Chapter 2 Introduction to Matroids

2.1. Axiom systems. A collection $\mathbf{I}$ of subsets of a finite set S is an *independence structure* on S if it satisfies:

(I1) $\emptyset \in \mathbf{I}$ ($\mathbf{I}$ is *nonempty*);

(I2) $X \in \mathbf{I}$ and $Y \subseteq X \Longrightarrow Y \in \mathbf{I}$ ($\mathbf{I}$ is *hereditary*);

(I3) if $X, Y \in \mathbf{I}$ and $|Y| > |X|$ then $\exists\, y \in Y \setminus X$ s.t. $X \cup \{y\} \in \mathbf{I}$ (the *exchange* or *replacement property*).

The pair $(S, \mathbf{I})$ is called a *matroid* $\mathbf{M}$ (H. Whitney (1907–1989), 1935). Sets in $\mathbf{I}$ are *independent*, all others are *dependent*. $(S_1, \mathbf{I}_1)$ and $(S_2, \mathbf{I}_2)$ are *isomorphic* ($\cong$) if there is a bijection $f : S_1 \to S_2$ s.t. $X \in \mathbf{I}_1 \iff f(X) \in \mathbf{I}_2$.

Examples.

(1) *Trivial matroids*: $S =$ any (finite) set, only $\emptyset \in \mathbf{I}$.

(2) *Free* (or *discrete*) *matroids*: $S =$ any set, all subsets $\in \mathbf{I}$.

(3) *k-uniform matroids*: $S =$ any set, $X \in \mathbf{I} \iff |X| \leqslant k$.

(4) *Representable matroids*: V = a vector space, $S \subseteq V$, independence = linear independence. (E.g., S = the set of rows of a matrix — hence the word *matroid*). Because of this example, a maximal independent subset of S (or of a subset X of S) is called a *base* of $\mathbf{M}$ (or of X), and its cardinality is the *rank* $r(S)$ of $\mathbf{M}$ (or $r(X)$ of X).
Exercise: Prove that (I1), (I2) and (I3) $\iff$ (I1), (I2) and
(I3′) $\forall\, X \subseteq S$, all maximal independent subsets of X have the same cardinality.

(5) *Geometric matroids*: S = a subset of an affine or projective space, independence = geometric independence (i.e., $X \in \mathbf{I}$ iff X spans a subspace of dimension $|X| - 1$; so dimension = rank -1). So a maximal set of given rank is a *flat*, *closed set* or *subspace*, and a flat of rank $r(S) - 1$ is a *hyperplane*.

(6) *Algebraic matroids*: S = a subset of an extension field of a field F, independence = algebraic independence over F.

(7) *Graphic matroids* (H. Whitney, 1935): S = the set of edges of a graph, $\mathbf{I}$ = the collection of circuit-free subsets (subforests). Hence a minimal dependent set in a matroid is a *circuit*, $x \in S$ is a *loop* if $\{x\}$ is dependent, and x_1 and x_2 are *parallel elements* if $\{x_1\}$ and $\{x_2\} \in \mathbf{I}$ but $\{x_1, x_2\} \notin \mathbf{I}$.

(8) *Transversal matroids* (J. Edmonds and D. R. Fulkerson, 1965): S = any set, $\mathbf{I}$ = the partial transversals of some family of subsets of S. For example:

$A_1 = \{a, b, c\}$,	Partial transversals:
$A_2 = \{c, d\}$,	$\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{d\}$, $\{c, d\}$,
$A_3 = \{c, d\}$,	$\{a, c\}$, $\{a, d\}$, $\{a, c, d\}$,
$A_4 = \{d\}$.	$\{b, c\}$, $\{b, d\}$, $\{b, c, d\}$.

Theorem 2.1. The set $\mathbf{B}$ of bases of a matroid satisfies:

(B1) no proper subset of a set in $\mathbf{B}$ is in $\mathbf{B}$;

(B2) if B_1 and $B_2 \in \mathbf{B}$ and $e_1 \in B_1 \setminus B_2$, then $\exists\, e_2 \in B_2 \setminus B_1$ s.t. $(B_1 \setminus \{e_1\}) \cup \{e_2\} \in \mathbf{B}$.

