Matroid Theory

Evan Simanovskis Andrew Tam Robert Chung
University of Toronto Scarborough
Toronto, ON M1C 1A4

July 29, 2026

1 Introduction

This document was written to explain the theory needed to understand the correctness of the matroid intersection and second-best spanning tree algorithms. It's expected that you've read the USACO Guide modules on matroids and matroid intersection as we will use the definitions and examples introduced there. Specifically, you should know what the matroid intersection algorithm is. This is a long document, but bear in mind it is completely self-contained apart from the definition of a matroid/independent-set and a description of the matroid intersection algorithm.

2 Credit

- Almost all of the definitions, results, and proofs are taken from A First Course in Combinatorial Optimization by Jon Lee
- The proof of strong basis exchange is from notes provided by MIT
- The proof of 'termination implies optimality' is from notes provided by the University of Illinois Urbana-Champaign

The presentation is mostly our own. Some proofs have been modified or simplified to make them easier to understand.

3 Matroid Theory

3.1 Circuits

A circuit in a matroid generalizes the concept of a cycle of edges in a graphical matroid.

Definition 1. A circuit is a dependent set C such that every proper subset of C is independent.

Remark 1. A set is dependent iff it contains a circuit.

Proposition 3.1 (Circuit Elimination)**.** *Let X and Y be distinct circuits both containing e. Then, $(X \cup Y) - e$ is dependent.*

Proof. Suppose for contradiction that $(X \cup Y) - e$ is independent. To obtain a contradiction, we'll construct an independent set inside $X \cup Y$ whose cardinality is less than $(X \cup Y) - e$, but also cannot be extended.

Recall that $X \neq Y$. Moreover, we don't have $X \subset Y$ or $Y \subset X$ because circuits are minimal in terms of containment. Hence, we can pick an element $x \in X \setminus Y$.

Next, let W be a maximum cardinality independent set inside of $X \cup Y$ that contains $X - x$. Observe that W cannot contain all of Y because Y is dependent and W is independent (by assumption). Hence, we can find $y \in Y \setminus W$.

Therefore,

$$|W| \leq |X \cup Y| - 2 \text{ since } W \text{ doesn't contain } x \text{ and } y$$

However, we assumed that $(X \cup Y) - e$ is independent. So, there exists some element $z \in ((X \cup Y) - e) \setminus W$ that we could add to W to make it even larger. Furthermore, $z \neq x$ because W contains $X - x$ and X is dependent. This contradicts the fact that W's cardinality is maximum provided it contains $X - x$. $\square$

The following lemma generalizes the fact that if you take a spanning tree of a graph and add an edge, the resulting graph contains a unique cycle.

Lemma 3.2 (Unique Circuit)**.** *Suppose I is independent and $I+x$ is dependent. Then, there exists a unique circuit $C \subseteq I + x$. Furthermore, $x \in C$.*

Proof. The existence of a circuit follows immediately because $I+x$ is dependent. Hence, there exists a minimally dependent subset. Also, the fact that $x \in C$ is easy because if not, then $C \subseteq I$ and C is dependent, contradicting the heredity axiom.

To see uniqueness, suppose there are distinct circuits C_1 and C_2 in $I + x$. By the above reasoning, $x \in C_1 \cap C_2$. Applying the circuit elimination property, we find that $(C_1 \cup C_2) - x$ is dependent. However, $(C_1 \cup C_2) - x \subseteq I$. This is a contradiction since I is independent. $\square$

3.2 Rank

The rank of a set of elements is defined in a way that generalizes the rank of a set of vectors in linear algebra (as the maximum cardinality of a linearly independent subset).

Definition 2 (Rank)**.** Let X be a subset of elements. Its rank is:

$$r(X) = \max \left\{ |I| : I \subseteq X \text{ and } I \text{ is independent} \right\}$$

We denote the rank of the entire ground set of a matroid M as $r(M)$.

The following are natural properties from linear algebra. Submodularity says that adding an element to a set will increase its rank *more* than if we add that element to a superset.

Proposition 3.3. *The following holds of the rank:*

1. *If* $A \subseteq B$*, then* $r(A) \leq r(B)$
2. *Submodularity*[1]*: If* $A \subseteq B$ *and* e *is an element, then:* $r(A + e) - r(A) \geq r(B + e) - r(B)$

Proof of 1. Let $I \subseteq A$ so that I is an independent set with maximum cardinality. By definition,

$$r(A) = |I| \leq r(B)$$

since we also have $I \subseteq B$. □

Proof of 2. Notice that $0 \leq r(A+e) - r(A) \leq 1$ for any A and e. This is because adding an element cannot cause the rank to decrease, and it can cause the rank to increase by at most 1.

