Matroid Intersection

In these lecture notes, we make use of some unconventional notation for set union and difference to keep things cleaner. In particular, let $A + B := A \cup B$, and $A - B := A \setminus B$, and let $A + a := A \cup \{a\}$ and $A - a := A \setminus \{a\}$. We will always denote sets by capital roman letters (e.g. A, B, C) and elements of sets by lower-case roman letters (e.g. a, b, c) to ensure the prior notation is unambiguous.

We use the independent set formulation of a matroid. A finite matroid $M = (E, \mathcal{I})$ is a pair consisting of a *ground set* E and a family of subsets of E, $\mathcal{I} \subseteq 2^E$, called the *independent sets* of M with the following two properties:

M1. *(Heredity Axiom)* Subsets of an independent sets are independent, i.e. $F \in \mathcal{I}, F' \subseteq F \implies F' \in \mathcal{I}$.

M2. *(Exchange Axiom)* If $A, B \in \mathcal{I}$, and $|A| > |B|$, then there is an element of $A - B$ which when added to B forms an independent set. i.e., $|A| > |B| \implies \exists\, a \in A - B : B + a \in \mathcal{I}$.

Matroids have the property that they are amenable to using a greedy algorithm. Many important problems such as finding spanning trees can be formulated and solved as matroids. In a general setting, this is the problem of finding a maximum-size independent set in a matroid. That is, given matroid $M = (E, \mathcal{I})$, find $F \in \mathcal{I}$ such that $|F|$ is maximum.

Given two matroids defined over the same ground set, we are interested in finding a maximum-size set which is independent in *both* matroids. This is known as the matroid intersection problem. As we will show, it has a polynomial time algorithm which produces a correct solution. Furthermore, the algorithm we describe uses augmenting path techniques which are similar to those used in algorithms for maximum-flow and matching.

Formally, our problem is defined as follows: Given two matroids, $M_1 = (E, \mathcal{I}_1)$, and $M_2 = (E, \mathcal{I}_2)$, find $F \in \mathcal{I}_1 \cap \mathcal{I}_2$ such that $|F|$ is maximum.

Krogdahl Graphs

The algorithm we describe makes use of a bipartite graph construction due to S. Krogdahl [4]. We will spend some time motivating its construction and examining the properties of this graph.

Given M_1 and M_2, defined over ground set E, suppose we are given some set $I \in \mathcal{I}_1 \cap \mathcal{I}_2$. In the course of the algorithm, we would like to add elements from $E - I$ to I in order to obtain some I' of strictly larger size. We can always greedily add elements from $E - I$ to I as long as the result is independent in both matroids, i.e. if there is an $e \in E - I$, such that $I + e \in \mathcal{I}_1 \cap \mathcal{I}_2$. However, when we cannot augment I in a greedy manner, we must have some mechanism for removing some elements from I and replacing them with other elements in such a way that the size of I increases. We do this by finding a path in the *Krogdahl graph*. The process we use is similar to finding an augmenting path in network flows (where we find an $s - t$ path which strictly increases the amount of flow we can send) and in matching (where we find an alternating path between two free nodes which strictly increases the size of the matching).

To define the Krogdahl graph given an independent set $I \in \mathcal{I}_1 \cap \mathcal{I}_2$, we define a directed bipartite graph $G_I = (I, E - I, D_I)$ with disjoint sets I and $E - I$, and edge set D_I, where for $i \in I$ and $j \in E - I$,

$$\text{edge } (i, j) \in D_I \iff I - i + j \in \mathcal{I}_1, \text{ and}$$
$$\text{edge } (j, i) \in D_I \iff I - i + j \in \mathcal{I}_2.$$

That is to say, for $i \in I$ and $j \in X - I$, i connects to j via a directed edge if, replacing i with j in I maintains independence in matroid M_1. Likewise, j connects to i if replacing i with j maintains independence in M_2.

Potential Pitfall: Be careful to note that the orientation of the edge does *not* indicate which element is added to I and which is removed from I. Regardless of the orientation of (i, j), the element from I is always removed, and the element from $E - I$ is always added.

