NOTES FOR LECTURE 1

These are lecture notes for our first "in-person" lecture. They follow largely the beginning of Oxley's book. Comments and corrections are welcome!

1. Independent sets

Definition 1.1. A matroid M is a pair $(E, \mathcal{I})$ where E is a finite set and $\mathcal{I} \subseteq 2^E$ is such that

($\mathcal{I}$1) $\emptyset \in \mathcal{I}$

($\mathcal{I}$2) If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$.

($\mathcal{I}$3) For any $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$, there is an element $e \in I_2 \setminus I_1$ such that $I_1 \cup \{e\} \in \mathcal{I}$.

Two matroids $M = (E, \mathcal{I})$ and $M' = (E', \mathcal{I}')$ are *isomorphic*, written $M \simeq M'$ if there is a bijection $f : E \to E'$ such that, for all $I \subseteq E$, $I \in \mathcal{I}$ if and only if $f(I) \in \mathcal{I}'$.

Remark-Definition 1.2. Let $M = (E, \mathcal{I})$ be a matroid. Given $X \subseteq E$, let $\mathcal{I}[X] := \{I \cap X \mid I \in \mathcal{I}\}$. Then $\mathcal{I}[X]$ satisfies ($\mathcal{I}$1-3). The matroid $M[X] := (X, \mathcal{I}[X])$ is called the "restriction" of M to X.

We point out some terminology:

- Members of $\mathcal{I}$ are called "independent sets" of M. Any $A \subseteq E$, $A \notin \mathcal{I}$, is called *dependent*.
- E is called the *ground set* of $\mathcal{I}$.
- Write $\mathcal{I}(M)$, $E(M)$ if specification is needed.

$U_{n,r}$
Uniform matroid

Example-Definition 1.3. Let $n, r \in \mathbb{N}$ with $n \geq r$. Recall that we write $[n]$ as a shorthand for the set $\{1, \ldots, n\}$, where we set $[0] = \emptyset$.

The set $\mathcal{I}_{n,r} := \{I \subseteq [n] \mid |I| \leq r\}$ satisfies axioms ($\mathcal{I}$1-3). The matroid

$$U_{r,n} := ([n], \mathcal{I}_{n,r})$$

is called *uniform matroid of rank r on n elements.*

Representable matroids

Example-Definition 1.4. Let A be an $n \times m$-matrix with entries in a field $\mathbb{K}$ and let $a_1, \ldots, a_m$ be its columns. Let then

$$\mathcal{I}(A) := \{I \subseteq [m] \mid (a_i)_{i \in I} \text{ is linearly independent in } \mathbb{K}^n\}.$$

Then, our warm-up exercises show that $M(A) := ([m], \mathcal{I}(A))$ is a matroid. Any matroid (isomorphic to one) of this type is called *representable* over $\mathbb{K}$.

Example 1.5. Let $a_1, \ldots, a_5$ denote the column vectors of the 2×5 matrix with entries in $\mathbb{R}$

$$A := \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Then the matroid $M(A)$ has ground set $[5]$ and independent sets

$$\mathcal{I}(A) = \{\emptyset, 1, 2, 4, 5, 12, 15, 24, 25, 45\}$$

(**Notice:** here and often in the following, when no confusion is possible, we simplify notation writing 15 for $\{1, 5\}$ and 2 for $\{2\}$, etc.)

The *dependent* sets of $M(A)$ are then

$$3, 13, 14, 23, 34, 35 \text{ as well as any } X \subseteq [5] \text{ with } |X| \geq 3.$$

Notice that $\mathcal{I}$ is known as soon as its inclusion-maximal elements are. Analogously, the set of dependent sets is determined once its inclusion-minimal elements are known.

2. Circuits

Definition 2.1. Given a matroid $M = (E, \mathcal{I})$, let $\mathcal{C}(M)$ be the family of minimal dependent sets of M, i.e.,

$$\mathcal{C}(M) := \{C \subseteq E \mid C \notin \mathcal{I}, \forall e \in C : C \setminus \{e\} \in \mathcal{I}\}.$$

The elements of $\mathcal{C}(M)$ are called *circuits* of M.

