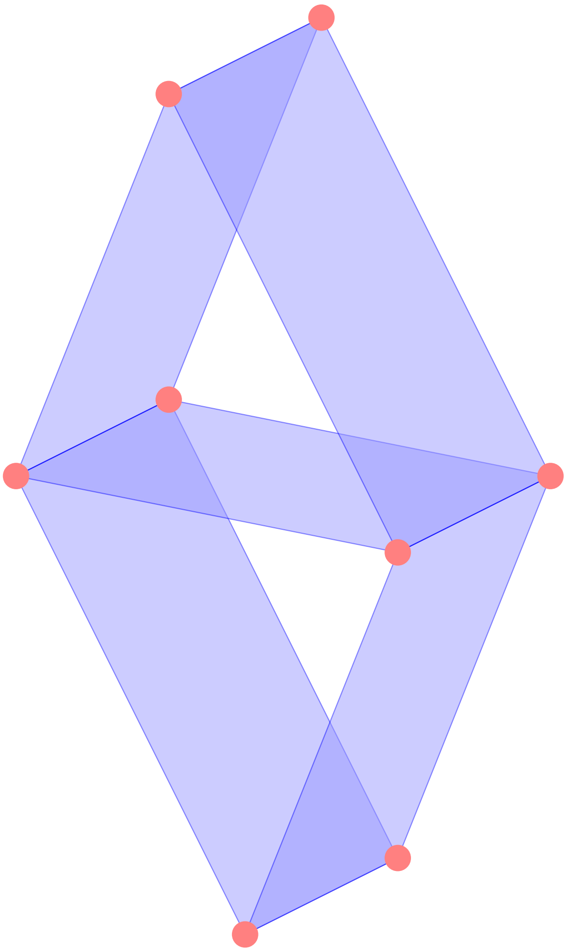
Matroid Theory

Tomáš Turek[1]



April 15, 2024

[1]These are my notes on the course Matroid Theory, which was taught by Ondřej Pangrác in the year 2024. Keep in mind there may be some mistakes. You may visit GitHub.

Contents

Chapter 1

Basic definitions

Definition 1. ***Matroid*** *$\mathcal{M} = (E, \mathcal{I})$ is for E finite non-empty set and $\mathcal{I} \subseteq 2^E$ (also called as independent sets) satisfying these properties:*

(I1) $\emptyset \in \mathcal{I}$,

(I2) $I \in \mathcal{I} \Rightarrow \forall I' \subseteq I : I' \in \mathcal{I}$,

(I3) $I_1, I_2 \in \mathcal{I}, |I_1| < |I_2| \Rightarrow \exists e \in I_2 \setminus I_1 : I_1 \cup \{e\} \in \mathcal{I}$.

Notation. *For further use and simplification we will sometimes use $I + e$ as a substitution for $I \cup \{e\}$. Similarly also $I - e$ for $I \setminus \{e\}$.*

Example. For a given multi-graph $G = (V, F)$ we will set $E = F$ (or in other words E stands for edges and the set). Independent sets $\mathcal{I}$ will be all acyclic subsets of E. Easily seen (I1) and (I2) is satisfied. For the third one (I3) it is also quite easily seen, because if we have one larger and smaller non-cycles then we can append one edge from the larger to the smaller.

Example. Let E be some elements of a vector space V. If $X \subseteq E$ is independent then it is linearly independent in V.

Definition 2. *Matroid* ***isomorphism*** *for two matroids $\mathcal{M}_i = (E_i, \mathcal{I}_i)$ for $i = 1, 2$ is a bijection $f : E_1 \to E_2$ satisfying $\forall X \subseteq E_i : X \in \mathcal{I}_1 \Leftrightarrow f(X) \in \mathcal{I}_2$.*

1.1 Circuits

Definition 3. *$X \subseteq E$ is a* ***circuit*** *if $X \notin \mathcal{I}$ and $\forall x \in X : X - x \in \mathcal{I}$. Also we will denote $\mathcal{C}(\mathcal{M})$ as the set of all circuits of $\mathcal{M}$.*

Lemma 1. *Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid and $\mathcal{C}$ its collection of circuits, then*

(C1) $\emptyset \notin \mathcal{C}$,

(C2) $\forall C_1, C_2 \in \mathcal{C} : C_1 \subseteq C_2 \Rightarrow C_1 = C_2$ *and*

(C3) $\forall C_1, C_2 \in \mathcal{C}, C_1 \neq C_2, e \in C_1 \cap C_2 \Rightarrow C_3 \subseteq (C_1 \cup C_2) - e, C_3 \in \mathcal{C}$.

Proof. (C1) and (C2) are easily seen from (I1) and (I2). Now for the third part (C3). So for contradiction let C_1, C_2, e be as mentioned in the first part, but $(C_1 \cup C_2) - e \in \mathcal{I}$. Then $\exists f \in C_2 \setminus C_1 : C_2 - f \in \mathcal{I}$. Now find $I \in \mathcal{I}$ max s.t. $C_2 \setminus \{f\} \subseteq I \subseteq C_1 \cup C_2$. If $f \notin I$ then it would contain C_2 which is dependent and $\exists g \in C_1 \setminus C_2 : g \notin I$ otherwise it would contain C_1 which is dependent. Therefore

$$|I| \leq |C_1 \cup C_2| - 2 < |(C_1 \cup C_2) - e|$$

and now we may use the third axiom (I3) that is $\exists x \in |(C_1 \cup C_2) - e| \setminus I$ s.t. $I + e \in \mathcal{I}$ (this cannot be otherwise I contains the whole C_2). Now $I + x$ contradicts the maximality of I. □

Claim 1. *Lets have E and $\mathcal{C} \subseteq 2^E$ satisfying all (C1), (C2) and (C3). Then set $\mathcal{I} = \{X \subseteq E | \forall C \in \mathcal{C} : C \nsubseteq X\}$ and $\mathcal{M} = (E, \mathcal{I})$ is a matroid.*

Proof. We have to show all properties of matroid. That is (I1) is trivially satisfied and (I2) also trivially holds. For the last (I3) we use a contradiction. For that we have $I_1, I_2 \in \mathcal{I}$, then $\forall e \in I_2 \setminus I_1 : I_1 + e \notin \mathcal{I}$. Let $I_3 \subseteq I_1 \cup I_2$ s.t. $|I_3| > |I_1|$ and $|I_1 \setminus I_3|$ is minimal. If $|I_1 \setminus I_3|$ would be empty then (I3) will hold, therefore assume it is non-empty.

Fix $e \in I_1 \setminus I_3$. Let $I_k = |I_3 - f| + e$ for $(f \in I_3 \setminus I_1)$. This cannot be independent $(\notin \mathcal{I})$ therefore $\exists C_k \subseteq T_k : C_k \in \mathcal{C}$ and $f \notin C_k, e \in C_k$.

$(I_3 \setminus I_1) \cap C_k = \emptyset$ hence $C_k \subseteq T_k \setminus (I_3 \setminus I_1) = (I_1 \cap I_3) + e \subseteq I_1$ this is not possible so it must be non-empty. Then $\exists g \in (I_3 \setminus I_1) \cap C_k \Rightarrow C_k, C_g \in \mathcal{C}, e \in C_k \cap C_g, f \notin C_k, g \notin C_g$ but $(C_k \cup C_g) - e \subseteq I_3$ which is contradiction with (C3). □

1.2 Basis

Definition 4. *Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid. Then B is a **basis** iff $B \in \mathcal{I}, \forall x \in E \setminus B : B + x \notin \mathcal{I}$.*

Proposition 2. *Let B_1, B_2 be bases of $\mathcal{M}$, then $|B_1| = |B_2|$.*

Proof. If $|B_1| < |B_2|$ then by (I3) $\exists x \in B_2 \setminus B_1 : B_1 + x \in \mathcal{I}$. □

Definition 5. *Let $\mathcal{B}(\mathcal{M}) = \{B \subseteq E, B \text{ is a basis}\}$ be a collection of basis satisfying*

(B1) $\mathcal{B} \neq \emptyset$ and

(B2) $B_1, B_2 \in \mathcal{B}, e \in B_1 \setminus B_2 \Rightarrow \exists f \in B_2 \setminus B_1 : (B_1 - e) + f \in \mathcal{B}$.

One can see that (B2) can be proven using $I_1 - e =: B_1$ and $I_2 = B_2$. And alternatively we may exchange the second property for the following.
(B2') $B_1, B_2 \in \mathcal{B}, \forall x \in B_2 \setminus B_1, \exists y \in B_1 \setminus B_2$ s.t. $(B_1 - y) + x \in \mathcal{B}$.

Proof. To proof that indeed we can exchange these properties we see that $B_1 + x$ has to be dependent therefore $\exists C \in \mathcal{C}, C \subseteq B_1 + x$. Now we show that C is unique, otherwise $C_1, C_2 \subseteq B_1 + x, x \in C_1 \cap C_2, \exists C_3 \subseteq (C_1 \cup C_2) - x \subseteq B_1$ which is a contradiction. Also this is sometimes called **fundamental circuit w.r.t.** B_1 **and** x. See that $C \setminus B_2 \neq \emptyset$ so $\exists y \in C \setminus B_2 \subseteq B_1 \setminus B_2$; hence $(B_1 + x) - y$ does not contain a circuit and $|(B_1 + x) - y| = |B_1| \Rightarrow (B_1 + x) - y \in \mathcal{B}$. □

Proposition 3. *Let $E \neq \emptyset$ finite set and $\mathcal{B} \subseteq 2^E$ satisfying (B1) and (B2). Let $\mathcal{I} = \{X \subseteq E : \exists B \in \mathcal{B} : X \subseteq B\}$ then $\mathcal{M} = (E, \mathcal{I})$ is a matroid.*

Proof. (I1) and (I2) are trivial. For (I3) use the following lemma.

