Math 233B: Polyhedral techniques in combinatorial optimization
Instructor: Jan Vondrák
Lecture date: 2/7/2017 **Original scribe: Hao Su**

1 Matroid duality

Definition 1 *For a matroid, $\mathcal{M} = (E, \mathcal{I})$, the dual matroid $\mathcal{M}^* = (E, \mathcal{I}^*)$ is defined so that the bases in $\mathcal{I}^*$ are exactly the complements of the bases in $\mathcal{I}$.*

Theorem 2 *$\mathcal{M}^*$ is a matroid and its rank function is*

$$r^*(S) = |S| - (r(E) - r(E \setminus S)).$$

Proof: First, we show that r^* is the rank function of a matroid. Its marginal values are in $\{0, 1\}$, and it's submodular, because

$$\begin{aligned} r^*(S \cup T) + r^*(S \cap T) &= |S \cup T| + |S \cap T| - 2r(E) + r(E \setminus (S \cup T)) + r(E \setminus (S \cap T)) \\ &= |S| + |T| - 2r(E) + r((E \setminus S) \cap (E \setminus T)) + r((E \setminus S) \cup (E \setminus T)) \\ &\leq |S| + |T| - 2r(E) + r(E \setminus S) + r(E \setminus T) \\ &= r^*(S) + r^*(T). \end{aligned}$$

This implies that $\mathcal{I}^* = \{I : r^*(I) = |I|\}$ are the independent sets of some matroid, in fact exactly the dual matroid, since

$$\begin{aligned} I \text{ is a base of } \mathcal{M}^* &\Leftrightarrow r^*(I) = |I| = r^*(E) \\ &\Leftrightarrow r(E \setminus I) = r(E) \text{ and } |I| = |E| - r(E) \\ &\Leftrightarrow E \setminus I \text{ is a base of } \mathcal{M}. \end{aligned}$$

□

Definition 3 *For a matroid $\mathcal{M} = (E, \mathcal{I})$ and $e \in E$,*

1. *the "deletion" of e produces*

$$\mathcal{M} \setminus e = (E - e, \{I \subseteq E - e : I \in \mathcal{I}\})$$

2. *the "contraction" of e produces*

$$\mathcal{M}/e = (E - e, \{I \subseteq E - e : I + e \in \mathcal{I}\})$$

if $r(\{e\}) = 1$, and $\mathcal{M}/e = \mathcal{M} \setminus e$ if $r(\{e\}) = 0$.

Note that the bases in $\mathcal{M} \setminus e$ are the same as the bases of $E - e$ in $\mathcal{M}$ (which could be smaller than the bases of $\mathcal{M}$ if every base of $\mathcal{M}$ contains e). The bases of $\mathcal{M}/e$, assuming $r(\{e\}) = 1$, are the sets $B \subseteq E - e$ such that $B + e$ is a base in $\mathcal{M}$.

How does deletion/contraction affect the rank function?

- $r_{\mathcal{M}\setminus e}(S) = r_{\mathcal{M}}(S)$, for any $S \subseteq E - e$
  (nothing changes in terms of independence in $\mathcal{M} \setminus e$).
- $r_{\mathcal{M}/e}(S) = r_{\mathcal{M}}(S + e) - r_{\mathcal{M}}(e)$, for any $S \subseteq E - e$
  (if $r_{\mathcal{M}}(\{e\}) = 0$, nothing changes in terms of independence;
  if $r_{\mathcal{M}}(\{e\}) = 1$, then B is a base of S in $\mathcal{M}/e$ iff $B + e$ is a base of $S + e$ in $\mathcal{M}$).

Lemma 4 *Contraction is dual to deletion, i.e.*

$$(\mathcal{M}/e)^* = \mathcal{M}^* \setminus e.$$

Proof: If $r(\{e\}) = 0$, then the bases of $\mathcal{M}/e$ the same as the bases of $\mathcal{M}$, which never contain the element e. On the other hand, e in this case appears in every base of $\mathcal{M}^*$ and $\mathcal{M}^* \setminus e$ has the same bases minus the element e. These are exactly the complements of the bases of $\mathcal{M}/e$ in $E - e$.

