Notes on Matroid Intersection (COL 758)

Recall that a matroid $\mathcal{M} = (X, \mathcal{I})$ has two properties :

1. (containment property) If $S \in \mathcal{I}$ and $T \subseteq S$, then $T \in \mathcal{I}$.
2. (exchange property) If $S, T \in \mathcal{I}$ and $|S| < |T|$, then there exists $x \in T - S$ such that $S + x \in \mathcal{I}$ ($S + x$ is shorthand for $S \cup \{x\}$).

There are several statements which look intuitive (when viewed in special cases of graphic matroid, but one needs to prove them using these two properties only). For a subset U of X, define $\texttt{rank}(U)$ as the size of a maximal independent set in U. Note that this property is well defined – if S and T are two maximal independent sets in U, then $|S| = |T|$ (if, e.g., $|S| < |T|$, then the exchange property implies that we can add an element of $T - S$ to S and so, S will not be maximal). Some useful facts:

- Suppose $U, V \subseteq X$, and $U \subseteq V$. Then, for any $x \notin V$,

$$\texttt{rank}(V + x) - \texttt{rank}(V) \leq \texttt{rank}(U + x) - \texttt{rank}(U) \tag{1}$$

  Clearly $\texttt{rank}(V - x) - \texttt{rank}(V)$ is either 0 or 1 – if it is 0, then there is nothing to prove. So assume it is 1. Let $\texttt{rank}(V)$ be t, and $\texttt{rank}(U)$ be s. Let I be a maximal independent set (of size $t + 1$) in $V + x$. I must contain x (otherwise it will be an independent set in V, but $\texttt{rank}(V)$ is t only). Let J be a maximal independent set (of size s) in U. Warning: J may not be a subset of I. By the exchange property, we can keep on adding elements of $I - J$ to J till its size becomes $t + 1$ (and it remains in $\mathcal{I}$) – let this set of size $t + 1$ be J'. J' must contain x (since it is an independent set and cannot be a subset of V). Now by the subset property $J + x$, which is a subset of J', must be in $\mathcal{I}$ as well. Thus, $\texttt{rank}(U + x) = s + 1$. This property is also called *submodularity* of the rank function.

- Let $U \subseteq X$ and $x_1, \ldots, x_k$ be elements in $X - U$. Suppose it is the case that adding any of these elements to U does not increase the rank of U, i.e., $\texttt{rank}(U + x_i) = \texttt{rank}(U)$ for all $i = 1, \ldots, k$. Then, adding *all* of these elements to U will also not increase its rank, i.e., $\texttt{rank}(U \cup \{x_1, \ldots, x_k\}) = \texttt{rank}(U)$. Its enough to show this for $k = 2$ (the general case can be proved in a similar manner, or by induction on k) :

$$\texttt{rank}(U + x_1 + x_2) - \texttt{rank}(U) = (\texttt{rank}(U + x_1 + x_2) - \texttt{rank}(U + x_1)) - (\texttt{rank}(U + x_1) - \texttt{rank}(U)).$$

  The second term is 0 by assumption. For the first term, if $V = U + x_1$, then the above statement implies that this is also 0.

  This allows us to define $\texttt{span}(U)$ as the set of all elements whose addition to U does not increase the rank :

$$\texttt{span}(U) = \{x \in X : \texttt{rank}(U + x) = \texttt{rank}(U)\}.$$

  Clearly, $U \subseteq \texttt{span}(U)$, but in general it can be larger. It is motivated by the special case of linear algebraic matroid. What we have shown is that even if we add all of $\texttt{span}(U)$ to U *simultaneously*, it does not increase the rank, i.e., $\texttt{rank}(U) = \texttt{rank}(\texttt{span}(U))$.