Moreover, any nonempty collection $\mathbf{B}$ of subsets of S satisfying (B1) and (B2) is the set of bases of a unique matroid on S (whose independent sets are precisely the subsets of the bases).

Proof. Exercise. //

Theorem 2.2. The rank function r of a matroid on S satisfies:

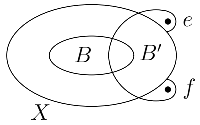
(R1) $r(\emptyset) = 0$;

(R2) if $X \subseteq S$ and $e \in S$ then $r(X \cup \{e\}) = r(X)$ or $r(X) + 1$;

(R3) if $X \subseteq S$ and $e, f \in S$ and $r(X \cup \{e\}) = r(X \cup \{f\}) = r(X)$, then $r(X \cup \{e, f\}) = r(X)$.

Moreover, any function $r : 2^S \to \mathbb{R}$ satisfying (R1)–(R3) is the rank function of a unique matroid on S (with $X \subseteq S$ independent iff $r(X) = |X|$).

Proof. (R1) and (R2) are straightforward. Suppose (R3) is false. Let B and B' be bases for X and $X \cup \{e, f\}$, where $|B'| > r(X) = |B|$. (Clearly $e, f \in B'$.) By (I3), $\exists\ y \in B' \setminus B$ s.t. $B \cup \{y\}$ is independent. But $B \cup \{y\} \subseteq X \cup \{e\}$ or $X \cup \{f\}$, and so one of these must have rank $> r(X)$, $\Rightarrow\Leftarrow$.



Conversely, suppose r satisfies (R1)–(R3), and let $\mathbf{I} := \{X \subseteq S : r(X) = |X|\}$. (I1) and (I2) are straightforward. To prove (I3), suppose X and Y are sets in $\mathbf{I}$ with $|Y| > |X|$ and $\nexists\ y \in Y \setminus X$ s.t. $X \cup \{y\} \in \mathbf{I}$. Let $Y \setminus X = \{y_1, \ldots, y_h\}$. Then
$r(X \cup \{y_i\}) = r(X)$ $(1 \leqslant i \leqslant h)$. So, by (R3),
$r(X \cup \{y_1, y_i\}) = r(X) = r(X \cup \{y_1\})$ $(2 \leqslant i \leqslant h)$. So, by (R3),
$r(X \cup \{y_1, y_2, y_i\}) = r(X) = r(X \cup \{y_1, y_2\})$ $(3 \leqslant i \leqslant h)$.
Continuing in this way, we see that $r(X \cup \{y_1, \ldots, y_h\}) = r(X)$, which is impossible since $X \cup \{y_1, \ldots, y_h\} = X \cup Y$ and

$$r(X \cup Y) \geqslant r(Y) = |Y| > |X| = r(X).$$

This contradiction proves (I3). It is straightforward to prove that r is the rank function of the matroid. //

Theorem 2.3. The rank function r of a matroid on S satisfies:

(R1′) $0 \leqslant r(X) \leqslant |X|$ $\forall X \subseteq S$ (r is *nonnegative* and *subcardinal*);

(R2′) $r(X) \leqslant r(Y)$ if $X \subseteq Y \subseteq S$ (r is *nondecreasing*);

(R3′) $r(X \cap Y) + r(X \cup Y) \leqslant r(X) + r(Y)$ $\forall X, Y \subseteq S$ (r is *submodular*).

Moreover, any function $r : 2^S \to \mathbb{Z}$ satisfying (R1′)–(R3′) is the rank function of a unique matroid on S.

Proof. (R1′) and (R2′) are straightforward. To prove (R3′), let $\{z_1, \ldots, z_i\}$ be a base for $X \cap Y$. Extend it to a base $\{z_1, \ldots, z_i, x_{i+1}, \ldots, x_a, y_{i+1}, \ldots, y_b\}$ for $X \cup Y$, where the x's $\in X$ and the y's $\in Y$. Then $\{z_1, \ldots, z_i, x_{i+1}, \ldots, x_a\}$ is an independent subset of X, so that $a \leqslant r(X)$. Likewise $b \leqslant r(Y)$. Thus

$$r(X \cap Y) + r(X \cup Y) = i + (a + b - i) = a + b \leqslant r(X) + r(Y)$$

as required.