If $r(\{e\}) = 1$, then we have:

I is independent in $(\mathcal{M}/e)^*$
$\Leftrightarrow$ $I \subseteq B$ for some base B of $(\mathcal{M}/e)^*$
$\Leftrightarrow$ $I \subseteq (E - e) \setminus B'$ for some base B' of $\mathcal{M}/e$
$\Leftrightarrow$ $I \subseteq E \setminus B''$ for some base of $\mathcal{M}$, $B'' = B' + e$
$\Leftrightarrow$ $I \subseteq B'''$ for some base B''' of $\mathcal{M}^*$ and $e \notin I$
$\Leftrightarrow$ I is independent in $\mathcal{M}^* \setminus e$. □

An alternative proof is based on what happens with the rank function under these operations. For any $S \subseteq E - e$, we have

$$\begin{aligned} r_{(\mathcal{M}/e)^*}(S) &= |S| - r_{\mathcal{M}/e}(E - e) + r_{\mathcal{M}/e}((E - e) \setminus S) \\ &= |S| - (r_{\mathcal{M}}(E) - r_{\mathcal{M}}(e)) + (r_{\mathcal{M}}(E \setminus S) - r_{\mathcal{M}}(e)) \\ &= |S| - r_{\mathcal{M}}(E) + r_{\mathcal{M}}(E \setminus S) \\ &= r_{\mathcal{M}^*}(S) = r_{\mathcal{M}^*\setminus e}(S). \end{aligned}$$

Matroid duality in a nutshell

contraction	$\leftrightsquigarrow$	*deletion*
base	$\leftrightsquigarrow$	*complement of a base*
independent set	$\leftrightsquigarrow$	*complement of a spanning set*
circuit (minimal dependent set)	$\leftrightsquigarrow$	*cut (minimal, intersects every base)*
loop (no independent set contains it)	$\leftrightsquigarrow$	*bridge (every base contains it)*

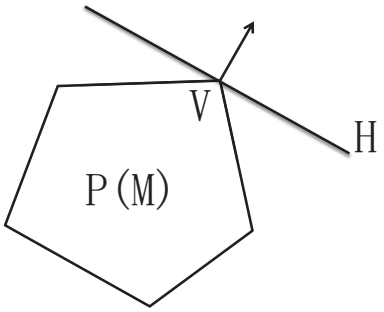
(The terminology comes from graphic matroids.)

2 The matroid polytope

Theorem 5 *For a matroid $\mathcal{M} = (E, \mathcal{I})$, the matroid polytope $P(M) \equiv conv\{\mathbf{x}_I : I \in \mathcal{I}\}$ is described by*

$$P(\mathcal{M}) = \{\mathbf{x} \in \mathbb{R}_+^E : \forall S \subseteq E, x(S) \leq r_{\mathcal{M}}(S)\}$$

where $r_{\mathcal{M}}$ is the rank function of $\mathcal{M}$.



Proof: We show that for any weight function $\mathbf{w} \in \mathbb{R}^E$

$$\begin{array}{rcl} \max & & \mathbf{w}^T\mathbf{x} \\ \forall S; x(S) & \leq & r(S), \\ \mathbf{x} & \geq & 0 \end{array}$$

has an optimal solution in $\{0,1\}^E$. For any vertex $\mathbf{v}$, there is some direction $\mathbf{w}$ such that $\mathbf{v}$ is the unique optimum of $\max\{\mathbf{w}^T\mathbf{x} : \mathbf{x} \in P\}$, Hence, this will imply that all vertices are in $\{0,1\}^E$.

Consider LP duality: (for now, let $\mathbf{w} \geq 0$)

$$\begin{array}{ll} \max \mathbf{w}^T\mathbf{x}: & \min \sum_S y_S r(S): \\ \forall S; \sum_{i \in S} x_i \leq r(S), & \forall i; \sum_{S: i \in S} y_S \geq w_i, \\ \mathbf{x} \geq 0 & \mathbf{y} \geq 0 \end{array}$$

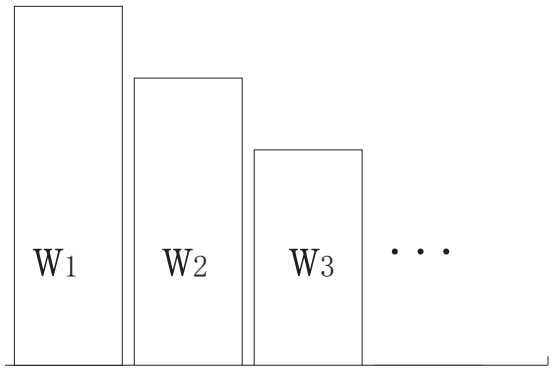
Define a primal solution by the greedy algorithm:

$$w_1 \geq w_2 \geq w_3 \geq ...$$

$$x_i = \begin{cases} 1 & \text{if greedy takes } i \\ 0 & \text{otherwise} \end{cases}$$

($\mathbf{x} \in P(\mathcal{M})$ clearly).

$$\begin{aligned} \text{Greedy takes element i} &\Leftrightarrow i \notin span(\{1, 2, ..., i-1\}) \\ &\Leftrightarrow r(\{1, 2, ..., i\}) = r(\{1, 2, ..., i-1\}) + 1 \end{aligned}$$



