Massachusetts Institute of Technology
18.433: Combinatorial Optimization
Michel X. Goemans

Handout 9
March 20th, 2009

4. Lecture notes on matroid optimization

4.1 Definition of a Matroid

Matroids are combinatorial structures that generalize the notion of linear independence in matrices. There are many equivalent definitions of matroids, we will use one that focus on its *independent sets*. A matroid M is defined on a finite ground set E (or $E(M)$ if we want to emphasize the matroid M) and a collection of subsets of E are said to be *independent*. The family of independent sets is denoted by $\mathcal{I}$ or $\mathcal{I}(M)$, and we typically refer to a matroid M by listing its ground set and its family of independent sets: $M = (E, \mathcal{I})$. For M to be a matroid, $\mathcal{I}$ must satisfy two main axioms:

(I_1) if $X \subseteq Y$ and $Y \in \mathcal{I}$ then $X \in \mathcal{I}$,

(I_2) if $X \in \mathcal{I}$ and $Y \in \mathcal{I}$ and $|Y| > |X|$ then $\exists e \in Y \setminus X : X \cup \{e\} \in \mathcal{I}$.

In words, the second axiom says that if X is independent and there exists a larger independent set Y then X can be extended to a larger independent by adding an element of $Y \setminus X$. Axiom (I_2) implies that every *maximal* (inclusion-wise) independent set is maximum; in other words, all maximal independent sets have the same cardinality. A maximal independent set is called a *base* of the matroid.

Examples.

- One trivial example of a matroid $M = (E, \mathcal{I})$ is a **uniform** matroid in which

  $$\mathcal{I} = \{X \subseteq E : |X| \leq k\},$$

  for a given k. It is usually denoted as $U_{k,n}$ where $|E| = n$. A base is any set of cardinality k (unless $k > |E|$ in which case the only base is $|E|$).

  A **free** matroid is one in which all sets are independent; it is $U_{n,n}$.

- Another is a **partition** matroid in which E is partitioned into (disjoint) sets $E_1, E_2, \cdots, E_l$ and

  $$\mathcal{I} = \{X \subseteq E : |X \cap E_i| \leq k_i \text{ for all } i = 1, \cdots, l\},$$

  for some given parameters $k_1, \cdots, k_l$. As an exercise, let us check that (I_2) is satisfied. If $X, Y \in \mathcal{I}$ and $|Y| > |X|$, there must exist i such that $|Y \cap E_i| > |X \cap E_i|$ and this means that adding any element e in $E_i \cap (Y \setminus X)$ to X will maintain independence.

  Observe that M would *not* be a matroid if the sets E_i were *not* disjoint. For example, if $E_1 = \{1, 2\}$ and $E_2 = \{2, 3\}$ with $k_1 = 1$ and $k_2 = 1$ then both $Y = \{1, 3\}$ and $X = \{2\}$ have at most one element of each E_i, but one can't find an element of Y to add to X.

- **Linear** matroids (or representable matroids) are defined from a matrix A, and this is where the term *matroid* comes from. Let E denote the index set of the columns of A. For a subset X of E, let A_X denote the submatrix of A consisting only of those columns indexed by X. Now, define

$$\mathcal{I} = \{X \subseteq E : rank(A_X) = |X|\},$$

i.e. a set X is independent if the corresponding columns are linearly independent. A base B corresponds to a linearly independent set of columns of cardinality $rank(A)$.

Observe that (I_1) is trivially satisfied, as if columns are linearly independent, so is a subset of them. (I_2) is less trivial, but corresponds to a fundamental linear algebra property. If A_X has full column rank, its columns span a space of dimension $|X|$, and similarly for Y, and therefore if $|Y| > |X|$, there must exist a column of A_Y that is not in the span of the columns of A_X; adding this column to A_X increases the rank by 1.

A linear matroid can be defined over any field $\mathbb{F}$ (not just the reals); we say that the matroid is **representable over** $\mathbb{F}$. If the field is $\mathbb{F}_2$ (field of 2 elements with operations (mod 2)) then the matroid is said to be **binary**. If the field is $\mathbb{F}_3$ then the matroid is said to be **ternary**.

For example, the binary matroid corresponding to the matrix

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

corresponds to $U_{2,3}$ since the sum of the 3 columns is the 0 vector when taking components modulo 2. If A is viewed over the reals or over $\mathbb{F}_3$ then the matroid is the free matroid on 3 elements.

Not every matroid is linear. Among those that are linear, some can be represented over some fields $\mathbb{F}$ but not all. For example, there are binary matroids which are not ternary and vice versa (for example, $U_{2,4}$ is ternary but not binary). Matroids which can be represented over *any* field are called **regular**.

- Here is an example of something that is not a matroid. Take a graph $G = (V, E)$, and let $\mathcal{I} = \{F \subseteq E : F \text{ is a matching}\}$. This is not a matroid since (I_2) is not necessarily satisfied ((I_1) is satisfied[1], however). Consider, for example, a graph on 4 vertices and let $X = \{(2, 3)\}$ and $Y = \{(1, 2), (3, 4)\}$. Both X and Y are matchings, but one cannot add an edge of Y to X and still have a matching.