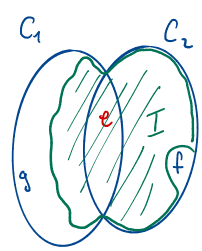
Notice, that for every matroid M the set $\mathcal{I}(M)$ determines $\mathcal{C}(M)$, and vice-versa.

Lemma 2.2. *Let M be a matroid and write $\mathcal{C}$ for the set of circuits $\mathcal{C}(M)$. Then $\mathcal{C}$ satisfies the following three properties.*

- *($\mathcal{C}$1) $\emptyset \notin \mathcal{C}$;*
- *($\mathcal{C}$2) For all $C_1, C_2 \in \mathcal{C}$, $C_1 \subseteq C_2$ implies $C_1 = C_2$;*
- *($\mathcal{C}$3) For all $C_1, C_2 \in \mathcal{C}$ with $C_1 \neq C_2$ and every $e \in C_1 \cap C_2$ there is $C_3 \in \mathcal{C}$ such that $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.*

Proof. ($\mathcal{C}$1) follows from ($\mathcal{I}$1). ($\mathcal{C}$2) holds because, by definition of $\mathcal{C}(M)$, any nontrivial subset of a circuit is independent.

We now prove ($\mathcal{C}$3) by way of contradiction. Let C_1, C_2 be as in ($\mathcal{C}$3) and assume that $(C_1 \cup C_2) \setminus \{e\}$ does not contain any circuit. Then, $(C_1 \cup C_2) \setminus \{e\} \in \mathcal{I}(M)$. Moreover, by ($\mathcal{C}$2) we can choose an element $f \in C_2 \setminus C_1$ and, by definition, $C_2 \setminus \{f\}$ is independent. Then, we can choose an $I \in \mathcal{I}(M)$ maximal with the property that $C_2 \setminus \{f\} \subseteq I \subseteq C_1 \cup C_2$. Clearly $f \notin I$ and $C_1 \setminus I$ is not empty (otherwise I would be dependent). Choose $g \in C_1 \setminus I$, and notice that $g \neq f$.



We can now compute

$$|I| \leq |(C_1 \cup C_2) \setminus \{f, g\}| = |C_1 \cup C_2| - 2 < |(C_1 \cup C_2) \setminus \{e\}|.$$

Now, ($\mathcal{I}$3) applied to $I_1 := I$ and $I_2 := (C_1 \cup C_2) \setminus \{e\}$ gives us an $e' \in I_2 \setminus I_1$ with $I' := I_1 \cup \{e'\} \in \mathcal{I}(M)$. We have $I_1 \subsetneq I' \subseteq C_1 \cup C_2$, contradicting the maximality of $I = I_1$. $\square$

Theorem 2.3. *Let E be a finite set and $\mathcal{C} \subseteq 2^E$ be any collection of subsets of E satisfying ($\mathcal{C}$1), ($\mathcal{C}$2), ($\mathcal{C}$3). Let*

$$\mathcal{I} := \{X \subseteq E \mid C \not\subseteq X \text{ for all } C \in \mathcal{C}\}. \tag{†}$$

Then, $M = (E, \mathcal{I})$ is a matroid with $\mathcal{C}(M) = \mathcal{C}$.

Proof. We first check ($\mathcal{I}$1-3) for $\mathcal{I}$, and then we'll prove $\mathcal{C} = \mathcal{C}(M)$.

($\mathcal{I}$1) The set $\emptyset$ is independent by ($\mathcal{C}$1).

($\mathcal{I}$2) Let $I \in \mathcal{I}$ and $I' \subseteq I$. If I' is not independent, then there is some circuit $C \in \mathcal{C}$ with $C \subseteq I'$, and so $C \subseteq I$, which contradicts independence of I. Therefore $I' \in \mathcal{I}$.