Conversely, if r satisfies (R1′)–(R3′) and is integer-valued, it is straightforward to prove that it satisfies (R1)–(R3), and the result follows from Theorem 2.2. //

2.2. The dual matroid.

Theorem 2.4. The *cobases* (complements of the bases) of a matroid $\mathbf{M} = (S, \mathbf{I}) = (S, \mathbf{B}) = (S, r)$ form the bases of another matroid $\mathbf{M}^* = (S, \mathbf{I}^*) = (S, \mathbf{B}^*) = (S, r^*)$, called the *dual matroid* of $\mathbf{M}$, whose rank function r^* is given by

$$r^*(X) = |X| + r(S \setminus X) - r(S) \quad \forall X \subseteq S. \qquad (*)$$

(Note that $(\mathbf{M}^*)^* = \mathbf{M}$ and $r(S) + r^*(S) = |S|$.)

Proof. We prove first that r^*, *defined* by $(*)$, satisfies (R1′)–(R3′). From (R2) (for r), if $P \subseteq Q$ then $r(P) \leqslant r(Q) \leqslant r(P) + |Q| - |P|$. Thus

$$\begin{aligned} S \setminus X \subseteq S &\Longrightarrow r(S \setminus X) \leqslant r(S) \leqslant r(S \setminus X) + |X| \\ &\Longrightarrow 0 \leqslant r^*(X) \leqslant |X|, \end{aligned}$$

and

$$\begin{aligned} X \subseteq Y &\Longrightarrow S \setminus Y \subseteq S \setminus X \\ &\Longrightarrow r(S \setminus X) \leqslant r(S \setminus Y) + |Y| - |X| \\ &\Longrightarrow r^*(X) \leqslant r^*(Y). \end{aligned}$$

This proves (R1′) and (R2′). To prove (R3′), note that

$$
\begin{aligned}
&r^*(X \cap Y) + r^*(X \cup Y) = \\
&= |X \cap Y| + |X \cup Y| + r(S \setminus (X \cap Y)) + r(S \setminus (X \cup Y)) - 2r(S) \\
&= |X| + |Y| + r((S \setminus X) \cup (S \setminus Y)) + r((S \setminus X) \cap (S \setminus Y)) - 2r(S) \\
&\leqslant |X| + |Y| + r(S \setminus X) + r(S \setminus Y) - 2r(S) \quad \text{by (R3}'\text{) for } r \\
&= r^*(X) + r^*(Y) \quad \text{as required.}
\end{aligned}
$$

Thus r^* is the rank function of a matroid $\mathbf{M}^*$ on S. And the bases of $\mathbf{M}^*$ are the subsets B^* of S s.t. $|B^*| = r^*(S)$ and $r^*(B^*) = |B^*|$; i.e., $|B^*| = |S| - r(S)$ and $r(S \setminus B^*) = r(S)$; that is, they are the complements of the subsets B of S s.t. $|B| = r(S)$ and $r(B) = r(S)$, which are the bases of $\mathbf{M}$. //

The circuits of $\mathbf{M}^*$ are the *cocircuits* of $\mathbf{M}$, and $r^*(X)$ is the *corank* of X. The cocircuits are the complements of the hyperplanes, since a hyperplane is a maximal set containing no base, and a cocircuit is a minimal set contained in no cobase.

2.3. Circuits, hyperplanes and flats.

Theorem 2.5. The set $\mathbf{C}$ of circuits of a matroid on S satisfies:

(C1) no proper subset of a set in $\mathbf{C}$ is in $\mathbf{C}$;

(C2) if C_1 and $C_2 \in \mathbf{C}$, $C_1 \neq C_2$, and $e \in C_1 \cap C_2$, then $\exists\, C \in \mathbf{C}$ s.t. $C \subseteq (C_1 \cup C_2) \setminus \{e\}$.

Moreover, any collection $\mathbf{C}$ of nonempty subsets of S satisfying (C1) and (C2) consists of the circuits of a unique matroid on S (with $X \subseteq S$ independent iff X contains no set in $\mathbf{C}$).

Proof. (C1) is straightforward. To prove (C2), note that if $(C_1 \cup C_2) \setminus \{e\}$ does not contain a circuit, then it is independent. $C_1 \cap C_2$ is also independent (a proper subset of C_1), and so it can be extended to a base B of $C_1 \cup C_2$. But $|B| \geqslant |(C_1 \cup C_2) \setminus \{e\}| = |C_1 \cup C_2| - 1$, and so C_1 or $C_2 \subseteq B$, $\Rightarrow\Leftarrow$. Thus (C2) must hold.