- There is, however, another matroid associated with matchings in a (general, not necessarily bipartite) graph $G = (V, E)$, but this time the ground set of M corresponds to V. In the **matching matroid**, $\mathcal{I} = \{S \subseteq V : S \text{ is covered by some matching } M\}$. In this definition, the matching does not need to cover precisely S; other vertices can be covered as well.

[1]When (I_1) alone is satisfied, $(E, \mathcal{I})$ is called an *independence system.*

- A very important class of matroids in combinatorial optimization is the class of **graphic** matroids (also called cycle matroids). Given a graph $G = (V, E)$, we define independent sets to be those subsets of edges which are forests, i.e. do not contain any cycles. This is called the graphic matroid $M = (E, \mathcal{I})$, or $M(G)$.

  (I_1) is clearly satisfied. To check (I_2), first notice that if F is a forest then the number of connected components of the graph (V, F) is given by $K(V, F) = |V| - |F|$. Therefore, if X and Y are 2 forests and $|Y| > |X|$ then $K(V, Y) < K(V, X)$ and therefore there must exist an edge of $Y \setminus X$ which connects two different connected components of X; adding this edge to X results in a larger forest. This shows (I_2).

  If the graph G is connected, any base will correspond to a spanning tree T of the graph. If the original graph is disconnected then a base corresponds to taking a spanning tree in each connected component of G.

  A graphic matroid is a linear matroid. We first show that the field $\mathbb{F}$ can be chosen to be the reals. Consider the matrix A with a row for each vertex $i \in V$ and a column for each edge $e = (i, j) \in E$. In the column corresponding to (i, j), all entries are 0, except for a 1 in i or j (arbitrarily) and a -1 in the other. To show equivalence between the original matroid M and this newly constructed linear matroid M', we need to show that any independent set for M is independent in M' and vice versa. This is left as an exercise.

  In fact, a graphic matroid is *regular*; it can be represented over any field $\mathbb{F}$. To obtain a representation for a field $\mathbb{F}$, one simply needs to take the representation given above for $\mathbb{R}$ and simply view/replace all -1 by the additive inverse of 1 (i.e. by $p - 1$ for $\mathbb{F}_p$).

4.1.1 Circuits

A minimal (inclusionwise) dependent set in a matroid is called a *circuit*. In a graphic matroid $M(G)$, a circuit will be the usual notion of a cycle in the graph G; to be dependent in the graphic matroid, one needs to contain a cycle and the minimal sets of edges containing a cycle are the cycles themselves. In a partition matroid, a circuit will be a set $C \subseteq E_i$ with $|C \cap E_i| = k_i + 1$.

By definition of a circuit C, we have that if we remove any element of a circuit then we get an independent set. A crucial property of circuit is given by the following property,

Theorem 4.1 (Unique Circuit Property) *Let $M = (E, \mathcal{I})$ be a matroid. Let $S \in \mathcal{I}$ and e such that[2] $S + e \notin \mathcal{I}$. Then there exists a unique circuit $C \subseteq S + e$.*

The unicity is very important. Indeed, if we consider any $f \in C$ where C is this unique circuit then we have that $C + e - f \in \mathcal{I}$. Indeed, if $C + e - f$ was dependent, it would contain a circuit C' which is distinct from C since $f \notin C'$, a contradiction.

[2]For a set S and an element e, we often write $S + e$ for $S \cup \{e\}$ and $S - e$ for $S \setminus \{e\}$.

As a special case of the theorem, consider a graphic matroid. If we add an edge to a forest and the resulting graph has a cycle then it has a unique cycle.

Proof:

Suppose $S+e$ contains more than one circuit, say C_1 and C_2 with $C_1 \neq C_2$. By minimality of C_1 and C_2, we have that there exists $f \in C_1 \setminus C_2$ and $g \in C_2 \setminus C_1$. Since $C_1 - f \in \mathcal{I}$ (by minimality of the circuit C_1), we can extend it to a maximal independent set X of $S + e$. Since S is also independent, we must have that $|X| = |S|$ and since $e \in C_1 - f$, we must have that $X = S + e - f \in \mathcal{I}$. But this means that $C_2 \subseteq S + e - f = X$ which is a contradiction since C_2 is dependent. $\triangle$

Exercise 4-1. Show that any partition matroid is also a linear matroid over $\mathbb{F} = \mathbb{R}$. (No need to give a precise matrix A representing it; just argue its existence.)

Exercise 4-2. Prove that a matching matroid is indeed a matroid.

Exercise 4-3. Show that $U_{2,4}$ is representable over $\mathbb{F}_3$.

Exercise 4-4. Consider the linear matroid (over the reals) defined by the 3×5 matrix:

$$A = \begin{pmatrix} 1 & 2 & 1 & 0 & 1 \\ 1 & 2 & 0 & 1 & -1 \\ 1 & 2 & 0 & 1 & -1 \end{pmatrix}.$$

The ground set $E = \{1, 2, 3, 4, 5\}$ has cardinality 5, corresponds to the columns of A, and the independent sets are the set of columns which are linearly independent (over the reals).