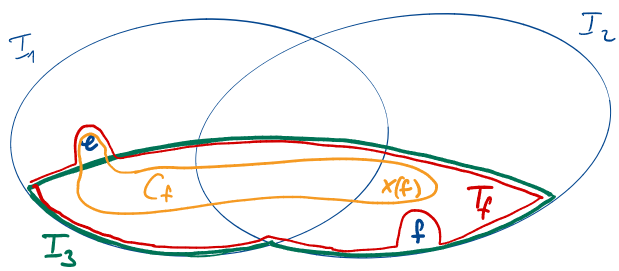
($\mathcal{I}$3) Let $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$. Consider $I_3 \in \mathcal{I}$ with $I_3 \subseteq I_1 \cup I_2$, $|I_3| > |I_1|$, and such that $|I_1 \setminus I_3|$ is minimal.

Assume that ($\mathcal{I}$3) fails: then, $I_1 \setminus I_3 \neq \emptyset$, and we can choose and fix an $e \in I_1 \setminus I_3$.

Idea: we want to use ($\mathcal{C}$3) in order to "eliminate" e from two circuits.

- For each $f \in I_3 \setminus I_1$ let $T_f := (I_3 \cup \{e\}) \setminus \{f\}$. Since T_f is dependent[1], it contains a circuit $C_f \in \mathcal{C}$ with: (a) $f \notin C_f$, (b) $e \in C_f$ (the latter because otherwise $C_f \subseteq I_3$, which is impossible because I_3 is independent), and (c) $C_f \subseteq I_3 \cup \{e\}$.

  Moreover, $C_f \cap (I_3 \setminus I_1)$ is not empty (otherwise $C_f \subseteq I_1$, a contradiction), thus we can choose an element $x(f) \in C_f \cap (I_3 \setminus I_1)$.



- Now fix $g \in I_3 \setminus I_1$ and let $h := x(g)$ as above. Then, $C_f \neq C_g$ (because $h \in C_g \setminus C_h$), and $e \in C_g \cap C_h$.

  By ($\mathcal{C}$3), there is $C \in \mathcal{C}$ with $C \subseteq (C_g \cup C_h) \setminus \{e\} \subseteq I_3$ (the last inclusion by (c) above), which contradicts independence of I_3.

We have so far proved that $(E, \mathcal{I})$ is a matroid, it remains to prove that $\mathcal{C} = \mathcal{C}(M)$. For this we turn to the definition: $C \in \mathcal{C}(M)$ means "$C \notin \mathcal{I}$ and $C \setminus \{x\} \in \mathcal{I}$ for all $x \in C$". Expanding the definition of $\mathcal{I}$ from the Theorem's claim, the former is equivalent to " $C' \subseteq C$ for some $C' \in \mathcal{C}$, but $C' \not\subseteq C \setminus \{x\}$ for all $x \in C$". Equivalently (by ($\mathcal{C}$2)), $C \in \mathcal{C}$. □

Corollary 2.4. *A $\mathcal{C} \subseteq 2^E$ is the set of circuits of a matroid if and only if ($\mathcal{C}$1)-($\mathcal{C}$3).*

This leads us to the following **Cryptomorphic definition** of a matroid: *a matroid M "is" any pair $(E, \mathcal{C})$ where E is a finite set and $\mathcal{C} \subseteq 2^E$ satisfies ($\mathcal{C}$1-3).* $\mathcal{C}$ is called the set of *circuits* of M.

The word "cryptomorphism" is used to indicate the "translation rule" from one axiomatization to the other:

[1]In fact, by maximality of I_3 , $T_f \subseteq I_1 \cup I_2$ and $|I_1 \setminus T_f| < |I_1 - I_3|$ imply $T_f \notin \mathcal{I}$.

