| | |
|---|---|
| **Matroids and Submodular Optimization** | August 24, 2026 |

**Lecture 1**

*Lecturer: Siyue Liu* *Scribe: ChatGPT*

A matroid is denoted $M = (E, \mathcal{I})$, where the ground set $E$ is finite. For $X \subseteq E$ and $e \in E$, we abbreviate $X + e = X \cup \{e\}$ and $X - e = X \setminus \{e\}$. The rank of $M$ is $r(M) = r_M(E)$. A *basis of $X$* is a maximal independent subset of $X$; a *base of $M$* is a basis of $E$.

# 1 Independent sets and the augmentation axiom

**Definition 1.1** (Independent-set axioms)**.** A pair $M = (E, \mathcal{I})$ is a *matroid* if $\mathcal{I} \subseteq 2^E$ satisfies

$$\begin{aligned} &(\text{I1}) \quad \varnothing \in \mathcal{I};\\ &(\text{I2}) \quad J \subseteq I \in \mathcal{I} \implies J \in \mathcal{I};\\ &(\text{I3}) \quad I, J \in \mathcal{I},\ |I| < |J| \implies \exists e \in J \setminus I \text{ such that } I + e \in \mathcal{I}. \end{aligned}$$

Members of $\mathcal{I}$ are *independent*; all other subsets are *dependent*. Axiom (I3) is the *augmentation* or *independent-set exchange* axiom.

The next consequence is elementary but fundamental.

**Proposition 1.2** (Extension and equicardinality)**.** *Let $I$ be independent and $I \subseteq X \subseteq E$.*

*(a) $I$ extends to a basis of $X$.*

*(b) Every two bases of $X$ have the same cardinality.*

*Proof.* Because $E$ is finite, repeatedly add an element of $X$ while independence is preserved; the process ends at a maximal independent subset of $X$. For (b), let $B_1, B_2$ be bases of $X$. If $|B_1| < |B_2|$, axiom (I3) gives an element $e \in B_2 \setminus B_1$ for which $B_1 + e$ is independent, contradicting the maximality of $B_1$. Interchanging the roles of $B_1, B_2$ proves equality. □

**Maximal is not the same as maximum.** In an arbitrary hereditary system, a maximal feasible set can be smaller than a maximum one. A matroid is special because every maximal independent subset of a fixed $X$ has the same size.

## 1.1 Canonical examples

**Example 1.3** (Uniform matroid)**.** For $0 \le r \le n$ and $|E| = n$, the uniform matroid $U_{r,n}$ has

$$\mathcal{I} = \{I \subseteq E : |I| \le r\}.$$

Every set of size at most $r$ is independent; there is no other structure.

**Example 1.4** (Linear or vector matroid)**.** Let $A$ be a matrix over a field $\mathbb{F}$ with columns indexed by $E$. Declare $I \subseteq E$ independent when the columns indexed by $I$ are linearly independent. The vector-space exchange lemma gives (I3). The resulting matroid is denoted $M_{\mathbb{F}}(A)$.

**Example 1.5** (Graphic matroid)**.** For a graph $G = (V, E)$, let $\mathcal{I}$ be the edge sets containing no cycle. Thus the independent sets are forests, and bases are maximal forests. If $G$ is connected, its bases are spanning trees. To verify (I3), observe that a forest with more edges has fewer connected components, so some edge of the larger forest joins two components of the smaller one.

**Example 1.6** (Partition matroid)**.** Let $E = P_1 \dot\cup \cdots \dot\cup P_k$ and choose quotas $0 \le q_i \le |P_i|$. Set

$$\mathcal{I} = \{I \subseteq E : |I \cap P_i| \le q_i \text{ for every } i\}.$$

If $|I| < |J|$, then some block contains fewer elements of $I$ than of $J$; an element from that block augments $I$.

**Example 1.7** (Transversal matroid)**.** Let a bipartite graph have left vertex set $E$ and right vertex set $R$. A subset $X \subseteq E$ is independent if it can be matched into $R$. Augmentation follows by superimposing matchings and flipping along an alternating path. Notice the distinction: matchable subsets on *one side* form a matroid, whereas arbitrary edge matchings generally do not.

## 2 Bases and basis exchange

**Definition 2.1.** A *basis of* $X \subseteq E$ is a maximal independent subset of $X$. A *base* is a basis of $E$, and $\mathcal{B}(M)$ denotes the family of all bases.

