Topics in Theoretical Computer Science	March 23, 2015

Lecture 6

Lecturer: Ola Svensson *Scribes: Arnaud Robert, David Gilgien*

1 Introduction

Last week we explored the notion of Linear Programming Duality and several examples of applications: minimum cost perfect matching (Hungarian algorithm), maximum cardinality matching and maximum spanning tree.
Today we will be seeing combinatorial structures that generalize the notion of linear independence in matrices: matroids.
The notes that follow are based on lecture notes on this topic from Jan Vondrak, Standford University and from Michel X. Goemans, Massachusetts Institute of Technology.

2 Matroids

There exist different definitions of a matroid. In this course will use the following, based on its independence set.

2.1 Definitions

Definition 1 *A matroid $M = (E, \mathcal{I})$ is a structure with a finite ground set E, the universe, and a family of subset of E said to be independent $\mathcal{I}$ satisfying:*

(I_1) *if $A \subseteq B$, $B \in \mathcal{I}$, then $A \in \mathcal{I}$*

(I_2) *if $A, B \in \mathcal{I}$ and $|B| > |A|$, then $\exists e \in B \setminus A$ such that $A + e \in \mathcal{I}$*

In what follows, we will keep using notation of the form $A + e$ when it is technically $A \cup \{e\}$.

Definition 2 *A maximal (inclusion-wise) independent set is called a base.*

Note that by (I_2), all bases have the same cardinality.

2.2 Examples

2.2.1 k-Uniform matroid

A matroid $M = (E, \mathcal{I})$ is k-Uniform if $\mathcal{I}$ satisfies:

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

2.2.2 Partition matroid

A matroid $M = (E, \mathcal{I})$ is a partition matroid if E is partitioned into *disjoint* sets $E_1, E_2, ..., E_e$ and

$$\mathcal{I} = \{X \subseteq E : |E_i \cap X| \leq k_i \text{ for } i = 1, 2, ...e\}$$

2.2.3 Linear matroid

A matroid $M = (E, \mathcal{I})$ is a linear matroid when it is defined from a matrix A. Let E be the index set of the columns and for $X \subseteq E$ let A_X be the matrix consisting of the columns indexed by X. define $\mathcal{I}$ by

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

2.2.4 Graphic matroid

A matroid $M = (E, \mathcal{I})$ is a graphic matroid when it is defined from a graph $G = (V, E)$, with the edges being the universe and $\mathcal{I}$ defined by

$$\mathcal{I} = \{X \subseteq E : X \text{ is acyclic}\}$$

I_1 obviously holds because any subset of an acyclic set of edges will also be acyclic. In order to verify that I_2 holds, we can consider $A, B \in \mathcal{I}$, $|B| > |A|$. A and B are forests consisting of $|V| - |A|$ and $|V| - |B|$ connected components respectively (because A and B are acyclic). The number of connected components in the forest A is thus higher than in the forest B, which means that $B \setminus A$ must have an edge e between two components of A. We have $A + e \in \mathcal{I}$.

2.2.5 Truncated matroid

A truncated matroid $M_k = (E, \mathcal{I}_k)$ is defined from a matroid $M = (E, \mathcal{I})$ such that

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

It is quite easy to verify that the axioms still hold for M_k, as $X \in \mathcal{I}_k$ implies $X \in \mathcal{I}$ for all $X \subseteq E$.
(I_1) holds because $B \in \mathcal{I}_k$ means that $|B| \leq k$ and $A \subseteq B$ thus means $|A| \leq k$ as well. We know that M is a matroid so I_1 holds for M, which implies $A \in \mathcal{I}$. We conclude that $A \in \mathcal{I}_k$
The same reasoning can verify I_2: if $A, B \in \mathcal{I}_k$ and $|B| > |A|$, then $|B| \leq k$ and $|A| \leq k - 1$. We know that I_2 holds for M, so the inclusion of $\mathcal{I}_k$ in $\mathcal{I}$ tells us that $\exists e \in B \setminus A$ such that $A + e \in \mathcal{I}$. The fact that $|A + e| \leq k - 1 + 1 = k$ allows us to conclude.

