Lecture 11: Matroid Intersection

Lecturer: Michel X. Goemans *Scribe: Jacob Steinhardt*

1 Overview

The main goal of this lecture is to prove the min-max relation from last time regarding the maximum size of a common independent set in two matroids:

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{U \subseteq S} r_1(U) + r_2(S \backslash U),$$

where r_1 and r_2 are the respective rank functions of the matroids $M_1 = (S, \mathcal{I}_1)$ and $M_2 = (S, \mathcal{I}_2)$.

As a preliminary step, we will prove the strong basis exchange property of matroids.

2 Strong Basis Exchange

Our goal is to prove the following lemma:

Lemma 1 (Strong Basis Exchange) *Let $\mathcal{B}$ be the set of all bases of a matroid $M = (S, \mathcal{I})$. Let B and B' be two elements of $\mathcal{B}$. Then for all $x \in B \backslash B'$, there exists $y \in B' \backslash B$ such that $B - x + y \in \mathcal{B}$ and $B' - y + x \in \mathcal{B}$.*

We begin with a useful definition:

Definition 1 *Given a set $A \subseteq S$ in a matroid $M = (S, \mathcal{I})$, define the* span *of A as* $\operatorname{span}(A) := \{e \in S \mid r(A + e) = r(A)\}$.

Proposition 2

1. *If $A \subseteq B$, then* $\operatorname{span}(A) \subseteq \operatorname{span}(B)$.
2. *If $e \in \operatorname{span}(A)$, then* $\operatorname{span}(A + e) = \operatorname{span}(A)$.

The proofs of 1 and 2 use the submodularity of the rank function. Recall that this is the property that

$$r(X) + r(Y) \geq r(X \cap Y) + r(X \cup Y).$$

Proof of 1: Suppose that $e \in \operatorname{span}(A)$. Then, using submodularity with $X = A + e$, $Y = B$, we get

$$r(A + e) + r(B) \geq r((A + e) \cap B) + r(B + e) \geq r(A) + r(B + e).$$

Since $e \in \operatorname{span}(A)$, we have $r(A) = r(A + e)$, hence $r(B) \geq r(B + e)$. This implies that $r(B) = r(B + e)$, so $e \in \operatorname{span}(B)$. Thus $e \in \operatorname{span}(B)$ whenever $e \in \operatorname{span}(A)$, so $\operatorname{span}(A) \subseteq \operatorname{span}(B)$, as claimed. $\square$

Proof of 2: By 1, we know that $\mathrm{span}(A) \subseteq \mathrm{span}(A+e)$, so we need only show that $\mathrm{span}(A+e) \subseteq \mathrm{span}(A)$. So suppose that $e \in \mathrm{span}(A)$ and that $f \in \mathrm{span}(A+e)$. We need to show that $f \in \mathrm{span}(A)$. If we let $X = A+e$ and $Y = A+f$, then using submodularity we see that

$$r(A+e)+r(A+f) \geq r(A+e+f)+r((A+e)\cap(A+f)) \geq r(A+e+f)+r(A).$$

Since $e \in \mathrm{span}(A)$, $r(A) = r(A+e)$, so we get

$$r(A+f) \geq r(A+e+f),$$

which implies that $r(A+f) = r(A+e+f)$. But $f \in \mathrm{span}(A+e)$, so $r(A+e+f) = r(A+e)$. Then $e \in \mathrm{span}(A)$, so $r(A+e) = r(A)$. Hence $r(A+f) = r(A)$, so $f \in \mathrm{span}(A)$, as was to be shown. □

As a corollary to the above proposition, we have:

Corollary 3 $\mathrm{span}(\mathrm{span}(A)) = \mathrm{span}(A)$.

Proof: Add all of the elements of $\mathrm{span}(A)\backslash A$ to A. By part 2, this won't change the span. □

We are now ready to prove the strong basis exchange lemma.

