Matroid Theory Fundamentals

for Combinatorial Optimization

Morteza Alimi

Table of Contents

Table of Contents

Matroid definition

Definition

Given a set S and a non-empty collection $\mathcal{I}$ of subsets of S, the pair $(S, \mathcal{I})$ is called a *matroid* if the following two conditions are satisfied:

1. If $T \in \mathcal{I}$ and $U \subseteq T$, then $U \in \mathcal{I}$.
2. If $U, T \in \mathcal{I}$ and $|T| > |U|$ then there exists $x \in T \setminus U$ such that $U + x \in \mathcal{I}$.

Matroid definition

Condition 2 is equivalent to the following weaker version:

2' If $U, T \in \mathcal{I}$, $|T \setminus U| = 2$, and $|U \setminus T| = 1$, then there exists $x \in T \setminus U$ such that $U + x \in \mathcal{I}$.

- To prove $2' \to 2$, given 1, we use induction on $k = |U \setminus T|$ (given $U, T \in \mathcal{I},\ |T| > |U|$). We can assume $|T| = |U| + 1$.
- The case $k = 0$ is trivial, and $k = 1$ is equivalent to $2'$. So assume $k > 1$.
- A certain degree of manuevring does the job! Take $y, z \in T \setminus U$. By the induction hypothesis, there is $x \in U \setminus T$ such that $V = (T - y - z) + x \in \mathcal{I}$. Now, 2' means $w \in T \setminus V = \{y, z\}$ exists such that $W = V + w$ is independent. Now, $|W| = |T|$ and $|U \setminus W| < |U \setminus T|$, so by the induction hypothesis $s \in W \setminus U \subseteq T \setminus U$ exists such that $U + s \in \mathcal{I}$.

Bases, Circuits

Definition

- Given matroid $M = (S, \mathcal{I})$, a *base* for a subset $U \subseteq S$ is a maximal independent set contained in U. A *base* (without any qualifications) indicates a base for S.
- A *circuit* is a minimal dependent set.
- The collection of bases and circuits of a matroid are usually denoted by $\mathcal{B}$ and $\mathcal{C}$ (when the matroid is understood).

Base Characterization

- Assuming condition 1, condition 2 is equivalent to the following:
  3. For any $U \subseteq S$, the bases of U have the same size.
- Proof: Straightforward. Think about it!

Unique Circuit Characterization

- Assuming condition 1, condition 2 is equivalent to the following:
  4. For any independent set $I \in \mathcal{I}$, and $x \in S \setminus I$, $I + x$ contains at most one circuit.

Proof.

$4 \to 2'$:

- Take independent sets $T + x$ and $T + y + z$. Suppose $T + x + y$ and $T + x + z$ are both dependent.
- Then there are circuits $C_y \ni y$ and $C_z \ni z$ with $C_y \subseteq T + x + y$, and $C_z \subseteq T + x + z$.
- But then adding x to $T + y + z$ creates two distinct circuits C_y and C_z, which contradicts 4.

Unique Circuit Characterization

Proof (Continued).

$2 \to 4$:

- Suppose $I \in \mathcal{I}$, and $I + x$ contains distinct circuits C_1 and C_2.
- Take $y \in C_1 \setminus C_2$. Extend $C_1 - y$ to a maximal independent set X of $I + x$.
- I is also a maximal independent subset of $I + x$. Hence, $|X| = |I|$.
- But then we should have $X = I + x - f$. As $C_2 \subseteq I + x$ and $f \notin C_2$, we have $C_2 \subseteq X$. Contradiction.

$\square$

Greedy Algorithm I

- Let be given matroid $M = (S, \mathcal{I})$ on set $S = \{s_1, \ldots, s_n\}$, together with a weight function $w : S \to R$. Assume the elements of S are indexed such that $w(s_1) \geq w(s_2) \geq \ldots \geq w(s_n)$. The objective is to find a base of M haveing maximum total weight.
- The greedy algorithm is defined as follows.

$T \leftarrow \emptyset$
for $i = 1$ **to** n **do**
  if $T \cup \{s_i\} \in \mathcal{I}$ **then**
    $T \leftarrow T \cup \{s_i\}$
  end
end
return T

Greedy Algorithm II

Theorem

The greedy algorithm finds a maximum weight base for every weight function if and only if M is a matroid.

Rank Function

Definition

Given a matroid $M = (S, \mathcal{I})$, the *rank function* of M is a function $r : 2^S \to \mathbb{Z}_+$ defined as $r(U) = max\{|I| \mid I \subseteq U, I \in \mathcal{I}\}$.