Exercise 1 *Suppose $U, V \subseteq X$, $U \subseteq V$. Prove that* $\texttt{span}(U) \subseteq \texttt{span}(V)$ *(again, it is intuitive, but you need to prove it formally).*

Another intuitive (but more general) statement:

Exercise 2 *Suppose $U, V \subseteq X$. Suppose $U \subseteq \mathtt{span}(V)$. Then $\mathtt{span}(U) \subseteq \mathtt{span}(V)$.*

A circuit is defined as a *minimal* dependent set (a set is dependent if it is not independent). From the above exercise, the following follows.

Exercise 3 *Suppose U is a circuit. Prove that for any $z \in U$, $\mathtt{span}(U) = \mathtt{span}(U - z)$.*

Now we come to matroid intersection. We are given two matroids $\mathcal{M}_1 = (X, \mathcal{I}_1)$ and $\mathcal{M}_2 = (X, \mathcal{I}_2)$ over the same set of elements X. We would like to find a set I of largest size such that $I \in \mathcal{I}_1 \cap \mathcal{I}_2$. Let r_1, r_2 be the rank functions in $\mathcal{M}_1$ and $\mathcal{M}_2$ respectively. We will give an iterative algorithm which starts with a set I and incrementally improves it till we can no longer improve its size. First we need an upper bound on the size of an optimal set (i.e., largest set which is in $\mathcal{I}_1 \cap \mathcal{I}_2$). In fact, the way we will prove that our set I is optimal is by using this upper bound – we will show that our algorithm stops when $|I|$ reaches this upper bound. Let I be any set in $\mathcal{I}_1 \cap \mathcal{I}_2$. Let U be any subset of X. We observe:

$$|I| = |I \cap U| + |I \cap (X - U)| \leq r_1(U) + r_2(X - U).$$

The second inequality follows because $I \cap U$ is an independent set in $\mathcal{I}_1$ (by the containment property), and so, $r_1(U) \geq |I \cap U|$. Similarly, for the second term. Since this holds for any I, it follows that it is true for an optimal I as well:

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| \leq r_1(U) + r_2(X - U).$$

Thus, every U gives an upper bound on the size of an optimal solution. Note that we are free to pick any U – if we want to get the best possible upper bound we should pick a U for which the bound is as small as possible. So,

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| \leq \min_{U : U \subseteq X} (r_1(U) + r_2(X - U)).$$

The matroid intersection theorem states that we have equality above.

Theorem 1 **Matroid Intersection Theorem.** *For any two matroids $\mathcal{M}_1 = (X, \mathcal{I}_1), \mathcal{M}_2 = (X, \mathcal{I}_2)$ with rank functions r_1 and r_2 respectively,*

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{U : U \subseteq X} (r_1(U) + r_2(X - U)).$$

Our algorithm will prove this theorem as well. We will exhibit an $I \in \cap I_1 \cap I_2$ and a set U such that

$$|I| = r_1(I \cap U) + r_2(I \cap (X - U)).$$

It will follow that I must be an optimal solution (indeed, no set can be bigger than the term on RHS). Further this will prove the matroid intersection theorem.

Exercise 4 *We are given a connected undirected graph $G = (V, E)$, and a set C of colours. Each edge in E is assigned a colour from C. We would like to know if it is possible to find a spanning tree where no two edges have the same colour. Using the matroid intersection theorem, prove that this is possible if and only if the following condition holds for any subset $C' \subset C$: let $n(C')$ be the number of connected components in G when we remove all the edges which have colour from the set C'. Then, $n(C')$ must be at most $|C'| + 1$.*

Now we describe the algorithm. We assume that we have a set $I \in \mathcal{I}_1 \cap \mathcal{I}_2$ (initially, this could be the empty set). One iteration of our algorithm will try to find another set in $\mathcal{I}_1 \cap \mathcal{I}_2$ of size $|I|+1$. To do this, we first construct a bipartite graph H which captures the notion of how we can locally modify I to get another independent set in $\mathcal{I}_1$ (or $\mathcal{I}_2$). The graph H will have elements of I on one side (say, left side) and elements of $X - I$ on the right side. There are two kinds of edges E_1 and E_2: E_1 will correspond to matroid $\mathcal{M}_1$ and E_2 to matroid $\mathcal{M}_2$. The edges of E_1 will be directed from left to right, and of E_2 will go in the other direction (from right to left). We will use the letter y to denote vertices on the left (i.e., in I) and x for those on the right.