**Theorem 2.2** (Basis exchange)**.** *If $B_1, B_2$ are bases and $x \in B_1 \setminus B_2$, then some $y \in B_2 \setminus B_1$ satisfies*

$$B_1 - x + y \in \mathcal{B}(M).$$

*Proof.* The set $B_1 - x$ is independent and has size $|B_2| - 1$. By (I3), it can be augmented by some $y \in B_2 \setminus (B_1 - x)$. Since $x \notin B_2$, this means $y \in B_2 \setminus B_1$. The resulting independent set has the same size as a base, hence is a base. □

Basis exchange can itself be taken as the axiom system.

**Theorem 2.3** (Basis axioms)**.** *A family $\mathcal{B} \subseteq 2^E$ is the family of bases of a matroid if and only if*

(B1) $\mathcal{B} \neq \varnothing$;

(B2) $B_1, B_2 \in \mathcal{B},\ x \in B_1 \setminus B_2 \implies \exists y \in B_2 \setminus B_1 :\ B_1 - x + y \in \mathcal{B}$.

*The independent sets are recovered by*

$$\mathcal{I} = \{I : I \subseteq B \textit{ for some } B \in \mathcal{B}\}.$$

The converse direction is a standard exchange argument. In particular, (B2) forces all members of $\mathcal{B}$ to have the same size and yields augmentation for their subsets.

**Symmetric exchange is stronger than the axiom.** The symmetric basis-exchange theorem says that $y$ may be chosen so that both $B_1 - x + y$ and $B_2 - y + x$ are bases. This is a derived theorem; ordinary basis exchange only promises the first swap.

# 3 Circuits and minimal dependence

**Definition 3.1.** A *circuit* is an inclusion-minimal dependent set. The circuit family is denoted $\mathcal{C}(M)$. Thus every proper subset of a circuit is independent.

Because $E$ is finite, every dependent set contains a circuit. Circuits obey an exchange-like law of their own.

**Theorem 3.2** (Circuit axioms)**.** *A family $\mathcal{C} \subseteq 2^E$ is the circuit family of a matroid if and only if*

$$\begin{array}{ll} \text{(C1)} & \varnothing \notin \mathcal{C}; \\ \text{(C2)} & C_1, C_2 \in \mathcal{C},\ C_1 \subseteq C_2 \implies C_1 = C_2; \\ \text{(C3)} & C_1 \neq C_2,\ e \in C_1 \cap C_2 \implies \exists C_3 \in \mathcal{C} :\ C_3 \subseteq (C_1 \cup C_2) - e. \end{array}$$

*The independent sets are exactly the subsets containing no member of $\mathcal{C}$. The circuit family is allowed to be empty, as in the free matroid $U_{n,n}$.*

Axiom (C3) is *circuit elimination.* It asserts the existence of some circuit inside the union minus $e$; that entire set need not be a circuit, and the circuit obtained need not be unique.

**Lemma 3.3** (Unique circuit after one dependent addition)**.** *If $I$ is independent and $I + e$ is dependent, then $I + e$ contains a unique circuit, and that circuit contains $e$.*

*Proof.* Existence follows by minimality, and any circuit must contain $e$ because $I$ is independent. Suppose distinct circuits $C_1, C_2 \subseteq I + e$ exist. Choose $x \in C_1 \setminus C_2$. Extend the independent set $C_1 - x$ to a basis $B$ of $I + e$. The set $I$ is also a basis of $I + e$, so $|B| = |I|$; hence $B$ omits exactly one element of $I + e$. It cannot contain $x$, since then it would contain $C_1$. Therefore $B = (I + e) - x$, which contains $C_2$, a contradiction. ☐

*Why circuit elimination holds.* Let $C_1 \neq C_2$ and $e \in C_1 \cap C_2$. If $I = (C_1 \cup C_2) - e$ contained no circuit, then $I$ would be independent. But $I + e$ would contain the two distinct circuits $C_1, C_2$, contradicting theorem 3.3. Thus $I$ contains a circuit, as required by (C3). ☐

## 3.1 Fundamental circuits and exchange

**Definition 3.4.** Let $B$ be a base and $e \notin B$. The unique circuit contained in $B + e$ is the *fundamental circuit of $e$ with respect to $B$*, denoted $C(e, B)$.