1. Give all bases of this matroid.
2. Give all circuits of this matroid.
3. Choose a base B and an element e not in B, and verify the unique circuit property for $B + e$.

Exercise 4-5. Given a family $A_1, A_2, \cdots, A_n$ of sets (they are not necessarily disjoint), a *transversal* is a set T such that $T = \{a_1, a_2, \cdots, a_n\}$, the a_i's are distinct, and $a_i \in A_i$ for all i. A partial transversal is a transversal for $A_{i_1}, A_{i_2}, \cdots, A_{i_k}$ for some subfamily of the A_i's.

Show that the family of all partial transversals forms a matroid (on the ground set $E = \cup A_i$). (Hint: Think of bipartite matchings.)

Exercise 4-6. Let $M = (E, \mathcal{I})$ be a matroid. Let $k \in \mathbb{N}$ and define

$$\mathcal{I}_k = \{X \in \mathcal{I} : |I| \leq k\}.$$

Show that $M_k = (E, \mathcal{I}_k)$ is also a matroid. This is known as a truncated matroid.

Exercise 4-7. A family $\mathcal{F}$ of sets is said to be *laminar* if, for any two sets $A, B \in \mathcal{F}$, we have that either (i) $A \subseteq B$, or (ii) $B \subseteq A$ or (iii) $A \cap B = \emptyset$. Suppose that we have a laminar family $\mathcal{F}$ of subsets of E and an integer $k(A)$ for every set $A \in \mathcal{F}$. Show that $(E, \mathcal{I})$ defines a matroid (a *laminar* matroid) where:

$$\mathcal{I} = \{X \subseteq E : |X \cap A| \leq k(A) \text{ for all } A \in \mathcal{F}\}.$$

4.2 Matroid Optimization

Given a matroid $M = (E, \mathcal{I})$ and a cost function $c : E \to \mathbb{R}$, we are interested in finding an independent set S of M of maximum total cost $c(S) = \sum_{e \in S} c(e)$. This is a fundamental problem.

If all $c(e) \geq 0$, the problem is equivalent to finding a maximum cost *base* in the matroid. If $c(e) < 0$ for some element e then, because of (I_1), e will not be contained in any optimum solution, and thus we could eliminate such an element from the ground set. In the special case of a graphic matroid $M(G)$ defined on a connected graph G, the problem is thus equivalent to the maximum spanning tree problem which can be solved by a simple greedy algorithm. This is actually the case for any matroid and this is the topic of this section.

The greedy algorithm we describe actually returns, for every k, a set S_k which maximizes $c(S)$ over all independent sets of size k. The overall optimum can thus simply be obtained by outputting the best of these. The greedy algorithm is the following:

- ▷ Sort the elements (and renumber them) such that $c(e_1) \geq c(e_2) \geq \cdots \geq c(e_{|M|})$
- ▷ $S_0 = \emptyset$, k=0
- ▷ For $j = 1$ to $|E|$
  - ▷ if $S_k + e_j \in \mathcal{I}$ then
    - ▷ $k \leftarrow k + 1$
    - ▷ $S_k \leftarrow S_{k-1} + e_j$
    - ▷ $s_k \leftarrow e_j$
- ▷ Output $S_1, S_2, \cdots, S_k$

Theorem 4.2 *For any matroid $M = (E, \mathcal{I})$, the greedy algorithm above finds, for every k, an independent set S_k of maximum cost among all independent sets of size k.*

Proof: Suppose not. Let $S_k = \{s_1, s_2, \cdots, s_k\}$ with $c(s_1) \geq c(s_2) \geq \cdots \geq c(s_k)$, and suppose T_k has greater cost ($c(T_k) > c(S_k)$) where $T_k = \{t_1, t_2, \cdots, t_k\}$ with $c(t_1) \geq c(t_2) \geq \cdots \geq c(t_k)$. Let p be the first index such that $c(t_p) > c(s_p)$. Let $A = \{t_1, t_2, \cdots, t_p\}$ and $B = \{s_1, s_2, \cdots, s_{p-1}\}$. Since $|A| > |B|$, there exists $t_i \notin B$ such that $B + t_i \in \mathcal{I}$. Since $c(t_i) \geq c(t_p) > c(s_p)$, t_i should have been selected when it was considered. To be more precise and detailed, when t_i was considered, the greedy algorithm checked whether t_i could be added to the current set at the time, say S. But since $S \subseteq B$, adding t_i to S should have resulted in an independent set (by (I_1)) since its addition to B results in an independent set. This gives the contradiction and completes the proof. $\triangle$

Observe that, as long as $c(s_k) \geq 0$, we have that $c(S_k) \geq c(S_{k-1})$. Therefore, to find a maximum cost set over all independent sets, we can simply replace the loop

▷ For $j = 1$ to $|E|$

by

▷ For $j = 1$ to q

where q is such that $c(e_q) \geq 0 > c(e_{q+1})$, and output the last S_k.

For the maximum cost spanning tree problem, the greedy algorithm reduces to Kruskal's algorithm which considers the edges in non-increasing cost and add an edge to the previously selected edges if it does not form a cycle.

One can show that the greedy algorithm actually characterizes matroids. If M is an independence system, i.e. it satisfies (I_1), then M is a matroid if and only if the greedy algorithm finds a maximum cost set of size k for every k and every cost function.