To understand how augmenting paths in the Krogdahl graph increase the size of our independent set, consider any path in G_I which starts in $E - I$ and ends in $E - I$. Since the graph is bipartite, every pair of adjacent nodes must be on opposite sides of the graph. Let $Q = j_1, i_1, j_2, i_2, ...j_n, i_n, j_{n+1}$ be the sequence of nodes on such a path, and let $Q_j = \{j_1, ..., j_{n+1}\}$, $Q_i = \{i_1, ..., i_n\}$. Since path Q starts and ends in $E - I$, every node in Q_j must be in $E - I$, and every node in Q_i must be in set I, so we have $Q_j \subseteq E - I$, and $Q_i \subseteq E$.

If Q is a simple path, (i.e. no node is visited more than once) then we have that $|Q_j| = |Q_i| + 1$. Suppose we then were to form $I' = I - Q_i + Q_j$, then clearly, $|I'| = |I| + 1$. This is true for any simple path from $E - I$ back to $E - I$.

So by taking a simple path from $E - I$ back to $E - I$ we can form I' with strictly larger size. However, we *also* want I' to be independent in *both* matroids. This can be achieved by selecting a path Q from $E - I$ to $E - I$ with the following three properties,

1. *(Start point)* Q starts from a node in set $X_1 = \{x \in E - I \mid I + x \in \mathcal{I}_1\}$.

2. *(End point)* Q ends at a node in set $X_2 = \{x \in E - I \mid I + x \in \mathcal{I}_2\}$.

3. *(Shortest path)* Q is a shortest simple path from X_1 to X_2.

Any path having these properties is called an *augmenting path* in G_I. The proof that any such augmenting path can be used to yield a set which is independent in both M_1 and M_2 is non-trivial. We will leave this proof until the end of the lecture notes.

Matroid Intersection Algorithm

The algorithm for matroid intersection starts with $I = \emptyset$ and greedily adds elements which maintain membership in $\mathcal{I}_1 \cap \mathcal{I}_2$. When no more elements can be added, the algorithm forms a Krogdahl graph G_I, in which it finds an augmenting path Q (a shortest path from X_1 to X_2). The algorithm then augments I by Q, and again greedily adds elements until no more elements can be added. The algorithm continues in this manner until no augmenting path can be found. More specifically:

1. Set $I \leftarrow \emptyset$.
2. In a greedy manner, add to I a node $z \in E - I$ for which $I + z \in \mathcal{I}_1 \cap \mathcal{I}_2$. Do this until no other z meeting these criteria can be found.
3. Form Krogdahl graph $G_I = (I, E - I, D_I)$ as defined above. Let $X_1 = \{z \in E - I \mid I + z \in \mathcal{I}_1\}$, $X_2 = \{z \in E - I \mid I + z \in \mathcal{I}_2\}$.
4. Find a shortest *simple* path Q from X_1 to X_2 in G_I. If none exists, **stop** and return I.
5. Augment I using Q. That is, $I \leftarrow I - Q_i + Q_j$. Goto step 2 and continue.

Notice that step 2 is not strictly needed. Without it, the algorithm would find paths of length zero consisting of nodes in $X_1 \cap X_2$. However, including step 2 avoids the wasteful reconstruction of new Krogdahl graphs every time such an element is added to I. Bcause step 2 is included, by step 3 every path has at least 2 edges, so we make use of augmenting paths in this algorithm only when we need to.

We provide a proof of correctness in the next section. The rest of this section is concerned with efficiency and termination of our algorithm.

Efficiency is clear as follows. We start with $I = \emptyset$ and clearly $|I| \leq |E|$ at any point, giving a total of $|E| = n$ iterations. In the worst case, we form the graph G_I at each step. Given I, we need to consider $|I| \times |E - I| = O(n^2)$ potential edges. But, how do we know whether to include a given edge between i

and j? To do so, we have to be able to test and see if $I - i + j$ is independent in M_1 and run a separate test to see if it is independent in M_2.

Because the size of $\mathcal{I}_1$ and $\mathcal{I}_2$ could be exponential in n, we assume that *matroid oracles* M_1 and M_2 are given. A matroid oracle for a matroid $M = (E, \mathcal{I})$ is a program which can respond to queries consisting of subsets $U \subseteq E$. The question the oracle answers is: "is $U \in \mathcal{I}$"? As a concrete example, consider the matroid M_G defined on a graph $G = (V, E)$, where the independent sets are cycle-free subsets of E. For any subset of edges, E' we can compute whether or not E' contains a cycle, and answer "yes" or "no". Such a program would constitute an oracle for M_G.