Matroids as $(E,\mathcal{C})$		Matroids as $(E,\mathcal{I})$

$$\begin{tikzcd}
(E,\mathcal{C}) \arrow[rr, mapsto] & & (E,(\dagger)) \\
(E,\min_{\subseteq}(2^E\setminus\mathcal{I})) & & (E,\mathcal{I}) \arrow[ll, mapsto]
\end{tikzcd}$$

Proposition 2.5. *Let G be a graph with set of edges E. Set*

$$\mathcal{C}(G) := \{C \subseteq E \mid C \text{ is the edge set of a circuit in } G.\}$$

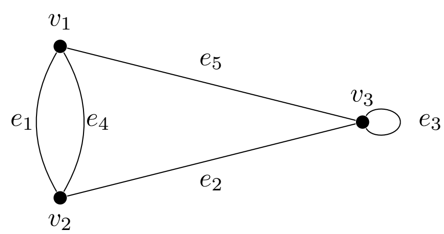
Then, $M(G) := (E, \mathcal{C}(G))$ is a matroid (called the cycle matroid *of G).*

Proof. See the warm-up! □

Graphic matroids

Definition 2.6. Any matroid isomorphic to the cycle matroid of a graph is called *graphic*.

Example 2.7. Consider the graph in the picture below:



The sets of edge sets of circuits is

$$\mathcal{C}(G) = \{\{e_1, e_4\}, \{e_3\}, \{e_1, e_2, e_5\}, \{e_2, e_4, e_5\}\}.$$

Notice that the assignment $e_i \mapsto i$ defines an isomorphism with the matroid of Example 1.5. This matroid is thus graphic as well as representable over $\mathbb{R}$.

Theorem 2.8. *Graphic matroids are representable over every field.*

Proof. Let G be a graph with vertex set V and edge set E, $\mathbb{K}$ any field. For every edge $e \in E$ call (arbitrarily) $h(e)$, $t(e)$ the vertices at the two ends of E (so that $h(e) = t(e)$ if e is a loop).

Consider then the matrix

$$A(G) \in \mathbb{K}^{V \times E}$$

defined by letting the e-th column be the vector

$$a_e := \mathbb{1}_{h(e)} - \mathbb{1}_{t(e)}$$

where $\mathbb{1}_v$ denotes the v-th standard basis vector in $\mathbb{K}^V$.

Notice that the linear dependency of the a_e does not depend on the choice of h and t.

Example 2.9. For the graph in Example 2.7 (choosing $h(e_1) = t(e_4) = v_1$, $h(e_5) = h(e_2) = v_3$) we have

$$A(G) = \begin{bmatrix} 1 & 0 & 0 & -1 & -1 \\ -1 & -1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix}$$

We now claim that $M(A(G)) \simeq M(G)$.

We have to prove the following:

$$X \subseteq E \textit{ is a cycle} \Leftrightarrow (a_e)_{e\in X} \textit{ is linearly dependent}$$

- $\Rightarrow$ If X is a cycle, it contains a circuit C, say $e_1, \dots, e_k$. We can assume that h, t are so that $t(e_i) = h(e_{i+1})$, and $t(e_k) = h(e_1)$. Then, $\sum_{i=1}^k a_{e_i} = 0$ is a nontrivial linear dependency in $(a_e)_{e\in X}$.
- $\Leftarrow$ Suppose $(a_e)_{e\in X}$ is linearly dependent. If $a_e = 0$ for some e, then the loop e is the required cycle. Otherwise there is a nonempty $Y \subseteq X$ with $\sum_{e\in Y} \lambda_e a_e = 0$ with $\lambda_e a_e \neq 0$ for all $e \in Y$. In particular, for every component v of this sum, there are $f, g \in Y$, $f \neq g$, with $(a_f)_v, (a_g)_v \neq 0$. This means that the graph with edge set Y and vertex set $h(Y) \cup t(Y)$ has degree at least 2 everywhere and thus, as was proved in the warm-up, contains a circuit.

□

Corollary 2.10. *The independent sets of a graphic matroid with graph G are the edge-sets of cycle-free subgraphs of G.*

3. Bases and rank

We have seen that, by the hereditary property, to specify a matroid $(E, \mathcal{I})$ is equivalent to specifying the (inclusion-)maximal elements of $\mathcal{I}$.

Definition 3.1. Let $M = (E, \mathcal{I})$ be a matroid. Let

$$\mathcal{B}(M) := \max_{\supseteq} \mathcal{I} = \{B \in \mathcal{I} \mid I \supseteq B,\, I \in \mathcal{I} \Rightarrow I = B\}.$$

The elements of $\mathcal{B}(M)$ are called *bases* of M.