Exercise 4-8. We are given n jobs that each take one unit of processing time. All jobs are available at time 0, and job j has a profit of c_j and a deadline d_j. The profit for job j will only be earned if the job completes by time d_j. The problem is to find an ordering of the jobs that maximizes the total profit. First, prove that if a subset of the jobs can be completed on time, then they can also be completed on time if they are scheduled in the order of their deadlines. Now, let $E(M) = \{1, 2, \cdots, n\}$ and let $\mathcal{I}(M) = \{J \subseteq E(M) : J$ can be completed on time $\}$. Prove that M is a matroid and describe how to find an optimal ordering for the jobs.

4.3 Rank Function of a Matroid

Similarly to the notion of rank for matrices, one can define a rank function for any matroid. The rank function of M, denoted by either $r(\cdot)$ or $r_M(\cdot)$, is defined by:

$$r_M : 2^E \to \mathbb{N} : r_M(X) = \max\{|Y| : Y \subseteq X, Y \in \mathcal{I}\}.$$

Here are a few specific rank functions:

- For a linear matroid, the rank of X is precisely the rank in the linear algebra sense of the matrix A_X corresponding to the columns of A in X.
- For a partition matroid $M = (E, \mathcal{I})$ where

$$\mathcal{I} = \{X \subseteq E : |X \cap E_i| \leq k_i \text{ for } i = 1, \cdots, l\}$$

(the E_i's forming a partition of E) its rank function is given by:

$$r(X) = \sum_{i=1}^{l} \min(|E_i \cap X|, k_i).$$

- For a graphic matroid $M(G)$ defined on graph $G = (V, E)$, the rank function is equal to:
$$r_{M(G)}(F) = n - K(V, F),$$
where $n = |V|$ and $K(V, F)$ denotes the number of connected components (including isolated vertices) of the graph with edges F.

The rank function of any matroid $M = (E, \mathcal{I})$ has the following properties:

(R_1) $0 \leq r(X) \leq |X|$ and is integer valued for all $X \subseteq E$

(R_2) $X \subseteq Y \Rightarrow r(X) \leq r(Y)$,

(R_3) $r(X) + r(Y) \geq r(X \cap Y) + r(X \cup Y)$.

The last property is called *submodularity* and is a key concept in combinatorial optimization. It is clear that, as defined, any rank function satisfies (R_1) and (R_2). Showing that the rank function satisfies submodularity needs a proof.

Lemma 4.3 *The rank function of any matroid is submodular.*

Proof: Consider any two sets $X, Y \subseteq$. Let J be a maximal independent subset of $X \cap Y$; thus, $|J| = r(X \cap Y)$. By (I_2), J can be extended to a maximal (thus maximum) indenpendent subset of X, call it J_X. We have that $J \subseteq J_X \subseteq X$ and $|J_X| = r(X)$. Furthermore, by maximality of J within $X \cap Y$, we know

$$J_X \setminus Y = J_X \setminus J. \tag{1}$$

Now extend J_X to a maximal independent set J_{XY} of $X \cup Y$. Thus, $|J_{XY}| = r(X \cup Y)$.

In order to be able to prove that

$$r(X) + r(Y) \geq r(X \cap Y) + r(X \cup Y)$$

or equivalently

$$|J_X| + r(Y) \geq |J| + |J_{XY}|,$$

we need to show that $r(Y) \geq |J| + |J_{XY}| - |J_X|$. Observe that $J_{XY} \cap Y$ is independent (by (I_1)) and a subset of Y, and thus $r(Y) \geq |J_{XY} \cap Y|$. Observe now that

$$J_{XY} \cap Y = J_{XY} \setminus (J_X \setminus Y) = J_{XY} \setminus (J_X \setminus J),$$

the first equality following from the fact that J_X is a maximal independent subset of X and the second equality by (1). Therefore,

$$r(Y) \geq |J_{XY} \cap Y| = |J_{XY} \setminus (J_X \setminus J)| = |J_{XY}| - |J_X| + |J|,$$

proving the lemma. $\triangle$

4.3.1 Span

The following definition is also motivated by the linear algebra setting.

Definition 4.1 *Given a matroid $M = (E, \mathcal{I})$ and given $S \subseteq E$, let*

$$span(S) = \{e \in E : r(S \cup \{e\}) = r(S)\}.$$

Observe that $S \subseteq span(S)$. We claim that $r(S) = r(span(S))$; in other words, if adding an element to S does not increase the rank, adding many such elements also does not increase the rank. Indeed, take a maximal independent subset of S, say J. If $r(span(S)) > |J|$ then there exists $e \in span(S) \setminus J$ such that $J + e \in \mathcal{I}$. Thus $r(S + e) \geq r(J + e) = |J| + 1 > |J| = r(S)$ contradicting the fact that $e \in span(S)$.

Definition 4.2 *A set S is said to be closed if $S = span(S)$.*

Exercise 4-9. Given a matroid M with rank function r and given an integer $k \in \mathbb{N}$, what is the rank function of the truncated matroid M_k (see Exercise 4-6 for a definition).