Hence if $r(A+e) - r(A) = 1$, we're done. So, suppose $r(A+e) = r(A)$. We'd like to show that $r(B + e) = r(B)$ (it can't be negative as stated above). To do that, let I_A be a max cardinality independent set in A. Using the exchange axiom repeatedly, we may extend it to a max cardinality independent set in B: $I_A \subseteq I_B$.

Suppose for contradiction that $I_B + e$ is independent. Then, $I_A + e \subseteq I_B + e$ is independent as well, by the matroid axioms. This contradicts that $r(A) = r(A + e)$, so we must have that $I_B + e$ is dependent.

Hence, I_B is a *maximal* independent set in $B + e$. This implies that it's a max cardinality independent set in $B + e$ by the exchange axiom. Hence, $r(B + e) = |I_B| = r(B)$. □

[1] You may have seen another definition of submodularity. Namely: $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ for any subsets A, B. This is actually *equivalent* to our definition. The proof of equivalence essentially just adds one element at a time to build this inequality. We won't need it, but you can read about it on pages 421-422 here.

3.3 Span

We can define the span of a set of elements in a way motivated by linear algebra.

Definition 3 (Span)**.** Let $A \subseteq S$ be a subset of elements. Then:

$$\mathrm{span}(A) = \Big\{ x : r(A+x) = r(A) \Big\}$$

The following span properties come directly from the rank properties we've just established.

Proposition 3.4. *The following holds of the span:*

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

Proof of 1. Let $e \in \mathrm{span}(A)$, so $r(A+e) = r(A)$. We want to prove that $r(B+e) = r(B)$. Recall that submodularity says: $r(A+e) - r(A) \geq r(B+e) - r(B)$. So: $0 \geq r(B+e) - r(B)$ which implies that $r(B) \geq r(B+e)$. We also know that $r(B) \leq r(B+e)$ by rank properties, so: $r(B) = r(B+e)$. □

Proof of 2. By 1, we know $\mathrm{span}(A) \subseteq \mathrm{span}(A+e)$ so we just need to show the reverse containment. Let $f \in \mathrm{span}(A+e)$, so: $r((A+e)+f) = r(A+e)$.

To show that $f \in \mathrm{span}(A)$, we must prove that: $r(A+f) = r(A)$. By properties of the rank function, we have $r(A) \leq r(A+f)$. To get the opposite inequality:

$$\begin{aligned} r(A+f) &\leq r((A+e)+f) \text{ by prop. of the rank function} \\ &= r(A+e) \text{ by def. of } f \in \mathrm{span}(A+e) \\ &= r(A) \text{ by def. of } e \in \mathrm{span}(A) \end{aligned}$$

Hence, $r(A+f) = r(A)$, implying: $f \in \mathrm{span}(A)$. □

The following lemma will be very useful in matroid intersection, among other things.

Lemma 3.5 (Strong Basis Exchange)**.** *Let B_1 and B_2 be bases of a matroid. For all $x \in B_1 \setminus B_2$, there exists $y \in B_2 \setminus B_1$ such that the following are also bases:*

- $B_1 - x + y$
- $B_2 - y + x$

Proof. Let $x \in B_1 \setminus B_2$. Observe that $B_2 + x$ contains a unique circuit C, and $x \in C$ (by circuit properties). Notice that if we pick any $y \in C$, then $B_2 - y + x$ would be independent (and hence a basis) as we eliminate the only circuit $B_2 + x$ has.

We need to show that there exists a choice of $y \in C \setminus B_1$ such that $B_1 - x + y$ is independent as well.

Let's reason about this intuitively using the idea of span, and then we'll prove it formally. Notice that as C is dependent, $x \in \text{span}(C - x)$. Hence, we should be able to *replace* x inside B_1 with $C - x$ in order to have a set of elements spanning the entire matroid (recall that B_1 originally has this property as it's a basis). Since we are only replacing one element x, it is reasonable to guess that a single element $y \in C - x$ is enough to take its place.

