CMPUT 675: Topics in Algorithms and Combinatorial Optimization (Fall 2009)
Lecturer: Mohammad R. Salavatipour   **Scriber:** Siamak Ravanbakhsh
Date: Oct 20-22, 2009

This lecture continues our previous discussion on matroids. This includes some new definitions and theorems on the relation of matroids with submodular functions and greedy algorithms.

1 Matroids (cont.)

Suppose we are given a set system $M = (E, \mathcal{I})$ where E is a ground set and $\mathcal{I}$ is a collection of subsets of of E. We say M is a matroid if

1. $\mathcal{I}$ is close under subset operation.
2. For any $X, Y \in \mathcal{I},\ |X| < |Y|$ we have $\exists e \in Y \backslash X\ s.t.\ X + e \in \mathcal{I}$.

Some of the examples we saw included: linear matroids and graphic matroids. We also proved the following theorem

Theorem 1.1 *For $I \in \mathcal{I}$ and $e \in E$, either $I + e \in \mathcal{I}$ or it contains a unique circuit.*

The *rank function* $r_m : 2^{|E|} \rightarrow \mathbb{N}$ of a matroid $M = (E, \mathcal{I})$ was defined as:

$$r_m(A) = \max\{|X| : X \subseteq A \text{ and } X \in \mathcal{I}\}$$

Definition 1.2 *For any subset of elements $A \subseteq E$, of a matroid $M = (E, \mathcal{I})$ the* span *of A is the maximal superset S of A such that $r(S) = r(A)$.*

Alternatively, we have the following definition.

Definition 1.3 *For any subset of elements $A \subseteq E$, of a matroid $M = (E, \mathcal{I})$ the* span *of A is defined as*

$$Sp(A) = \{e | r(A + e) = r(A)\}$$

Theorem 1.4 *These two definitions are equivalent.*

Proof: Let S be the span of A as defined by the first definition, and S' the span as defined by the second definition. Then

$$\forall\ e \in S :\ r(A + e) = r(A) \tag{1}$$

This is because if $r(A + e) > r(A)$, since $A + e \subseteq S$ we have $r(S) \geq r(A + e) < r(A)$ and therefore which contradicts the first definition. Eq(1) implies that $\forall\ e \in S : e \in S'$ and therefore $S \subseteq S'$.

Now it remains to show that $r(S') = r(A)$. It is not hard to see that a common basis of two sets is a basis of their union (prove this!). So a basis of A is a basis of $Sp(A) = S'$, since it is a basis of $A + e$ for each $e \in S'$.

■

Example: A *partition matroid* is defined as follows. Let $E = E_1 \cup E_2 \cup \ldots \cup E_p$ be a partitioning of E. Say I is an independent set if no two elements of I belong to the same part– *i.e.* $|I \cap E_i| \leq 1$ for all $1 \leq i \leq p$. Then $M = (E, \mathcal{I})$ is a matroid because:

1. $\forall\ I \in \mathcal{I};\ I' \subseteq I$ also belongs to $\mathcal{I}$. This is because here by definition of independent set, by removing any element, it remains an independent set –*i.e.,* $|I \cap E_i| \leq 1$ still holds by removing elements from I.

2. For $X, Y \in \mathcal{I}$ such that $|X| < |Y| \quad \exists j\ s.t.\ |Y \cap E_j| = 1$ and $|X \cap E_j| = 0$. Because otherwise $|X| \geq |Y|$. Now by adding any $e \in E_j$ to X, $X + e$ it remains independent. This shows that the second axiom of definition of matroid holds for M as we defined.

For $A \subseteq E$ let $J(A) = \{i\ s.t.\ |A \cap E_i| \neq 0\}$ denote the partitions in which elements of A participates. We have $r(A) = |J(A)|$ and $Sp(A) = \bigcup_{i \in J(A)} E_i$. For this example any circuite is a set of any two elements from the same set E_i. ■

Lemma 1.5 *Let $M = (E, \mathcal{I})$ be a matroid and B_1, B_2 be two bases and let $x \in B_1 \backslash B_2$ then:*

$$\exists y \in B_2 \backslash B_1\ s.t.\ B_1 - x + y \ \text{ and } \ B_2 - y + x \text{ are both bases.}$$

Proof: Exercise. ■

Theorem 1.6 *Let $r : 2^{|E|} \rightarrow \mathbb{N}$, then r is a rank function of a matroid* iff *for all $T, U \subseteq E$:*

1. $r(T) \leq r(U) \leq |U|$ *if* $T \subseteq U$
2. r *is submodular:* $r(T \cap U) + r(T \cup U) \leq r(T) + r(U)$

Proof: First we show that for any matroid, these relations hold for the corresponding rank function:

1. $r(T) \leq r(U) \leq |U|$ if $T \subseteq U$.
   This relation holds by definition of the rank. Since T is a subset of U the size of the maximum independent set contained in T should be at most as big as the corresponding set for U. This maximal independent set is always contained in U and therefore $r(T) \leq r(U) \leq |U|$.