3 Greedy Optimization

We want to optimize a matroid, meaning finding the subset in $\mathcal{I}$ that maximizes the sum of the weights of its elements. We give for this task the following greedy algorithm.

Input: Matroid $M = (E, \mathcal{I})$, weight function $w : E \to \mathbb{R}$
Output: Find $S^* \in \mathcal{I}$ such that[1] $w(S^*) = \max\limits_{S \in \mathcal{I}} w(s)$

1. Order and rename elements such that $w_1 \geq w_2 \geq \cdots \geq w_n$
2. $S \leftarrow \varnothing$
3. for $i = 1$ to n

   if $S + i \in \mathcal{I}$ then $S \leftarrow S + i$
4. return S

This algorithm always outputs a base, so when there are negative weights it actually does not return the maximum weight set in $\mathcal{I}$. If we want it, we can simply change the loop at 3. to "for $i = 1$ to q" where q is such that $w_q \geq 0 > w_{q+1}$.

Theorem 3 *(Rado '57 / Gale '68). The greedy algorithm works for any $w : E \to \mathbb{R}$ if and only if $M = (E, \mathcal{I})$ is a matroid.*

[1] The weight function w applied to a set S means $w(S) = \sum\limits_{e \in S} w(e)$

Proof
Let's start by the "if" direction ($\Longleftarrow$)
Suppose towards contradiction that the algorithms returns a non-optimal solution $S_k = \{s_1, s_2, \cdots, s_k\}$. Let $T_k = \{t_1, t_2, \cdots, t_k\}$ be a higher weight solution and p be the smallest index such that $w(t_p) > w(s_p)$. Define $A = \{t_1, \cdots, t_p\}$ and $B = \{s_1, \cdots, s_{p-1}\}$.
By (I_1) (and the way the algorithm works), we have $A, B \in \mathcal{I}$. Since $|A| > |B|$, (I_2) gives that $\exists e \in A \setminus B$ such that $B + e \in \mathcal{I}$. But this is a contradiction, because by definition $w(e) > w(s_p)$, and therefore the greedy algorithm would add e before s_p.

Now the "only if" direction ($\Longrightarrow$)
We prove the contrapositive: if M is not a matroid, then $\exists w : E \to \mathbb{R}$ for which the algorithm fails.

Case 1: Axiom (I_1) is not satisfied
There is a $S \subseteq T$ such that $T \in \mathcal{I}$ but $S \notin \mathcal{I}$. Then we set

$$w(e) = \begin{cases} 2 & \text{if } e \in S \\ 1 & \text{if } e \in T \setminus S \\ 0 & \text{if } otherwise \end{cases}$$

The algorithm first inspects elements in S, then in T. Let S_q be those elements of S that the algorithm picks. As $S \notin \mathcal{I}$ we have $S_1 \subsetneq S$, hence the weight of the returned solution is at most $2(|S| - 1) + |T \setminus S|$. But $w(T) = 2|S| + |T \setminus S|$, so the algorithm fails.

Case 2: Axiom (I_1) is satisfied, but (I_2) is not
There is a $S, T \in \mathcal{I}$ such that $|T| > |S|$ but $\forall i \in T \setminus S, s + i \notin \mathcal{I}$. Then we set

$$w(e) = \begin{cases} 1 + \frac{1}{2|S|} & \text{if } e \in S \\ 1 & \text{if } e \in T \setminus S \\ 0 & \text{if } otherwise \end{cases}$$

Since (I_1) holds, all subsets of S are independent and thus the algorithm picks S and then can not pick any element in $T \setminus S$. The weight of the returned solution is $|S|(1 + \frac{1}{2|S|}) = |S| + \frac{1}{2}$. But $w(T) = |T| \geq |S| + 1$, so the algorithm fails.

■

4 Circuits

Definition 4 *A minimal (inclusion-wise) dependent set is called a circuit. In the case of a graphic matroid derived from the graph G, a circuit is thus a cycle in G.*

Theorem 5 *Let $M = (E, \mathcal{I})$ be a matroid. Let $S \in \mathcal{I}$ and $e \in E$ such that $S + e \notin \mathcal{I}$, then there exists a unique circuit $C \subseteq S + e$.*

Before proving the theorem, we can derive an important property: if we consider any $f \in C$, then $S + e - f \in \mathcal{I}$.