Formally, if there exists a basis inside $(B_1 \cup C) - x$, then we would be able to extend $B_1 - x \subseteq (B_1 \cup C) - x$ using some element $y \in ((B_1 \cup C) - x) \setminus (B_1 - x)$ so that $B_1 - x + y$ is a basis, too. Observe:

$$((B_1 \cup C) - x) \setminus (B_1 - x) = (B_1 \cup C) \setminus B_1 = C \setminus B_1$$

Therefore, it's sufficient to show that the rank of $(B_1 \cup C) - x$ is the full rank of the matroid (and hence contains a basis). To see this, note that $x \in \text{span}(C - x)$ as discussed earlier. This implies that $x \in \text{span}((B_1 \cup C) - x)$ by span properties. Lastly:

$$\begin{aligned} r((B_1 \cup C) - x) &= r(B_1 \cup C) \text{ as } x \in \text{span}((B_1 \cup C) - x) \\ &= r(M) \text{ as } B_1 \text{ is a basis} \end{aligned}$$

$\square$

4 Matroid Intersection

We will use the following fact about matchings in bipartite graphs.

Lemma 4.1 (Unique Matching Implies Crucial Edge)**.** *Let $G = (V, E)$ be an undirected graph with bipartition: $V_1 \sqcup V_2 = V$. If $V_1 \neq \emptyset$ and G has a unique matching X that covers all vertices in V_1, then there exists an edge $\{v_1, v_2\} \in X$ where $v_1 \in V_1$ and $v_2 \in V_2$ such that:*

$$\{v_1, v_2'\} \notin E \quad \forall v_2' \in V_2 - v_2$$

We call the edge $\{v_1, v_2\}$ crucial. In other words, there exists a degree 1 vertex in V_1.

Proof. Suppose for contradiction that there is no crucial edge. For each vertex $v \in V_1$, pick any edge incident to v that is not used in the matching (one is guaranteed to exist because there is no crucial edge), and let the set of all such edges be Y. We will get a contradiction by creating another matching covering all vertices in V_1 by swapping out some edges from X with edges from Y.

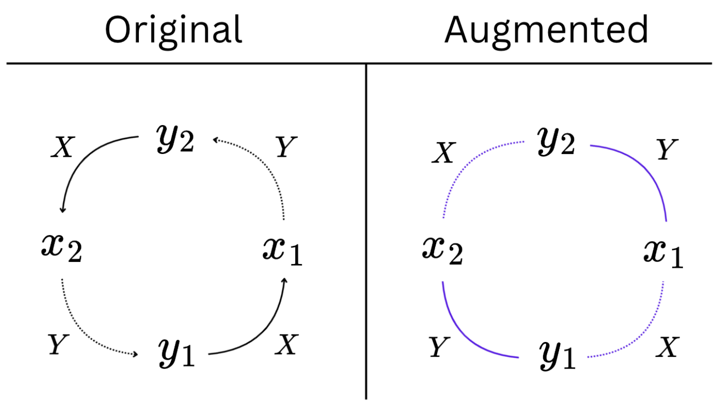
To this end, we build a simple path or simple cycle (depending on how we terminate) with the following process:

1. Set our current vertex to some $y \in V_2$ which is matched in X and start with the sequence of vertices: $P = (y)$
2. Repeat the following steps:
   (a) Let $x \in V_1$ be the vertex matched to our current vertex $y \in V_2$, terminating if there is not such a vertex.
   (b) Let $y' \in V_2$ be the unique vertex that x is adjacent to according to Y.
   (c) Add x and y' to P in that order, and set $y := y'$ to be our new current vertex.
   (d) If we've already seen this y, then we remove vertices from the beginning of P so that it starts with the first occurrence of y and ends with this new occurrence of y. Then, we stop.

Observe that by doing this algorithm, we never repeat any vertices until possibly at the very end. Notably, we don't repeat any vertices in V_1 because the only way for us to reach a vertex in V_1 is by taking its corresponding edge in the matching X from the V_2 side. So, we must've already repeated a vertex in V_2 first, in which case, we would have exited according to step (d).

There are now two cases for how we construct a new matching, depending on how the above algorithm terminates. First, suppose the algorithm terminates by repeating a vertex. We repeat only at the very end, so we obtain a simple cycle. Depicted below is an example consisting of 4 edges.