Back to the Krogdahl graph, it should be clear that we need to query both oracles once for each edge of G_I. Specifically, for edge (i, j), with $i \in I$ and $j \in E - I$, we ask, "is $I - i + j \in \mathcal{I}_1$?" We can construct the graph in at most $O(n^2)$ such queries. If both M_1 and M_2 have oracles with polynomial running times, the running time of the matroid intersection algorithm will be polynomial. More specifically, if $T(M_1)$ and $T(M_2)$ are running times for the oracles for M_1 and M_2, then the matroid intersection algorithm runs in time $O(n^3 \max[T(M_1), T(M_2)])$.

In order to halt, we must be able to detect when no $X_1 \rightsquigarrow X_2$ path exists in G_I. To do this efficiently, we can do the following:

- In G_I, connect a special node r to every node in X_1.
- Run breadth-first search from r, obtaining breadth-first search tree T.
- If T doesn't reach X_2, then there is no $X_1 \rightsquigarrow X_2$ path. Else, the shortest path from X_1 to X_2 can be found in T.

Breadth-first search runs in $O(|V| + |E|)$ time, which is dominated by the $O(n^2)$ graph construction in each step.

Example – Common Labeled Spanning Tree

The following is an example of the matroid intersection algorithm in action. Our current matroids $M_1 = (V, \mathcal{I}_1)$ and $M_2 = (V, \mathcal{I}_2)$ are forest matroids based on graphs G_1 and G_2 respectively. That is, $\mathcal{I}_1$ (respectively $\mathcal{I}_2$)is the set of all cycle-free edges in G_1 (respectively, G_2). The graphs are shown in Figure 1. Essentially, we will be looking for a largest common spanning tree. When the algorithm starts, our intersecting independent set I is empty.

Any element $e \in \mathcal{I}_1 \cap \mathcal{I}_2$ is then greedily added to I such that I remains independent in $\mathcal{I}_1$ and $\mathcal{I}_2$. When no new element can be added to I, the algorithm then searches for an augmenting path to increase $|I|$. Figure 2 shows the current scenario. We greedily chose elements a, d, and e to be added to I and now cannot add any more elements. Notice that in G_2 we can either add g or h to I and still remain independent in $\mathcal{I}_2$. However, for G_1 this will cause I to lose independence in $\mathcal{I}_1$.

This is where the augmenting path comes in to help rearrange things to where we can potentially add more elements. We construct the Krogdahl graph, G_I. Along with G_I, two sets (X_1 and X_2) are defined. G_I is shown in Figure 3 with elements in X_1 colored red and elements in X_2 colored green.

At this point a shortest path from an element in X_1 to an element in X_2 is selected. The algorithm then updates I by removing all $y \in I$ and adding all $z \in V - I$ that are along the selected path. Figure 3 highlights an arbitrarily selected shortest path (b, a, g). I will then be updated to $I - a + b + g$ and increase in size by one.

Figure 4 highlights the elements in the updated I. A new Krogdahl graph D_I (Figure 5) is created based on this set. Since there are no elements in either X_1 or X_2, this indicates there is no augmenting path to increase $|I|$. The algorithm terminates and returns $I = \{b, d, e, g\}$.

The next example provides a case scenario demonstrating the necessity of choosing a shortest $X_1 - X_2$ path. Figure 6 shows graphs G_1 and G_2 with a common independent set highlighted. The directed bipartite graph is constructed and instead of choosing a shortest path, a non-shortest path is chosen instead. Figure 7 shows the selected path and the resulting augmentation. Notice that the common set