Proof Suppose towards contradiction that $S + e$ contains two circuits C_1 and C_2 with $C_1 \neq C_2$. By minimality of C_1, C_2, we have that $\exists f \in C_1 \setminus C_2$. Clearly $C_1 - f \in \mathcal{I}$ (minimality of C_1), so we can expand it to X, the maximal independent set of $S + e$ containing $C_1 - f$. Since S is also independent, we have that $|X| = |S|$ and since $e \in C_1 - f$ we have $X = S + e - f \in \mathcal{I}$. This is a contradiction because $C_2 \subseteq S + e - f = X$ but C_2 is dependent. ■

We give without proof[2] the following lemma.

Lemma 6 *(Strong Basis Exchange property)*
Given two basis B_1 and B_2, $\exists e \in B_1$ and $f \in B_2$ such that $B_1 - e + f \in \mathcal{I}$ and $B_2 - f + e \in \mathcal{I}$

5 Rank Function

Similarly to the rank function of a matrix, we can define the rank function for a matroid.

Definition 7 *The rank of a matroid $M = (E, \mathcal{I})$ is a function $2^E \to \mathbb{N}$ denoted r or simply r_M such that*

$$r(S) = max\{|X| : X \subseteq S, X \in \mathcal{I}\} \text{ for any } S \subseteq E$$

5.1 Examples

The rank function for a k-Uniform matroid is $r(S) = min(|S|, k)$.
The rank function for a graphic matroid from the graph $G = (V, E)$ is $r(A) = n-$ #componants in (V, A).
The rank function for a truncated matroid M_k is $r_k(S) = min(r(S), k)$, where r is the rank function of the original matroid.

5.2 Matroid Rank Theorem

Theorem 8 *$r : 2^E \to \mathbb{N}$ is a rank function for a matroid if and only if*

(i) $r(\varnothing) = 0$ and $r(A + e) - r(A) \in \{0, 1\}$ $\forall A \subseteq E, e \in E$

(ii) r is submodular: for $S, T \subseteq E$: $r(S) + r(T) \geq r(S \cap T) + r(S \cup T)$

Proof
We start by the "only if" direction ($\Longrightarrow$):
Condition (i) is clear. We need to prove that r is submodular. Let J be the maximal independant set of $S \cap T$. Extend J to obtain maximal independent set J_S of S. Extend J_S to obtain maximal independent set J_{ST} of $S \cup T$.
We have $J \subseteq J_S$ and $|J_S| = r(S)$, $|J| = r(S \cap T)$. Moreover, $J_S \setminus J = J_S \setminus T$ because J was maximal. In order to verify that

$$\begin{gathered} r(S) + r(T) \geq r(S \cap T) + r(S \cup T) \\ \Updownarrow \\ |J_S| + r(T) \geq |J| + |J_{ST}| \\ \Updownarrow \\ r(T) \geq |J_{ST}| - |J_S| + |J| \end{gathered}$$

And we have that $r(T) \geq |J_{ST} \setminus (J_S \setminus T)| = |J_{ST} \setminus (J_S \setminus J)| = |J_{ST}| - |J_S| + |J|$.
The "if" direction ($\Longleftarrow$):
We will use the following property of submodular functions: for any $A \subseteq B$ and $e \notin B$, one has $f(A + e) - f(A) \geq f(B + e) - f(B)$.
We will prove that the two matroid axioms hold for $\mathcal{I} := \{A : r(A) = |A|\}$
It is clear from the first condition on r that $\mathcal{I}$ is closed under taking subsets. Since $r(\varnothing) = 0$ and

[2] The proof can be found online in Michel X. Goemans notes on matroid intersection.

$r(B) = |B|$ then we can see by induction that for all set $A \subseteq B$ $r(A) = |A|$
We claim that for any set S, all maximal subset of S which are in $\mathcal{I}$ have the same size, which clearly implies (I_2). In order to prove this claim let's consider any set A such that $A \subset S$ and $r(A) = |A|$. We have $r(A+i) - r(A) \in \{0, 1\}$. Moreover as long as $r(A) < r(S)$ it is the case (by submodularity) that $r(A+i) = r(A) + 1$. Hence if A is maximal such that $r(A) = |A|$, we have $r(A) = r(S)$. So all bases have the same size: $r(S)$. ■

5.3 Span

Definition 9 *Given a matroid $M = (E, \mathcal{I})$ and $S \subseteq E$, let*

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

We can state the following observations: $S \subseteq span(S)$ and $r(S) = r(span(S))$.