Exercise 4-10. What is the rank function of a laminar matroid, see exercise 4-7?

4.4 Matroid Polytope

Let

$$X = \{\chi(S) \in \{0,1\}^{|E|} : S \in \mathcal{I}\}$$

denote the incidence (or characteristic) vectors of all independent sets of a matroid $M = (E, \mathcal{I})$, and let the *matroid polytope* be defined as $conv(X)$. In this section, we provide a complete characterization of $conv(X)$ in terms of linear inequalities. In addition, we illustrate the different techniques proposed in the polyhedral chapter for proving a complete description of a polytope.

Theorem 4.4 *Let*

$$P = \{x \in \mathbb{R}^{|E|} : \begin{array}{ll} x(S) \leq r(S) & \forall S \subseteq E \\ x_e \geq 0 & \forall e \in E\} \end{array}$$

where $x(S) := \sum_{e \in S} x_e$. Then $conv(X) = P$.

It is clear that $conv(X) \subseteq P$ since $X \subseteq P$. The harder part is to show that $P \subseteq conv(X)$. In the next three subsections, we provide three different proofs based on the three techniques to prove complete polyhedral descriptions.

4.4.1 Algorithmic Proof

Here we provide an algorithmic proof based on the greedy algorithm. From $conv(X) \subseteq P$, we know that

$$\max\{c^T x : x \in X\} = \max\{c^T x : x \in conv(X)\} \leq \max\{c^T x : \begin{array}{ll} x(S) \leq r(S) & S \subseteq E \\ x_e \geq 0 & e \in E\}. \end{array}$$

Using LP duality, we get that this last expression equals:

$$\min\{\textstyle\sum_S r(S) y_S : \begin{array}{ll} \sum_{S: e \in S} y_S \geq c(e) & \forall e \in E \\ y_S \geq 0 & S \subseteq E\}. \end{array}$$

Our goal now is, for any cost function c, to get an independent set S and a dual feasible solution y such that $c^T \chi(S) = \sum_S r(S) y_S$ which proves that $conv(X) = P$.

Consider any cost function c. We know that the maximum cost independent set can be obtained by the greedy algorithm. More precisely, it is the last set S_k returned by the greedy algorithm when we consider only those elements up to e_q where $c(e_q) \geq 0 \geq c(e_{q+1})$. We need now to exhibit a dual solution of the same value as S_k. There are exponentially many variables in the dual, but this is not a problem. In fact, we will set most of them to 0.

For any index $j \leq k$, we have $S_j = \{s_1, s_2, \cdots, s_j\}$, and we define U_j to be all elements in our ordering up to and excluding s_{j+1}, i.e. $U_j = \{e_1, e_2, \cdots, e_l\}$ where $e_{l+1} = s_{j+1}$. In other words, U_j is all the elements in the ordering just before s_{j+1}. One important property of U_j is that

$$r(U_j) = r(S_j) = j.$$

Indeed, by independence $r(S_j) = |S_j| = j$, and by (R_1), $r(U_j) \geq r(S_j)$. If $r(U_j) > r(S_j)$, there would be an element say $e_p \in U_j \setminus S_j$ such that $S_j \cup \{e_p\} \in \mathcal{I}$. But the greedy algorithm would have selected that element (by (I_1)) contradicting the fact that $e_p \in U_j \setminus S_j$.

Set the non-zero entries of y_S in the following way. For $j = 1, \cdots, k$, let

$$y_{U_j} = c(s_j) - c(s_{j+1}),$$

where it is understood that $c(s_{k+1}) = 0$. By the ordering of the $c(\cdot)$, we have that $y_S \geq 0$ for all S. In addition, for any $e \in E$, we have that

$$\sum_{S: e \in S} y_S = \sum_{j=t}^{k} y_{U_j} = c(s_t) \geq c(e),$$

where t is the least index such that $e \in U_t$ (implying that e does not come before s_t in the ordering). This shows that y is a feasible solution to the dual. Moreover, its dual value is:

$$\sum_S r(S) y_S = \sum_{j=1}^{k} r(U_j) y_{U_j} = \sum_{j=1}^{k} j(c(s_j) - c(s_{j+1})) = \sum_{j=1}^{k} (j-(j-1)) c(s_j) = \sum_{j=1}^{k} c(s_j) = c(S_k).$$

This shows that the dual solution has the same value as the independent set output by the greedy algorithm, and this is true for all cost functions. This completes the algorithmic proof.

4.4.2 Vertex Proof

Here we will focus on any vertex x of

$$P = \{x \in \mathbb{R}^{|E|} : \begin{array}{ll} x(S) \leq r(S) & \forall S \subseteq E \\ x_e \geq 0 & \forall e \in E\} \end{array}$$

and show that x is an integral vector. Since $x(\{e\}) \leq r(\{e\}) \leq 1$, we get that $x \in \{0,1\}^{|E|}$ and thus it is the incidence vector of an independent set.

Given any $x \in P$, consider the *tight* sets S, i.e. those sets for which $x(S) = r(S)$. The next lemma shows that these tight sets are closed under taking intersections or unions. This lemma is really central, and follows from submodularity.