Lemma 2. *Let $\mathcal{B}$ be such that it satisfies (B1) and (B2). Then $\forall B_1, B_2 \in \mathcal{B} : |B_1| = |B_2|$.*

Proof. By contradiction suppose $|B_1| > |B_2|$ with minimal $|B_1 \setminus B_2|$. Then $e \in B_1 \setminus B_2 \Rightarrow \exists f \in B_2 \setminus B_1 : (B_1 - e) + f \in \mathcal{B}$ and also $|(B_1 - e) + f| = |B_1|$ which leads to $|((B_1 - e) + f) \setminus B_2| < |B_1 \setminus B_2|$ which is a contradiction with the minimality. □

□

1.3 Rank function

Definition 6. *For a matroid $\mathcal{M} = (E, \mathcal{I})$ define a **rank function** $\mathsf{r} : 2^E \to \mathbb{Z}_0^+$, such that $\mathsf{r}(X) = \max_{I \subseteq X, I \in \mathcal{I}} |I|$ and $\mathsf{r}(\mathcal{M}) = \mathsf{r}(E)$.*

Claim 4. *Rank function has the following properties:*

(R1) $X \subseteq E : 0 \leq \mathsf{r}(X) \leq |X|$,

(R2) $X \subseteq Y \subseteq E \Rightarrow \mathsf{r}(X) \leq \mathsf{r}(Y)$ and

*(R3) $X, Y \subseteq E : \mathsf{r}(X \cup Y) + \mathsf{r}(X \cap Y) \leq \mathsf{r}(X) + \mathsf{r}(Y)$ (which is called **submodularity**).*

Proof of the properties. While (R1) and (R2) are obvious and now we will show that (R3) also holds. Let I_1 be the max independent in $X \cap Y$ and I_2 be an extension $I_2 \supseteq I_1$ and max independent in $X \cup Y$. Now $\mathsf{r}(X \cup Y) + \mathsf{r}(X \cap Y) = |I_2| + |I_1|$ and also $|I_2 \cap X| \leq \mathsf{r}(X)$ and $|I_2 \cap Y| \leq \mathsf{r}(Y)$. We apply simple rule $|A| + |B| = |A \cup B| + |A \cap B|$ and get

$$\mathsf{r}(X) + \mathsf{r}(Y) \geq |I_2 \cap X| + |I_2 \cap Y| = |I_2| + |I_1| = \mathsf{r}(X \cup Y) + \mathsf{r}(X \cap Y)$$

□

Theorem 5. *For $E \neq \emptyset$ finite set and $\mathsf{r} : 2^E \to \mathbb{Z}_0^+$ satisfying (R1), (R2) and (R3). Then $\mathcal{I} = \{X \subseteq E | \mathsf{r}(X) = |X|\}$ and $\mathcal{M} = (E, \mathcal{I})$ is a matroid.*

Lemma 3. *For $E \neq \emptyset$ finite set and $\mathsf{r} : 2^E \to \mathbb{Z}_0^+$ satisfying (R1), (R2) and (R3). It holds that if $X, Y \subseteq E$ $\forall y \in Y : \mathsf{r}(X) = \mathsf{r}(X + y)$ then $\mathsf{r}(X) = \mathsf{r}(X \cup Y)$.*

Proof of lemma 3. Let $Y \setminus X = \{y_1, y_2, \ldots, y_k\}$ and now we will prove it by induction on k. For $k = 1$ it obviously holds. For $k \geq 2$ we use the submodularity.

$$\begin{aligned}
\mathsf{r}(X) + \mathsf{r}(X) &= \mathsf{r}(X \cup \{y_1, y_2, \ldots, y_{k-1}\}) + \mathsf{r}(X + y_k) &&\geq \mathsf{r}(X \cup \{y_1, y_2, \ldots, y_k\}) + \mathsf{r}(X) \\
&\quad \text{(by induction hypothesis)} && \\
\mathsf{r}(X) &= &&\geq \mathsf{r}(X \cup \{y_1, y_2, \ldots, y_k\}) \\
\mathsf{r}(X) & &&\geq \mathsf{r}(X \cup Y)
\end{aligned}$$

For the other inequality we use (R2) and hence we obtain equality. □

Proof of theorem 5. Again we have to prove all the properties of matroids. For (I1) $\emptyset \in \mathcal{I}$ we use (R1) to get that $0 \leq \mathsf{r}(X) \leq |\emptyset| = 0$ therefore it is satisfied. For (I2) $I \in \mathcal{I}, I' \subseteq I \Rightarrow I' \in \mathcal{I}$ we have that $\mathsf{r}(I) = |I|$ and $I' \subseteq I$ so $\mathsf{r}(I') + \mathsf{r}(I \setminus I') \geq \mathsf{r}(I) + \mathsf{r}(\emptyset) = |I| + 0$ and also by (R1) $\mathsf{r}(I') + \mathsf{r}(I \setminus I') \leq |I'| + |I \setminus I'| = |I|$ so all inequalities are actually equalities.

Lastly the third (I3). Let $I_1, I_2 \in \mathcal{I}, |I_1| < |I_2| \Rightarrow \exists e \in I_2 \setminus I_1$ s.t. $I_1 + e \in \mathcal{I}$. For this we will use Lemma 3. We have that $\mathsf{r}(I_i) = |I_i|$ for $i = 1, 2$ where $|I_1| < |I_2|$ for contradiction assume that $\forall e \in I_2 \setminus I_1 : I_1 + e \notin \mathcal{I}$ therefore $|I_1| = \mathsf{r}(I_1) \leq \mathsf{r}(X + e) < |I_1| + 1$. This means that the $\leq$ is $=$ instead. Now use the lemma

$$|I_2| = \mathsf{r}(I_2) \leq \mathsf{r}(I_1 \cup (I_2 \setminus I_1)) = \mathsf{r}(I_1) = |I_1|$$

where $I_1 \cup (I_2 \setminus I_1) \supseteq I_2$ and we get that $|I_2| \leq |I_1|$ which is a contradiction. □

For this part we could use any field F but as of now $\mathbb{R}$ is sufficient enough. Let $A \in \mathbb{R}^{n \times n}$. Where n-columns are the elements of matroid. We usually take the multi-set of the columns or indexes, since they may be the same (parallel) columns. Also observe that for every operation as in Gauss elimination it will preserve the matroid same up to isomorphism. So we may use the Gauss-Jordan elimination. By other operations we may have matrix I of $\mathsf{r}(E)$ rows and number of basis columns. This format is often called *the standard form.* An example is when $A = (0, 0, \ldots, 0)$ where this is a special case when $|\mathcal{I}| = 1$ and $\mathcal{I} = \{\emptyset\}$.

1.4 Uniform matroids

Definition 7. *For $0 \leq r \leq n \neq 0, |E| = n$ and $\mathcal{I} = \{X \subseteq E : |X| \leq r\}$ is* ***Uniform matroid*** *$U_{r,n} = (E, \mathcal{I})$.*

All the properties should be formally proven, but one can already see that all (I1), (I2) and (I3) are really satisfied. Now we will show us some examples.

Example. The matroid $A = (0, 0, \ldots, 0)$ is actually $\mathcal{M}(A) \cong U_{0,n}$.

Example. Now remind ourselves the example in the beginning, that is the graphic matroid. If we take graph as a trees then $\mathsf{r}(\mathcal{M}) = \mathsf{r}(E) =$ the size of spanning tree. For a tree with n vertices we obtain $U_{n,n}$ matroid. Note that we can now see that every operation that does not effect circuits neither effects the matroid.

Example. For other graphic matroids see:

- $\mathcal{M}(C_n) = U_{n-1,n}$;
- $U_{0,n}$ is for a graph with n-loops;
- $U_{1,n}$ is for n-parallel edge;
- $U_{2,n}$ is more interesting, because $U_{2,2}$ is a P_3 and $U_{2,3}$ is C_3, but for $n \geq 4$ there is no (multi-)graph representing it.

1.5 Visualization of matroids

From the previous part we see that some matroids cannot be visualized by graphs. So the question is whether we can visualize it in some other way. Lets take $U_{2,4}$ for an example, for which we construct the matrix:

$$\begin{pmatrix} 1 & 0 & \color{red}{1} & \color{blue}{1} \\ 0 & 1 & \color{red}{1} & \color{blue}{-1} \end{pmatrix}$$

See that the red numbers are forced to be ones and then the blue ones are forced to use some other element. This also implies that the field has to have at least three elements. This way we can visualize the $U_{2,4}$ by depicting the vectors in the plane.

Alternatively we may use affine spaces. For them we know that one element is always independent and so are two points which also forms a line. To add dependent points we have to put them on the line. Therefore four points on the line also visualize $U_{2,4}$. Also for $U_{1,3}$ we use single coordinate for all points.

Also when using affine spaces we can easily visualize $U_{3,n}$ by simply putting n points in general position.

(a) Representation by vectors.

(b) Affine representation.

Figure 1.1: Some different ways of visualization of $U_{2,4}$.

Some additional notes are for when we use some other field one can use the Fano's plane which specifically represents a Fano's matroid F_7. Which cannot be represented by reals.

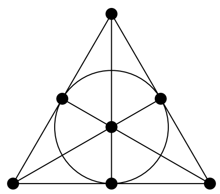


Figure 1.2: Fano's plane.