**Proposition 3.5** (Fundamental-circuit exchange rule)**.** *For $x \in B$ and $e \notin B$,*

$$B - x + e \text{ is a base} \iff x \in C(e, B).$$

*Proof.* If $x \notin C(e, B)$, then $B - x + e$ still contains $C(e, B)$ and is dependent. If $x \in C(e, B)$, any circuit in $B - x + e$ would also be a circuit in $B + e$; by uniqueness it would equal $C(e, B)$, which is impossible because $x$ was removed. Thus $B - x + e$ is independent and has base cardinality. ☐

**Running example.** For the running graph and $B = \{a, b, c\}$,

$$C(e, B) = \{a, b, e\}, \qquad C(d, B) = \{a, b, c, d\}.$$

Consequently, $B - x + e$ is a base for $x \in \{a, b\}$ but not for $x = c$.

**Definition 3.6** (Loops and parallel elements)**.** An element $e$ is a *loop* if $\{e\}$ is a circuit. Distinct nonloops $e, f$ are *parallel* if $\{e, f\}$ is a circuit. In a graphic matroid these notions agree with graph loops and parallel graph edges.

The *strong circuit-elimination theorem* strengthens (C3): if $e \in C_1 \cap C_2$ and $f \in C_1 \setminus C_2$, then $C_3$ may be chosen with $f \in C_3 \subseteq (C_1 \cup C_2) - e$.

# 4 Rank and submodularity

**Definition 4.1** (Rank)**.** The rank of $X \subseteq E$ is

$$r_M(X) = \max\{|I| : I \subseteq X,\ I \in \mathcal{I}\}.$$

Equivalently, $r_M(X)$ is the size of any basis of $X$. The nullity of $X$ is $\mathrm{null}_M(X) = |X| - r_M(X)$.

For a graph $G = (V, E)$,

$$r_{M(G)}(X) = |V| - c(V, X),$$

where $c(V, X)$ counts the connected components of $(V, X)$, including isolated vertices. For a matrix, $r(X)$ is the dimension of the span of the indexed columns.

**Theorem 4.2** (Rank axioms)**.** *An integer-valued function $r : 2^E \to \mathbb{Z}_{\geq 0}$ is a matroid rank function if and only if, for all $X, Y \subseteq E$,*

$$\begin{aligned} &\text{(R1)} \quad 0 \leq r(X) \leq |X|; \\ &\text{(R2)} \quad X \subseteq Y \implies r(X) \leq r(Y); \\ &\text{(R3)} \quad r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y). \end{aligned}$$

*The independent sets are recovered by*

$$\mathcal{I}_r = \{I \subseteq E : r(I) = |I|\}.$$

Axiom (R3) is *submodularity.* It formalizes diminishing returns: rank gained by an element cannot increase as the set around it grows.

**Proposition 4.3** (Rank is submodular)**.** *For every matroid and $X, Y \subseteq E$,*

$$r(X) + r(Y) \geq r(X \cup Y) + r(X \cap Y).$$

*Proof.* Choose a basis $I$ of $X \cap Y$. Extend it to a basis $I \cup J$ of $X$, and then extend $I \cup J$ to a basis $I \cup J \cup K$ of $X \cup Y$. The new elements may be chosen from $Y \setminus X$, so $I \cup K$ is an independent subset of $Y$. Therefore

$$\begin{aligned} r(X) + r(Y) &\geq (|I| + |J|) + (|I| + |K|) \\ &= r(X \cup Y) + r(X \cap Y). \end{aligned}$$

□

Two useful consequences are

$$r(X) \le r(X+e) \le r(X)+1$$

and, whenever $X \subseteq Y$ and $e \notin Y$,

$$r(X+e) - r(X) \ge r(Y+e) - r(Y).$$

The latter follows by applying submodularity to $X+e$ and $Y$.

*Why the rank axioms recover a matroid.* Define $\mathcal{I}_r = \{I : r(I) = |I|\}$. Since one element raises rank by at most one, every subset of a set $I$ satisfying $r(I) = |I|$ has the same property, giving heredity. If $I, J \in \mathcal{I}_r$, $|I| < |J|$, and no $e \in J \setminus I$ raises $r(I)$, diminishing returns implies $r(I \cup J) = r(I) = |I|$. But monotonicity gives $|J| = r(J) \le r(I \cup J)$, a contradiction. Hence some $e$ augments $I$. $\square$

**Rank dictionary.** For $X \subseteq E$:

$$\begin{aligned}
X \text{ is independent} &\iff r(X) = |X|, \\
X \text{ is spanning} &\iff r(X) = r(E), \\
X \text{ is a base} &\iff |X| = r(X) = r(E), \\
C \text{ is a circuit} &\iff r(C) = |C| - 1 \text{ and } r(C - c) = |C| - 1 \ \forall c \in C.
\end{aligned}$$

**Running example.** The running matroid has rank 3. Each triangle has rank 2, the four-cycle has rank 3, and every other set of at least three edges has rank 3. For example, $r(abe) = 2$, $r(abcd) = 3$, and $r(E) = 3$.