Definition 10 *A set S is said to be closed if $S = span(S)$.*

We note that our greedy algorithm of section 3 actually returns for $w_1 \geq w_2 \geq \cdots \geq w_n$ the set

$$\{i : i \notin span(\{1, \ldots, i-1\})\}$$

because it checks to increment the rank of S every time it adds an element to it. This results in the fact that this set is the base of maximum weight of a matroid.

6 Matroid Polytope

Definition 11 *Given a matroid $M = (E, \mathcal{I})$, we define by P(M) the matroid polytope*

$$P(M) = conv(\{x_S \in \{0,1\}^{|E|} : S \in \mathcal{I}\})$$

Theorem 12 *We have that*

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

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

Proof There exist multiple ways to prove this theorem. We will present here the outline of a Primal-Dual proof[3].
We need to show that all extreme points are integral. But for any extreme point, there exists an objective function for which it is the unique optimal. We can write down the two linear programming formulations:
PRIMAL:

$$\begin{aligned} \textbf{maximize} : & \sum w_e x_e \\ \textbf{subject to} : & x(S) \leq r(S) \ \forall S \subseteq E \\ & x \geq 0 \end{aligned}$$

[3]Other versions of this proof can be found in Jan Vondrak lecture 9 notes, section 3 (references [3]) and in Gomans' Lecture Notes on matroid optimization, section 4.4 (references [1])

DUAL:

$$\begin{aligned} \textbf{minimize}: & \sum_{S \subseteq E} y_S r(S) \\ \textbf{subject to}: & \sum_{S: e \in S} y_S \geq w(e) \ \forall e \in E \\ & y \geq 0 \end{aligned}$$

We then state complementary slackness and define the primal solution x^* and the dual solution y^*. We first run our greedy algorithm of section 3, and note $S = \{s_1, \ldots, s_k\}$ the set it returns indexed in the order they were picked. Let

$$x_e = \begin{cases} 1 & \text{if } e \in S \\ 0 & \text{if } otherwise \end{cases}$$

For $j = 1, \ldots, k$ define $S_j = \{s_1, \ldots, s_j\}$ the first j elements picked and let U_j be all elements in our ordering up to and excluding S_{j+1}. We observe that $r(U_j) = r(S_j) = j$. Indeed by the independence of S_j, $r(S_j) = |S_j| = j$ and if $r(U_j) > r(S_j)$ then there would be an element $e_p \in U_j \setminus S_j$ that the greedy algorithm would have picked, a contradiction.
Now we set non-zero elements of y^* to be ${y^*}_{U_j} = w(S_j) - w(S_{j+1})$ for $j = 1, \ldots, k$.
By the ordering of the elements we have that $y^* \geq 0$. In addition, for any $e \in E$, we have

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

where t is the least index such that $e \in U_t$ (implying that e does not come before s_t in the ordering). We have thus showed that y^* is a feasible dual solution. Let's verify complementarity slackness. First, $y_{U_j}^* > 0 \Rightarrow x^*(U_j) = |S_j| = r(S_j) = r(U_j)$, by the observation mentioned above. Second, $x_{s_t}^* > 0 \Rightarrow \sum_{S: e \in S} y_S^* = \sum_{j=t}^{k} y_{U_j}^* = w(s_t)$. Therefore x^* is optimal which finishes the proof. ■

References

[1] Michel X. Gomans, *Lecture Notes on matroid optimization*, Massachusetts Institute of Technology, March 20th, 2009.

[2] Michel X. Gomans, *Lecture Notes on matroid intersection*, Massachusetts Institute of Technology, March 30th, 2011.

[3] Jan Vondrak, *Lecture 9 Notes* of the course *Polyhedral techniques in combinatorial optimization*, Standford University, October 19, 2010.