Proof of lemma: Suppose $x \in B\backslash B'$. Since B' is a basis, $B'+x$ contains a unique circuit C, and C must contain x (since any subset of B' would be independent). We then conclude that $x \in \mathrm{span}(C-x)$, which implies that also $x \in \mathrm{span}((B\cup C)-x)$. By the proposition, then, $\mathrm{span}((B\cup C)-x) = \mathrm{span}(B\cup C) = S$, where the last step follows since B is a basis. Hence $B\cup C-x$ contains a basis, call it B''. Then $B-x$ and B'' are both independent, and $|B''| > |B-x|$. Hence there exists $y \in B''\backslash(B-x)$ such that $(B-x)+y \in \mathcal{B}$. But $B''\backslash(B-x) \subseteq ((B\cup C)-x)\backslash(B-x) \subseteq C-x$, so there exists $y \in C-x$ such that $(B-x)+y \in \mathcal{B}$. On the other hand, since C is a circuit and $x, y \in C$, it follows that $(B'-y)+x \in \mathcal{B}$, so that we have established the lemma. □

3 Matroid Intersection

Recall our goal, which is to prove:

Theorem 4 (Min-max Formula)

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

We will prove this min-max formula by providing an algorithm that returns sets I and U that have equality in the above formula (we proved last time that $|I| \leq r_1(U)+r_2(S\backslash U)$ for all $I \in \mathcal{I}_1\cap\mathcal{I}_2$ and all $U \subseteq S$). For the algorithm, we will start with $I = \emptyset$ and at each step either augment I or produce a U that gives equality. Our algorithm will rely heavily on a structure called the exchange graph.

Definition 2 *Given a matroid $M = (S, \mathcal{I})$ and an independent set $I \in \mathcal{I}$, the* exchange graph *$\mathcal{D}_M(I)$ (or just $\mathcal{D}(I)$) is the bipartite graph with bipartition I and $S \backslash I$ with an edge between $y \in I$ and $x \in S \backslash I$ if $I - y + x \in \mathcal{I}$.*

Lemma 5 *Let I and J be two independent sets in M with $|I| = |J|$. Then there exists a perfect matching between $I \backslash J$ and $J \backslash I$ in $\mathcal{D}_M(I)$.*

Proof: Start by defining the truncated matroid $M' = (S, \{I' \in \mathcal{I} \mid |I'| \leq |I|\})$. Then I and J are bases in M'. Take $x \in J \backslash I$. By the strong basis exchange lemma, there exists $y \in I \backslash J$ such that $I - y + x \in \mathcal{B}$ and $J - x + y \in \mathcal{B}$, where $\mathcal{B}$ is the set of bases of M'. In particular, $I - y + x$ and $J - x + y$ are independent in M. It follows that (y, x) is an edge in $\mathcal{D}_M(I)$. We can now replace I, J with $I, J - x + y$ and induct (as $I \backslash (J - x + y)$ has one less element than $I \backslash J$), and we will eventually end up with a perfect matching. Note that we needed strong basis exchange, not just weak basis exchange, to ensure both that $I - y + x$ would be independent to get an edge in $\mathcal{D}_M(I)$ and that $J - x + y$ would be independent for the induction. $\square$

The converse to Lemma 5 does not hold as can be easily seen. We next prove a proposition that is a partial converse to the above lemma.

Proposition 6 *Let $I \in \mathcal{I}$ with exchange graph $\mathcal{D}_M(I)$. Let J be a set with $|J| = |I|$ and such that $\mathcal{D}_M(I)$ has a* unique *matching between $I \backslash J$ and $J \backslash I$. Then $J \in \mathcal{I}$.*

Proof: Let N be the unique matching. Orient edges in N from $S \backslash I$ to I, and orient the rest from I to $S \backslash I$. The uniqueness of the matching implies that there is no directed cycle in this orientation of $\mathcal{D}_M(I)$. Hence $\mathcal{D}_M(I)$ is a directed acyclic graph, so we can number the vertices so that all edges point from smaller-numbered vertices to larger-numbered vertices (for example, by performing a topological sort). So, number $J \backslash I$ and $I \backslash J$ such that $N = \{(y_1, x_1), (y_2, x_2), \ldots, (y_t, x_t)\}$ and such that (y_i, x_j) is never an edge for $i < j$.