1.6 (Direct) Sum of matroids (also disjoint union)

Definition 8. *We have two matroids $\mathcal{M}_i = (E_i, \mathcal{I}_i)$ for $i = 1, 2$, then the (direct) sum $\mathcal{M}_1 \bigoplus \mathcal{M}_2$ is defined as a matroid $\mathcal{M} = (E, \mathcal{I})$ where $E = E_1 \dot\cup E_2$ and $\mathcal{I} = \{X \subseteq E, X \cap E_i \in \mathcal{I}_i, i = 1, 2\}$.*

Observation. *Lets see the basis and circuits:*

$$\mathcal{B}(\mathcal{M}_1 \bigoplus \mathcal{M}_2) = \{B_1 \cup B_2, B_i \in \mathcal{B}_i, i = 1, 2\}$$
$$\mathcal{C}(\mathcal{M}_1 \bigoplus \mathcal{M}_2) = \mathcal{C}_1 \cup \mathcal{C}_2$$
$$X \subseteq E : \mathsf{r}(X) = \mathsf{r}_1(X \cap E_1) + \mathsf{r}_2(X \cap E_2)$$

Chapter 2

Duals & Minors

2.1 Duals

Firstly we will take a look at duals of matroids.

Claim 6. *Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid and $\mathcal{B}$ its bases. We set $\mathcal{B}^* = \{E \setminus B : B \in \mathcal{B}\}$ then $\mathcal{B}^*$ satisfies (B1) and (B2).*

Proof. Firstly (B1) is easy. For (B2) $(E \setminus B_1), (E \setminus B_2) \in \mathcal{B}^*, \forall e \in (E \setminus B_1) \setminus (E \setminus B_2) = B_2 \setminus B_1, \exists f \in B_1 \setminus B_2 = (E \setminus B_2) \setminus (E \setminus B_1)$. Now we apply (B2') and get that $(B_1 - f) + e \in \mathcal{B}$ then $E \setminus ((B_1 - f) + e) = ((E \setminus B_1) - e) + f$. □

Therefore $\exists \mathcal{M}^*$ matroid with $\mathcal{B}(\mathcal{M}^*) = \mathcal{B}^*$ which will be called a **dual**. Generally we will denote duals $\mathcal{M}$ as $\mathcal{M}^*$. Also we will call such elements with a prefix co-. For example $\mathcal{B}^*$ will be a co-bases and so on.

Observation. $(\mathcal{M}^*)^* = \mathcal{M}$

Proposition 7. *There are two basic observations:*

1. $\mathsf{r}(\mathcal{M}) + \mathsf{r}(\mathcal{M}^*) = |E|$
2. $\forall X \subseteq E : \mathsf{r}^*(X) = |X| - \mathsf{r}(\mathcal{M}) + \mathsf{r}(E \setminus X)$

Proof. 1. is obvious from the definitions. 2. we denote I^* as the max independent subset of X in $\mathcal{M}^*$ and I as the max independent subset of $E \setminus X$ in $\mathcal{M}$. Then $\exists B \in \mathcal{B}, B \cap I^* = \emptyset$. We may assume $I \subseteq B \Rightarrow \mathsf{r}(B) = |B| = \mathsf{r}(\mathcal{M})$.

$$\begin{aligned} B &\subseteq E \setminus I^* \\ \mathsf{r}(B) &\leq \mathsf{r}(E \setminus I^*) \leq \mathsf{r}(\mathcal{M}) \text{ therefore we get equality} \\ \mathsf{r}(B) &= \mathsf{r}(E \setminus I^*) \end{aligned}$$

Let $B^* = E \setminus B$ be the basis of $\mathcal{M}^*$ and $I^* \subseteq B^*$, moreover $I^* = B^* \cap X$. Also $I = B \cap (E \setminus X)$.

$$|X| = |X \cap B| + |X \cap B^*| = |B| - |I| + |I^*| = \mathsf{r}(\mathcal{M}) - \mathsf{r}(E \setminus X) + \mathsf{r}^*(X)$$

□

Definition 9. *We say that $H \subseteq E$ is a* ***hyperplane*** *in $\mathcal{M}$ if H is $\subsetneq$-max subset with $\mathsf{r}(H) < \mathsf{r}(\mathcal{M})$. Or in other words*

$$\forall e \in E \setminus H : \mathsf{r}(H) < \mathsf{r}(H + e) < \mathsf{r}(\mathcal{M}) \textit{ so } \mathsf{r}(H) = \mathsf{r}(\mathcal{M}) - 1$$

Lemma 4. *For a matroid $\mathcal{M} = (E, \mathcal{I})$ the following holds:*

$$\forall C^* \subseteq E, C^* \in \mathcal{C}^*(\mathcal{M}) \Leftrightarrow E \setminus C^* \textit{ is a hyperplane of } \mathcal{M}.$$

Proof. "$\Rightarrow$" Suppose $C^* \in \mathcal{C}^*$ by the dual of proposition 7 we get

$$\begin{aligned} \mathsf{r}(X) &= |X| - \mathsf{r}^*(\mathcal{M}) + \mathsf{r}^*(E \setminus X) \\ \mathsf{r}(E \setminus C^*) &= |E \setminus C^*| - \mathsf{r}^*(\mathcal{M}) + \mathsf{r}^*(\mathcal{C}^*) \\ &= |E| - |C^*| - \mathsf{r}^*(\mathcal{M}) + |C^*| - 1 \\ &= \mathsf{r}(\mathcal{M}) - 1 \end{aligned}$$

then this is maximal with this property, therefore it is a hyperplane.

"$\Leftarrow$" is analogous. □

Lets now diverge to the graphic matroids, where when we decrease $\mathsf{r}(\mathcal{M})$ by 1 this will result in increasing components of connectivity; hence co-circuits are edge-cuts.

Proposition 8. *Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid, $C \in \mathcal{C}, C^* \in \mathcal{C}^*$ then $|C \cap C^*| \neq 1$.*

Proof. By contradiction assume that $C \cap C^* = \{e\}$. Lets define $H = E \setminus C^*$ a hyperplane for which $e \notin H$. Now we compute the following

$$\begin{aligned}\mathsf{r}(C) + \mathsf{r}(E) &= \mathsf{r}(C - e) + \mathsf{r}(H + e)\\ &= \mathsf{r}(C \cap H) + \mathsf{r}(C \cup H)\\ &\leq \mathsf{r}(C) + \mathsf{r}(H)\\ &= \mathsf{r}(H) + \mathsf{r}(E) - 1, \text{ which is a contradiction.}\end{aligned}$$

□

Now we take a look at how does a direct sum of duals look like.

$$\begin{aligned}\mathcal{B}((\mathcal{M}_1 \bigoplus \mathcal{M}_2)^*) &= \{E \setminus B, B \in \mathcal{B}(\mathcal{M}_1 \bigoplus \mathcal{M}_2)\}\\ &= \{E \setminus (B_1 \cup B_2), B_1 \in \mathcal{B}_1, B_2 \in \mathcal{B}_2\}\\ &= \{(E_1 \cup E_2) \setminus (B_1 \cup B_2), B_1 \in \mathcal{B}_1, B_2 \in \mathcal{B}_2\}\\ &= \{(E_1 \setminus B_1) \cup (E_2 \setminus B_2), B_1 \in \mathcal{B}_1, B_2 \in \mathcal{B}_2\}\\ &= \{B_1^* \cup B_2^*, B_1^* \in \mathcal{B}^*(\mathcal{M}_1), B_2^* \in \mathcal{B}^*(\mathcal{M}_2)\}\\ &= \mathcal{B}(\mathcal{M}_1^* \bigoplus \mathcal{M}_2^*)\end{aligned}$$

Therefore we may say that $(\mathcal{M}_1 \bigoplus \mathcal{M}_2)^* = \mathcal{M}_1^* \bigoplus \mathcal{M}_2^*$.

2.2 Minors

Reader may already know minors in graph theory. They are made by two operations. Deletions of vertices and edges and contractions of edges. For minors it will work similarly, therefore we define such operations.

Definition 10 (Deletion)**.** *For a matroid $\mathcal{M} = (E, \mathcal{I})$ for $T \subseteq E$ we define $\mathcal{M} \setminus T = (E \setminus T, \mathcal{I}')$ where $\mathcal{I}' = \{I \in \mathcal{I}, I \subseteq E \setminus T\}$.*

Definition 11 (Contraction)**.** $\mathcal{M}/T = (\mathcal{M}^* \setminus T)^*$

Proposition 9. *For $\mathcal{M} = (E, \mathcal{I}), T \subseteq E$ assume $X \subseteq E \setminus T$, then*

1. $\mathsf{r}_{\mathcal{M} \setminus T}(X) = \mathsf{r}_{\mathcal{M}}(X)$ *and*
2. $\mathsf{r}_{\mathcal{M}/T}(X) = \mathsf{r}_{\mathcal{M}}(X \cup T) - \mathsf{r}_{\mathcal{M}}(T)$.