Theorem

The rank function of any matroid $M = (S, \mathcal{I})$ is submodular:

$$r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y), \quad \forall X, Y \subseteq S$$

Proof.

- Let $B_\cap$ be a base for $X \cap Y$.
- Grow $B_\cap$ to a get a base $B_\cup \supseteq B_\cap$ for $X \cup Y$.
- We have $r(X) \geq |B_\cup \cap X|$, and $r(Y) \geq |B_\cup \cap Y|$.
- Hence
  $r(X)+r(Y) \geq |B_\cup \cap X|+|B_\cup \cap Y| = |B_\cup|+|B_\cap| = r(X \cup Y)+r(X \cap Y)$.

Table of Contents

Linear Matroid

- Take a fixed matrix A. Let S denote the set of columns of A. Then $M = (S, \mathcal{I})$ is a matroid, where a set of columns of A is independent if they are linearly independent.

Graphic Matroid

- Let $G = (V, E)$ be an undirected graph.
- Then $M = (E, \mathcal{I})$ is a matroid, where $\mathcal{I} = \{F \subseteq E \mid (V, F) \text{ is a forest. }\}$.
- M is said to be the *cycle matroid* of G. A matroid that is the cycle matroid of some graph is called a *graphic matroid*.

Partition Matroid

- Let $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ be a partition of S, and let $k_1, \ldots, k_n$ be nonnegative integers. Take $I \subseteq S$ to be independent if $I \cap A_i \leq k_i$ for each i. It can easily be seen that $(S, \mathcal{I})$ is a matroid, called a *partition matroid*.

Transversal Matroid

- Let $\mathcal{A} = \{A_1, A_2, \ldots, A_n\}$ be a collection of subsets of S. Take $I \subseteq S$ to be independent if I is a partial transversal for $\mathcal{A}$. Let $\mathcal{I}$ denote such I's. It can be shown that $M = (S, \mathcal{I})$ is a matroid.
- A partition matroid is a special case of a transversal matroid where the A_i's are disjoint.

Matching Matroid I

- Given a graph $G = (V, E)$, the collection of matchings of G is not necessarily a matroid (taking E as the ground set), as a maximal matching is not necessarily a maximum matching.
- However, there is a way to define a *matching matroid* on the *vertices* of G.
- Let $M = (V, \mathcal{I})$, where a set $U \subseteq V$ belongs to $\mathcal{I}$, iff there is a matching covering U (and possibly some other vertices). We claim M is a matroid.
- Property 1 of matroids is easy to check. To prove property 2, suppose $U_1, U_2 \in \mathcal{I}$, $|U_1| > |U_2|$. Let matchings N_1 and N_2 cover U_1 and U_2 respectively.
- We can assume N_2 does not cover any vertex in $U_1 \setminus U_2$ (Otherwise we are done).

Matching Matroid II

- Let $N = N_1 \triangle N_2$. Each vertex $u \in U_1 \setminus U_2$ is an endpoint of a path P_u in (V, N).
- Not all these paths can have a vertex in $U_2 \setminus U_1$ as their other endpoint (because $|U_1| > |U_2|$). Let $v \in U_1 \setminus U_2$ be such that P_v does not end at a vertex in $U_2 \setminus U_1$.
- Then $N_2 \triangle P_v$ is a matching that covers $U_2 \cup \{v\}$.

Table of Contents

Dual matroid

Theorem

Let $M = (S, \mathcal{I})$ be a matroid. Let $\mathcal{I}^* = \{I \mid r_M(S \setminus I) = r_M(S)\}$. Then $M^* = (S, \mathcal{I}^*)$ is again a matroid, called the dual of M.

Dual matroid

Proof.

- Take sets $T + x$ and $T + y + z$ in $\mathcal{I}^*$. We need to show that one of $T + x + y$ or $T + x + z$ is in $\mathcal{I}^*$.
- Let B_1 be a base of M contained in $S \setminus (T + x)$, and let B_2 be a base of M contained in $S \setminus (T + y + z)$.
- If either of y or z is not contained in B_1, the corresponding element can be added to $T + x$ and keep it independent in M^*. So assume $y, z \in B_1$.
- We show how to build a set $B \in \mathcal{B}$ avoiding T, x, and either y or z.
- We have $(B_1 \setminus \{y, z\}) + u + v \in I^*$ for some $u, v \in B_2 \setminus B_1$.
- If $x \notin \{u, v\}$ we are done. Otherwise, $B' = B - x + w \in \mathcal{B}$ is the desired set, where $w \in B_1 \setminus B$.