$$E_1 = \{(y,x) : I - y + x \in \mathcal{I}_1\}, E_2 = \{(x,y) : I - y + x \in \mathcal{I}_2\}.$$

Let X_1 be the elements on the right side (i.e., in $X - U$) which can be added to I such that the set remains in $\mathcal{I}_1$, and define X_2 analogously. What if X_1 is empty? In this case, I must be a maximal independent set in $\mathcal{I}_1$, and so, there cannot be a solution of larger size. Thus, I is optimal (the matroid intersection theorem also follows by taking U to be X). So, assume X_1 (and similarly, X_2) is not empty. Further, if $x \in X_1 \cap X_2$, then adding $I + x \in \mathcal{I}_1 \cap \mathcal{I}_2$. Thus, we have obtained a solution of larger size, and our algorithm can not start another iteration. Therefore, assume that $X_1 \cap X_2 = \emptyset$.

Let P be a directed path from a vertex in X_1 to a vertex in X_2 in H – in fact among all such paths, we will pick the shortest (in number of edges) such path. It is not clear why we need a shortest path, but we will see its importance later in the analysis. The path P starts with an edge in E_2 (because edges of E_2 go from right to left, and of E_1 go in the other direction), alternated between edges of E_2 and E_1, and ends with an edge of E_1. So, if we use $e_1, e_2, \ldots, e_{2k}$ to denote the edges in the path P, then $e_1, e_3, \ldots$ belong to E_2 and $e_2, e_4, \ldots$ belong to E_1. Let the vertices in the path be $x_0, y_1, x_1, y_2, x_2, \ldots, y_k, x_k$, where $x_0, x_1, \ldots, x_k$ lie on the right side, and $y_1, y_2, \ldots, y_k$ lie on the left side (i.e., in I). So, $e_1 = (x_0, y_1), e_2 = (y_1, x_1), e_3 = (x_1, y_2)$, and so on. We would like to remove the elements $y_1, \ldots, y_k$ from I and add $x_0, \ldots, x_k$ to I, i.e., define $I' = (I - \{y_1, \ldots, y_k\}) \cup \{x_0, \ldots, x_k\}$. First of all, $|I'| = |I| + 1$, and so, if indeed I' happens to be in $\mathcal{I}_1 \cap \mathcal{I}_2$, we will be done with this iteration of our algorithm.

Why should such a set I' be in $\mathcal{I}_1 \cap \mathcal{I}_2$? This makes sense *locally*. If we want to add, say, x_1 to I, then we know that $I + x_1 - y_2 \in \mathcal{I}_2$ and $I + x_1 - y_1 \in \mathcal{I}_1$ (because $(x_1, y_2) \in E_2, (y_1, x_1) \in E_1$), and so, locally we will be fine if we remove y_1 and y_2. The non-triviality lies in showing that adding *all* of $x_0, \ldots, x_k$ and removing all of $y_1, \ldots, y_k$ still leads to an independent set in $\mathcal{I}_1 \cap \mathcal{I}_2$. In fact, this is far from obvious as the following exercise shows:

Exercise 5 *Give an example of a graphic matroid $(X, \mathcal{I})$ where the following happens: there is an independent set $I \in \mathcal{I}$, elements $y_1, y_2 \in I$ and $x_1, x_2 \notin I$ such that :*

$$I + x_1 - y_1, I + x_2 - y_2 \in \mathcal{I}, \textit{but } I + \{x_1, x_2\} - \{y_1, y_2\} \notin \mathcal{I}.$$