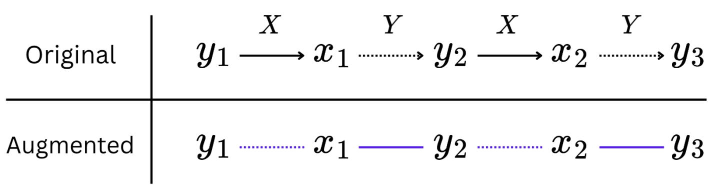
$$P = (y_1, x_1, y_2, x_2, y_1)$$



We can create an 'augmented' matching by taking the symmetric difference of X and the edges in P.

Now, suppose the algorithm terminates by finding a vertex in V_2 that is not matched to any V_1 in X. Then, we have a simple path. An example with 4 edges is shown below.

$$P = (y_1, x_1, y_2, x_2, y_3)$$



We again create an augmented matching by taking the symmetric difference of X and the edges in P. In the prior case, it was easy to see why we still got a matching after augmenting along the cycle. In this case, we need to observe that the last vertex in our path (y_3 in the example) is not matched in X by the termination condition of our algorithm. Hence, we get a matching after augmenting, and it still covers all of V_1. □

Definition 4 (Bipartite Exchange Graph)**.** Let M be a matroid. The bipartite exchange graph with respect to the independent set S is denoted: $\mathcal{G}_M(S)$ and is defined as the following undirected graph:

- Its vertex set is the ground set of the matroid: $E(M)$
- It has bipartition: $S \sqcup (E(M) \setminus S)$
- For $e \in S$ and $f \notin S$, $\{e, f\}$ is an edge iff $S - e + f$ is independent

The following lemma for bipartite exchange graphs will be useful for proving that the augmenting paths choosen by matroid intersection algorithm always yield independent sets.

Lemma 4.2 (Unique Perfect Matching Implies Exchange)**.** *Let $S, T \subseteq E(M)$ such that:*

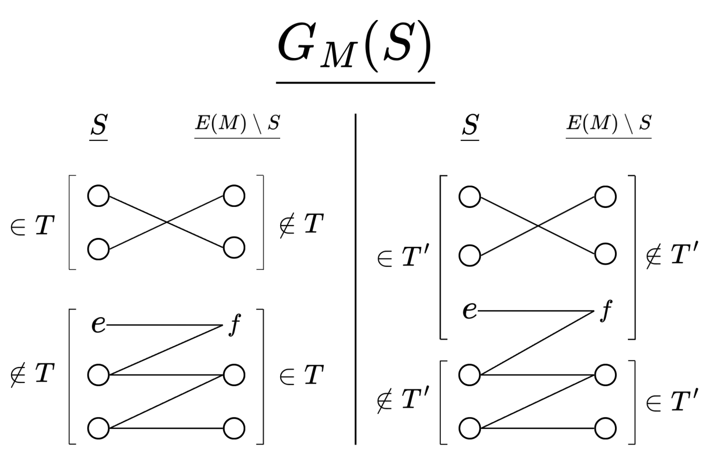
1. $|S| = |T|$
2. *S is independent*
3. *$\mathcal{G}_M(S)$ contains a unique perfect matching between $S \setminus T$ and $T \setminus S$*

Then, T is independent.

Proof. We will prove the statement inductively on the cardinality: $|S \setminus T| = |T \setminus S|$. If $|S \setminus T| = |T \setminus S| = 0$, then $S = T$. Hence, T is independent.

Next, let S, T be arbitrary such that $|S \setminus T| \geq 1$ and assume the statement holds for smaller cardinalities. First, since we have a unique perfect matching, let $\{e, f\}$ be a crucial edge (as in 4.1) for $e \in S \setminus T$ and $f \in T \setminus S$.

Observe by the diagram that if we define $T' := T - f + e$, then: $S \setminus T' = S \setminus T - e$ and $T' \setminus S = T \setminus S - f$. As an immediate consequence, we get $|S \setminus T'| = |T' \setminus S| = |S \setminus T| - 1$. See the diagram below for an illustration.



Furthermore, we can construct a perfect matching between $S \setminus T'$ and $T' \setminus S$ in $\mathcal{G}_M(S)$ by simply removing the edge $\{e, f\}$ from our original perfect matching. Observe that this perfect matching is unique. If it's not, then we can add back $\{e, f\}$ to get a contradiction.