Conversely, suppose $\mathbf{C}$ satisfies (C1) and (C2). Let $\mathbf{I} := \{X \subseteq S : X \text{ contains no set in } \mathbf{C}\}$. It is straightforward to prove (I1) and (I2) and that the sets in $\mathbf{C}$ are the minimal sets not in $\mathbf{I}$. It remains to prove (I3).

Let $X, Y \in \mathbf{I}$ with $|X| < |Y|$. We seek $y \in Y \setminus X$ s.t. $X \cup \{y\} \in \mathbf{I}$. Choose $Y_0 \in \mathbf{I}$ s.t. $|X \cap Y_0|$ is maximal subject to $|Y_0| > |X|$ and $Y_0 \subseteq X \cup Y$. If $X \subseteq Y_0$, we can choose $y \in Y_0 \setminus X \subseteq Y \setminus X$, so that $X \cup \{y\} \subseteq Y$ and hence $\in \mathbf{I}$, as required, by (I2). So we may suppose $X \not\subseteq Y_0$. Choose $x \in X \setminus Y_0$. Then $Y_0 \cup \{x\} \notin \mathbf{I}$, by the maximality of $|X \cap Y_0|$, and so $Y_0 \cup \{x\}$ contains some set $C \in \mathbf{C}$. C is unique, since if $C' \subseteq Y_0 \cup \{x\}$ is also in $\mathbf{C}$ then $x \in C \cap C'$ and, by (C2), $\exists\, C'' \in \mathbf{C}$ s.t. $C'' \subseteq (C \cup C') \setminus \{x\} \subseteq Y_0$, a contradiction. Clearly $C \not\subseteq X$, and so $\exists\, y \in C \setminus X$. Let $Y_1 := (Y_0 \cup \{x\}) \setminus \{y\}$. Then $Y_1 \in \mathbf{I}$, $|Y_1| = |Y_0| > |X|$, and $|X \cap Y_1| = |X \cap Y_0| + 1$, contradicting the maximality of $|X \cap Y_0|$. //

Corollary 2.5.1. The set $\mathbf{H}$ of hyperplanes of a matroid on S satisfies:

(H1) no set in $\mathbf{H}$ properly contains any other;

(H2) if H_1 and $H_2 \in \mathbf{H}$, $H_1 \neq H_2$, and $x \in S \setminus (H_1 \cup H_2)$, then $\exists\, H \in \mathbf{H}$ s.t. $(H_1 \cap H_2) \cup \{x\} \subseteq H$.

Moreover, any collection $\mathbf{H}$ of nonempty subsets of S satisfying (H1) and (H2) consists of the hyperplanes of a unique matroid on S.

Proof. Immediate, since the hyperplanes are the complements of the cocircuits. //

It follows from Theorems 2.5 and 1.1(c) that the circuits and cocircuits (minimal cutsets) of a graph G form the circuits of two matroids on $E(G)$, the *circuit matroid* or *cycle matroid* $\mathbf{M}(G)$ and the *cutset matroid* or *cocycle matroid* $\mathbf{M}^*(G)$ of G. By

Theorem 1.1(f), the bases of $\mathbf{M}(G)$ and $\mathbf{M}^*(G)$ are respectively the skeletons of G and their complements, and so $\mathbf{M}^*(G) = (\mathbf{M}(G))^*$ (the dual of $\mathbf{M}(G)$). If G^* is an abstract dual of G (exercise 2 of Chapter 1), it follows by definition that $\mathbf{M}(G^*) \cong \mathbf{M}^*(G) = (\mathbf{M}(G))^*$.

A matroid $\mathbf{M}$ is *graphic* (or *cographic*) if it is isomorphic to $\mathbf{M}(G)$ (or $\mathbf{M}^*(G)$) for some graph G. (So $\mathbf{M}$ is graphic $\iff \mathbf{M}^*$ is cographic.) $\mathbf{M}$ is *planar* if it is graphic and cographic, i.e., if it is isomorphic to $\mathbf{M}(G)$ (or $\mathbf{M}^*(G)$) for some planar graph G (since a graph has an abstract dual iff it is planar).