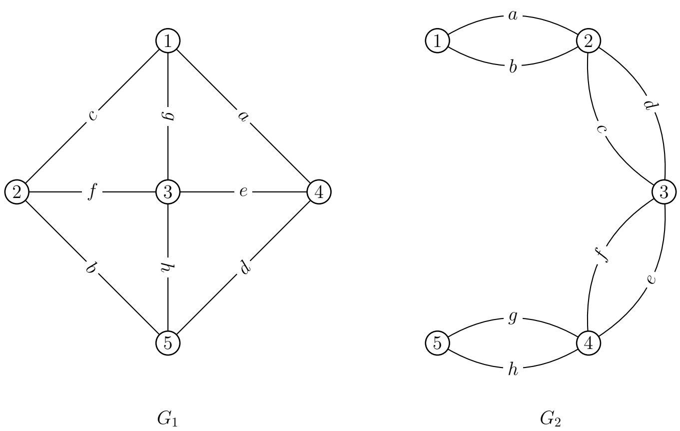

Figure 1: Initial graphs where $I = \emptyset$

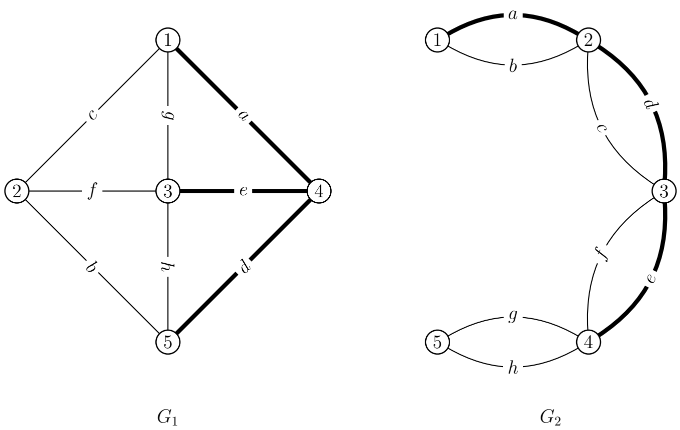

Figure 2: Highlighted edges in G_1 and G_2 form a common independent set. $I = \{a, d, e\}$.

is no longer independent. If we had chosen a shortest path such as in Figure 8, the resulting augmentation would have yielded a larger common independent set.

Algorithm Correctness

To prove the correctness of the matroid intersection algorithm, we need to show two things.

1. I is of maximum size at the end of the algorithm.
2. $I \in \mathcal{I}_1 \cap \mathcal{I}_2$ at the end of the algorithm.

We can refine these statements more formally into Theorem 1 and Theorem 2. Notice that these statements are slightly reminiscent of the augmenting path theorems for max-flow.

Theorem 1. *If there is no $X_1 \rightsquigarrow X_2$ path in G_I, then I is of maximum size.*

Theorem 2. *If there is an $X_1 \rightsquigarrow X_2$ path, $Q = j_1, i_1, j_2, i_2, ..., j_n, i_n, j_{n+1}$ which is an augmenting path, then $I - Q_i + Q_j \in \mathcal{I}_1 \cap \mathcal{I}_2$.*

To prove Theorem 1 we will need the concepts of the *rank* and *basis* of any set $U \subseteq E$. Given a set $U \subseteq E$, where E is the base set of matroid M, we define the *rank* $r_M(U)$ as the maximum size indepedendent subset of U. If U is independent then $r_M(U) = |U|$, otherwise we can remove elements from U which cause it to be dependent. Removing the fewest number of such elements yields a maximum size $U' \subseteq U$, where U' is independent in M, and therefore $r_M(U) = |U'|$. A *basis* of a set $U \subseteq E$, denoted B_U, is a

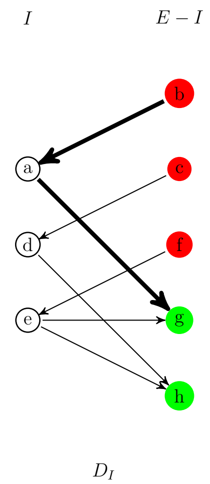

Figure 3: D_I shows paths from X_1 (red) to X_2 (green).

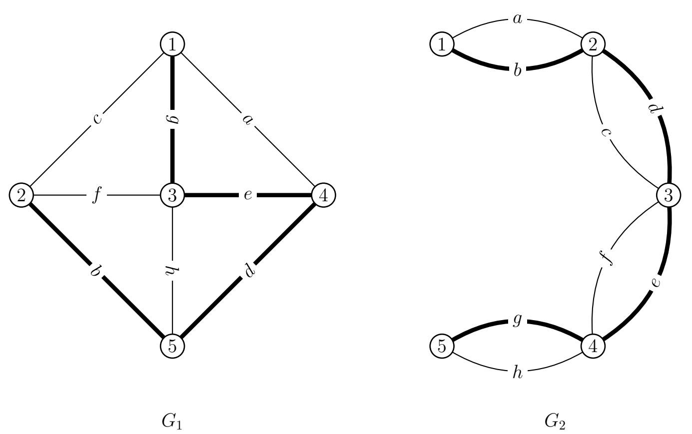

Figure 4: Highlighted edges in G_1 and G_2 form new common independent set after adding elements b and g and removing a. $I = \{b, d, e, g\}$.