Hence by the induction hypothesis, $T - f + e$ is independent, which implies that $T - f$ is independent. To show that we can add f to $T - f$ and get an independent set, we'll use the exchange axiom with $S - e + f$ (this is independent by definition of the exchange graph). Doing this, we obtain $\tilde{f} \in (S - e + f) \setminus (T - f)$ such that $T - f + \tilde{f}$ is independent. If we're lucky, then we would have $\tilde{f} = f$ and be done immediately. Suppose for contradiction that $\tilde{f} \neq f$. It follows that we have $\tilde{f} \in (S - e) \setminus (T - f)$ such that $T - f + \tilde{f}$ is independent.

Notice that we've never actually used our *crucial* edge yet. Therefore, one way to get a contradiction would be to find some $\tilde{e} \in T \setminus S$ distinct from f such that $S - e + \tilde{e}$ is independent. Notice that it would be possible to do this if we could extend the independent set $S - e$ using an $\tilde{e} \in (T \setminus S) - f$. However:

$$\begin{aligned}(T \setminus S) - f &= (T - f) \setminus S \\ &= (T - f) \setminus (S - e) \text{ as } e \notin T\end{aligned}$$

Therefore, it would be a contradiction if $r((T - f) \cup (S - e)) > r(S - e)$ because then we would be able to extend $S - e$ using some $\tilde{e} \in ((T - f) \cup (S - e)) \setminus (S - e) = (T - f) \setminus (S - e)$. Finally:

$$\begin{aligned}r((T - f) \cup (S - e)) &\geq r(T - f + \tilde{f}) \text{ by rank prop. as } \tilde{f} \in S - e \\ &= |T| \text{ as } T - f + \tilde{f} \text{ is independent} \\ &= |S| \text{ as we assume } S \text{ and } T \text{ have the same cardinality} \\ &> |S - e| \text{ as } e \in S\end{aligned}$$

□

Recall the following definition:

Definition 5 (Bipartite Augmentation Digraph)**.** Let M_1 and M_2 be matroids over the common ground set E. The bipartite augmentation directed graph with respect to the independent set $S \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)$ is denoted: $\mathcal{G}_{M_1,M_2}(S)$ and is defined as follows:

- Its vertex set is the common ground set: E
- It has bipartition: $S \sqcup (E \setminus S)$
- For $e \in S$ and $f \notin S$:
  - (e, f) is an edge iff $S - e + f \in \mathcal{I}(M_1)$
  - (f, e) is an edge iff $S - e + f \in \mathcal{I}(M_2)$

We give names to special vertices:

- A *source* is an element $f \in E \setminus S$ such that $S + f \in \mathcal{I}(M_1)$.
- A *sink* is an element $f \in E \setminus S$ such that $S + f \in \mathcal{I}(M_2)$.

Definition 6 (Augmenting Path)**.** In the context of the above definition, we define an *augmenting path* to be a path from a source to a sink: $(f_0, e_1, f_1, e_2, f_2, \ldots, e_n, f_n)$ with the property that: $S - \{e_1, \ldots, e_n\} + \{f_0, \ldots, f_n\} \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)$.

The following theorem proves that after each iteration of our algorithm, we still have an independent set in both matroids.

Theorem 4.3 (Shortest Implies Augmenting)**.** *Let M_1 and M_2 be matroids over the common ground set E and let $S \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)$. Then, if $(f_0, e_1, f_1, \ldots, e_n, f_n)$ is a shortest source-sink path in $\mathcal{G}_{M_1,M_2}(S)$, then it's an augmenting path.*

Proof. We'll show that $S - \{e_1, \ldots, e_n\} + \{f_0, \ldots, f_n\}$ is independent in M_1 and M_2 separately. To see independence in M_1, we'll do it in two steps. First, we prove that: $S - \{e_1, \ldots, e_n\} + \{f_1, \ldots, f_n\} \in \mathcal{I}(M_1)$ our using unique perfect matching lemma. Then, we'll show that we can add f_0 and remain independent. It will be very similar to prove independence in M_2.

We claim that there exists a unique perfect matching between $\{e_1, \ldots, e_n\}$ and $\{f_1, \ldots, f_n\}$ in $\mathcal{G}_{M_1}(S)$ (*not* in the augmentation digraph). We definitely have a perfect matching because the edges extending from $S \to E \setminus S$ in the bipartite augmentation digraph are the same as those edges in $\mathcal{G}_{M_1}(S)$. For example in the diagram to the right, we have $e_1 \to f_1$, $e_2 \to f_2$, and $e_3 \to f_3$ forming a perfect matching. To see that it's unique, suppose for contradiction that we have *another* perfect matching in $\mathcal{G}_{M_1}(S)$. In this different matching, we must have some e_i matched to an f_j where $i < j$. However, that implies (e_i, f_j) is an edge in $\mathcal{G}_{M_1,M_2}(S)$ which contradicts the fact that we have a *shortest* source-sink path.