Proof. 1. can be easily seen. For 2. we de the following computation.

$$\begin{aligned}\mathsf{r}_{\mathcal{M}/T}(X) &= \mathsf{r}^*_{\mathcal{M}^* \setminus T}(X)\\ &= |X| - \mathsf{r}_{\mathcal{M}^* \setminus T}(E \setminus T) + \mathsf{r}_{\mathcal{M}^* \setminus T}((E \setminus T) \setminus X)\\ &= |X| - \mathsf{r}^*(E \setminus T) + \mathsf{r}^*(E \setminus (T \cup X))\\ &= |X| - (|E \setminus T| - \mathsf{r}(E) + \mathsf{r}(T)) + |E \setminus (T \cup X)| - \mathsf{r}(E) + \mathsf{r}(E \setminus (E \setminus (T \cup X)))\\ &= |X| - |E| + |T| + |E| - |T| - |X| + \mathsf{r}(E) - \mathsf{r}(E) - \mathsf{r}(T) + \mathsf{r}(T \cup X)\\ &= \mathsf{r}(T \cup X) - \mathsf{r}(T)\end{aligned}$$

□

Proposition 10. *We can prove that $\mathcal{M}?T = (E \setminus T, \mathcal{I}')$ where $\mathcal{I}' = \{I \subseteq E \setminus T | I \cup B_T \in \mathcal{I}\}$, where B_T is max independent subset of T.*

Proof. In one direction lets have $I \subseteq E \setminus T$ s.t. $U \cup B_T \in \mathcal{I}$ now its rank has to be equal to its size.

$$\begin{aligned}\mathsf{r}_{\mathcal{M}/T}(I) &= \mathsf{r}(I \cup T) - \mathsf{r}(T)\\ &= \mathsf{r}(I \cup B_T) - \mathsf{r}(B_T)\\ &= |I \cup B_T| - |B_T|\\ &= |I| + |B_T| - |B_T| = |I|\end{aligned}$$

Now the other direction. For that lets have $X \in \mathcal{I}'$ then the following holds.

$$
\begin{aligned}
|X| &= \mathsf{r}_{\mathcal{M}/T}(X) = \mathsf{r}(X \cup T) - \mathsf{r}(T) = \mathsf{r}(X \cup T) - \mathsf{r}(B_T) = \mathsf{r}(X \cup B_T) - |B_T| \\
|X \cup B_T| &= |X| + |B_T| = \mathsf{r}(X \cup B_T) \Rightarrow X \cup B_T \in \mathcal{I}
\end{aligned}
$$

□

Therefore we may say that for dual it is true that: $B' \in \mathcal{B}(\mathcal{M}/T) \Leftrightarrow \exists B_T \in \mathcal{B}(\mathcal{M}|T)$ s.t. $B' \cup B_T \in \mathcal{B}(\mathcal{M})$ where existential kvantificator can be replaced by for all. Also on notation $\mathcal{M}|T = \mathcal{M} \setminus (E \setminus T)$ called the *restriction*.

Proposition 11. *$\mathcal{C}(\mathcal{M}/T)$ are minimal non-empty members $\{C \setminus T | C \in \mathcal{C}(\mathcal{M})\}$.*

Proof. For "$\Rightarrow$" consider $C_1 \in \mathcal{C}(\mathcal{M}/T)$ and B_T max independent in $\mathcal{M}|T$. $C_1 \cup B_T \notin \mathcal{I}, \forall e \in C_1 : (C_1 - e) \cup B_T \in \mathcal{I}$ and therefore $\exists C \in \mathcal{C}(\mathcal{M})$ s.t. $C_1 \subseteq C \subseteq C_1 \cup B_T \Rightarrow C_1 = C \setminus B_T = C \setminus T$.

Now for "$\Leftarrow$" let $D \setminus T$ be min non-empty member $\{C \setminus T | C \in \mathcal{C}(\mathcal{M})\}$ so $D \cap T \subsetneq D \Rightarrow D \cap T \in \mathcal{I} \Rightarrow \exists B_T$ max independent in $\mathcal{M}|T$ s.t. $D \cap T \subseteq B_T$ and now $D \subseteq D \cup B_T = (D \setminus T) \cup B_T \notin \mathcal{I}$ because it contains a circuit $\Rightarrow (D \setminus T) \notin \mathcal{I}(\mathcal{M}/T)$ therefore $\exists D' \in \mathcal{C}(\mathcal{M}/T) : D' \subseteq D \setminus T$ if $D' \subsetneq D \setminus T$ then it would contradicts the minimality. □

Claim 12. *For $\mathcal{M} = (E, \mathcal{I}), T_1, T_2 \subseteq E, T_1 \cap T_2 = \emptyset$ we have:*

1. $(\mathcal{M} \setminus T_1) \setminus T_2 = (\mathcal{M} \setminus T_2) \setminus T_1 = \mathcal{M} \setminus (T_1 \cup T_2)$*;*
2. $(\mathcal{M}/T_1)/T_2 = (\mathcal{M}/T_2)/T_1 = \mathcal{M}/(T_1 \cup T_2)$*;*
3. $(\mathcal{M} \setminus T_1)/T_2 = (\mathcal{M}/T_2) \setminus T_1$*.*

Proof. Lets go through all statements.

1. This is obviously true, since we only delete sets which is same.
2. For this see

$$
\begin{aligned}
(\mathcal{M}/T_1)/T_2 &= (\mathcal{M}^* \setminus T_1)^*/T_2 = ((\mathcal{M}^*\ T_1)\ T_2)^* \\
&= (\mathcal{M}^* \setminus (T_1 \cup T_2))^* = \mathcal{M}/(T_1 \cup T_2).
\end{aligned}
$$

3. Lets have $X \subseteq E \setminus (T_1 \cup T_2)$, then:

$$
\begin{aligned}
\mathsf{r}_{(\mathcal{M}/T_2)\setminus T_1}(X) &= \mathsf{r}_{\mathcal{M}/T_2}(X) = \mathsf{r}_{\mathcal{M}}(X \cup T_2) - \mathsf{r}_{\mathcal{M}}(T_2) \\
&= \mathsf{r}_{\mathcal{M}\setminus T_1}(X \cup T_2) - \mathsf{r}_{\mathcal{M}\setminus T_1}(T_2) = \mathsf{r}_{(\mathcal{M}\setminus T_1)/T_2}(X).
\end{aligned}
$$

□

Corollary. $\mathcal{M}$ has minor $\mathcal{N}$, then $\mathcal{M}^*$ has minor $\mathcal{N}^*$. Namely $\mathcal{N} = (\mathcal{M} \setminus T_1)/T_2$ then $\mathcal{N}^* = (\mathcal{M}^* \setminus T_2)/T_1$.

2.3 Duals and minors of vector matroids

Theorem 13. *Let $\mathcal{M} = \mathcal{M}(A)$ be a matroid over matrix A s.t. $\mathcal{M} \ncong U_{0,n}$ and $\mathcal{M} \ncong U_{n,n}$. We may consider standard form which is $A = (I_n|D)$ and $\mathcal{M}(A) = \mathcal{M}((I_n|D))$ and $r = \mathsf{r}(\mathcal{M})$ then $\mathcal{M}^* = \mathcal{M}(D^T|I_{n-r})$.*

Proof. See that $B \in \mathcal{B}(\mathcal{M}) \Leftrightarrow B = \{e_1, e_2, \dots, e_n\}$ which all e_i are linearly independent in $(I_n|D)$. Now take a look at the matrix:

$$
\left[\begin{array}{c|cc}
\multirow{2}{*}{I_n} & D_{11} & D_{12} \\
 & D_{21} & D_{22}
\end{array}\right]
$$

Consider that first s columns are taken as first columns from I_n and the rest is from D_{11}. Which also means that $\mathsf{r}(D_{21}) = r - s$. Now take the transposed matrix.

$$
\left[\begin{array}{cc|c}
D_{11}^T & D_{21}^T & \multirow{2}{*}{I_{n-r}} \\
D_{12}^T & D_{22}^T &
\end{array}\right]
$$

There the rank $\mathsf{r}(D_{21}^T) = r - s$ which means that all of $E \setminus B$ are linearly independent in $(D^T|I_n)$. □

Now we take a moment to explore the deletion. For that we just erase the columns which are about to be deleted. So for contraction is is also nicely working from the dual and deletion. All in all vector matroids are closed under both **minors** and **duals**. Also note that if D would be symmetric (i.e. $D = D^T$) then $\mathcal{M} \cong \mathcal{M}^*$ also called **self-dual**.

2.4 Duals and minors of graphic matroids

Firstly consider a deletion in a graphic matroid. This will correspond to simple deletion of all such edges. Now for contractions we will be looking at it just for one single element.

Proposition 14. *$\mathcal{M} = \mathcal{M}(G), e \in E$ which is an element of $\mathcal{M}$ and also an edge. Them $\mathcal{M}(G)/\{e\} = \mathcal{M}(G/e)$.*

Proof. If e is a loop, then we can simply delete it in matroid and also in the graph. Otherwise $U \subseteq E - e$ is acyclic in G/e if and only if $I \cup \{e\}$ is acyclic in G if and only if $I \in \mathcal{M}(G/e) \iff I \cup \{e\} \in \mathcal{I}$. $\square$

From this proposition and the easy observation we obtain the fact that graphic matroids are closed under **minor** operations. Let now consider duals of graphic matroids for a moment. The duals are quite nice since it follows from graph duals which are fairly known. That is we have one-to-one correspondence between $E(G)$ and $E(G^*)$. Also $(G^*)^* = G$ and $\mathcal{M}^*(G) = \mathcal{M}(G^*)$. Moreover having a circuit in G corresponds to min cut of the dual hence the co-circuit. There the duality works.

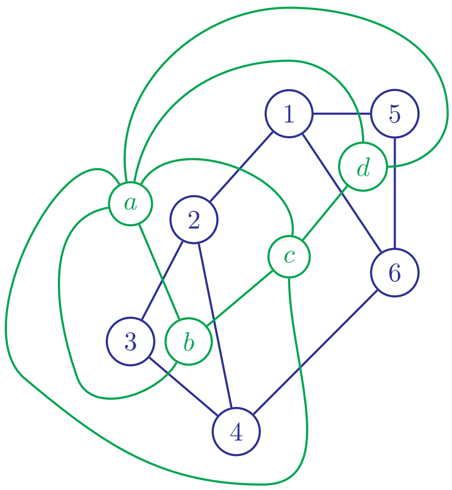


Figure 2.1: A primal graph G and its dual G^*.

Also duals in Matroids (and also minors) were inspired from graphs. Now we have encountered only planar graphs. But one can ask what about non-planar ones. By Kuratowsku and the fact that graphic matroids are closed under minor operations we get the following proposition.