Lemma 2.6.1. (a) If F_1 and F_2 are flats in a matroid then so is $F_1 \cap F_2$.
(b) A set X of rank r is contained in a unique flat of rank r.

Proof. (a) Suppose not. Then $\exists\ x \notin F_1 \cap F_2$ s.t.

$$r((F_1 \cap F_2) \cup \{x\}) = r(F_1 \cap F_2).$$

Suppose w.l.o.g. $x \notin F_1$. Then $r(F_1 \cup \{x\}) > r(F_1)$, so every base of $F_1 \cup \{x\}$ contains x. Choose a base B for $F_1 \cap F_2$ and extend it to a base B_1 for $F_1 \cup \{x\}$. Then $x \in B_1$, so that $B \cup \{x\}$ is independent, whence $r((F_1 \cap F_2) \cup \{x\}) > r(F_1 \cap F_2)$, $\Rightarrow\Leftarrow$.
(b) Suppose $F_1 \neq F_2$ are two flats of rank r containing X. Then $X \subseteq F_1 \cap F_2$, which is a flat by (a), necessarily of rank $< r$ since it is properly contained in F_1; $\Rightarrow\Leftarrow$. //

Theorem 2.6. The sets $\mathbf{F}_r$ of flats of rank r in a matroid on S satisfy:
(F1) $|\mathbf{F}_0| = 1$;
(F2) if $F \in \mathbf{F}_r$ and $x \in S \setminus F$, then there is a unique $F' \in \mathbf{F}_{r+1}$ s.t. $F \cup \{x\} \subseteq F'$;
(F3) every set in $\bigcup_r \mathbf{F}_r$ is generated by (F1) and (F2).

Moreover, if $\mathbf{F}_0, \mathbf{F}_1, \ldots$ are collections of subsets of S satisfying (F1)–(F3), then $\bigcup_r \mathbf{F}_r$ is the collection of flats of a unique matroid on S (in which $X \subseteq S$ is independent iff $X \not\subseteq F$ for any F in $\bigcup_{r<|X|} \mathbf{F}_r$).

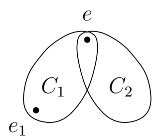
Proof. Exercise. //

2.4. Connectedness. Let $\mathbf{M} = (S, r)$ be a matroid.

Lemma 2.7.1. If $e \in X \subseteq S$, then $r(X) = r(X \setminus \{e\})$ iff there is a circuit in X containing e.

Proof. If there is no such circuit, then $B \cup \{e\}$ is independent for each base B of $X \setminus \{e\}$, so that $r(X) > r(X \setminus \{e\})$. Conversely, if $r(X) > r(X \setminus \{e\})$, then every base of X contains e. Thus if C were a circuit in X containing e, then $C \setminus \{e\}$ would be independent and extendable to a base of X containing e and hence C, $\Rightarrow\Leftarrow$. //

Lemma 2.7.2. If C_1 and C_2 are circuits and $e \in C_1 \cap C_2$ and $e_1 \in C_1 \setminus C_2$, then there is a circuit in $C_1 \cup C_2$ containing e_1 but not e.



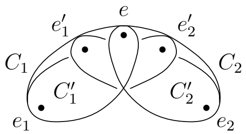
Proof. There is a circuit (C_1) in $C_1 \cup C_2$ containing e_1 and a circuit (C_2) in $(C_1 \cup C_2) \setminus \{e_1\}$ containing e. By Lemma 2.7.1,

$$r(C_1 \cup C_2) = r((C_1 \cup C_2) \setminus \{e_1\}) = r((C_1 \cup C_2) \setminus \{e, e_1\}).$$

Thus $r((C_1 \cup C_2) \setminus \{e\} = r((C_1 \cup C_2) \setminus \{e, e_1\})$, and so there is a circuit in $(C_1 \cup C_2) \setminus \{e\}$ containing e_1. //

Lemma 2.7.3. If there is a circuit containing e_1 and e_3 and one containing e_3 and e_2, then there is one containing e_1 and e_2.