2. We want to show that any rank function is submodular: $r(T \cap U) + r(T \cup U) \leq r(T) + r(U)$. Let $I \subseteq T \cap U$ be a maximum independent set of $\mathcal{I}$ in $T \cap U$ and also let $J \subseteq T \cup U$ be a maximal independent set such that $I \subseteq J \subseteq T \cup U$. From the definition of I and J follows $r(T \cup U) = |J|$ and $r(T \cap U) = |I|$.

   Since J is independent any subset of it would be independent too therefore $J \cap U$ and $J \cap T$ are independent subsets of T and U. Since by definition $r(T)$ and $r(U)$ are the size maximum independent subset of T and U, we have:

   $$r(T) \geq |J \cap T|$$
   $$r(U) \geq |J \cap U|$$

   and therefore

   $$\begin{aligned} r(T) + r(U) &\geq |J \cap T| + |J \cap U| \\ &= |J \cap (T \cap U)| + |J \cap (T \cup U)| \\ &\geq |I| + |J| \\ &= r(T \cap U) + r(T \cup U) \end{aligned}$$

   where in the last inequality we have $|J \cap (T \cap U)| \geq |I|$ because J contains I by construction. Here the first equality follows by application of another equality that states $|A| + |B| = |A \cup B| + |A \cap B|$ (by setting $A = T \cap J$ and $B = U \cap J$).

Now we want to prove that given a function $r : 2^{|E|} \to \mathbb{N}$ satisfying the conditions of the theorem it is the rank function for a matroid. We construct such matroid. Suppose that $\mathcal{I}$ is a collection of subsets of E such that

$$r(I) = |I| \quad \forall\, I \in \mathcal{I}$$

Claim 1.7 *$(E, \mathcal{I})$ is a matroid with the rank function r.*

We show that two requirements for matroid hold for set $\mathcal{I}$. We do this by induction. Clearly $\emptyset \in \mathcal{I}$.

- Given $I \in \mathcal{I}$ with $r(I) = |I|$, we want to show that for any $J \subseteq I$ also $r(J) = |J|$ and therefore $J \in \mathcal{I}$.

  Consider two disjoint sets J and $I - J$ and assume for $I \backslash J$ we already have $J(I \backslash J) = |I \backslash J|$ (assumption of the induction). By submodularity of r we have

  $$\begin{aligned} r(J) + r(I \backslash J) \geq & r(I) + r(\emptyset) \Rightarrow \\ r(J) \geq & |I| - |I \backslash J| = |J| \end{aligned}$$

  On the other hand by the first property of r we have $r(J) \leq |J|$ and therefore $r(J) = |J|$.

- To prove the satisfaction of second requirement in definition of matroid we use the following substitution

  Lemma 1.8 *Axiom 2 of definition of matroid is equivalent to the following. For any $X, Y \in \mathcal{I}$ such that $|X \backslash Y| = 1$ and $|Y \backslash X| = 2$ then*

  $$\exists y \in Y \backslash X \quad s.t. \quad X + y \in \mathcal{I}$$

  Proof: Can be proved by induction. ■

  Now we show the condition of this lemma holds for $(E, \mathcal{I})$ constructed using r. Let $X, Y \in \mathcal{I}$ with $|X \backslash Y| = 1$ and $|Y \backslash X| = 2$ when $Y \backslash X = \{y_1, y_2\}$.

  Now consider $X + y_1$ and $X + y_2$, if one of them belongs to $\mathcal{I}$ the requirement of previous lemma holds. Suppose none of them belongs to $\mathcal{I}$, therefore

  $$r(X + y_1) = r(X + y_2) = |X|$$

  From the assumptions we have

  $$r(X + y_1) + r(X + y_2) \geq r(X + y_1 + y_2) + r(X).$$

  But since $Y \subseteq X \cup \{y_1, y_2\}$,

  $$\begin{aligned} r(Y) &\leq r(X + y_1 + y_2) \\ &\leq r(X + y_1) + r(X + y_2) - r(X) \\ &= |X| \end{aligned}$$

  Which contradicts the fact that $Y \in \mathcal{I}$ and therefore $r(Y) = |Y| > |X|$.

