Goemans — *Scribe: Bridget Eileen Tenner*

For reference, see Chapter 39 of Schrijver's book.

Definition 1 *A* matroid $M = (S, \mathcal{I})$ *is a finite ground set S together with a collection of sets $\mathcal{I} \subseteq 2^S$, known as the* independent sets*, satisfying the following axioms:*

1. *If $I \in \mathcal{I}$ and $J \subseteq I$ then $J \in \mathcal{I}$.*
2. *If I, $J \in \mathcal{I}$ and $|J| > |I|$, then there exists an element $z \in J \setminus I$ such that $I + z \in \mathcal{I}$, where $+$ indicates union.*

If $I \subseteq S$ is not an element of $\mathcal{I}$, I is called a *dependent set*. An element $I \in \mathcal{I}$ is a *basis* if it is a maximal (inclusion-wise) independent set. A *circuit* C of M is a minimal dependent set. A set $I \in \mathcal{I}$ is a *spanning set* if I contains a basis.

Example 1 *Linear matroids.*
Let A be an m-by-n matrix. Let $S = \{1, \ldots, n\}$ be the index set of the columns of A. $I \subseteq S$ is independent if the columns indexed by I are linearly independent.

It is straightforward to check that the axioms for a matroid hold in this example.

Observation 1 *All bases of a matroid have the same cardinality by the second axiom.*

For $T \subseteq S$, let the *rank* of T be $r_M(T) = r(T) = \max\{|I| : I \subseteq T \text{ and } I \in \mathcal{I}\}$. Note that this is a generalization of the linear algebra definition of rank. Letting the set T equal S, we find that $r_M(S) = |B|$, the size of a basis of the matroid.

If F is a field, a matroid is said to be *representable* over F if the matrix A and linear independence are taken over F.

Example 2 *Uniform matroids.*
For any ground set S and a specific k, let $I \in \mathcal{I}$ if $|I| \leq k$. Denote this matroid $U^k_{|S|}$.

The matroid U^2_4 is a linear matroid: consider four vectors in the plane such that no two are multiples of each other. Then let each column of a 2-by-4 matrix A correspond to one of these vectors.

Can the matroid U^2_4 be represented over another field? Let us consider this question for $GF(2)$. That is, can we find a matrix A in which all entries are 0 or 1, no column is the zero vector, no two columns sum to the zero vector, but any three columns sum to the zero vector?

Before answering this question, observe the following: for any linear matroid, we can assume that the rank of the matrix A is m, since otherwise we could remove the redundant rows. By elementary operations, we can further assume that A has the form

$$\begin{bmatrix} I_m & B \end{bmatrix}$$

where B is an m-by-$(n-m)$ matrix.

Returning to the question of U^2_4 being representable over $GF(2)$, if there was such a representation, then it would have the form

$$\begin{bmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{bmatrix}$$

where each $*$ is either 0 or 1. However, each of the columns must be distinct, and none can be $(0,0)^T$ so there is no such representation. Thus the matroid U_4^2 is uniform and linear, but is not representable over $GF(2)$.

Definition 2 *A* binary *matroid is a linear matroid that can be represented over $GF(2)$. A matroid is* regular *if it is representable over any field F.*

Example 3 *Graphic matroids.*
For an undirected graph $G = (V, E)$, let the ground set S be the set E of edges of the graph. The matroid $M(G)$, sometimes called the cycle matroid of G, is defined as $M(G) = (E, \mathcal{I})$ where $\mathcal{I} = \{F \subseteq E : F \text{ is acyclic}\}$.

It is straightforward to check that the axioms of a matroid hold in this example. In a graphic matroid, we can make the following observations:

- The bases are the spanning trees of G.
- The circuits are the circuits of the graph G.
- The spanning sets are the connected sets of G.
- The rank function is defined as $r_{M(G)}(F) = |V| - \kappa(V, F)$ where $\kappa(H)$ is the number of connected components of a graph H.

Graphic matroids are linear. This can be seen by looking at the vertex/edge incidence matrix with a $+1$ and a -1 in each edge column (the order of these is unimportant). In fact, this representation works over any field F: let the $+1$ be the multiplicative identity in F and let the -1 be the additive inverse of this $+1$. Thus graphic matroids are regular.

The matroids defined so far can be classified in the following manner:

$$\{\text{graphic matroids}\} \subseteq \{\text{regular matroids}\} \subseteq \{\text{binary matroids}\} \subseteq \{\text{linear matroids}\}.$$

Example 4 *Matching matroids.*
Start with a graph $G = (V, E)$. Let $S = V$, the set of vertices. A set $I \subseteq S$ is independent if I can be covered by a matching. Note, if G has a perfect matching, every subset of the vertices can be covered.

The first axiom of a matroid is easy to check for matching matroids. Given the hypotheses of the second axiom, let M_J and M_I be the corresponding matchings of the independent sets J and I, respectively. If M_I covers one element in $J \setminus I$, the axiom obviously holds. So suppose this is not the case. Consider $M_I \Delta M_J$. Every vertex in $J \setminus I$ has an alternating path that starts from that vertex. Some of these paths may end in $I \setminus J$, but they cannot all end there, since $|J \setminus I| > |I \setminus J|$. Thus at least one vertex in $J \setminus I$ has a path that ends somewhere else. And that endpoint cannot be in $J \cap I$ since these vertices have degree 0 or 2 in $M_I \Delta M_J$. Thus we have an alternating path P from $J \setminus I$ to a vertex not in I. Now $M_I \Delta P$ is a matching that covers I and one more vertex in $J \setminus I$.