□

It can be seen that $M^{**} = M$.

The rank function of the dual matroid

Theorem

Let $M = (S, \mathcal{I})$ be a matroid, and let $M^* = (S, \mathcal{I}^*)$ be its dual. Then

$$r_{M^*}(U) = |U| - (r_M(S) - r_M(S \setminus U)).$$

Proof.

$$\begin{aligned} r_{M^*}(U) &= \max\{|I| \mid I \subseteq U, r(S \setminus I) = r(S)\} \\ &= |U| - \min\{B \cap U \mid B \in \mathcal{B}\} \\ &= |U| + r(S) - \max\{B \cap (S \setminus U) \mid B \in \mathcal{B}\} \\ &= |U| + r(S) - r(S \setminus U) \end{aligned}$$

□

Table of Contents

Deletion and Truncation

Definition

Given a matroid $M = (S, \mathcal{I})$ and a set $Z \subseteq S$, the matroid $M \setminus Z$ is the pair $(S \setminus Z, \mathcal{I}')$ where $\mathcal{I}' = \{U \subseteq S \setminus Z \mid U \in \mathcal{I}\}$. The matroid $M \setminus Z$ is said to be obtained from M by deleting Z. If $Y = S \setminus Z$, $M \setminus Z$ might also be denoted as $M|Y$.

Definition

Given a matroid $M = (S, \mathcal{I})$ and natural number k, defined $\mathcal{I}' = \{I \in \mathcal{I} \mid |I| \leq k\}$. Then $(S, \mathcal{I}')$ is again a matroid, called the *k-truncation* of M.

Contraction

Definition

Given a matroid $M = (S, \mathcal{I})$ and a set $Z \subseteq S$, the matroid denoted by M/Z, said to obtain from M by *contracting* Z, is the matroid $(M^* \setminus Z)^*$.

Theorem

$$r_{M/Z}(X) = r_M(X \cup Z) - r_M(Z), \quad \textit{for } X \subseteq S \setminus Z.$$

Proof.

$$\begin{aligned}
&r_{M/Z}(X) = |X| - r_{M^*\setminus Z}(S \setminus Z) + r_{M^*\setminus Z}((S \setminus Z) \setminus X) \\
&= |X| - r_{M^*}(S \setminus Z) + r_{M^*}((S \setminus Z) \setminus X) \\
&= |X| - (|S \setminus Z| - r_M(S) + r_M(Z)) + |(S \setminus Z) \setminus X| - r_M(S) + r_M(X \cup Z) \\
&= |X| + |(S \setminus Z) \setminus X| - |S \setminus Z| + r_M(S) - r_M(S) - r_M(Z) + r_M(X \cup Z) \\
&= r_M(X \cup Z) - r_M(Z)
\end{aligned}$$

Contraction

- Suppose W is a base of set Z. Then a set $X \subseteq S \setminus Z$ is independent in M/Z iff $X \cup W$ is independent in M.
- It can be shown that deletion and contraction commute.
- If matroid M' arises from M by a series of deletions and contractions, M' is called a minor of M.

Table of Contents

Matroid Polytope I

Definition

Let $M = (S, \mathcal{I})$ be a Matroid. Define the *matroid polytope* (or the independent set polytope) associated with M as
$P(M) = CH(\{\chi^I \mid I \in \mathcal{I}\})$.

Theorem

The matroid polytope $P(M)$ of a matroid $M = (S, \mathcal{I})$ is equal to the polytope Q defined as

$$\begin{array}{rcl} x(U) & \leq & r(U), \quad \forall U \subseteq S \\ x & \geq & 0 \end{array}$$

Matroid Polytope II

Proof

- It is easy to see that the characteristic vector of any intependent set belongs to Q, and hence $P(M) \subseteq Q$.
- For the converse, take the dual pair of LPs

$$\begin{array}{ll} \text{maximize} & w^T x \\ \text{subject to} & x(U) \le r(U), \quad \forall U \subseteq S \\ & x \ge 0. \end{array}$$

and

$$\begin{array}{ll} \text{minimize} & \sum_{U \subseteq S} r(U) y_U \\ \text{subject to} & \sum_{U \subseteq S, U \ni s} y_U \ge w(s), \quad s \in S \\ & y \ge 0. \end{array}$$

Matroid Polytope III

- For any weight function w, we find integer solutions for the primal and dual LPs with equal value.
- Assume $w \geq 0$, and that the items are sorted accroding to their weights, i.e. $w(s_1) \geq w(s_2) \geq \ldots \geq w(s_n)$. For the primal solution, take the output I of the greedy algorithm, that is, $s_i \in I$ iff $r(U_i) > r(U_{i-1})$. Here U_i is the set consisting of the first i elements. Let x be the characteristic vector of I.
- For the dual solution, take $y_{U_i} = w(s_i) - w(s_{i+1})$. For all other $U \subseteq S$, $y_U = 0$.