  It is not hard to prove that the rank function for $\mathcal{I}$ is the same as r.

■

2 Matroid Optimization

The problem of matroid optimization is defined as follows. Given a matroid $M = (E, \mathcal{I})$ and a cost function $C : E \rightarrow \mathbb{R}^{\geq 0}$ find an independent set of maximum (minimum) weight.

If the cost of an element is negative then droping it from the solution independent set gives another feasible set with larger cost; so we can assume $C(e) \geq 0$ and any optimum solution is a maximum independent set (*i.e.* a basis). The following greedy algorithm finds such basis.

Matroid Optimization Algorithm

Start with an empty set; $S \leftarrow \emptyset$
Sort elements so that $C(e_1) \geq C(e_2) \geq ... \geq C(e_n)$
for $i \leftarrow 1$ **to** n **do**
  if $S \cup \{e_i\} \in \mathcal{I}$ **then**
    $S \leftarrow S \cup \{e_i\}$
return S

Theorem 2.1 *The pair $(E, \mathcal{I})$, when $\mathcal{I}$ is a collection of subsets of E closed under taking subset, is a matroid* iff *for each function $C : E \rightarrow \mathbb{R}^{\geq 0}$ the given greedy algorithm returns a set $S \in \mathcal{I}$ with maximum cost.*

Proof: The proof has two directions. First we prove that given $(E, \mathcal{I})$ is a matroid the greedy algorithm gives the optimum solution. Then we prove that if for every cost function $C : E \rightarrow \mathbb{R}^{\geq 0}$ the algorithm finds the set with maximum cost then $(E, \mathcal{I})$ is a matroid.

- Suppose $(E, \mathcal{I})$ is a matroid. Let S_i be the value of S after iteration i. We say S_i is *good* if there is an optimum base B such that $S_i \subseteq B$ and each $e_j \in B \backslash S_i$ has $j \geq i + 1$.

  We prove by induction on i that S_i is good.

  Base Step $S = \emptyset$ is subset of all optimum solutions.

  Induction Step Suppose there is an optimum base B such that $S_i \subseteq B$ and we consider e_{i+1}

  - *Case 1:* $S_i = S_{i+1}$; meaning $e_{i+1} + S_i$ has a circuit. Therefore $e_{i+1} \notin B$ (or we will have circuit.)
  - *Case 2:* $S_{i+1} = S_i \cup \{e_{i+1}\}$. If $e_{i+1} \in B$ then we are fine becasue S_{i+1} remains a subset of B. Assume $e_{i+1} \notin B$. Then $B + e_{i+1}$ has a circuit and there is an element e_j such that $B' = B + e_{i+1} - e_j$ is a base; in this case $e_j \in B \backslash S_{i+1}$. Note that $S_{i+1} \subseteq B'$.

    Claim 2.2 $C(B') \geq C(B)$.
    For this, it is enough to show that $C(e_{i+1}) \geq C(e_j)$ or $i + 1 \leq j$. We know that any $e_j \in B \backslash S_{i+1}$ has $j \geq i + 2$ and at least one of them is in the circuit in $B + e_{i+1}$ because otherwise S_{i+1} has a circuit. By choosing e_j to be that element we have $C(e_{i+1}) \geq C(e_j)$.

- Suppose the greedy algorithm gives the optimum set for any cost function C. The goal is to show $(E, \mathcal{I})$ is a matroid. By assumption $(E, \mathcal{I})$ is a set system closed under subset operation. Therefore the first axiom of matroid is by assumption satisfied.

  To prove the second axiom is satisfied we drive a contradiction by assuming the existence of $I, J \in \mathcal{I},\ |J| > |I| \quad s.t. \forall\, e \in J \backslash I : \quad I + e \notin \mathcal{I}$.

Let $k = |I|$. Define $C : E \to \mathbb{R}^{\geq 0}$ as

$$C(e) = \begin{cases} k+2 & e \in I \\ k+1 & e \in J \backslash I \\ 0 & e \in E \backslash (I \cup J) \end{cases}$$

Greedy algorithm stops with $S = I$, because adding any element of J to the set I will result in a circuit. This set (S) has a cost of $k(k+2)$ while there is an independent set with cost at least $(k+1)^2 > k(k+2)$, namely by picking J. This contradiction completes the proof of the theorem.