Proposition 15. *$\mathcal{M}^*(K_5)$ (and $\mathcal{M}^*(K_{3,3})$) are not graphic.*

Proof. By a contradiction: $\exists G : \mathcal{M}(G) = G^*(K_5)$. By that $|E| = 10, \mathsf{r}(\mathcal{M}^*(K_5)) = 6 = 10-4$. Also $|V(G)| = 7$ so average degree is $\frac{20}{7} < 3$. Which means that there exists a vertex v s.t. $\deg(v) = 1$ or 2. This leads to at most 2 edges therefore the size of min edge cut is 2 and so is the size of co-circuit of $\mathcal{M}^*(K_5)$ hence the size of circuit in $\mathcal{M}(K_5)$ is 2 which is a contradiction. Similar argument can be made for $K_{3,3}$. $\square$

From these facts if we have a non-planar graph its dual is **not graphic**. Therefore we get the following diagram.

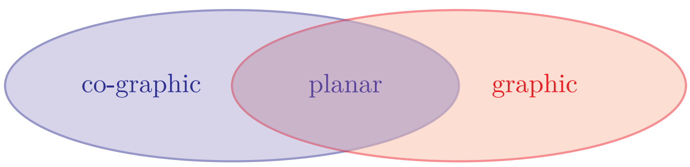


Figure 2.2: Diagram of graphic duals.

Chapter 3

Algorithms

In this section we will walk through some of the known matroid algorithms for solving some problems. Also we may derive some more information about the matroids themselves by looking at the solution of the given algorithms.

3.1 Greedy algorithm

The main algorithm is greedy one. One can already know the greedy algorithm for min spanning tree which is gradually putting lightest edges not forming cycle into the set. Now it will be pretty much the same only we will be maximizing and not minimizing. That is for minimizing we create a constant C and subtract every value from it and still look for maximum which will indeed be a minimum with the original values.

First question is how to save all values for given matroid. Because the isze of $\mathcal{I}$ can be exponentially large. Therefore we will be working with so called **oracle**. That is for $X \subseteq E$ we ask if X is independent $\in \mathcal{I}$ or not.

Algorithm 1 Greedy algorithm.

Require: Matroid $\mathcal{M} = (E, \mathcal{I})$ and weight function $w : E \to \mathbb{R}_0^+$.
Ensure: $I \in \mathcal{I}$ with max $w(I) = \sum_{e \in I} w(e)$.

Sort E s.t. $w(e_1) \geq w(e_2) \geq \cdots \geq w(e_n)$.
$E_0 = \emptyset$
for $i = 1, 2, \ldots, n$ **do**
    if $E_{i-1} + e_i \in \mathcal{I}$ **then**
        $E_i = E_{i-1} + e_i$
    else
        $E_i = E_{i-1}$
    end if
end for
return E_n

3.1.1 Correctness

Firstly we can clearly see that $\forall i : E_i \subseteq E$ and $E_i \in \mathcal{I} \Rightarrow E_n \in \mathcal{I}$ which also means that $E_n \in \mathcal{I}$ and $E_n \in \mathcal{B}$.

Now look at maximality. For contradiction $\exists E' \in \mathcal{B}$ s.t. $w(E') > w(E_n)$. See that E_n is formed by $e_{i_1}, e_{i_2}, \ldots, e_{i_r}$ if $r = \mathsf{r}(\mathcal{M})$ $(i_1 < i_2 < \cdots < i_r)$ and also E' is formed by $e_{j_1}, e_{j_2}, \ldots, e_{j_r}$ $(j_1 < j_2 < \cdots < j_r)$, where the lower index the higher weight. Therefore $\exists k$ s.t. $w(e_{i_k}) > w(e_{j_k})$ and lets take such smallest one. Now lets have $I_1 = \{e_{i_1}, \ldots, e_{i_{k-1}}\}$ and $I_2 = \{e_{j_1}, \ldots, e_{j_k}\}$ and apply (I3) because $|I_1| < |I_2|$ therefore $\exists l : I_1 + e_{j_l} \in \mathcal{I}$ and $w(e_{j_l}) \geq w(e_{j_k}) > w(e_{i_k})$ and $e_{j_l} \notin I_1$ which is a contradiction because algorithm would have chosen e_{j_l} instead of e_{i_k}.

3.1.2 Time complexity

Firstly sorting E is in $O(n \log n)$. Then the loop has n repetitions where in every step we call an oracle. Lets say that the oracle has time complexity t so the entire loop take nt time. So altogether we obtain $O(n \log n + nt)$.

Lastly note that non-negative weight function is important for the algorithm to work. But we may see that this procedure can be used to define the matroid. Which we will talk about now.

3.1.3 Defining matroid by greedy algorithm

Proposition 16. *We have E finite non-empty set, let $\mathcal{F} \subseteq 2^E, \emptyset \in \mathcal{F}$ s.t. $\forall w : E \to \mathbb{R}_0^+$ greedy algorithm find max weighted member of $\mathcal{F}$, then $\mathcal{F}$ satisfies (I1),(I2) and (I3).*

Proof. Firstly (I1) is easy, since $\emptyset \in \mathcal{F}$.

Now take a look at (I2). By contradiction $I' \subseteq I$ and $I \in \mathcal{F}$ but $I' \notin \mathcal{F}$. WLOG $|I| = |I'| + 1$. We will define the weight function like this:

$$w(e) = \begin{cases} 2 & \text{if } e \in I' \\ 1 & \text{if } e \in I \setminus I' \\ 0 & \text{otherwise} \end{cases}.$$

So $w(I) = 2 \cdot |I'| + 1$ and greedy algorithm find $|I'|$, but at least one element has to be skipped. So the weight of the result is $\leq 2(|I'| - 1) + 1 = 2 \cdot |I'| - 1 < w(I)$ which is a contradiction.

Finally (I3) which is $I_1, I_2 \in \mathcal{F}, |I_1| < |I_2| : \exists e \in I_2 \setminus I_1 : I_1 + e \in \mathcal{F}$ and WLOG $|I_2| = |I_1| + 1$. By contradiction $I_1, I_2 \in \mathcal{F}, |I_1| = |I_2| - 1$ and $\forall e \in I_2 \setminus I_1 : I_! + e \notin \mathcal{F}$. Denote $k = |I_1|$. Lets define the weight function.

$$w(e) = \begin{cases} k+2 & \text{if } e \in I_1 \\ k+1 & \text{if } e \in I_2 \setminus I_1 \\ 0 & \text{otherwise} \end{cases}.$$

Where $w(I_2) \geq |I_2| \cdot (k+1) = (k+1)^2$. The greedy algorithm firstly takes all $e \in I_1$ so after k steps $E_k = I_1$, but then non-zero elements are skipped $(I_2 \setminus I_1)$ so the result has $w = I_1 \cdot (k+2) = k(k+2)$ but $k(k+2) = k^2 + 2k < k^2 + 2k + 1 = (k+1)^2$ so we got the contradiction. □

3.2 Matroid intersection problem

Firstly we must define this problem. As an **input** we have $\mathcal{M}_i = (E, \mathcal{I}_i)$ for $i = 1, 2$ and **output** is to find max $I \in \mathcal{I}_1 \cap \mathcal{I}_2$. Firstly observe that there always exists a solution $\emptyset$.

Theorem 17. *Having $\mathcal{M}_i = (E, \mathcal{I}_i)$ for $i = 1, 2$ then*

$$\max_{I \in \mathcal{I}_1 \cap \mathcal{I}_2} |I| = \min_{E_1 \cup E_2 = E} \mathsf{r}_1(E_1) + \mathsf{r}_2(E_2).$$

Proof. For "$\leq$" we have $I \in \mathcal{I}_1 \cap \mathcal{I}_2, E_1 \cup E_2 = E$. We may consider it is disjoint since $E_2 = E \setminus E_1$ might only decrease the rank.

$$\begin{array}{rcccl} |I \cap E_1| & = & \mathsf{r}_1(I \cap E_1) & \leq & \mathsf{r}_1(E_1) \\ |I \cap E_2| & = & \mathsf{r}_2(I \cap E_2) & \leq & \mathsf{r}_2(E_2) \quad \text{(sum both together)} \\ |I| & & & \leq & \mathsf{r}_1(E_1) + \mathsf{r}_2(E_2) \end{array}$$

Now "$\geq$" for which we will state the algorithm. Firstly start in $I = \emptyset$. Then $I \in \mathcal{I}_1 \cap \mathcal{I}_2$ construct H bipartite graph with $I, X = E \setminus I$ parts. Create arc $y \to x$ if $(I - y) + x \in \mathcal{I}_1$ and arc $y \leftarrow x$ if $(I - y) + x \in \mathcal{I}_2$. Then define $X_1 = \{x \in X | I + x \in \mathcal{I}_1\}$ and $X_2 = \{x \in X | I + x \in \mathcal{I}_2\}$.

1. If $X_1 \cap X_2 = \emptyset$ we just add such element from intersection to I.

2. Otherwise find $X_1 \to X_2$ path if there is one, and choose shortest one. That is $x_0 y_1 x_1 y_2 x_2 \ldots y_k x_k$ this path where $x_0 \in X_1$ and $x_k \in X_2$. Now we update I like this $I' = (I \setminus \{y_1, y_2, \ldots, y_k\}) \cup \{x_0, x_1, x_2, \ldots, x_k\}$. Clearly the size is bigger but it is independent? We will sketch the proof of this. We have to show that $I' \in \mathcal{I}_1 \cap \mathcal{I}_2$.