Lemma 3.2. *Let M be a matroid and let $B_1, B_2 \in \mathcal{B}(M)$. Then, $|B_1| = |B_2|$.*

Proof. By way of contradiction: assume $|B_1| < |B_2|$, then by ($\mathcal{I}3$) there is $e \in B_2 \setminus B_1$ with $B_1 \cup \{e\} \in \mathcal{I}(M)$. Since $B_1 \subsetneq B_1 \cup \{e\}$, this contradicts maximality of B_1. Thus, $|B_1| \geq |B_2|$. By symmetry, $|B_1| \leq |B_2|$. □

Definition 3.3. The *rank* of a matroid $M = (E, \mathcal{I})$ is the cardinality $\mathrm{rk}(M) = |B|$ of any basis $B \in \mathcal{B}(M)$.

We can assign a rank to every subset of E by setting

$$\mathrm{rk}(X) := \mathrm{rk}(M[X]) \text{ for every } X \subseteq E.$$

The resulting function $\mathrm{rk} : 2^E \mapsto \mathbb{N}$ is called the *rank function of M*.

There is a cryptomorphic definition of matroids via the rank function, given as follows.

Theorem 3.4. *Let E be a finite set. A function $\mathrm{rk} : 2^E \to \mathbb{N}$ is the rank function of a matroid on E if and only if it satisfies the following criteria.*

(R1) For all $X \subseteq E$: $\mathrm{rk}(X) \leq |X|$.

(R2) For all $X \subseteq Y \subseteq E$: $\mathrm{rk}(X) \leq \mathrm{rk}(Y)$

(R3) For all $X, Y \subseteq E$: $\mathrm{rk}(X) + \mathrm{rk}(Y) \geq \mathrm{rk}(X \cap Y) + \mathrm{rk}(X \cup Y)$.

See pages 20 and ff. of Oxley's book for a proof.

Here we continue by stating two properties of bases of matroids.

Proposition 3.5. *Let M be a matroid and let $\mathcal{B} = \mathcal{B}(M)$ be its set of bases. Then*

($\mathcal{B}$1) $\mathcal{B}$ is not empty

($\mathcal{B}$2) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$, then there is $y \in B_2 \setminus B_1$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Proof. ($\mathcal{B}$1) is immediate from ($\mathcal{I}$1). For ($\mathcal{B}$2) take $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$. We split the proof in two parts.

Existence of y. By Lemma 3.2, $|B1 \setminus \{x\}| < |B_2|$, and thus by ($\mathcal{I}$3) there is $y \in B_2 \setminus (B_1 \setminus \{x\})$ such that $(B_1 \setminus \{x\}) \cup \{y\} \in \mathcal{I}(M)$.

Maximality of $(B_1 \setminus \{x\}) \cup \{y\}$. Let $B' \in \mathcal{B}(M)$ with

$$B' \supseteq (B_1 \setminus \{x\}) \cup \{y\}. \tag{‡}$$

We compute $|B'| = |B| = |(B_1 \setminus \{x\}) \cup \{y\}|$ (the last equality since $x \in B_1$ and $y \notin B_1$), and with (‡) we conclude $B' = (B_1 \setminus \{x\}) \cup \{y\}$.

□

We conclude by proving that, in fact, axioms ($\mathcal{I}$1) and ($\mathcal{I}$2) five yet another cryptomorphic definition of matroids.

Theorem 3.6. *Let E be a finite set, $\mathcal{B} \subseteq 2^E$ be any collection satisfying ($\mathcal{B}$1) and ($\mathcal{B}$2). Consider*

$$\mathcal{I} := \{I \subseteq E \mid I \subseteq B \text{ for some } B \in \mathcal{B}\}.$$

Then $M = (E, \mathcal{I})$ is a matroid with $\mathcal{B}(M) = \mathcal{B}$.

Proof. If M is a matroid, clearly $\mathcal{B}$ is its set of bases. It is then enough to prove that $\mathcal{I}$ satisfies ($\mathcal{I}$1-3).