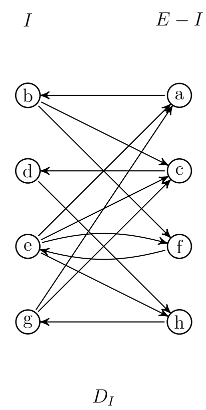

Figure 5: No $X_1 \rightsquigarrow X_2$ path in D_I.

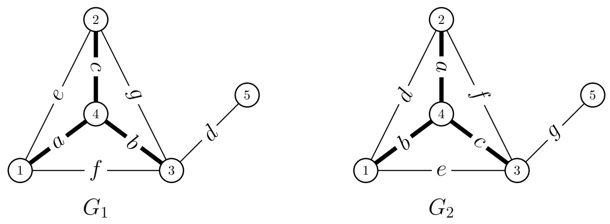

Figure 6: Necessity of shortest path

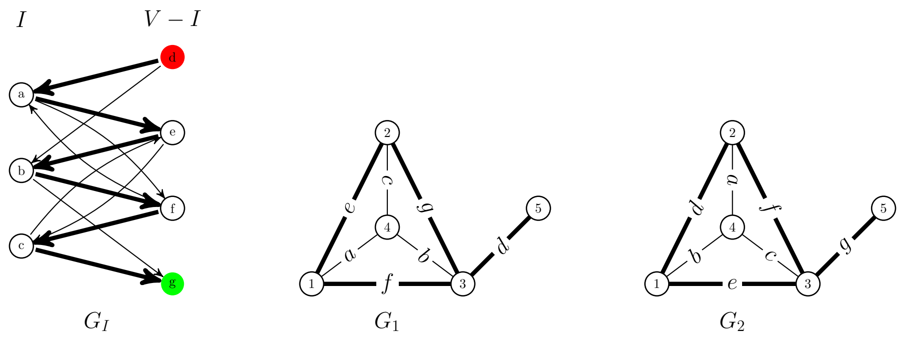

Figure 7: Non-shortest path augmentation yields a non-independent set.

maximum size independent subset of U. Note that the basis of a given subset need not be unique, but matroid theory tells us that all bases *must* have the same cardinality. That is, for any two bases B_U, B'_U of a set U, $|B_U| = |B'_U| = r_M(U)$.

Armed with these concepts, we can finally give the following proof. These proofs were originally expressed in a more concise form, however great care has been taken to add additional details to aid the confused reader, who may not have previously seen matroid theory applied. We have drawn from all the references cited at the end of this section, and based our proof primarily on those in [3, 5].

Proof (Theorem 1). Given that there is no $X_1 \rightsquigarrow X_2$ path, we need to show that I is of maximum size. First, notice that given any $J \in \mathcal{I}_1 \cap \mathcal{I}_2$, and any $U \subseteq E$, we have

$$|J| = |J \cap U| + |J \cap (E - U)| \leq r_{M_1}(U) + r_{M_2}(E - U). \tag{1}$$

Which says roughly that the portions of J on either side of the partition $(U, E - U)$ cannot exceed the maximum independent sets on either side of the cut. This is reasonably intuitive, but we must give a formal proof.

To prove (1) note that since any subset of J is independent, this must also hold for $J \cap U \subseteq J$. So, for any M_1 basis of the superset U we must have $|J \cap U| \leq |B_U| = r_{M_1}(U)$. Similarly, since $J \cap (E-U) \subseteq J$, for any M_1 basis of $E - U$, we must have $|J \cap (E - U)| \leq |B_{E-U}| = r_{M_2}(E - U)$. Taking the sum of these inequalities yields (1).

We will show that if there is no $X_1 \rightsquigarrow X_2$ path, that we have equality in (1), which implies that we cannot[1] increase $|I|$ any further. To show equality for I we must produce a suitable set U.

Let U be the set of elements in E which can reach X_2. More formally, let

$$U = \{z \in E \mid \text{there is a path in } G_I \text{ from } z \text{ to } X_2\}.$$

Clearly, any node in X_2 must be in U, so $X_2 \subseteq U$. Furthermore, since there is no path from X_1 to X_2, $X_1 \cap U = \emptyset$. We claim that $r_{M_1}(U) = |I \cap U|$ and $r_{M_2}(E - U) = |I \cap (E - U)|$, which proves that we have

[1] If we could increase $|I|$ while equality holds for (1), that would imply that (1) is invalid, since $|I|$ would exceed the right-hand side. But we just proved (1) so we must not be able to increase it further.