Lemma 4.5 *Let $x \in P$. Let*

$$\mathcal{F} = \{S \subseteq E : x(S) = r(S)\}.$$

Then

$$S \in \mathcal{F}, T \in \mathcal{F} \Rightarrow S \cap T \in \mathcal{F}, S \cup T \in \mathcal{F}.$$

Observe that the lemma applies even if S and T are disjoint. In that case, it says that $\emptyset \in \mathcal{F}$ (which is always the case as $x(\emptyset) = 0 = r(\emptyset)$) and $S \cup T \in \mathcal{F}$.

Proof: The fact that $S, T \in \mathcal{F}$ means that:

$$r(S) + r(T) = x(S) + x(T). \tag{2}$$

Since $x(S) = \sum_{e \in S} x_e$, we have that

$$x(S) + x(T) = x(S \cap T) + x(S \cup T), \tag{3}$$

i.e. that the function $x(\cdot)$ is modular (both x and $-x$ are submodular). Since $x \in P$, we know that $x(S \cap T) \leq r(S \cap T)$ (this is true even if $S \cap T = \emptyset$) and similarly $x(S \cup T) \leq r(S \cup T)$; this implies that

$$x(S \cap T) + x(S \cup T) \leq r(S) + r(T). \tag{4}$$

By submodularity, we have that

$$r(S \cap T) + r(S \cup T) \leq r(S) + r(T). \tag{5}$$

Combining (2)–(5), we get

$$r(S) + r(T) = x(S) + x(T) = x(S \cap T) + x(S \cup T) \leq r(S \cap T) + r(S \cup T) \leq r(S) + r(T),$$

and therefore we have equality throughout. This implies that $x(S \cap T) = r(S \cap T)$ and $x(S \cup T) = r(S \cup T)$, i.e. $S \cap T$ and $S \cup T$ in $\mathcal{F}$. △

To prove that any vertex or extreme point of P is integral, we first characterize any face of P. A *chain* $\mathcal{C}$ is a family of sets such that for all $S, T \in \mathcal{C}$ we have that either $S \subseteq T$ or $T \subseteq S$ (or both if $S = T$).

Theorem 4.6 *Consider any face F of P. Then there exists a chain $\mathcal{C}$ and a subset $J \subseteq E$ such that:*

$$\begin{aligned} F = \{x \in \mathbb{R}^{|E|} : \quad & x(S) \leq r(S) && \forall S \subseteq E \\ & x(C) = r(C) && \forall C \in \mathcal{C} \\ & x_e \geq 0 && \forall e \in E \setminus J \\ & x_e = 0 && \forall e \in J.\} \end{aligned}$$

Proof: By Theorem 3.5 of the polyhedral notes, we know that any face is characterized by setting some of the inequalities of P by equalities. In particular, F can be expressed as

$$\begin{aligned} F = \{x \in \mathbb{R}^{|E|} : \quad & x(S) \leq r(S) && \forall S \subseteq E \\ & x(C) = r(C) && \forall C \in \mathcal{F} \\ & x_e \geq 0 && \forall e \in E \setminus J \\ & x_e = 0 && \forall e \in J.\} \end{aligned}$$

where $J = \{e : x_e = 0 \text{ for all } x \in F\}$ and $\mathcal{F} = \{S : x(S) = r(S) \text{ for all } x \in F\}$. To prove the theorem, we need to argue that the system of equations:

$$x(C) = r(C) \quad \forall C \in \mathcal{F}$$

can be replaced by an equivalent (sub)system in which $\mathcal{F}$ is replaced by a chain $\mathcal{C}$. To be equivalent, we need that

$$span(\mathcal{F}) = span(\mathcal{C})$$

where by $span(\mathcal{L})$ we mean

$$span(\mathcal{L}) := span\{\chi(C) : C \in \mathcal{L}\}.$$

Let $\mathcal{C}$ be a maximal subchain of $\mathcal{F}$, i.e. $\mathcal{C} \subseteq \mathcal{F}$, $\mathcal{C}$ is a chain and for all $S \in \mathcal{F} \setminus \mathcal{C}$, there exists $C \in \mathcal{C}$ such that $S \not\subseteq C$ and $C \not\subseteq S$. We claim that $span(\mathcal{C}) = span(\mathcal{F})$.

Suppose not, i.e. $H \neq span(\mathcal{F})$ where $H := span(\mathcal{C})$. This means that there exists $S \in \mathcal{F} \setminus \mathcal{C}$ such that $\chi(S) \notin H$ but S cannot be added to $\mathcal{C}$ without destroying the chain structure. In other words, for any such S, the set of 'chain violations'

$$V(S) := \{C \in \mathcal{C} : C \not\subseteq S \text{ and } S \not\subseteq C\}$$

is non-empty. Among all such sets S, choose one for which $|V(S)|$ is as small as possible ($|V(S)|$ cannot be 0 since we are assuming that $V(S) \neq \emptyset$ for all possible S). Now fix some set $C \in V(S)$. By Lemma 4.5, we know that both $C \cap S \in \mathcal{F}$ and $C \cup S \in \mathcal{F}$. Observe that there is a linear dependence between $\chi(C), \chi(S), \chi(C \cup T), \chi(C \cap T)$:

$$\chi(C) + \chi(S) = \chi(C \cup S) + \chi(C \cap S).$$

This means that, since $\chi(C) \in H$ and $\chi(S) \notin H$, we must have that either $\chi(C \cup S) \notin H$ or $\chi(C \cap S) \notin H$ (otherwise $\chi(S)$ would be in H). Say that $\chi(B) \notin H$ where B si either $C \cup S$ or $C \cap S$. This is a contradiction since $|V(B)| < |V(S)|$, contradicting our choice of S. Indeed, one can see that $V(B) \subset V(S)$ and $C \in V(S) \setminus V(B)$. $\triangle$

As a corollary, we can also obtain a similar property for an extreme point, starting from Theorem 3.6.