■

3 Matroid Polytope

For the matroid $M = (E, \mathcal{I})$, let $\chi(S) \in \{0,1\}^{|E|}$ denote the incident vector for the set S (*i.e.* this is a vector that has a one for an element if it is a member of S and zero otherwise.)

The convex hull of $\chi(S)$ for $S \in \mathcal{I}$ is the matroid polytope for M:

$$P_1(M) = Convex(\chi).$$

As we see shortly this is the same polytope as the following which we call P_2

$$\begin{aligned} \forall\, U \subseteq E \quad & x(U) \leq r_m(U) \\ & x_e \geq 0 \\ \text{where,} \quad & x(U) = \sum_{e \in U} x_e \end{aligned}$$

Theorem 3.1 *(Edmonds) P_2 is the matriod polytope i.e. $P_1 = P_2$.*

Proof:

- It is easy to see that every point in $P_1(M)$ also belongs to P_2 (i.e. $P_1 \subseteq P_2$) because for any independent set $I \in \mathcal{I}$ the incident vector of I satisfies the conditions of P_2. Here $x(I) = |I|$ which is always greater than or equal to $r(U)$.

- Now we want to show $P_2 \subseteq P_1(M)$. For this we show that for any cost function $C(e)$, P_2 and its dual D, have a feasible solution that coincide with each other and the independent set that gives the optimum solution for P_2 is the set S returned by the greedy algorithm. Since every vertex of a polytope is an optimal solution for some cost function, this implies that all the vertices of P_2 are answers to some independent set returned by the greedy algorithm and therefore $P_2 \subseteq P_1(M)$.

  The **P**rimal program reads as

$$\begin{aligned} & \max \sum C(e) x_e \\ \forall U \subseteq E \quad & \sum_{e \in U} x_e \leq r_m(U) \\ & x_e \geq 0 \end{aligned}$$

and the **D**ual program is

$$\min \sum_{U \subseteq E} r_M(U) y_u$$
$$\forall e \in E \quad \sum_{U \ni e} y_U \geq C(e)$$
$$y_u \geq 0$$

We prove that for any cost $C(e)$ we can find a set S and a dual solution such that $C^T\chi(S) = \sum_U y_U r(U)$– that is the solution to primal and dual coincides.

Suppose we run the greedy algorithm and find the set $S = \{\underbrace{s_1, s_2, ..., s_j}_{S_j}, ..., s_k\}$. This is a feasible solution for P_2. We build a feasible dual solution.

Define $U_j = \{e_1, \ldots, e_j\}$ such that $e_{j+1} = s_{j+1}$. In other words, U_j includes all the elements in the ordering of E just before s_{j+1}. We we claim:

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

Clearly we have $r(S_j) = |S_j| = j$. Also, since $S_j \subseteq U_j$, we have $r(S_j) \leq r(U_j)$. On the other hand we can not have $r(U_i) > r(S_i)$ because it means the basis for the set $\{e_1, ..., e_i\}$ has more elements than S_i. This is contradictory because by construction of S_i we would have selected those elements.

Now we define the dual solution:

$$\begin{aligned} y_{U_i} &= C(e_i) - C(e_{i+1}) \quad \text{for } i = 1, ..., n-1 \\ y_{U_n} &= C(e_n) \\ y_Q &= 0 \quad \text{for every other set, } Q \end{aligned}$$

Claim 3.2 *y_U as defined above is a feasible solution for the dual program (D).*

This is because $\forall\ e_i : \quad \sum_{S \ni e_i} y_S \geq C(e_i)$. Now we want to show costs are equal for the primal and dual and therefore optimal.

$$\begin{aligned} C(S) = \sum_{e \in S} C(e) &= \sum_{i=1}^{n} C(e_i) \underbrace{(r(U_i) - r(U_{i-1}))}_{=1 \text{ iff } e_i \in S} \\ &= C(e_n) r(U_n) \ + \sum_{i=1}^{n-1} (C(e_i) - C(e_{i+1}))\, r(U_i) \\ &= y_{U_n} r(U_n) + \sum_{i=1}^{n-1} y_{U_i} r(U_i) \\ &= \sum_{i=1}^{n} y_{U_i} r(U_i) \end{aligned}$$

The fact that the optimum solution coincide with the result of greedy algorithm shows that for any arbitrary cost function the corners of P_2 are subsets of the corners of $P_1(M)$ which completes the proof.

■