Example 5 *Let $G = (V, A)$ be a digraph. Suppose $S \subseteq V$. Assume there is a distinguished vertex $s \in V$. Let $I \subseteq S$ be independent if there exist arc-disjoint paths from s to v for all $v \in I$.*

As in the previous examples, the first axiom of matroids is clear for this example. The second axiom is essentially network flows: reverse the paths from s to the elements of the set J. These could share some of the arcs of the paths from s to the elements of the set I. When viewed as a whole, there are more sources (vertices of $J \setminus I$) than sinks (vertices of $I \setminus J$). Decompose this into paths and cycles. This yields at least one path from $v \in J \setminus I$ to s.

This example can be generalized in the following manner. The ground set S is still a subset of V, but now instead of having a distinguished vertex s, there is a distinguished set $U \subseteq V$. A set $I \subseteq S$ is independent if there exist *vertex*-disjoint paths from a subset $T \subseteq U$, $|T| = |I|$, to I. Such matroids are known as *gammoids*, and were developed by Perfect in 1968.

Consider a matroid $M = (S, \mathcal{I})$. The *dual matroid* is $M^* = (S, \mathcal{I}^*)$ where $\mathcal{I}^* = \{I \subseteq S : S \setminus I \text{ is a spanning set for } M\}$. That is, the complement of a basis of M, as well as all subsets of this, is independent in M^*. The bases of M^* are the complements of the bases of M. It is straightforward to check that this is a matroid.

Suppose we take the cycle matroid of a planar graph G that is sufficiently connected to guarantee a unique embedding (three-connectivity does this). Define the dual graph in the standard way. Take a spanning tree of G and consider the edges not selected by this. Look at the corresponding edges in the dual graph. This gives a spanning tree in the dual graph. So the dual of this matroid is also graphic, and in this particular situation the dual matroid corresponds to the dual graph of the original graph. Tutte has shown that the dual of the cycle matroid of a graph G is also a graphic matroid if and only if G is planar.

Several properties of dual matroids are worth mentioning here. First, let us understand $(M^*)^*$. This is certainly a matroid, and the bases of this matroid are the bases of M. Thus $(M^*)^* = M$. Also, recall that to a matroid M we associate a rank function r_M. What is the rank function r_{M^*} associated to the dual M^*? Let U be an independent set in M^*. Then, given that any basis B of M has size $r_M(S)$ and that $B \setminus U = B \cap (S \setminus U)$ is a largest independent set in $S \setminus U$,

$$\begin{aligned} r_{M^*}(U) &= \max_{\text{basis } B \text{ of } M} |U \setminus B| \\ &= |U| - \min_{\text{basis } B \text{ of } M} |U \cap B| \\ &= |U| - \left(r_M(S) - \max_{\text{basis } B \text{ of } M} |B \setminus U| \right) \\ &= |U| - r_M(S) + r_M(S \setminus U). \end{aligned}$$

There are additional operations (besides taking the dual) that can be performed on a matroid. For example if $Z \subseteq S$, we have the *deletion* $M \setminus Z$ and the *contraction* M/Z.

Deletion: $M \setminus Z = (S \setminus Z, \{I \subseteq S \setminus Z : I \text{ independent in } M\})$. For example, take a graphic matroid and delete some of its edges. Look at acyclic subsets of the remaining edges. The rank function for this matroid is $r_{M \setminus Z}(U) = r_M(U)$ for $U \subseteq S \setminus Z$.

Contraction: $M/Z = (M^* \setminus Z)^*$. From the formulas for the rank after taking the dual or after deleting elements, we get that

$$\begin{aligned} r_{M/Z}(U) &= r_{(M^* \setminus Z)^*}(U) = |U| - r_{M^* \setminus Z}(S \setminus Z) + r_{M^* \setminus Z}(S \setminus Z \setminus U) \\ &= |U| - r_{M^*}(S \setminus Z) + r_{M^*}(S \setminus Z \setminus U) \\ &= |U| - (|S \setminus Z| - r_M(S) + r_M(Z)) + (|S \setminus Z \setminus U| - r_M(S) + r_M(Z \cup U)) \\ &= r_M(Z \cup U) - r_M(Z). \end{aligned}$$

This can be interpreted as follows. Take any $X \subseteq Z$ such that $|X| = r_M(Z)$, i.e. X is a maximal independent set in Z. Now, U will be independent in M/Z if $r_M(Z \cup U) = |U| + r_M(Z) = |U| + |X| = |U \cup X|$ which means that $U \cup X$ is independent in M. In other words, another (equivalent) definition for the contraction is

$$M/Z = (S \setminus Z, \{I \subseteq S \setminus Z : I \cup X \in \mathcal{I}\}).$$

By playing with the rank function, one can check that, for any disjoint sets Y and Z, $(M/Z)/Y = M/(Y \cup Z) = (M/Y)/Z$. And similarly for deletions. Moreover, $(M/Z) \setminus X = (M \setminus X)/Z$.

If M is representable over F, then M^* is also representable over F. This can be seen by taking the standard representation $A = [I_m \; B]$ for M. This corresponds to a representation A' for M^* where $A' = \left[B^T \; I_{n-m}\right]$.

Also, $M \setminus Z$ and M/Z can be represented over F if M can. The class of matroids representable over F is thus closed under taking minors.

Consider non-binary matroids. Look at the minor minimal non-binary matroids. There is only one, and this is U_4^2. Any other non-binary matroid has U_4^2 as a minor.

A major open problem, posed by Rota, is: for $GF(q)$, do you need only a finite number of obstructions for non-$GF(q)$-representable matroids? The $GF(2)$ case was done by Tutte in 1958, and the $GF(3)$ and $GF(4)$ cases have been done since then. However, the general case is still open.