

And now similar to with circuits, we can characterise a matroid by way of it's bases as proved below.

Definition 0.1. A base is a maximally independent subset of \mathcal{I} .

As seen previously all maximally independent sets in a matroid have the same cardinality.

Theorem 0.2. Let \mathcal{B} be a set of subsets of a finite set E . Then \mathcal{B} is the collection of bases of a matroid on E if and only if \mathcal{B} satisfies the following conditions:

(B1) \mathcal{B} is non-empty.

(B2) If B_1 and B_2 are members of \mathcal{B} and $x \in B_1 \setminus B_2$, then there is an element y of $B_1 \setminus B_2$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Proof:

By (I1) \emptyset is always independent, so \mathcal{B} must always contain at least the \emptyset , (B1) holds.

Let $B_1, B_2 \in \mathcal{B}, B_1 \neq B_2$.

$|B_1| = |B_2|$ so (I3) does not directly apply here.

Let $x \in B_1 \setminus B_2 \implies x \in B_1, x \notin B_2$

$|B_1| = |B_1 \setminus \{x\}| + 1 \implies B_1 \setminus \{x\} \in \mathcal{I}$ but not in \mathcal{B}

$|B_2| = |B_1 \setminus \{x\}| + 1$ so now we can use (I3)

Now $\exists y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{I}$

$|(B_1 \setminus \{x\}) \cup \{y\}| = |B_1 \setminus \{x\}| + 1 = |B_1| = \dots = |B_r|$ as all maximal elements of \mathcal{I} have the same cardinality $\implies (B_1 \setminus \{x\}) \cup \{y\}$ is maximal in \mathcal{I}

$\implies (B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$, (B2) holds.

Conversely, suppose that \mathcal{B} satisfies (B1) and (B2).

By B1 \mathcal{B} is always non-empty which shows I1 holds.

By definition, a base $B_1 \in \mathcal{B}$ is a maximally independent subset of E . Then for all $B_i \in \mathcal{B}$ the subsets $b_{i,k} \subseteq B_i$ are independent. Therefore all the $b_{i,k}$ are in \mathcal{I} .

\implies (I2) holds. Showing a matroid can be generated through the bases.

Assume that (I3) fails. That, for $I_1, I_2 \in \mathcal{I}$, where $|I_1| = |I_2| + 1$,

there $\exists y \in I_1 \setminus I_2$ such that $I_2 \cup \{y\} \in \mathcal{I}$.

Let $B_1, B_2 \in \mathcal{B}, |B_1| = |B_2|$.

Let $x \in B_1 \setminus B_2$ then $B_1 \setminus \{x\} \subset B_1$.

$\implies B_1 \setminus \{x\}$ is independent.

Then there exists a $y \in B_2 \setminus (B_1 \setminus \{x\})$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$ from (B2). And if $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$ it is also in \mathcal{I} . A contradiction.

\implies (I3) holds and we have a matroid.

□