Now suppose for the sake of contradiction that $J \notin \mathcal{I}$. Then J has a circuit C. Take the smallest i such that $x_i \in C$ (there must exist at least one element of C in $J \backslash I$ since $C \subseteq J$ and I is independent). By construction, (y_i, x) is not an arc for $x \in C - x_i$. This implies that $x \in \text{span}(I - y_i)$ for all $x \in C - x_i$. Hence $C - x_i \subseteq \text{span}(I - y_i)$, so $\text{span}(C - x_i) \subseteq \text{span}(\text{span}(I - y_i)) = \text{span}(I - y_i)$. C is a cycle, so $x_i \in \text{span}(C - x_i)$, so $x_i \in \text{span}(I - y_i)$. This is a contradiction, since $(x_i, y_i) \in \mathcal{D}_M(I)$ by assumption. Therefore J must be in $\mathcal{I}$, which proves the proposition. $\square$

We are now ready to describe the algorithm for proving the Min-Max Formula. First, we define a new type of exchange graph.

Definition 3 *For $I \in \mathcal{I}_1 \cap \mathcal{I}_2$, the exchange graph $\mathcal{D}_{M_1,M_2}(I)$ is the directed bipartite graph with bipartition I and $S \backslash I$ such that (y, x) is an arc if $I - y + x \in \mathcal{I}_1$ and (x, y) is an arc if $I - y + x \in \mathcal{I}_2$.*

Also define $X_1 := \{x \notin I \mid I + x \in \mathcal{I}_1\}$ and $X_2 := \{x \notin I \mid I + x \in \mathcal{I}_2\}$. Then the algorithm is to find a path (we call it an *augmenting path*) from X_1 to X_2 that does not contain any shortcuts (arcs that point from an earlier vertex on the path to a non-adjacent later vertex on the path). Then replace I with $I \triangle P$, where P is the set of vertices on the path. As a special case, if $X_1 \cap X_2 \neq \emptyset$, then we end up with a path that consists of a singleton vertex and we can just add that element to I. If there is no such path, then set $U := \{z \in S \mid z \text{ can reach some vertex in } X_2 \text{ in } \mathcal{D}_{M_1,M_2}(I)\}$.

To prove that this algorithm is correct, we need to show that

1. When we stop, the sets I and U do indeed give equality in the Min-Max Formula.

2. At each stage in the algorithm, $I \triangle P \in \mathcal{I}_1 \cap \mathcal{I}_2$.

Proof of 1: First note that $X_2 \subseteq U$ and that $X_1 \cap U = \emptyset$ (as otherwise we could keep running out algorithm to increase the size of I). We claim that $r_1(U) = |I \cap U|$ and $r_2(S \backslash U) = |I \cap (S \backslash U)|$. Together, these would imply that $|I| = r_1(U) + r_2(S \backslash U)$, which is what we need.

Suppose first that $|I \cap U| \neq r_1(U)$. Since $I \cap U \subseteq U$ and $I \cap U$ is independent, this would imply that $|I \cap U| < r_1(U)$. Then there would have to exist some $x \in U \backslash I$ such that $(I \cap U) + x \in \mathcal{I}_1$. Then $\{x\}$ is not a singleton independent set, so $I + x$ is either independent or contains a unique cycle, which contains at least one element not in $(I \cap U) + x$; either way we can find $y \in I \backslash U$ such that $I - y + x \in \mathcal{I}_1$. But then (y, x) is an arc in $\mathcal{D}_{M_1,M_2}(I)$, so $y \in U$ (since $x \in U$). This is a contradiction, so we must have $|I \cap U| = r_1(U)$.

