18.438 Advanced Combinatorial Optimization 8 October 2009

Lecture 8: Matroids

Lecturer: Michel X. Goemans *Scribe: Elette Boyle**

(*Based on notes from Bridget Eileen Tenner and Nicole Immorlica.)

1 Matroids

1.1 Definitions and Examples

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* $I \cup \{z\} \in \mathcal{I}$*.*

Terminology:

- $I \in \mathcal{I} \implies$ called *independent*; $I \notin \mathcal{I} \implies$ *dependent.*
- A *circuit* is an inclusionwise minimally dependent set of M.
- A *basis* is any maximal independent set.
- I is a *spanning set* if $I \supseteq B$ for some basis B.

Observation 1 *Note that all bases of a matroid* M *must have the same cardinality by axiom 2.*

Example 1 *Uniform matroids* U_n^k*: Given by* $|S| = n$*,* $\mathcal{I} = \{I \subseteq S : |I| \leq k\}$*. The circuits are all sets of cardinality* $k+1$*, and the bases are all sets of cardinality* k*.*

Example 2 *Linear Matroids.*
Let F *be a field,* $A \in F^{m \times n}$ *an* $m \times n$ *matrix over* F*. 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.*

Definition 2 *Rank function of* M

$$r : 2^S \to \mathbb{Z}_+ \quad by \quad r(U) = \max_{I \subseteq U, I \in \mathcal{I}} |I|.$$

Note that this is a generalization of the linear algebra definition of rank. Indeed, for a linear matroid M, $r(U) =$ the rank of the submatrix formed by the columns indexed by U. Taking $U = S$, we find that $r(S) = |B|$, the size of any basis of the matroid.

For a linear matroid, we can assume the matrix A has rank m; otherwise, we could remove the redundant rows without changing the structure of the matroid. Further, by elementary row operations and column swaps, we can uniquely express A in the form

$$A = \left[\; I_m \;\middle|\; B \; \right]$$

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

Definition 3 *If* F *is a field, a matroid is said to be* representable *over* F *if it can be expressed as a linear matroid with matrix* A *and linear independence taken over* F*.*

Example 3 *U_4^2 is not representable over $GF(2)$.*
From the definition of U_4^2, for any $U \subseteq S$, $r(U) = |U|$ if $|U| \leq 2$, and $r(U) = 2$ if $|U| > 2$. In particular, the rank of U_4^2 is 2. If there existed a representation of U_4^2 over $GF(2)$, the corresponding matrix A would be of the form

$$A = \begin{bmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{bmatrix},$$

where each $* \in GF(2)$, no column is the zero vector, and any two columns are linearly independent. However, this cannot be the case, since there are only three possible distinct nonzero columns over $GF(2)$.

We note, however, that U_4^2 can be represented over other fields. For instance, over $\mathbb{R}$, U_4^2 is given by the matrix

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

Definition 4 *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.*

One can show that regular matroids are precisely those that are representable over $\mathbb{R}$ by a ± 1 totally unimodular matrix (ie, $\det B \in \{0, \pm 1\}$ for any submatrix B); in fact, this is sometimes the definition of regular matroids.

Example 4 *Graphic Matroids (also known as cycle matroids of a graph).*
Let $G = (V, E)$ be an undirected graph. Matroid $M = (E, \mathcal{I})$, where $\mathcal{I} = \{F \subseteq E : F is acyclic\}$; ie, forests in G.

It is straightforward to check that the axioms of a matroid hold in this example. Note, however, taking $G = (V, E)$ to be a directed graph and $\mathcal{I} = \{$sets of edges without directed cycles$\}$ does *not* in general form a matroid. For instance, consider G the complete graph on 4 vertices, and $I, J \subset \mathcal{I}$ the subsets of edges below.

Both I and J contain no cycles and $|J| > |I|$, but adding any edge from J to I will cause a cycle to be formed.

In a graphic matroid $M(G)$, we can make the following observations:

- The bases of $M(G)$ are the spanning trees of G; this assumes that G is connected.
- The circuits are simple cycles of the graph.
- The spanning sets are the connected sets of G.