This is where the fact that P is a *shortest* path from X_1 to X_2 comes to our rescue. We now show that $I' \in \mathcal{I}_1$. A similar argument shows that it is in $\mathcal{I}_2$. First observe that $I + x_k - y_k \in \mathcal{I}_1$ (since $(y_k, x_k) \in \mathcal{I}_1$. Continuing in the order $k, k-1, k-2, \ldots$, we stop at the first i such that $I + \{x_k, x_{k-1}, \ldots, x_i\} - \{y_k, \ldots, y_i\} \notin \mathcal{I}_1$ (if such an i exists). Now we use the notion of span introduced at the beginning – it jus shortens many of the arguments (do the exercises involving span if you have not done them). Let J denote the set $I + \{x_k, x_{k-1}, \ldots, x_i\} - \{y_k, \ldots, y_{i+1}\}$. Since $J - x_i \in \mathcal{I}_1$ (because of the definition of i), and $J \notin \mathcal{I}$, $x_i \in \texttt{span}(J - x_i)$ (adding x_i to $J - x_i$ does not increase the rank). Consider any element of $J - x_i$. We argue that it is contained in $\texttt{span}(I - y_i)$. Indeed, any $y_j \neq y_i$ is in $I - y_i$, and so in $\texttt{span}(I - y_i)$. Consider $x_j, j > i$. Observe that $(y_i, x_j) \notin E_1$, otherwise P will not be a shortest path! This means that $I - y_i + x_j \notin \mathcal{I}_1$, i.e.,

$x_j \in \texttt{span}(I - y_i)$. Thus, we see that $J - x_i \subseteq \texttt{span}(I - y_i)$, and so, $\texttt{span}(J - x_i) \subseteq \texttt{span}(I - y_i)$. But $x_i \in \texttt{span}(J - x_i)$, and so, $x_i \in \texttt{span}(I - y_i)$. But this cannot be true, because $I - y_i + x_i \in E_1$, i.e., adding x_i to $I - y_i$ increases its rank (it leads to an independent set in $\mathcal{I}_1$). Thus, we see that no such i can exist, i.e., $J := I + \{x_1, \ldots, x_k\} - \{y_1, \ldots, y_k\} \in \mathcal{I}_1$. It remains to show that $J + x_0 \in \mathcal{I}_1$ as well. This can be used by a very similar argument as above.

Exercise 6 *Show that $J + x_0 \in \mathcal{I}_1$.*

Exercise 7 *Show that $\mathcal{I}' \in \mathcal{I}_2$.*

Thus, we have managed to get an independent set I' of larger size than I. The only situation when this cannot happen is if there is no path from X_1 to X_2 in the graph H. In this case, we need to show that I is already an optimal solution. Recall that our strategy would be to exhibit a set U for which we can show that $|I| = r_1(U) + r_2(X - U)$. We define U as the set of all elements in X which have a directed path to a vertex in X_2 in the graph H. Clearly, $X_2 \subseteq U, X_1 \cap U = \emptyset$. We now show that $r_1(U) = |I \cap U|, r_2(X - U) = |I \cap (X - U)|$, which implies that

$$|I| = |I \cap U| + |I \cap (X - U)| = r_1(U) + r_2(X - U).$$

We show the first statement, the proof of the second one is similar.

Since $I \in I_1$, we know that $I \cap U \in \mathcal{I}_1$ as well (containment property). Can U contain an independent set larger than $I \cap U$? If it does, then the exchange property shows that there is an element $x \in U - (I \cap U)$ such that $(I \cap U) + x \in \mathcal{I}_1$. Such an x will lie on the right side of H (clearly, x cannot be in I). Repeated applications of the exchange property show that we can keep on adding elements of $I - (I \cap U)$ to $I \cap U + x$ till we get an independent set of size $|I|$. Such an independent set will contain $I \cap U + x$ and all the remaining elements will be from $I - (I \cap U)$. Thus it will look like $I - x + y$, where $y \in I - (I \cap U)$. But then, $(y, x) \in E_1$. In other words, there will be a path from y to a vertex in X_2 (since there is such a path starting from x). But $y \notin U$! Thus, we get a contradiction, and so, $r_1(U) = |I \cap U|$.

Exercise 8 *Show that $r_2(U) = |I \cap (X - U)|$.*