Matroid Polytope IV

- Then,

$$\begin{array}{rcl} w^T x & = & \sum_{i=1}^n w(s_i)(r(U_i) - r(U_{i-1})) \\ & = & \sum_{i=1}^n r(U_i)(w(s_i) - w(s_{i+1})) \\ & = & \sum\limits_{U \subseteq S} r(U) y_U. \end{array}$$

  So, both solutions are optimal.

- If $w(s_i) < 0$ for some i, setting $w(s_i) = 0$ does not change the primal optimum solution. So, there is always an integer primal optimum solution. This means that all vertices of Q are integer, which should correspond to characteristic vectors of independent sets.

Table of Contents

Matroid intersection

- Given Matroids $M = (S, \mathcal{I}_1)$ and $M = (S, \mathcal{I}_2)$, $(S, \mathcal{I}_1 \cap \mathcal{I}_2)$ is not necessarily a matroid. For example, the set of matchings in the graph P_3 (path of length 3) do not comprise a matroid (on the set of edges), but they can be represented as the intersection of two matroids (see the next slide).
- We will see that there exist efficient algorithms for finding a maximum independent set of two matroids.

Matroid intersection examples

Bipartite Matching

Let $G = (V, E)$ be a bipartite graph with color classes U_1 and U_2. For $i = 1, 2$, define $M_i = (E, \mathcal{I}_i)$, with $F \in \mathcal{I}_i$ if each vertex in U_i is covered by at most one edge in F. It can be seen that a common independent set of M_1 and M_2 is a matching of G.

Arborescence

Given a directed graph $D = (V, A)$, and $r \in V$, an r-arborescence is defined as a directed tree rooted at r, with all its edges pointing away from r. The r-arborescences are precisely the common bases of the graphic matroid of D (ignoring the direction of the edges), and the partition matroid $(A, \mathcal{I})$, with $\mathcal{I} = \{F \subseteq A \mid F \cap \delta^-(v) \leq 1, \; \forall r \neq v \in V\}$.

Intersection of three matroids

Using a similar modeling technique as the arborescence problem, it is not difficult to see that hamiltonian paths in a digraph can be represented as the intersection of three matroids, and hence finding a maximum cardinality independent set in the intersection of more than two matroids is NP-Hard.

Table of Contents

Matroid intersection theorem

Theorem

Let $M_1 = (S, \mathcal{I}_1)$ and $M_2 = (S, \mathcal{I}_2)$ be two matroids. Then the maximum size k of a set $I \in \mathcal{I}_1 \cap \mathcal{I}_2$ is equal to:

$$k = \min_{E \subseteq S} (r_1(E) + r_2(S \setminus E)).$$

Matroid intersection theorem (proof)

- Let the two matroids be $M_1 = (S, \mathcal{I}_1)$ and $M_2 = (S, \mathcal{I}_2)$.
- The fact that the maximum is no more than the minimum is easy to see. Let $I \in \mathcal{I}_1 \cap \mathcal{I}_2$, and let $U \subseteq S$. Then

$$|I| = |I \cap U| + |I \setminus U| \leq r_1(U) + r_2(S \setminus U).$$

- Now we prove the converse.
  Let $k = \min_{U \subseteq S}(r_1(U) + r_2(S \setminus U))$
- Choose $x \in S$ such that $r_1(\{x\}) = r_2(\{x\}) = 1$ (if no such x exists, it can easily be seen that both min and max are zero).
- We may assume the matroids $M_1 \setminus \{x\}$ and $M_2 \setminus \{x\}$ have no common independent set of size k (otherwise the same set would work for M_1 and M_2 and we are done). So, by the induction hypothesis,

$$r_1(A_1) + r_2(A_2) \leq k - 1$$

  for some partition (A_1, A_2) of $S \setminus \{x\}$.