Lemma 1 *Graphic matroids are regular.*

Proof: Take A to be the vertex/edge incidence matrix with a $+1$ and a -1 in each edge column (the order of the $+1/-1$ is unimportant). We see that a minimal collection of linearly dependent columns corresponds precisely to the simple cycles of the graph (adding the corresponding columns after possibly multiplyting them by -1 to make the orientation agree along the cycle). Note that this representation works over any field F, where we take $+1$ to be the multiplicative identity and -1 its additive inverse. Therefore, graphic matroids are regular.

$$\text{vertices} \begin{bmatrix} -1 & 0 & -1 & 1 & 0 \\ 0 & 1 & 0 & -1 & 1 \\ 0 & 0 & 1 & 0 & -1 \\ 1 & -1 & 0 & 0 & 0 \end{bmatrix}$$
$$\text{edges}$$

□

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 5 *Gammoid.*
Let (V, E) be a directed graph, and $S, U \subseteq V$.
$I \subseteq S$ is independent if $\exists J \subseteq U$ such that $|J| = |I|$ and there exists a collection of vertex-disjoint directed paths from $J \to I$ (allowing paths of length 0, corresponding to $v \in S \cap U$). See Figure 1.

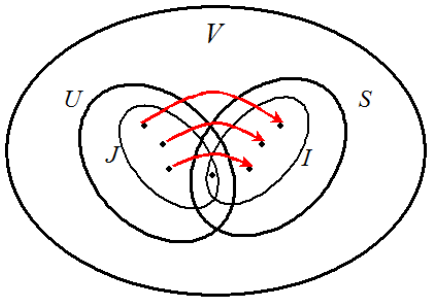

Figure 1: Example of independent set $I \in \mathcal{I}$ of the gammoid given by the directed graph (V, E) and sets $S, U \subseteq V$.

We can see that this definition for $\mathcal{I}$ satisfies axiom 2 by using network flows. (As an aside, it was mentioned in lecture that given k edge-disjoint paths from $s \to t$ and k edge-disjoint paths from $t \to u$, one can find k edge-disjoint paths from $s \to u$ using the stable marriage problem).

Example 6 *Matching Matroid.*
Let $G = (V, E)$ be a graph. The matching matroid $M = (V, \mathcal{I})$ for G corresponds to $U \subseteq V$ independent if there exists a matching that covers all of U (and possibly other vertices).

Note if G has a perfect matching then every subset of vertices is independent and we have the *free* matroid. This definition clearly satisfies the first matroid axiom; we will now show it satisfies axiom 2 as well. Suppose $I, J \in \mathcal{I}$ with $|J| > |I|$. Let M_J, M_I be matchings of G covering the vertices of J and I, respectively. If M_I covers an element in $J \setminus I$, then the axiom obviously holds, so suppose this is not the case. Consider the matching $M_I \Delta M_J$. 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. This 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 $J \setminus I$.

We defined matroids in terms of axioms for their independent sets, but we could also have defined them in terms of axioms for their bases, their circuits, or their rank function. The following definition in terms of the rank function can be shown to be equivalent to the definition in terms of independent sets.

Definition 5 *Rank Function Definition of a Matroid.* $r : 2^S \to \mathbb{Z}_+$ *is a rank function of a matroid iff* r *satisfies:*

1. $r(U) \leq |U|$ *for all* U,
2. *monotonicity:* $T \subseteq U \implies r(T) \leq r(U)$,
3. *submodularity:* $\forall A, B \subseteq S,\ r(A \cap B) + r(A \cup B) \leq r(A) + r(B)$.

For any such function, we can construct a matroid having this rank function by letting $\mathcal{I} = \{U \subseteq S : |U| = r(U)\}$.

Observation 2 *Condition 3 is equivalent to:*

3'. $\forall C \subseteq D,\ \forall j \notin D,\ r(D \cup \{j\}) - r(D) \leq r(C \cup \{j\}) - r(C)$.

One direction can be seen by taking $C = A \cap B$, $D = A$ *and successively adding all elements of* $B \setminus A$. *The other by considering* $A = C \cup \{j\}$ *and* $B = D$.

1.2 Dual Matroid

Definition 6 *Dual Matroid* M^*.
Consider a matroid $M = (S, \mathcal{I})$. *Then we define* $M^* = (S, \mathcal{I}^*)$, *where* $\mathcal{I} = \{U \mid \exists$ *basis* B *for* M *st* $B \subseteq U\}$.