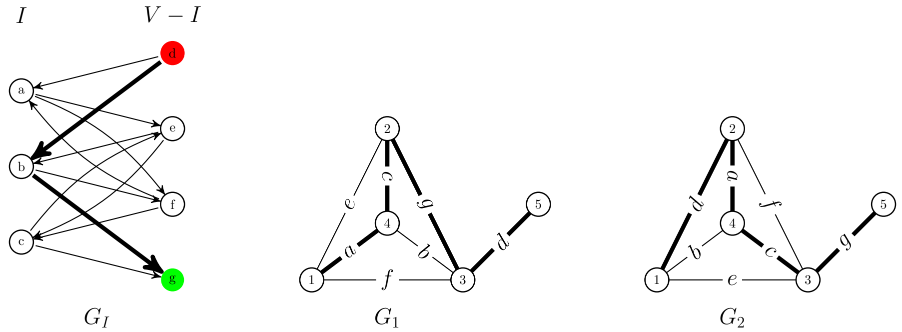

Figure 8: Shortest path augmentation yields a larger common independent set.

equality in (1). We will only show that $r_{M_1}(U) = |I \cap U|$, the proof that $r_{M_2}(E-U) = |I \cap (E-U)|$ is similar.

We will show $|I \cap U| = r_{M_1}(U)$ by contradiction. Suppose that $|I \cap U| < r_{M_1}(U)$. Since $I \cap U$ is independent in M_1, we can extend $I \cap U$ to a basis of U, for which $|I \cap U| < |B_U|$. But this means that there is a superset of $I \cap U$ which is independent in M_1, namely B_U. By the exchange axiom, we must have some $x \in B_U - (I \cap U)$ such that $(I \cap U) + x \in \mathfrak{I}_1$. Note that this guarantees that $x \in B_U - I$. Since $X_1 \cap U = \emptyset$, it must be that $I + x \notin \mathfrak{I}_1$, (by definition of X_1). Finally, since $(I \cap U) + x$ was shown to be independent in M_1, and $I + x$ is not, we have that $I \cap U \neq I$; therefore

$$|(I \cap U) + x| \leq |I|. \tag{2}$$

We will show that (2) implies that there must be some $y \in I - U$ such that $I - y + x \in \mathfrak{I}_1$, but first we will show how this completes the proof. Note that since $I - y + x \in \mathfrak{I}_1$, we must have that $(y, x) \in D_I$, and this edge is directed from I to $E - I$ since we have independence in M_1 for $I - y + x$. But we already know that there's a path from x to X_2, because $x \in B_U$ implies that $x \in U$. Therefore, since there is some node y which is not in U, yet which can reach X_2 (by way of a path through x), we obtain a contradiction.

It remains to show that (2) implies the existence of $y \in I - U$ such that $I - y + x \in \mathfrak{I}_1$. We consider two cases as follows.

Suppose that $|(I \cap U) + x| = |I|$. Since both sides have the same size, yet we added some $x \notin I$ to $(I \cap U)$, we must have that $(I \cap U) + x = I - y + x$ for some $y \in I - U$.

Suppose now instead that $|(I \cap U) + x| < |I|$. Since both sets are independent in M_1 we can apply the exchange axiom. Therefore we must have a $x' \in I - ((I \cap U) + x) = I - U$ such that $(I \cap U) + x + x' \in \mathfrak{I}_1$. We can repeat this by induction until we obtain $I - y + x \in \mathfrak{I}_1$ for some $y \in I - U$, just as before. This completes the proof. $\square$

To prove Theorem 2 we will need the concept of the *span* of a set $S \subseteq E$. The *span* of any set $S \subseteq E$ is defined as $span_M(S) = \{x \mid x \in E, r_M(S + x) = r_M(S)\}$. The span is those elements which, when added to S does not cause the rank of $S + x$ to differ from that of S. That is to say, the maximum size independent set of $S + x$ is the same as that of S. We will use the fact that, if $x \notin span_M(S)$, then $S + x \in \mathfrak{I}$. We will also need the following lemma.

Lemma 1. *Let $M = (E, \mathfrak{I})$ be a matroid. Let $I \in \mathfrak{I}$, and let $j_1, i_1, ..., j_k, i_k$ be a sequence of distinct elements of E such that*

(a) $j_m \notin I, i_m \in I$ for $1 \leq m \leq k$;

(b) $I + j_m \notin \mathfrak{I}, (I + j_m) - i_m \in \mathfrak{I}$ for $1 \leq m \leq k$;

(c) $I + j_m - i_\ell \notin \mathfrak{I}$ for $i \leq m < \ell \leq k$.