   For $I' \in \mathcal{I}_1$ we proceed by induction on k. Lets have $I \in \mathcal{I}$ and $(I - y_k) + x_k$ because $y_k \to x_k$ by the definition of arc it implies that it is $\in \mathcal{I}_1$. Lets denote $I_l = (I \setminus \{y_l, \ldots, y_k\}) \cup \{x_l, \ldots, x_k\} = (((I \setminus \{y_{l+1}, \ldots, y_k\}) \cup \{x_{l+1}, \ldots, x_k\}) - y_l) + x_l$ and I_{l+1} is $\in \mathcal{I}_1$ by induction. So $I_l = (I_{l+1} - y_l) + x_l$, $I_l + x_l \in \mathcal{I}_1$ and $y_l \to x_l$ therefore $(I - y_l) + x_l \in \mathcal{I}_1$. We obtained two independent sets where $|I_l - x_l| = |(I - y_l) + x_l| - 1$ so by (I3) $\exists z \in (I - y_l) + x_l$ s.t. $(I_l - x_l) + z \in \mathcal{I}_1$.

   If $z = x_l$ we are done, otherwise if $z \neq x_l$ we set $(I - y_l + x_l) \setminus (I_l - x_l) = \{x_l, y_{l+1}, \ldots, y_k\}$ so $\exists i : z = y_i$ $(I_l - x_l) + y_i \in \mathcal{I}_1$ and again apply (I3) so $\exists z' \in ((I_l - x_l) + y_i) \setminus (I - y_l)$ s.t. $(I - y_l) + z' \in \mathcal{I}_1$ and $z' = \{x_{l+1}, \ldots, x_k\}$. This implies that $y_l \to z'$ which contradicts the shortest path. Hence we may remove $y_1, \ldots, y_k$ and add $x_1, \ldots, x_k$. Now we only need to show we may also add x_0. For showing $I' \in \mathcal{I}_2$ we would proceed similarly.

3. Next step is what if the path does not exists? We want to show a partitioning E_1 and E_2 such that $X_2 \subseteq E_1$ and $X_1 \subseteq E_2$ and there is no edge from E_2 to E_1. We create the partition by adding all elements accesible from X_1 to E_2 and the rest will form E_1.

   Observation. $\mathsf{r}_i(E_i) = |I \cap E_i|, i = 1, 2$

   Proof of observation. For $i = 1$ we have that $\mathsf{r}_1(E_1) = |I \cap E_1|$ where $I \cap E_1$ is independent so $\mathsf{r}_1(E_1) \geq \mathsf{r}_1(I \cap E_1))$. Assume that it is strict, i.e. $\mathsf{r}_1(E_1) > \mathsf{r}_1(I \cap E_1)$. Then $\exists x \in E_1 \setminus I : \mathsf{r}(I \cap E_1 + x) > \mathsf{r}(I \cap E_1)$ where $I \cap E_1 + x \in \mathcal{I}_1$. But $I + x \notin \mathcal{I}_1$ because this $x \in X_1$ and $E_1 \cap X_1 = \emptyset$. Also $(I - y) + x \in \mathcal{I}_1, y \in I \cap E_2$ from (I3) property. This all implies that there is an arc $y \to x$ which contradicts $E_1 \to E_2$ having no edge. □

   With this observation we may see that $|I| = |I \cap E_1| + |I \cap E_2| = \mathsf{r}_1(E_1) + \mathsf{r}_2(E_2)$ which finishes the proof of the theorem.

□

3.2.1 Time complexity

We have at most $\mathsf{r}(\mathsf{r} \geq \mathsf{r}_1(E), \mathsf{r}_2(E))$ iterations. Then also $2 \cdot |I| \cdot |X|$ queries for independent sets which is $\leq 2\,\mathsf{r}\,n$ and also we have $2 \cdot |X| \leq 2n$ other queries. Thus in total $O(\mathsf{r}\,n)$ queries and if we denote the time for query as τ then the time complexity is $O(\tau\,\mathsf{r}\,n)$. So all together it is $O(\mathsf{r}^2\,n\tau)$. Another remark is that it is known that we could obtain $O(\mathsf{r}^{3/2}\,n\tau)$.

3.2.2 Applications

We will show us some usage of the theorem and the algorithm itself. The next theorems and algorithms are well known.

Maximal matching in bipartite graph

Theorem 18. *G is connected bipartite graph. Then maximum matching of G has size equal to minimum vertex cover of G.*

Proof. Let $G = (V_1 \cup V_2, E)$ and $\mathcal{M}_i = (E, \mathcal{I}_i)$ for $i = 1, 2$. The matroids are defined by independ sets, where $E \supseteq I \in \mathcal{I}_i$ iff $\forall v \in V_i$ $\deg(v_i) \leq 1$ in $(V_1 \cup V_2, I)$. See an example on Fig. 3.1. Therefore the maximal $I \in \mathcal{I}_1 \cap \mathcal{I}_2$ is equal to maximum matching of G. So by the theorem 17 $\exists E = E_1 \cup E_2$ s.t. $|I| = \mathsf{r}_1(E_1) + \mathsf{r}_2(E_2)$. Now take a look at the rank function. Denote $V_i' = \{v \in V_i | \exists e \in X : v \in e\}$ the rank function is $\mathsf{r}_i(X) = |V_i'|$. Then from $\mathsf{r}_1(E_1)$ we get $|V_1'|$ and similary $|V_2'|$ and hence $V_1' \cup V_2'$. Therefore by the theorem $= |V_1'| + |V_2'| = |V_1' \cup V_2'|$ which is indeed a minimum vertex cover.

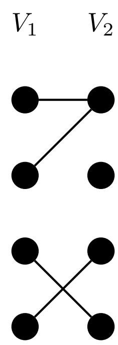


Figure 3.1: An example of matroids, where these edges are independent in $\mathcal{M}_1$ but not $\mathcal{M}_2$.

□

Nash-Williams

Theorem 19 (Nash-William)**.** *G is connected (multi)graph, $k \in \mathbb{N}$ there exists k pairwise disjoint spanning trees $\iff$ $\forall$ partition $V_1, \ldots, V_k$ of V we have $|\{e \in E, \forall i | e \cap V_i| \leq 1\}| \geq k(l-1)$.*

We will not prove this directly. Instead we will show more general matroid version which actually as a consequence proves this theorem.

Theorem 20. *Let $\mathcal{M} = (E, \mathcal{I})$ be a matroid and $k \in \mathbb{N}$. $\exists B_1, \ldots, B_k$ disjoint bases of $\mathcal{M} \iff \forall S \in E$ $|E \setminus S| \geq k(\mathsf{r}(E) - \mathsf{r}(S))$.*

Proof. Firstly we will create k copies of E that will be $E_0 = E \times \{1, \ldots, k\}$. Now we will define two matroids. $\mathcal{M}_1 = (E_0, \mathcal{I}_1)$ where $X \in \mathcal{I}_1$ if $\forall i = 1, \ldots, k$ $X_i = \{e : (e, i) \in X\} \in \mathcal{I}$, that is from the original matroid $\mathcal{M}$. And also $\mathcal{M}_2 = (E_0, \mathcal{I}_2)$ where $X \in \mathcal{I}_2 \iff \forall e \in E$ there is at most one i s.t. $(e, i) \in X$. Now we could say that it must be independent for every copy of E and they have to be disjoint to be in the intersection.

$\mathcal{M}$ has disjoint bases $B_1, \ldots, B_k \iff \exists I \in \mathcal{I}_1 \cap \mathcal{I}_2$ s.t. $|I| \geq k\,\mathsf{r}(E)$. And for the outline of the proof. Lets have k disjoint bases $X = \{(e, i), \exists i : e \in B_i\}$ and for the other implication $|I| = k\,\mathsf{r}(\mathcal{M})$ constuct $B_i = \{e, (e, i) \in I\}$ and $|B_i| = \mathsf{r}(B_i) \leq \mathsf{r}(\mathcal{M})$ since it is independent in $\mathcal{M}_2$ then $|I| = |\bigcup_i B_i|$ so $|B_i| = \mathsf{r}(\mathcal{M})$ for $i = 1, 2, \ldots, k$.

"$\Rightarrow$" Now $B_1, \ldots, B_k$ be disjoint bases of $\mathcal{M}$. See the following computation.

$$\begin{aligned}|E \setminus S| &\geq \sum_{i=1}^{k} |B_i \cap (E \setminus S)| = \sum_{i=1}^{k} |B_i \setminus (B_i \cap S)| = \sum_{i=1}^{k} |B_i| - |B_1 \cap S| \\ &= \sum_{i=1}^{k} \mathsf{r}(\mathcal{M}) - |B_i \cap S| = \sum_{i=1}^{k} \mathsf{r}(\mathcal{M}) - \mathsf{r}(B_i \cap S) \geq \sum_{i=1}^{k} \mathsf{r}(\mathcal{M}) - \mathsf{r}(S) = k \cdot (\mathsf{r}(\mathcal{M}) - \mathsf{r}(S))\end{aligned}$$

"$\Leftarrow$" Assume $\forall S \subseteq E : |E \setminus S| \geq k \cdot (\mathsf{r}(E) - \mathsf{r}(S))$. Now $|I| = \mathsf{r}_1(E_1) + \mathsf{r}_2(E_2)$ by the theorem 17. If $(e, i) \in E_2$ we can add all (e, j) to E_2 and $\mathsf{r}_2(E_2)$ does not increases. Let $E_2 = E' \times \{1, \ldots, k\}$ and $E_1 = E' \setminus E_2$. Set $S = E \setminus E'$. Then we have the following

$$\begin{aligned}\mathsf{r}_1(E_1) &= \sum_{i=1}^{k} \mathsf{r}(E_{1,i}) = k \cdot \mathsf{r}(S) \\ \mathsf{r}_2(E_2) &= |E'| \\ \mathsf{r}_1(E_1) + \mathsf{r}_2(E_2) &= k \cdot \mathsf{r}(S) + |E'| = k \cdot \mathsf{r}(S) + |E \setminus S| \geq k \cdot \mathsf{r}(S) + k \cdot \mathsf{r}(E) - k \cdot \mathsf{r}(S) = k \cdot \mathsf{r}(\mathcal{M})\end{aligned}$$

So it can be decomposed to $B_1, \ldots, B_k$ disjoint bases. $\square$

Chapter 4

Connectivity

We have seen some properties that were derived from graph theory. But now this is not the case. That is the connectivity of matroids is not directly translated from graphs, but instead 2-(vertex)-connectivity.