Axiom 1 of the matroid definition is clearly satisfied. To show axiom 2 holds, suppose $I, J \in \mathcal{I}$ with $|I| > |J|$. Then there exists a basis B_J in $S \setminus J$. If $\exists i \in I \setminus (B_J \cup J)$, then B_J is still outside $J \cup \{i\}$. The case when there is no such i follows from properties of bases we will discuss soon.

For now, we will show its rank function r^* satisfies the conditions of Definition 5. We have

$$\begin{aligned} r^*(U) &= \max_{I \subseteq U, I \in \mathcal{I}^*} |I| \\ &= \max_{\text{basis } B \text{ of } M} |U \setminus B| \\ &= |U| - \min_{\text{basis } B \text{ of } M} |U \cap B| \\ &= |U| - r(S) + \max_{\text{basis } B \text{ of } M} |B \cap (S \setminus U)| \\ &= |U| - r(S) + r(S \setminus U). \end{aligned}$$

We check the three axioms:

1. $r^*(U) \leq |U|$ since $r(S) \geq r(S \setminus U)$ by monotonicity of the rank function r.
2. Monotonicity: Suppose $T \subseteq U \subseteq S$. Then $r^*(T) = |T| - r(S) + r(S \setminus T) \leq |T| - r(S) + [r(S \setminus U) + r(U \setminus T) - r(\emptyset)]$ (by submodularity of r) $\leq |T| - r(S) + r(S \setminus U) + (|U| - |T|) = |U| - r(S) + r(S \setminus U) = r^*(U)$.
3. Submodularity: Let $A, B \subseteq S$. Take $T = S \setminus A$, $U = S \setminus B$. Then by submodularity of r applied to T, U, we have $r(T \cup U) + r(T \cap U) = r(S \setminus (A \cap B)) + r(S \setminus (A \cup B)) \leq r(S \setminus A) + r(S \setminus B)$. Further, we have $|A \cup B| + |A \cap B| = (|A| + |B| - |A \cap B|) + |A \cap B| = |A| + |B|$. Thus, it follows that $r^*(A \cup B) + r^*(A \cap B) \leq r^*(A) + r^*(B)$.

Example 7 *For example, if* M_G *is a graphic matroid then the independent sets of* M_G^* *are those sets of edges which, when removed, leave the graph* G *still connected.* M_G^* *is called a cographic matroid. Tutte has shown that a cographic matroid is graphic if and only if the graph* G *is planar. When* G *is planar, the dual matroid corresponds to the graphic matroid for the planar dual of* G *(more precisely, although the dual graph is not uniquely defined if the graph is not 3-connected, the dual matroid is, and corresponds to any planar dual of* G*).*

Theorem 2 *If M is representable over F, then so is M^*.*

Proof: Suppose the rank of the matroid (i.e. of its ground set) is m, i.e. the bases of M have size m. Then, by assumption, M can be represented by an $m \times n$ matrix $A = [I^{m\times m}|B^{m\times(n-m)}]$ over F. The columns of this matrix are indexed by the elements of the ground set. We claim that the dual matroid can be represented over F by the matrix:

$$A^* = [B^T|I^{(n-m)\times(n-m)}].$$

Consider any basis Z of M; we need to show that the complementary set of elements define a basis of M^* (and vice versa). For simplicity, assume we rearrange the rows and columns of A (and of A^*) such that the elements of Z correspond to the 2nd and 3rd blocks of columns; this does not change linear independence.

$$A = \left[\begin{array}{c|c|c|c} I & 0 & B_{11} & B_{12} \\ 0 & I & B_{21} & B_{22} \end{array}\right], \quad A^* = \left[\begin{array}{c|c|c|c} B_{11}^T & B_{21}^T & I & 0 \\ B_{12}^T & B_{22}^T & 0 & I \end{array}\right].$$

Since Z is a basis, B_{11} must have full rank, and so the 1st and 4th blocks of columns in A^* are independent. These columns correspond to a set Z^* of elements of the dual. By a similar argument, it is a maximal independent set of vectors, and so is a basis. As $Z^* = S \setminus Z$, Z^* is a basis of M^*. Since this is true for every basis Z of M, it follows that A^* is a representation of the dual matroid M^* of M.

□