Corollary 4.7 *Let x be any extreme point of P. Then there exists a chain $\mathcal{C}$ and a subset $J \subseteq E$ such that x is the unique solution to:*

$$\begin{array}{ll} x(C) = r(C) & \forall C \in \mathcal{C} \\ x_e = 0 & \forall e \in J. \end{array}$$

From this corollary, the integrality of every extreme point follows easily. Indeed, if the chain given in the corollary consists of $C_1 \subset C_2 \subset C_p$ the the system reduces to

$$\begin{array}{ll} x(C_i \setminus C_{i-1}) = r(C_i) - r(C_{i-1}) & i = 1, \cdots, p \\ x_e = 0 & \forall e \in J, \end{array}$$

where $C_0 = \emptyset$. For this to have a unique solution, we'd better have $|C_i \setminus C_{i-1} \setminus J| \leq 1$ for all i and the values for the resulting x_e's will be integral.

4.4.3 Facet Proof

Our last proof of Theorem 4.4 focuses on the facets of $conv(X)$.

First we need to argue that we are missing any equalities. Let's focus on the (interesting) case in which any singleton set is independent: $\{e\} \in \mathcal{I}$ for every $e \in E$. In that case $dim(conv(X)) = |E|$ since we can exhibit $|E| + 1$ affinely independent points in X: the 0 vector and all unit vectors $\chi(\{e\})$ for $e \in E$. Thus we do not need any equalities. See exercise 4-11 if we are not assuming that every singleton set is independent.

Now consider any facet F of $conv(X)$. This facet is induced by a valid inequality $\alpha^T x \leq \beta$ where $\beta = \max\{\sum_{e \in I} \alpha_e : I \in \mathcal{I}\}$. Let

$$\mathcal{O} = \{I \in \mathcal{I} : \sum_{e \in I} \alpha_e = \beta\},$$

i.e. $\mathcal{O}$ is the set of all independent sets whose incidence vectors belong to the face. We'll show that there exists an inequality in opur description of P which is satisfied at equality by the incidence vectors of all sets $I \in \mathcal{O}$.

We consider two cases. If there exists $e \in M$ such that $\alpha_e < 0$ then $I \in \mathcal{O}$ implies that $e \notin I$, implying that our face F is included in the face induced by $x_e \geq 0$ (which is in our description of P).

For the other case, we assume that for all $e \in E$, we have $\alpha_e \geq 0$. We can further assume that $\alpha_{\max} := \max_{e \in E} \alpha_e > 0$ since otherwise F is trivial. Now, define S as

$$S = \{e \in E : \alpha_e = \alpha_{\max}\}.$$

Claim 4.8 *For any $I \in \mathcal{O}$, we have $|I \cap S| = r(S)$.*

This means that the face F is contained in the face induced by the inequality $x(S) \leq r(S)$ and therefore we have in our description of P one inequality inducing each facet of $conv(X)$. Thus we have a complete description of $conv(X)$.

To prove the claim, suppose that $|I \cap S| < r(S)$. Thus $I \cap S$ can be extended to an independent set $X \in \mathcal{I}$ where $X \subseteq S$ and $|X| > |I \cap S|$. Let $e \in X \setminus (I \cap S)$; observe that $e \in S$ by our choice of X. Since $\alpha_e > 0$ we have that $I + e \notin \mathcal{I}$, thus there is a circuit $C \subseteq I + e$. By the unique circuit property (see Theorem 4.1), for any $f \in C$ we have $I + e - f \in \mathcal{I}$. But $C \setminus S \neq \emptyset$ since $(I \cap S) + e \in \mathcal{I}$, and thus we can choose $f \in C \setminus S$. The cost of $I + e - f$ satisfies:

$$c(I + e - f) = c(I) + c(e) - c(f) > c(I),$$

contradicting the definition of $\mathcal{O}$.

4.5 Facets?

Now that we have a description of the matroid polytope in terms of linear inequalities, one may wonder which of these (exponentially many) inequalities define facets of $conv(X)$.

For simplicity, let's assume that $r(\{e\}) = 1$ for all $e \in E$ (e belongs to some independent set). Then, every nonnegativity constraint defines a facet of $P = conv(X)$. Indeed, the 0 vector and all unit vectors except $\chi(\{e\})$ constitute $|E|$ affinely independent points satisfying $x_e = 0$. This mean that the corresponding face has dimension at least $|E| - 1$ and since the dimension of P itself is $|E|$, the face is a facet.