So:

$$\begin{aligned}\mathbf{w}^T\mathbf{x} &= \sum_{i=1}^{n} w_i(r([i]) - r([i-1])) \\ &= \sum_{j=1}^{n} r([j])(w_j - w_{j+1})\end{aligned}$$

This suggests a dual solution: $y_{[j]} = w_j - w_{j+1}, \forall j$ (formally, $w_{n+1} = 0$)
We have:

$$\sum_{S:i\in S} y_S = \sum_{j=i}^{n} y_{[j]} = \sum_{j=i}^{n}(w_j - w_{j+1}) = w_i,$$

$$\sum_{S} y_S r(S) = \sum_{j=1}^{n} y_{[j]} r([j]) = \mathbf{w}^T\mathbf{x}.$$

This proves that both $\mathbf{x}, \mathbf{y}$ are optimal primal/dual solutions.

For $\mathbf{w} \in \mathbb{R}^E$, note that the primal optimum does not change if we replace $w_i < 0$ by $w_i = 0$; in any case, we can assume $x_i = 0$. Therefore, there is an optimal solution in $\{0,1\}^E$ for any $\mathbf{w} \in \mathbb{R}^E$. □

Note: We have proved more: if $\mathbf{w} \in \mathbb{Z}^E$, then both primal and dual optimal solutions are integral ("a totally dual integral system").

Corollary 6 *The matroid base polytope $P_{base}(\mathcal{M})$ is*

$$P_{base}(\mathcal{M}) = \{\mathbf{x} \in \mathbb{R}_+^E : \forall S; x(S) \le r(S), x(E) = r(E)\}.$$

Proof: Obviously, $\chi_B \in P_{base}(\mathcal{M})$ for every base B. Suppose that $\mathbf{x}$ satisfies the constraints $\forall S; x(S) \le r(S)$, and $x(E) = r(E)$. In particular, $\mathbf{x} \in P(\mathcal{M})$, the matroid polytope, and

$$\mathbf{x} = \sum_{I\in\mathcal{I}} \alpha_I \mathbf{x}_I, \sum \alpha_I = 1, \alpha_I \ge 0.$$

We have $x(E) = \sum_{I \in \mathcal{I}} \alpha_I |I| \leq \sum_{I \in \mathcal{I}} \alpha_I r(E) = r(E)$. But $x(E) = r(E)$, so we have an equality for each I with a positive coefficient α_I and each such I must be a base. □

What does it mean for spanning trees?

$$\mathcal{M} = \text{ graphic matroid, } G = (V, E)$$

$$r_{\mathcal{M}}(S) = |V| - \#components \text{ in } (V, S)$$

$$r_{\mathcal{M}}(E) = |V| - 1 \text{ (assuming } G \text{ connected)}$$

If $S = E[W]$, then clearly $r_{\mathcal{M}}(S) \leq |W| - 1$. So we obtain a valid constraint

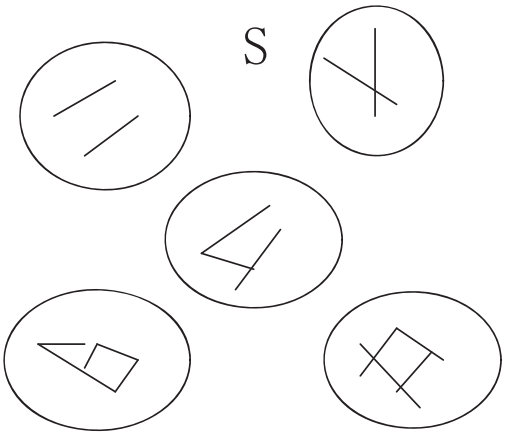
$$x(E[W]) \leq |W| - 1.$$

For any other $S \subseteq E$,

$$x(S) \leq r_{\mathcal{M}}(S) = |V| - \#components(S)$$

can be obtained by adding up $x(S \cap E[W_i]) \leq |W_i| - 1$ over all connected components W_i of S.

$\rightsquigarrow$ it is sufficient to keep $x(E[W]) \leq |W| - 1$ for every $W \subseteq V$.



Corollary 7 *The forest polytope of $G = (V, E)$ is given by*

$$P_{forest}(G) = \{\mathbf{x} \in \mathbb{R}_+^E : \forall W \subseteq V; x(E[W]) \leq |W| - 1\}$$

The spanning tree polytope is given by:

$$P_{spanning-tree}(G) = \{\mathbf{x} \in \mathbb{R}_+^E : \forall W \subset V; x(E[W]) \leq |W| - 1, x(E) = |V| - 1\}$$

Note: All these descriptions are exponentially large, but the polytopes are "nice". We can optimize over them, and by polarity we can also solve the separation problem.