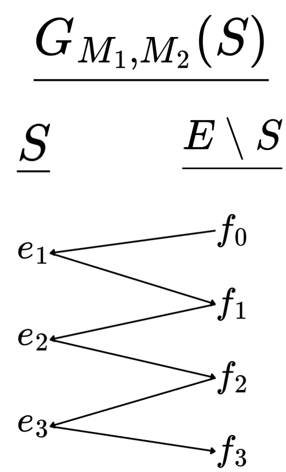


Figure 1: The path in $\mathcal{G}_{M_1,M_2}(S)$ if $n = 3$

Now, if we define $T := S - \{e_1, \ldots, e_n\} + \{f_1, \ldots, f_n\}$. Observe that:

- $|S| = |T|$
- $S \setminus T = \{e_1, \ldots, e_n\}$

- $T \setminus S = \{f_1, \ldots, f_n\}$

We've already seen that there's a unique perfect matching between the above two sets of vertices in $\mathcal{G}_{M_1}(S)$. Hence, by the unique perfect matching implies exchange lemma, we know that $T \in \mathcal{I}(M_1)$.

To show that $T + f_0 \in \mathcal{I}(M_1)$ (what we originally wanted), first note that *none* of $f_1, \ldots, f_n$ are sources (otherwise we would want to start our shortest path there instead of f_0). Hence, $f_i \in \text{span}(S)$ for all $i \in [1, n]$. By repeatedly using our span properties, we see that $\text{span}(S) = \text{span}(S + \{f_1, \ldots, f_n\})$. Moreover, f_0 is a source. So, $f_0 \notin \text{span}(S) = \text{span}(S + \{f_1, \ldots, f_n\})$. Lastly:

$\text{span}(S - \{e_1, \ldots, e_n\} + \{f_1, \ldots, f_n\}) \subseteq \text{span}(S + \{f_1, \ldots, f_n\})$ by span properties.

As we've seen that $f_0 \notin \text{span}(S + \{f_1, \ldots, f_n\})$, that implies $f_0 \notin \text{span}(S - \{e_1, \ldots, e_n\} + \{f_1, \ldots, f_n\})$. Hence by definition, $S - \{e_1, \ldots, e_n\} + \{f_0, \ldots, f_n\} \in \mathcal{I}(M_1)$.

Proving that $S - \{e_1, \ldots, e_n\} + \{f_0, \ldots, f_n\}$ is independent in M_2 is mostly symmetric, so we'll highlight exactly what parts of the argument change.

First, we'll instead have a unique perfect matching between $\{e_1, \ldots, e_n\}$ and $\{f_0, \ldots, f_{n-1}\}$ in $\mathcal{G}_{M_2}(S)$ because we have the edges $f_i \to e_{i+1}$ for $i \in [0, n)$ (this should be more clear from the diagram). Uniqueness follows exactly the same way, if there was another perfect matching in $\mathcal{G}_{M_2}(S)$, then we must match an e_i to an f_j with $i - j > 1$, implying the existence of a shorter source-sink path (the diagram should clarify this as well).

Lastly, we instead add f_n instead of f_0 like before. The argument is exactly the same apart from that detail, we use the fact that none of $f_0, \ldots, f_{n-1}$ are sinks (if they were, we'd have a shorter source-sink path), and we use that f_n is a sink.

Hence, $S - \{e_1, \ldots, e_n\} + \{f_0, \ldots, f_n\} \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)$. $\square$

In order to prove that upon termination we have a *maximum* cardinality independent set in both matroids, we will appeal to duality. It will be helpful to compare the argument to the proof of optimality of Ford-Fulkerson. For that algorithm, we prove that the value of every flow is at most the size of every cut. Hence, to prove that our flow is maximum, it's sufficient to exhibit a cut whose size is the same. This is exactly how the standard proof of optimality of Ford-Fulkerson works, and this is what we'll do for Edmonds' matroid intersection algorithm.

The following will be the equivalent of weak-duality (flows are less than or equal to cuts) for matroids.