Proof. Suppose not. Choose circuits C_1, C_2 s.t. $e_1 \in C_1$, $e_2 \in C_2$, $C_1 \cap C_2 \neq \emptyset$ (say $e \in C_1 \cap C_2$), and s.t. $C_1 \cup C_2$ is minimal subject to these restrictions. By Lemma 2.7.2 there are circuits C_1', C_2' in $(C_1 \cup C_2) \setminus \{e\}$ containing e_1, e_2 respectively, which are disjoint by the minimality of $C_1 \cup C_2$. $C_1' \not\subseteq C_1$, so $\exists\, e_2' \in C_1' \cap (C_2 \setminus C_1)$. Similarly $\exists\, e_1' \in C_2' \cap (C_1 \setminus C_2)$. Now C_1' and C_2 violate the minimality of $C_1 \cup C_2$ since $e_2' \in C_1' \cap C_2$ and $e_1' \notin C_1' \cup C_2$. //



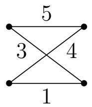
A *separating partition* for $\mathbf{M} = (S, \mathbf{I})$ is a partition $S = S_1 \cup S_2$ such that every circuit of $\mathbf{M}$ is contained in S_1 or S_2 ($S_1 \neq \emptyset \neq S_2$, $S_1 \cap S_2 = \emptyset$). $\mathbf{M}$ is *disconnected* or *separable* if it has a separating partition, and *connected* or *nonseparable* otherwise. Its *components* are the maximal connected submatroids of the form $\mathbf{M}|X$ ($X \subseteq S$; see handout).

Theorem 2.7. (a) A matroid $\mathbf{M}$ is connected iff each two distinct elements belong to a circuit.
(b) If $\mathbf{M}|S_i$ ($i = 1, \ldots, n$) are the components of $\mathbf{M}$, then the sets S_i partition S (i.e., are disjoint and cover S).
(c) If $\mathbf{M} = \mathbf{M}(G)$ and $|V(G)| \geqslant 3$ and G has no isolated vertices, then $\mathbf{M}$ is connected iff G is loopless and 2-connected.

Proof. Exercise. //

2.5. The greedy algorithm. Given a nonempty hereditary collection $\mathbf{I}$ of subsets of a finite set S, and a *value* function $v : S \to \mathbb{R}^+$, we wish to construct a most valuable set S' in $\mathbf{I}$. The *greedy algorithm* chooses the elements of S' one at a time, always choosing a most valuable element possible such that the set of elements so far chosen is in $\mathbf{I}$.

Example where it doesn't work: $\mathbf{I}$ comprises the matchings in the graph, with each edge having the value shown.



Theorem 2.8. (a) (R. Rado (1906–1989), 1957.) If $\mathbf{I}$ is an independence structure, then the greedy algorithm always works (i.e., it yields a base of maximum value).
(b) (Partial converse of (a).) If the greedy algorithm works for $\mathbf{I}$ for *every* $v : S \to \mathbb{R}^+$, then $\mathbf{I}$ is an independence structure.

Proof. (a) Let $x_1, x_2, \ldots$ be the elements chosen (in order) by the greedy algorithm, and choose k minimal (if it exists) s.t. $\exists$ an independent set $Y_k = \{y_1, \ldots, y_k\}$ of greater value than $X_k := \{x_1, \ldots, x_k\}$. Let $X_{k-1} := \{x_1, \ldots, x_{k-1}\}$. By the exchange property, $\exists\, y_i \in Y_k \setminus X_{k-1}$ s.t. $X_{k-1} \cup \{y_i\} \in \mathbf{I}$. Since the greedy algorithm chose x_k to add to X_{k-1}, $v(x_k) \geqslant v(y_i)$. But then

$$v(Y_k \setminus \{y_i\}) = v(Y_k) - v(y_i) > v(X_k) - v(x_k) = v(X_{k-1}),$$

contradicting the minimality of k. Thus k does not exist and the greedy algorithm works.

(b) Let $X, Y \in \mathbf{I}$ ($|X| < |Y|$) for which the exchange property fails. Let

$$v(x) := \begin{cases} 1 & \text{if } x \in X, \\ 1 - \epsilon & \text{if } x \in Y \setminus X, \\ 0 & \text{otherwise.} \end{cases}$$

Then the greedy algorithm will construct a set in $\mathbf{I}$ of value $|X|$. But since $|Y| > |X|$, $v(Y) \geqslant |Y|(1 - \epsilon) > |X|$ if ϵ is small enough. //