Proposition 21. *G without isolated vertices, G is 2-connected $\iff$ $\forall e, f \in E$ and $e \neq f$ $\exists C$ circuit s.t. $e, f \in E(C)$.*

Proof. This can be easily seen. Consider subdividing e (and f) by w_e (w_f) which by itself do not affect 2-connectivity, thic constructs G'. Therefore $\exists C'$ in G' where $w_e, w_f \in V(C')$. $\square$

Proposition 22. *The following properties are equivalent.*

(C3) $\forall C_1, C_2 \in \mathcal{C}, C_1 \neq C_2, e \in C_1 \cap C_2, \exists C_3 \subseteq (C_1 \cup C_2) - e, C_3 \in \mathcal{C}$

(C3') $\forall C_1, C_2 \in \mathcal{C}, C_1 \neq C_2, f \in C_1 \cap C_2, \exists C_3 : f \in C_3 \subseteq (C_1 \cup C_2) - e$

Proof. For contradiction let C_1, C_2 violates (C3') and $|C_1 \cup C_2|$ is minimal. By (C3) $\exists C_3$ where $e, f \notin C_3$ and by (C2) $\exists g \in C_2 \setminus C_1, g \in C_2 \cap C_3$. Since $f \notin C_2$ it implies $f \notin C_2 \cup C_3$ hence $|C_2 \cup C_3| < |C_1 \cup C_2|$. Use (C3') on $C_2, C_3, g \in C_2 \cap C_3, e \in C_2 \setminus C_3$ then $\exists C_4 : e \in C_4 \subseteq (C_2 \cup C_3) - g$. Now $g \notin C_1, C_4$ so $|C_1 \cup C_4| < |C_2 \cup C_3|$ therefore we again use (C3') $C_1, C_4, e \in C_1 \cap C_4, f \in C_1 \setminus C_4, \exists C : f \in (C_1 \cup C_4) - e \subseteq (C_1 \cup C_2) - e$ which is a contradiction. $\square$

Now we define a relation $\sim$ for $\mathcal{M} = (E, \mathcal{I})$ on $E \times E$ s.t. $e \sim f \iff (e = f) \vee (\exists C \in \mathcal{C} : e, f \in C)$.

Proposition 23. *Relation $\sim$ is an equivalence on E.*

Proof. We can easily see taht reflexivity and symmetry holds. Now for transitivity. $e \sim f$ and $f \sim g$ if one of these relations were obtained by $=$, then we can rename the elements and obtain $e \sim g$, thus we will assume both are obtained by the circuit property.

Suppose $\exists C'_1 \supseteq \{e, f\}, C'_2 \supseteq \{f, g\}$ and we want to find $C'_3 \supseteq \{e, g\}$. Let C_1, C_2 be s.t. $e \in C_1, g \in C_2$ and $C_1 \cap C_2 \neq \emptyset$ such that $|C_1 \cup C_2|$ is minimal. Denote $h \in C_1 \cap C_2, e \in C_1 \setminus C_2$ (otherwise we are done), this implies by (C3') that $e \in C_3 \subseteq (C_1 \cup C_2) - h$. If $g \in C_3$ we are done. Therefore assume $g \notin C_3$.

$\exists i \in C_2 \cap C_3, i \notin C_1, |C_2 \cup C_3| < |C_1 \cup C_2|, g \in C_2 \setminus C_3$ and by (C3') we get that $\exists C_4 : g \in C_4 \subseteq (C_2 \cup C_3) - i$. Due to the fact that $C_4 \cap (C_3 \setminus C_2) \neq \emptyset$, otherwise it would be a proper subset, and $C_3 \setminus C_2 \subsetneq C_1 \setminus C_2 \Rightarrow C_1 \cap C_4 \neq \emptyset$ and $i \notin C_! \cup C_4$ so $|C_1 \cup C_4| < |C_1 \cup C_2|$ which contradicts the minimality. $\square$

The classes of the equivalence $\sim$ on $E(\mathcal{M})$ form so called "**components**". Also one can easily see that $\mathcal{M}$ connected $\iff$ $|E| = 1$ or $\forall e, f \in E, \exists C \in \mathcal{C} : e, f \in C$.

4.1 Separators

Definition 12. ***Separation*** *$X \subseteq E$ s.t. X is union of components of $\mathcal{M}$.*

Proposition 24. *$\mathcal{M} = (E, \mathcal{I})$, X is separation $\iff$ $\forall C \in \mathcal{C} : C \subseteq X$ or $C \subseteq E \setminus X$.*

Proposition 25. *$\mathcal{M} = (E, \mathcal{I})$, X is separation $\iff$ $\mathsf{r}(X) + \mathsf{r}(E \setminus X) = \mathsf{r}(E)$.*

Proof. "⇒" by using submodularity we may see that $\mathsf{r}(X)+\mathsf{r}(E\setminus X) \geq \mathsf{r}(E)$ and now we have to show the other inequality. Let B_1 be max independent subset of X, hence $|B_1| = \mathsf{r}(X)$ and B_2 be max independent subset of $E \setminus X$, hence $|B_2| = \mathsf{r}(E \setminus X)$. Create $B = B_1 \cup B_2$. If X is a seprator then $B \in \mathcal{I}$ since B_1 and B_2 do not include a circuit and also no circuit is present in their union from the fact that X is a separator. Moreover

$$\mathsf{r}(E) \geq |B| = |B_1| + |B_2| = \mathsf{r}(X) + \mathsf{r}(E \setminus X).$$

"⇐" Assume that $\mathsf{r}(X) + \mathsf{r}(E \setminus X) = \mathsf{r}(E)$ and X is not a separator. Then $\exists C \in \mathcal{C} : C \cap X \neq \emptyset$ and $C \cap (E \setminus X) \neq \emptyset$. Now $C \cap X \in \mathcal{I}$ can be completed to B_1' max independent subset of X and similarly $C \cap (E \setminus X) \in \mathcal{I}$ can be completed to B_2'. Let $B' = B_1' \cup B_2'$ but $C \subseteq B' \Rightarrow B' \notin \mathcal{I}$ so $\mathsf{r}(B') < |B'|$, but on the other hand $|B'| = |B_1'| + |B_2'| = \mathsf{r}(X) + \mathsf{r}(E \setminus X) = \mathsf{r}(E)$. If $\mathsf{r}(B') < \mathsf{r}(E)$ this cannot happen, because otherwise we could add an elemnt so $\mathsf{r}(B') = \mathsf{r}(E)$. □

Proposition 26. *$\mathcal{M} = (E, \mathcal{I})$, X is separation* $\Rightarrow \forall F \subseteq E : \mathsf{r}(F) = \mathsf{r}(F \cap X) + \mathsf{r}(F \cap (E \setminus X)) = \mathsf{r}(F \cap X) + \mathsf{r}(F \setminus X)$.

Proof. THis proof is similar as in previous proposition, therefore is omitted. □

Proposition 27. $\mathcal{M} = (E, \mathcal{I}), X \subseteq E, \mathcal{M} \setminus X = \mathcal{M}/X \iff \mathsf{r}(X) + \mathsf{r}(E \setminus X) = \mathsf{r}(E)$

Proof. "⇒" Let B_x be max independent subset of X and B be max independent subset of $\mathcal{M} \setminus X = \mathcal{M}/X$. From $\mathcal{M}/X$ we get that $B \cup B_x \in \mathcal{B}(\mathcal{M})$ and from $\mathcal{M} \setminus X$ we get

$$\mathsf{r}(E) = |B \cup B_x| = |B| + |B_x| = \mathsf{r}(E \setminus X) + \mathsf{r}(X).$$

"⇐" Assume that $\mathsf{r}(X) + \mathsf{r}(E \setminus X) = \mathsf{r}(E)$ holds, compare $\mathcal{I}(\mathcal{M}/X)$ and $\mathcal{I}(\mathcal{M} \setminus X)$. Easily seen $\mathcal{I}(\mathcal{M}/X) \subseteq \mathcal{I}(\mathcal{M} \setminus X)$ is true for all X. Now $I \in \mathcal{I}(\mathcal{M} \setminus X) \Rightarrow \exists B$ max independent in $\mathcal{M} \setminus X$, $I \subseteq B \Rightarrow \exists B'$ s.t. $B \cup B' \in \mathcal{B}$ max independent in $\mathcal{M}$ therefore $|B \cup B'| = \mathsf{r}(X)$ and $|B| = \mathsf{r}(E \setminus X)$. From both we get the following

$$|B \cup B'| = \mathsf{r}(E) = \mathsf{r}(X) + \mathsf{r}(E \setminus X) = \mathsf{r}(X) + |B| \Rightarrow |B'| = \mathsf{r}(X)$$

and hence B' is max independent set of X. Lastly

$$I \cup B' \subseteq B \cup B' \in \mathcal{I} \Rightarrow I \cup B' \in \mathcal{I} \Rightarrow I \in \mathcal{I}(\mathcal{M}/X).$$

Therefore we get the other inclusion so it must be equal. □

Corollary. X is separator of $\mathcal{M} \iff X$ is a separator of $\mathcal{M}^*$. So also $\mathcal{M}$ is connected $\iff \mathcal{M}^*$ is connected.