We now consider the constraint $x(S) \leq r(S)$ for some set $S \subseteq E$. If S is not closed (see Definition 4.2) then $x(S) \leq r(S)$ definitely does not define a facet of $P = conv(X)$ since it is implied by the constraints $x(span(S)) \leq r(S)$ and $x_e \geq 0$ for $e \in span(S) \setminus S$.

Another situation in which $x(S) \leq r(S)$ does not define a facet is if S can be expressed as the disjoint union of $U \neq \emptyset$ and $S \setminus U \neq \emptyset$ and $r(U) + r(S \setminus U) = r(S)$. In this case, the inequality for S is implied by those for U and for $S \setminus U$.

Definition 4.3 *S is said to be inseparable if there is no U with $\emptyset \neq U \subset S$ such that $r(S) = r(U) + r(S \setminus U)$.*

From what we have just argued, a necessary condition for $x(S) \leq r(S)$ to define a facet of $P = conv(X)$ is that S is *closed and inseparable*. This can be shown to be sufficient as well, although the proof is omitted.

As an example, consider a partition matroid with $M = (E, \mathcal{I})$ where

$$\mathcal{I} = \{X \subseteq E : |X \cap E_i| \leq k_i \text{ for all } i = 1, \cdots, l\},$$

for disjoint E_i's. Assume that $k_i \geq 1$ for all i. The rank function for this matroid is:

$$r(S) = \sum_{i=1}^{l} \min(k_i, |S \cap E_i|).$$

For a set S to be inseparable, there must exist (i) $i \in \{1, \cdots, l$ with $S \subseteq E_i$, and (ii) $|S \cap E_i|$ is either ≤ 1 or $> k_i$ for every i. Furthermore, for $S \subseteq E_i$ to be closed, we must have that if

$|S \cap E_i| > k_i$ then $S \cap E_i = E_i$. Thus the only sets we need for the description of a partition matroid polytope are (i) sets $S = E_i$ for i with $|E_i| > k_i$ and (ii) singleton sets $\{e\}$ for $e \in E$. The partition matroid polytope is thus given by:

$$P = \{x \in \mathbb{R}^{|E|} : \quad x(E_i) \leq k_i \quad i \in \{1, \cdots, l\} : |E_i| > k_i \\ 0 \leq x_e \leq 1 \quad e \in E\}.$$

As another example, take M to be the graphic matroid $M(G)$. For a set of edges $F \subseteq E$ to be inseparable, we need that the subgraph (V, F) has only one non-trivial (i.e. with more than 1 vertex) connected component; indeed, if we partition F into the edge sets $F_1, \cdots, F_c$ of the (c non-trivial) connected components, we have that $r(F) = \sum_{i=1}^{c} r(F_i)$ and thus c must be 1 for F to be inseparable. Given a set F of edges, its span (with respect to the graphic matroid) consists of all the edges with both endpoints within the same connected component of F; these are the edges whose addition does not increase the size of the largest forest. Thus, for F to be inseparable and closed, we must have that there exists a vertex set $S \subseteq V$ such that $F = E(S)$ ($E(S)$ denotes all the edges with both endpoints in S) and $(S, E(S))$ is connected. Thus the forest polytope (convex hull of all forests in a graph $G = (V, E)$) is given by:

$$P = \{x \in \mathbb{R}^{|E|} : \quad x(E(S)) \leq |S| - 1 \quad S \subseteq V : \text{E(S) connected} \\ 0 \leq x_e \qquad\qquad\qquad e \in E\}.$$

(As usual, $x(E(S))$ denotes $\sum_{e \in E(S)} x_e$.) Observe that this polyhedral description still has a very large number of inequalities.

From this, we can also easily derive the *spanning tree polytope* of a graph, namely the convex hull of incidence vectors of all spanning trees in a graph. Indeed, this is a face of the forest polytope obtained by replacing the inequality for $S = V$ ($x(E) \leq |V| - 1$) by an equality:

$$P = \{x \in \mathbb{R}^{|E|} : \quad X(E) = |V| - 1 \\ x(E(S)) \leq |S| - 1 \quad S \subset V : \text{E(S) connected} \\ 0 \leq x_e \qquad\qquad\qquad e \in E\}.$$

Exercise 4-11. Let $M = (E, \mathcal{I})$ be a matroid and let $S = \{e \in E : \{e\} \in \mathcal{I}\}$. Show that $dim(conv(X)) = |S|$ (where X is the set of incidence vectors of indpendent sets) and show that the description for P has the required number of linearly independent equalities.

Exercise 4-12. Let $M = (E, \mathcal{I})$ be a matroid and let P be the corresponding matroid polytope, i.e. the convex hull of characteristic vectors of independent sets. Show that two independent sets I_1 and I_2 are adjacent on P if and only if either (i) $I_1 \subseteq I_2$ and $|I_1| + 1 = |I_2|$, or (ii) $I_2 \subseteq I_1$ and $|I_2| + 1 = |I_1|$, or (iii) $|I_1 \setminus I_2| = |I_2 \setminus I_1| = 1$ and $I_1 \cup I_2 \notin \mathcal{I}$.