Lemma 4.4 (Weak Matroid Intersection)**.** *Let M_1 and M_2 be matroids over the common ground set E. Then:*

$$\max\left\{|S| : S \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)\right\} \leq \min\left\{r_1(A) + r_2(B) : A \cup B = E\right\}$$

where r_1 and r_2 are the rank functions of matroids M_1 and M_2 respectively.

Proof. Let $S \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)$ and $A \cup B = E$. Then:

$$\begin{aligned}|S| &\leq |S \cap A| + |S \cap B| \text{ since } A \cup B = E \text{ and } S \subseteq E \\ &= r_1(S \cap A) + r_2(S \cap B) \text{ as } S \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2) \text{ and independence is closed under subsets} \\ &\leq r_1(A) + r_2(B) \text{ by rank prop.}\end{aligned}$$

□

Recall that in the proof of optimality of Ford-Fulkerson, we produce a cut $(U, V \setminus U)$ where U is the set of vertices reachable from the source using edges in the residual graph with positive capacity. We will do something very similar for the proof of optimality of our matroid intersection algorithm.

Theorem 4.5 (Termination Implies Optimality)**.** *Let M_1 and M_2 be matroids over the common ground set E and let $S \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)$. If there is no source-sink path in $\mathcal{G}_{M_1,M_2}(S)$, then there exists $U \subseteq E$ such that $|S| \geq r_1(U) + r_2(E \setminus U)$.*

Proof. We'll pick U to be the set of all elements that have a path to a sink in $\mathcal{G}_{M_1,M_2}(S)$. We'll show that:

$$\begin{aligned} r_1(U) &\leq |S \cap U| \\ r_2(E \setminus U) &\leq |S \setminus U| \end{aligned}$$

Together, these inequalities imply:

$$\begin{aligned} r_1(U) + r_2(E \setminus U) &\leq |S \cap U| + |S \setminus U| \\ &= |S| \end{aligned}$$

which is what we want.

First, we'll show that $r_1(U) \leq |S \cap U|$. By way of contradiction, suppose that $r_1(U) > |S \cap U|$. As $S \cap U \in \mathcal{I}(M_1)$, we may find $u \in U \setminus (S \cap U)$ such that $(S \cap U) + u \in \mathcal{I}(M_1)$.

As $u \in U$, we know that u is *not* a source (if it was, we'd have a source-sink path). Hence, $S + u \notin \mathcal{I}(M_1)$. Therefore, by circuit prop., we know that $S + u$ contains a *unique* circuit $C \subseteq S + u$. However, $C \not\subseteq (S \cap U) + u$ since that set is independent in M_1. Therefore, we may find some $v \in C$ such that $v \notin ((S \cap U) + u)$.

Since C is the *unique* circuit in $S+u$, we know that $S-v+u \in \mathcal{I}(M_1)$ as we remove its only circuit by removing v. We know u and v are distinct since $v \notin ((S \cap U)+u)$. Hence, we have the edge (v,u) in $\mathcal{G}_{M_1,M_2}(S)$. Furthermore, as $v \neq u$ but $v \in C \subseteq S+u$, we know that $v \in S$. Combining this with the fact that $v \notin ((S \cap U)+u)$, we derive that $v \notin U$. This is a contradiction to the definition of U because we have the edge (v,u) where $u \in U$, however $v \notin U$ (as v can reach a sink by going to $u \in U$).

The proof of $r_2(E \setminus U) \leq |S \setminus U|$ is essentially symmetric, but we show it for completeness. We again suppose for contradiction that $r_2(E \setminus U) > |S \setminus U|$. Then, we obtain $v \in (E \setminus U) \setminus (S \setminus U)$ such that $(S \setminus U)+v \in \mathcal{I}(M_2)$.

Also, $S+v \notin \mathcal{I}(M_2)$. It can't be a sink because all sinks lie in U, but we know $v \notin U$. Let $C \subseteq S+v$ be its unique circuit. We also know that $C \nsubseteq (S \setminus U)+v$ for the same reason as before, so we can obtain $u \in C$ such that $u \notin (S \setminus U)+v$.

Hence, we know $u \neq v$ and also that $S-u+v \in \mathcal{I}(M_2)$. So, (v,u) is an edge in $\mathcal{G}_{M_1,M_2}(S)$. But, note that $u \in S$ as $u \in C \subseteq S+v$ and $u \neq v$. Combining that with $u \notin (S \setminus U)+v$, we find that $u \in U$. Hence, as $v \notin U$ but (v,u) is an edge, we get a contradiction in exactly the same way as last time. □

Remark 2. We now conclude that the algorithm is correct because upon termination, the E-cover $U \cup (E \setminus U)$ given to us by the above theorem *certifies* the optimality of our independent set due to the weak-duality lemma.