Let $I' = I - \{i_1, ...i_k\} + \{j_1, ..., j_k\}$. Then $I' \in \mathfrak{I}$ and $span_M(I') = span_M(I)$.

Which roughly says that for an augmenting path $Q' = j_1, i_1, ..., j_n, i_n$, (that is, the original augmenting path Q *excluding* j_{n+1}), that augmenting by Q' yields an independent set in $\mathcal{I}_2$. This will become clear once we apply the lemma to prove Theorem 2. Note that condition (c) is equivalent to requiring Q to be a shortest path, since if $I - j_m + i_\ell$ were independent with $m < \ell$, this would imply that a "shortcut" edge exists in the Krogdahl graph. We will prove Lemma 1 at the end of this section. For now, we will show how it can be used to prove Theorem 2.

Proof (Theorem 2). Consider the augmenting $X_1 \rightsquigarrow X_2$ path $Q = j_1, i_1, ..., j_n, i_n, j_{n+1}$ which exists by the assumption of Theorem 2. We need to check the conditions of Lemma 1 in order to apply it. Since Q starts in $E - I$, and G_I is bipartite, we have that the sequence $j_1, i_1, ..., j_n, i_n$ satisfies condition (a). When we consider matroid M_2, condition (b) follows since we have that $I + j_m \notin \mathcal{I}_2$ (otherwise there is a shorter $X_1 \rightsquigarrow X_2$ path), and that $I - j_m + i_m \in \mathcal{I}_2$, since edge (j_m, i_m) is in the Krogdahl graph. Condition (c) follows since Q is a shortest path. Therefore, by Lemma 1, we have that $I' = I - \{i_1, ..., i_n\} + \{j_1, ..., j_n\} \in \mathcal{I}_2$, and furthermore that $span_{M_2}(I') = span_{M_2}(I)$.

Since $j_{m+1} \in X_2$, and therefore $I' + j_{m+1} \in \mathcal{I}_2$, we know that $j_{m+1} \notin span_{M_1}(I)$. Therefore, we get that $j_{m+1} \notin span_{M_2}(I') = span_{M_2}(I)$, so we have that $I' + j_{m+1} \in \mathcal{I}_2$.

It's easy to see that the same augmenting path yields a similar sequence $i_1, j_2, ..., i_n, j_{n+1}$ for which the conditions of the lemma hold with regard to matroid M_1. That is, $j_{m+1} \notin I$, but $i_m \in I$, for any $1 \leq m \leq n$, satsifying (a); we know that $I + j_{m+1} \notin \mathcal{I}_1$, yet $(I + j_{m+1}) - i_m \in \mathcal{I}_1$ for $i \leq m \leq n$, since edges (i_m, j_{m+1}) are in G_I, satisfying (b); condition (c) follows since Q is a shortest path, as before. Lemma 1 can therefore be applied as before, and a symmetric argument used to show $j_1 \notin span(I - \{i_1, ...i_n\} + \{j_2, ..., j_n\})$, implying that $I - \{i_1, ...i_n\} + \{j_1, ...j_n\} + j_1 \in \mathcal{I}_1$. Taken together with the previous result, we have that $I - Q_i + Q_j \in \mathcal{I}_1 \cap \mathcal{I}_2$, as desired. □

As a consequence of having a correct algorithm for matroid intersection, we can show the following fundamental max-min relation over the intersection of matroids.

Theorem 3. *The size of the maximum independent set common to M_1 and M_2 is equal to the size of the maximum independent sets on either side of a bipartition of E. Formally,*

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{U \subset X} [r_{M_1}(U) + r_{M_2}(E - U)].$$

Proof. Our proof relies on the existence of a correct algorithm which can produce an I and a U such that equality holds. The matroid intersection algorithm is such an algorithm, as evidenced by Theorems 1 and 2. Furthermore, we showed in the proof of Theorem 1 that $\leq$ holds, so no other I can exceed the size of that found by our algorithm. □

Of course, to be able to apply Lemma 1 in the proof of Theorem 2, it must be shown to be correct. We will show this fact by induction in the following proof.