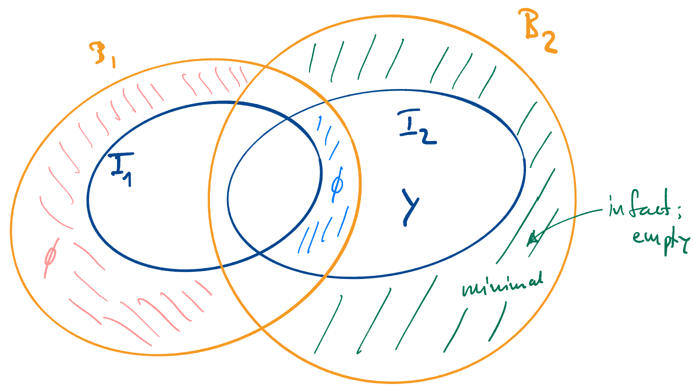
($\mathcal{I}$1) for $\mathcal{I}$ follows immediately from ($\mathcal{B}$1) for $\mathcal{B}$.

($\mathcal{I}$2) Let $I \in \mathcal{I}$ and consider $I' \subseteq I$. By definition there is $B \in \mathcal{B}$ with $I \subseteq B$ – but then $I' \subseteq B$ as well, and so $I' \in \mathcal{I}$.

($\mathcal{I}$3) By way of contradiction, suppose that ($\mathcal{I}$3) fails for $\mathcal{I}$ and choose I_1, I_2 with $|I_1| < |I_2|$ and $(I_1 \cup \{e\}) \notin \mathcal{I}$ for all $e \in I_2 \setminus I_1$.

Among all $B_1, B_2 \in \mathcal{B}$ with $B_1 \supseteq I_1$ and $B_2 \supseteq I_2$ choose a pair so that $|B_2 \setminus (I_2 \cup B_1)|$ is minimal.

Now we state a few claims about the relationships among the various sets, establishing the following diagram.



(1) $I_2 \setminus B_1 = I_2 \setminus I_1$ by the choice of I_1, I_2.

(2) $B_2 \setminus (I_2 \cup B_1) = \emptyset$.
Proof. By way of contradiction choose $x \in B_2 \setminus (I_2 \cup B_1) \subseteq B_2$. Then $(\mathcal{B}2)$ gives a $y \in B_1 \setminus B_2$ with $(B_2 \setminus \{x\}) \cup \{y\}) \in \mathcal{B}$. But this would imply

$$|[(B_2 \setminus \{x\}) \cup \{y\}] \setminus (I_2 \cup B_1)| < |B_2 \setminus (I_2 \cup B_2)|$$

contradicting the choice of B_1, B_2.

(3) $B_2 \setminus B_1 = I_2 \setminus I_1$ (by (1) and (2), e.g. after inspecting the diagram above).

(4) $B_1 \setminus (I_1 \cup B_2) = \emptyset$
Proof. By way of contradiction, choose $x \in B_1 \setminus (I_1 \cup B_2)$. Then $(\mathcal{B}2)$ gives an $y \in B_2 \setminus B_1$ with $(B_1 \setminus \{x\}) \cup \{y\}) \in \mathcal{B}$. In particular, $I_1 \cup \{y\} \in \mathcal{I}$ for some $y \in B_2 \setminus B_1 = I_2 \setminus I_1$ the last equality via (3)). This cannot be, since I_1, I_2 violate $(\mathcal{I}3)$ by assumption.

(5) $B_1 \setminus B_2 \subseteq I_1 \setminus I_2$. This is because (4) implies $B_1 \setminus B_2 = I_1 \setminus B_2$, and the latter is a subset of $I_1 \setminus I_2$ by definition.

(6) – The final contradiction!
By Lemma 3.2 we have $|B_1| = |B_2|$, whence the equality in the middle of the following expression:

$$|I_1 \setminus I_2| \overset{(5)}{\le} |B_1 \setminus B_2| = |B_2 \setminus B_1| \overset{(3)}{=} |I_2 \setminus I_1|.$$

Now, $|I_1 \setminus I_2| \le |I_2 \setminus I_1$ implies $|I_1| \ge |I_2|$, a contradiction!.

□