Now suppose that $|I \cap (S \backslash U)| \neq r_2(S \backslash U)$. Then as before we must have $|I \cap (S \backslash U)| < r_2(S \backslash U)$. Thus there exists $x \in (S \backslash U) \backslash I$ such that $(I \cap (S \backslash U)) + x \in \mathcal{I}_2$. So, by the same logic as before, we can find $y \in I \backslash (S \backslash U)$ such that $I - y + x \in \mathcal{I}_2$. But $I \backslash (S \backslash U) = I \cap U$, so we have $y \in I \cap U$ such that $I - y + x \in \mathcal{I}_2$. But then (x, y) is an arc in $\mathcal{D}_{M_1,M_2}(I)$, so $x \in U$ (since $y \in U$). This is a contradiction, so we must have $|I \cap (S \backslash U)| = r_2(S \backslash U)$. $\square$

Proof of 2: Recall that we need to show that $I \triangle P \in \mathcal{I}_1 \cap \mathcal{I}_2$ whenever P is a path from X_1 to X_2 with no shortcuts. We first show that $I \triangle P \in \mathcal{I}_1$. We start by definining a new matroid M_1' from M_1 as $M_1' := (S \cup \{t\}, \{J \mid J \backslash \{t\} \in \mathcal{I}_1\}$. In other words, we simply add a new element $\{t\}$ that is independent from all the other elements of the matroid. Then we know that $I \cup \{t\}$ is independent in M_1' and M_2' (where we define M_2' analogously to M_1'). On the other hand, if we view $\mathcal{D}_{M_1'}(I \cup \{t\})$ as a subgraph of $\mathcal{D}_{M_1',M_2'}(I \cup \{t\})$, then there exists a perfect matching in $\mathcal{D}_{M_1'}(I \cup \{t\})$ between $(I \cap P) \cup \{t\}$ and $P \backslash I$ (given by the arcs in P that are also arcs in $\mathcal{D}_{M_1'}(I \cup \{t\})$, together with the arc between $\{t\}$ and the first vertex in P). Furthermore, this matching is unique since P has no shortcuts, so by the proposition we know that $(I \cup \{t\}) \triangle P$ is independent in M_1', hence $I \triangle P$ is independent in M_1.

The proof that $I \triangle P \in \mathcal{I}_2$ is identical, except that this time the matching consists of the arcs in P that are also arcs in $\mathcal{D}_{M_2'}(I \cup \{t\})$, together with the arc between $\{t\}$ and the *last* vertex in P (rather than the first). $\square$

So, we have proved that our algorithm is correct, and as a consequence have established the Min-Max Formula.

4 Runtime of the Matroid Intersection Algorithm

Let $r = \max(r_1(S), r_2(S))$ and $n = |S|$. We can construct $\mathcal{D}_{M_1,M_2}(I)$ in $O(rn)$ oracle calls. We can also find augmenting paths in $O(rn)$ time. We will have to augment at most r times before we obtain a maximum independent set. Thus our algorithm takes $O(r^2 n)$ oracle calls and time.

Remark 1 *Cunningham has shown that we can find a maximum independent set with $O(r^{1.5}n)$ oracle calls. The idea is to take a shortest augmenting path each time.*

5 Weighted Matroid Intersection

We now define the weighted version of the matroid intersection problem and outline an algorithm for solving it.

Given a weight function $w : S \to \mathbb{R}$ and two matroids M_1 and M_2 with ground set S, the weighted matroid intersection problem is the problem of computing

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} \sum_{e \in I} w(e).$$

The algorithm for solving weighted matroid intersection is similar to the unweighted version of the algorithm. We start by defining an independent set I of a matroid to be *extreme* if for all $J \in \mathcal{I}$ with $|J| = |I|$ we have $w(J) \leq w(I)$. In other words, I is extreme if it has the maximum weight of all independent sets of its cardinality. We also define a length function on the vertices of the exchange graph:

$$l(x) = \begin{cases} w(x) & x \in I \\ -w(x) & x \notin I. \end{cases}$$

Now instead of finding an augmenting path without shortcuts, we find the shortest augmenting path, first based on $l(x)$, then based on the number of arcs in the path. We can show that there are no negative cycles in this graph, so that this problem can be solved with the Bellman-Ford algorithm.

6 Weighted Min-Max

We also have a weighted version of the Min-Max Formula:

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} \sum_{e \in I} w(e) = \min_{w_1, w_2 : w_1(x) + w_2(x) = w(x) \forall x} \left(\max_{I \in \mathcal{I}_1} w_1(I) \right) + \left(\max_{I \in \mathcal{I}_2} w_2(I) \right).$$

Furthermore, we can choose w_1 and w_2 to be integer-valued functions provided that w is an integer-valued function.