Theorem 28. *$\mathcal{M} = \mathcal{M}_1 \bigoplus \mathcal{M}_2 \bigoplus \cdots \bigoplus \mathcal{M}_k$, $\mathcal{M}_i$ is connected s.t. $\exists X_1, \ldots, X_k$, $\mathcal{M}|_{X_i} = \mathcal{M}_i \iff X_1, \ldots, X_k$ are connected components of $\mathcal{M}$.*

Proof. We won't show the whole proof, but this follows from proposition on curcuits in directed sums and circuits in separators. □

4.2 Higher connectivity

For brewity and this section we will usually denote $X \subseteq E$ and then the component $E \setminus X$ as Y. If we look again at the connectivity define by separators we get that X is separator if and only if $\mathsf{r}(X) + \mathsf{r}(Y) = \mathsf{r}(E)$, note that $\mathsf{r}(X) + \mathsf{r}(Y) \geq \mathsf{r}(E)$ always hold for arbitrary X. We may rewrite the equation like $\mathsf{r}(X) + \mathsf{r}(Y) - \mathsf{r}(E) = 0$ and from this we will generalize to other types of connectivity.

Definition 13. *Partition of $E = X \cup Y$ is k-separation if*

$$(🥕) \quad \mathsf{r}(X) + \mathsf{r}(Y) - \mathsf{r}(E) \leq k - 1.$$

Definition 14. *Now we will define more types of separations:*

- *Tutte k-separation – If (🥕) holds and $|X|, |Y| \geq k$.*
- *Essential k-separation – If (🥕) holds and $\mathsf{r}(X), \mathsf{r}(Y) \geq k$.*
- *Cyclic k-separation – If (🥕) holds and both X and Y contains circuit ($\mathsf{r}(X) < |X|, \mathsf{r}(Y) < |Y|$).*

Definition 15. *From the separations we define connectivities.*

- *(Tutte) connectivity $\lambda(\mathcal{M}) = \min k$ s.t. $\mathcal{M}$ has Tutte k-separation, or $+\infty$ if it does not have one.*

- *Essential connectivity* $\kappa(\mathcal{M}) = \min k$ *s.t.* $\mathcal{M}$ *has essential* k*-separation, or* $\mathsf{r}(\mathcal{M})$ *if it does not have one.*
- *Cyclic connectivity* $\kappa^*(\mathcal{M}) = \min k$ *s.t.* $\mathcal{M}$ *has cyclic* k*-separtaion, or* $\mathsf{r}^*(\mathcal{M})$ *if it does not have one.*

Lemma 5. (X, Y) *is* k*-separation of* $\mathcal{M}$ *if and only if it is a* k*-separation of* $\mathcal{M}^*$*.*

Proof. $\mathsf{r}(X) + \mathsf{r}(E \setminus X) - \mathsf{r}(E) = \mathsf{r}(X) + \mathsf{r}^*(X) - |X| = \mathsf{r}^*(X) + \mathsf{r}^*(E \setminus X) - \mathsf{r}^*(E)$. □

Proposition 29. $\lambda(\mathcal{M}) = \lambda(\mathcal{M}^*)$*.*

Proof. For proof see the previous lemma and also the fact that $|X|, |Y| \geq k$ is not affected by duality. □

Proposition 30. $\kappa(\mathcal{M}) = \kappa^*(\mathcal{M}^*)$*.*

Proof. Let (X, Y) be essential k-separation of $\mathcal{M}$ and assume, that it defines $\kappa(\mathcal{M})$. We have that $\mathsf{r}(X) \geq k, \mathsf{r}(Y) \leq \mathsf{r}(E)$ so then by $\mathsf{r}(X) + \mathsf{r}(Y) - \mathsf{r}(E) \leq k - 1$ implies that $\mathsf{r}(Y) < \mathsf{r}(E)$, therefore there $\exists H$ hyperplane of $\mathcal{M}$ s.t. $Y \subseteq H$. Hence $(E \setminus H)$ is co-circuit, $E \setminus H \subseteq X$. This can also be proven for Y instead of X. Thus (X, Y) is also a cyclic k-separation of $\mathcal{M}^*$.

For the other way X contains a circuit C^* of $\mathcal{M}^*$ which implies that $E \setminus C^*$ is hyperplane of $\mathcal{M}$ and $Y \subseteq E \setminus C^*$ and therefore $\mathsf{r}(Y) < \mathsf{r}(E)$ so $\mathsf{r}(Y) - \mathsf{r}(E) \leq -1$ and hence $\mathsf{r}(X) \geq k$. □

4.2.1 Tutte connectivity of uniform matroids

Lemma 6. $\mathcal{M}$ *is Tutte* k*-connected* $(\lambda(\mathcal{M}) \geq k)$*,* $|E| \geq 2(k-1)$*. Then* $\forall C \in \mathcal{C}(\mathcal{M}), |C| \geq k$*. (And* $\forall C^* \in \mathcal{C}^*(\mathcal{M}), |C^*| \geq k$*.)*

Proof. Assume we have $C \in \mathcal{C}$, where $|C| = k' < k$. Then set $X = C, Y = E \setminus C$, $|Y| \geq k'$. See $\mathsf{r}(C) + \mathsf{r}(E \setminus C) - \mathsf{r}(E) \leq k' - 1$ because $\mathsf{r}(C) = k' - 1$ and $\mathsf{r}(E \setminus C) - \mathsf{r}(E) \leq 0$. All these implies that (X, Y) is Tutte k'-separation which is contradiction since it implies $\lambda(\mathcal{M}) \leq k'$. □

Lemma 7. $\mathcal{M}$ *is Tutte* k*-connected,* $|E| \geq 2k - 1$*, then* $\mathcal{M}$ *has no* k*-element set* C *s.t.* $C \in \mathcal{C} \cap \mathcal{C}^*$*.*

Proof. Assume it is not satisfied, thus $\lambda(\mathcal{M}) \geq k, |E| \geq 2k - 1$ and we have $\exists C \in \mathcal{C} \cap \mathcal{C}^*, |C| = k$. Then $\mathsf{r}(C) = k - 1$ and $\mathsf{r}(E \setminus C) = \mathsf{r}(E) - 1$ since C is circuit and co-circuit. Next $\mathsf{r}(C) + \mathsf{r}(E \setminus C) - \mathsf{r}(E) = k - 1 + \mathsf{r}(E) - 1 - \mathsf{r}(E) = k - 2$. Lastly $|C| = k \geq k - 1$ and $|E \setminus C| = |E| - k \geq 2k - 1 - k = k - 1$. Thus altogether C and $E \setminus C$ is $(k-1)$-separation and hence $\lambda(\mathcal{M}) \leq k - 1$, which is a contradiction. □

Proposition 31. *Tutte connectivity can be prescribed as*

$$\mathcal{U}_{r,n} = \begin{cases} r + 1 & \text{if } n \geq 2r + 2 \\ n - r + 1 & \text{if } n \leq 2r - 2 \\ \infty & \text{otherwise.} \end{cases}$$

Proof. Firslty note that $\mathcal{U}_{r,n}^* \cong \mathcal{U}_{n-r,n}$, and with $\lambda\mathcal{M} = \lambda(\mathcal{M}^*)$ we can assume without loss of generality that $r \geq n/2$. Which means that $n \geq 2r$, this way we got rid of the middle option, since we just switch to the dual.

Now let (X, Y) be a Tutte k-separation, without loss of generality $k \leq |X| \leq |Y|$ so $|Y| \geq n/2 \geq r$ which also implies that $\mathsf{r}(Y) = \mathsf{r}(E) = r$. Because $k - 1 \geq \mathsf{r}(X) + \mathsf{r}(Y) - \mathsf{r}(E) = \mathsf{r}(X)$ we get that $X \notin \mathcal{I}$ and from that follows that $|X| > r$, therefore $\mathsf{r}(X) = r \leq k - 1$.

In the first case set $|X| = r + 1, \mathsf{r}(X) = r$ and $|Y| \geq r + 1$ and $\mathsf{r}(Y) = r$. Get that $\mathsf{r}(X) + \mathsf{r}(Y) - \mathsf{r}(E) = \mathsf{r}(X) = r = (r + 1) - 1$ so it is Tutte $(r + 1)$-separation.

From the first case and duality we also obtain the second case.

For the last case assume that either $n = 2r$ or $n = 2r + 1$ (otherwise use duality). From the part $k - 1 \geq \mathsf{r}(X) + \mathsf{r}(Y) - \mathsf{r}(E) = \mathsf{r}(X)$ and that $\mathsf{r}(X) = |X| \geq k$ we get a contradiction, because we got $k - 1 \geq k$. □

We mention a note on that, which says the following. If $\mathcal{M}$ has $\lambda(\mathcal{M}) = \infty$ then $\mathcal{M}$ is uniform ($\mathcal{M} \cong \mathcal{U}_{r,n}$).

Proposition 32. *Let* $\lambda(\mathcal{M}) = k$ *finite. Then* $\kappa(\mathcal{M}) \geq k$ *and* $\kappa^*(\mathcal{M}) \geq k$*.*

This will be without proof. Also we will state another theorem and again witout a proof, but before we do so we must define some terms. Let **girth** of matroid $\mathcal{M}$ be denoted and defined as $g(\mathcal{M}) = \min\{|C|, C \in \mathcal{C}(\mathcal{M})\}$. Also it is good to mention that in general girth is upper bound to $\kappa^*(\mathcal{M})$.

Theorem 33. *Let* $\mathcal{M}$ *be not isomorphic to a uniform matroid* $\mathcal{U}_{r,n}$*.*

$$\lambda(\mathcal{M}) = \min(\kappa(\mathcal{M}), g(\mathcal{M})).$$