The following result is now an immediate consequence of our matroid intersection algorithm and the weak-duality lemma.

Theorem 4.6 (Matroid Intersection)**.** *Let M_1 and M_2 be matroids over the common ground set E. Then:*

$$\max\left\{|S| : S \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)\right\} = \min\left\{r_1(A) + r_2(B) : A \cup B = E\right\}$$

Proof. We already have $\leq$ by the weak version. Running our matroid intersection algorithm provides S and (A,B) such that $|S| \geq r_1(A)+r_2(B)$ which gives us equality. □

This theorem is pretty powerful. It implies Kőnig's theorem.

Theorem 4.7 (Kőnig)**.** *Let $G=(V,E)$ be an undirected graph with bipartition: $V_1 \sqcup V_2 = V$. Then, the maximum cardinality of a matching in G equals the minimum cardinality of a vertex cover in G.*

Proof. We construct two colourful matroids M_1 and M_2 over the ground set E (our edges). For an edge (v_1,v_2) where $v_1 \in V_1$ and $v_2 \in V_2$, its colour in M_1 is v_1 and its colour in M_2 is v_2. By definition of a matching and our colourful matroids, every matching in G corresponds to a set $S \in \mathcal{I}(M_1) \cap \mathcal{I}(M_2)$ (given by the edges included in the matching) and vice versa.

We'll show a similar correspondence for vertex covers. Let's call a vertex cover *reduced* if every vertex in the cover has degree ≥ 1. It's not hard to see that the minimum cardinality of a vertex cover and the minimum cardinality of a reduced vertex cover in G are the same. Consider a vertex cover C, we construct an element cover of our ground set as follows:

$$\begin{aligned} A &= \text{edges adjacent to } C \cap V_1 \\ B &= \text{edges adjacent to } C \cap V_2 \end{aligned}$$

Then, $A \cup B = E$ because each edge must be adjacent to some vertex in $C \subseteq V$, and $V_1 \sqcup V_2 = V$. Also since colours in M_1 and M_2 correspond to vertices in V_1 and V_2, we have the following because every vertex in C has at least one edge adjacent to it (it's reduced):

$$\begin{aligned} r_1(A) &= |C \cap V_1| \\ r_2(B) &= |C \cap V_2| \end{aligned}$$

So, the 'value' of the element cover is equal to the cardinality of our reduced vertex cover: $r_1(A) + r_2(B) = |C|$.

Conversely, if $A \cup B = E$, we construct a vertex cover of cardinality $r_1(A) + r_2(B)$ by taking the representative vertices of A in M_1, and unioning them with the representative vertices of B in M_2. It's a vertex cover because $A \cup B = E$, so if $e \in A$, then we cover its endpoint in V_1 and otherwise we cover its endpoint in V_2.

We deduce the desired equality directly from the matroid intersection theorem after setting up this construction. $\square$

5 Appendix: Greedy Characterization

A neat fact about matroids is that they uniquely characterize independence systems (i.e., a system that satisfies the first two matroid axioms) in which the natural greedy can find minimum weight independent sets. Here, we complete the proof started in the USACO Guide Matroids article. Suppose that we have an independence system, and the greedy algorithm works for any choice of k and weight function w. Now, suppose for the sake of contradiction that the exchange axiom fails. More specifically, there exist $X, Y \subseteq E$ such that $|X| < |Y|$, and there is no $e \in Y \setminus X$ such that $X + e \in \mathcal{I}$.

Then, we can adversarially construct the weight function as follows:

$$w(e) = \begin{cases} -1 - \epsilon & \text{if } e \in X \\ -1 & \text{if } e \in Y \setminus X \\ 0 & \text{otherwise} \end{cases}$$

Letting $k = |Y|$, the greedy will pick all of the elements in X, but no elements from $Y \setminus X$. Notice that the greedy may already fail if it is unable to pick $|Y|$ elements in total. Supposing that it manages to pick k elements, the result will be an independent set of total weight $-(1+\epsilon)|X|$. However, Y is an independent set which has weight less than or equal to $-|Y|$. Since $|X| < |Y|$, the greedy still fails, so we are done.