Matroid intersection theorem (proof - continued)

- Likewise, the contractions $M_1/\{x\}$ and $M_2/\{x\}$ have no common independent set of size $k-1$ (otherwise, by adding x, we obtain a common independent set of size k for M_1 and M_2). So,

$$r_1(B_1 \cup \{x\}) - 1 + r_2(B_2 \cup \{x\}) - 1 \leq k - 2,$$

  for some partition (B_1, B_2) of $S \setminus \{x\}$.
- By submodularity we have

$$r_1(A_1 \cap B_1) + r_1(A_1 \cup B_1 \cup \{x\}) \leq r_1(A_1) + r_1(B_1 \cup \{x\}),$$
$$r_2(A_2 \cap B_2) + r_2(A_2 \cup B_2 \cup \{x\}) \leq r_2(A_2) + r_2(B_2 \cup \{x\}).$$

- Also, because $A_1 \cap B_1$ and $A_2 \cup B_2 \cup \{x\}$ form a partition of S, and likewise $A_2 \cap B_2$ and $A_l \cup B_1 \cup \{x\}$, we have

$$k \leq r_1(A_1 \cap B_1) + r_2(A_2 \cup B_2 \cup \{x\}),$$
$$k \leq r_1(A_2 \cap B_2) + r_2(A_1 \cup B_1 \cup \{x\}),$$

- So, we have $2k \leq 2k-1$, a contradiction.

Table of Contents

Konig's theorem

- Let $G = (V, E)$ be a bipartite graph with color classes U_1 and U_2. For $i = 1, 2$, define $M_i = (E, \mathcal{I}_i)$, with $F \in \mathcal{I}_i$ if each vertex in U_i is covered by at most one edge in F.
- It can be seen that a common independent set of M_1 and M_2 is a matching of G.
- The matroid intersection theorem implies the size of the largest matching equals the minimum value of $r_1(F) + r_2(E \setminus F)$. The latter is equal to the size of minimum vertex cover. Hence we have Konig's theorem.

Table of Contents

Matroid Intersection Polytope

Let $M_1 = (S, \mathcal{I}_1), M_2 = (S, \mathcal{I}_2)$. Define
$P(M_1 \cap M_2) = CH(\{\chi^I \mid I \in \mathcal{I}_1 \cap \mathcal{I}_2\})$.

Theorem

$$P(M_1 \cap M_2) = P(M_1) \cap P(M_2)$$

Matroid Intersection Polytope (proof) I

$\subseteq$: Easy! Let x be a vertex of $P(M_1 \cap M_2)$. Then $x = \chi^I$, with $I \in \mathcal{I}_1 \cap \mathcal{I}_2$. So $x \in P(M_1)$ and $x \in P(M_2)$.

$\supseteq$: [sketch]

- Let x be a vertex of $P(M_1 \cap M_2)$.
- If x has a 0 or 1 component, use the induction hypothesis for $M \setminus \{x\}$ or $M/\{x\}$ to deduce $x \in P(M_1 \cap M_2)$.
- So, we can assume all components of x are fractional.
- As x is a vertex, there exist $n = |S|$ linearly independent tight inequalities for x.
- These exist chains $\mathcal{C}$ and $\mathcal{D}$ the characteristic vectors of which generate all tight inequalities (proof omitted). Hence $|\mathcal{C}| + |\mathcal{D}| = n$.

Matroid Intersection Polytope (proof) II

- As each $0 < x_i < 1$, and the rank function is integer, $C_i \setminus C_{i-1}$ contains at least two elements, and likewise for D_i's.
- Hence $|\mathcal{C}| \leq n/2$, and $|\mathcal{D}| \leq n/2$. Therefore, $|\mathcal{C}| = n/2$, and $|\mathcal{D}| = n/2$.

Table of Contents

Cardinality matroid intersection algorithm

- **Input:** Matroids $M_1 = (S, \mathcal{I}_1)$, $M_2 = (S, \mathcal{I}_2)$, and $I \in \mathcal{I}_1 \cap \mathcal{I}_2$.
  Output: $J \in \mathcal{I}_1 \cap \mathcal{I}_2$, with $|J| = |I| + 1$ if such a set exists.
- Build a directed graph D with vertex set S, with $y \to x$ iff $y \in I$, $x \notin I$, and $I - y + x \in \mathcal{I}_1$. And $y \leftarrow x$ iff $y \notin I$, $x \in I$, and $I - x + y \in \mathcal{I}_2$.
- Define $X_1 = \{x \in S \setminus I \mid I + x \in \mathcal{I}_1\}$, and $X_2 = \{x \in S \setminus I \mid I + x \in \mathcal{I}_2\}$.
- If there exists a path P from X_1 to X_2 in D: Let P be the shortest such path. Set $I \leftarrow I \triangle VP$. (Here VP denotes the vertices of P). Otherwise, I is maximum.