Proof (Lemma 1). We perform induction on k, half the length of the sequence $j_1, i_1, ..., j_k, i_k$.

As our base case, consider the situation when $k = 1$. We have a sequence j_1, i_1, where the conditions of the Lemma hold. The lemma states that $I' = I - j_1 + i_1$. By condition (b), we have that $I' \in \mathcal{I}$. We need to show that $span_M(I') = span_M(I)$. Suppose that $span_M(I') \neq span_M(I)$, and that we have some $g \in span_M(I)$ for which $g \notin span_M(I')$. This means that I must be a basis of $I + i_1 + g$, but $I' + g$ forms a basis of a larger size. Since each basis of a subset of X must have the same size, this is a contradiction. Similarly, if $g \in span_M(I')$ but $g \notin span_M(I)$ then I' forms a basis of $I' + i_1 + g$, and we get $I + g$ as a basis of larger size, yielding a contradiction. So in either case, $span_M(I) = span_M(I')$.

For the inductive case, suppose $k \geq 2$ and the lemma holds for all values smaller than k. Fix $I' = I - Q_i + Q_j$ for the remainder of the proof. We will apply the lemma to smaller sized sequences in two ways. First, apply it to set I and the sequence $j_1, i_1, ..., j_{k-1}, i_{k-1}$, yielding that

$$I' - j_k + i_k \in \mathcal{I}, \text{ and } span_M(I' - j_k + i_k) = span_M(I). \tag{3}$$

(Note that $I' - j_k + i_k$ is just I augmented by the path of length $k-1$ which *excludes* the last pair (j_k, i_k)).

We also apply the lemma to set $I - i_k$ and the same sequence $(j_1, i_1, ..., j_{k-1}, i_{k-1})$ yielding that

$$I' - j_k \in \mathfrak{I}, \text{ and } span_M(I' - j_k) = span_M(I - i_k). \tag{4}$$

Note that $j_k \notin span_M(I - i_k)$, since by condition (b), $I - i_k + j_k$ is independent. Since the spans in (4) are the same, $j_k \notin span_M(I' - j_k)$, so we have that $I' - j_k + j_k = I' \in \mathfrak{I}$, which is the first consequence of the lemma that we needed to show.

Applying (3), it's clear that in order to show that $span_M(I') = span_M(I)$, it suffices to show $span_M(I') = span_M(I' - j_k + i_k)$. To do this, we apply induction where $k = 1$ to the set I' and the sequence i_k, j_k, yielding that $span_M(I') = span_M(I' - j_k + i_k)$. In order to do this, we must satisfy the conditions of the Lemma. Conditions (a) and (b) are the only two conditions of consequence, because of the small size of the sequence. Clearly, (a) is satisfied, since $i_k \notin I'$, and $j_k \in I'$. To see that (b) is satisfied, we must have that $I' - j_k + i_k \in \mathfrak{I}$, which follows easily from (3), and that $I' + i_k \notin \mathfrak{I}$, which also follows from (3), since $i_k \in I$, and $I \subseteq span_M(I) = span_M(I' - j_k + i_k)$. Therefore, all the conditions are satisfied, and we have that $span_M(I) = span_M(I')$, proving the lemma. □

References

[1] Chandra Chekuri. Lecture 16 on 3/11/2010: Uncrossing based proof of matroid polytope integrality, base exchange properties. http://courses.engr.illinois.edu/cs598csc/sp2010/, 2010.

[2] Chandra Chekuri. Lecture 17 on 3/16/2010: Matroid intersection. http://courses.engr.illinois.edu /cs598csc/sp2010/, 2010.

[3] William J. Cook, William H. Cunningham, William R. Pulleyblank, and Alexander Schrijver. *Combinatorial Optimization*. John Wiley & Sons, Inc., New York, NY, USA, 1998.

[4] Stein Krogdahl. A combinatorial base for some optimal matroid intersection algorithms. Technical Report STAN-CS-74-46, Computer Science Department, Stanford University, Stanford, California, 1974.

[5] Janos Pach. Matroid intersection. Lecture 7. http://dcg.epfl.ch/page-84766-en.html, 2012.

[6] Alexander Schrijver. The greedy algorithm and the independent set polytope. In *Combinatorial Optimization: Polyhedra and Efficiency*, volume B. Springer, 2003.

[7] Alexander Schrijver. Matroid intersection. In *Combinatorial Optimization: Polyhedra and Efficiency*, volume B. Springer, 2003.