## 5 Closure, span, flats, and hyperplanes

**Definition 5.1** (Closure)**.** For $X \subseteq E$, define

$$\mathrm{cl}_M(X) = \{e \in E : r_M(X+e) = r_M(X)\}.$$

Thus $e \in \mathrm{cl}(X)$ exactly when $e$ adds no new rank to $X$.

In a vector matroid, closure is linear span restricted to the represented columns. In a graphic matroid, an edge lies in $\mathrm{cl}(X)$ exactly when its endpoints are already connected in $(V, X)$.

**Theorem 5.2** (Closure axioms)**.** *Matroid closure satisfies, for all $X, Y \subseteq E$ and $x, y \in E$,*

$$\begin{aligned}
&\text{(CL1)} \quad X \subseteq \mathrm{cl}(X); \\
&\text{(CL2)} \quad X \subseteq Y \implies \mathrm{cl}(X) \subseteq \mathrm{cl}(Y); \\
&\text{(CL3)} \quad \mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X); \\
&\text{(CL4)} \quad y \in \mathrm{cl}(X+x) \setminus \mathrm{cl}(X) \implies x \in \mathrm{cl}(X+y).
\end{aligned}$$

*Conversely, every operator $\mathrm{cl} : 2^E \to 2^E$ satisfying these axioms is the closure operator of a matroid. Independence is recovered by*

$$I \in \mathcal{I} \quad \iff \quad x \notin \mathrm{cl}(I - x) \text{ for every } x \in I.$$

*Proof of closure exchange (CL4).* Assume $y \in \mathrm{cl}(X+x) \setminus \mathrm{cl}(X)$. If $x \in \mathrm{cl}(X)$, monotonicity and idempotence of closure would give $\mathrm{cl}(X+x) = \mathrm{cl}(X)$, a contradiction. Thus both $x$ and $y$ raise the rank of $X$ by one. Since $y$ does not raise the rank of $X+x$,

$$r(X+x+y) = r(X+x) = r(X)+1 = r(X+y),$$

so $x \in \mathrm{cl}(X+y)$. □

**Proposition 5.3** (Circuit characterization of closure)**.** *If $e \notin X$, then*

$$e \in \mathrm{cl}(X) \quad \Longleftrightarrow \quad \exists C \in \mathcal{C}(M) \text{ with } e \in C \subseteq X+e.$$

*Proof.* If such a circuit exists, then $e$ is dependent on $C - e \subseteq X$, so adding $e$ to $X$ cannot raise rank. Conversely, choose a basis $I$ of $X$. If $e \in \mathrm{cl}(X)$, then $I+e$ is dependent and contains a circuit. That circuit must contain $e$, because $I$ is independent, and it lies in $X+e$. □

## 5.1 Spanning sets, flats, and hyperplanes

**Definition 5.4.** A set $S$ is *spanning* if $\mathrm{cl}(S) = E$, equivalently $r(S) = r(E)$. A *flat* is a closed set $F = \mathrm{cl}(F)$. A *hyperplane* is a maximal proper flat.

For a flat $F$, every $e \notin F$ raises rank by one. Conversely, this property characterizes flats. A hyperplane has rank $r(M)-1$, and every rank $r(M)-1$ flat is a hyperplane.

Flats are closed under arbitrary intersections, while unions of flats need not be flats. In the lattice of flats,

$$F \wedge G = F \cap G, \qquad F \vee G = \mathrm{cl}(F \cup G).$$

**Running example.** For the running graph,

$$\mathrm{cl}(\{a,b\}) = \{a,b,e\}, \qquad \mathrm{cl}(\{a,c\}) = \{a,c\}, \qquad \mathrm{cl}(\{a,b,c\}) = E.$$

The first set closes up the triangle because the endpoints of $e$ are already connected. The set $\{a,b,e\}$ is a rank-two hyperplane.

| **Matroid** | Closure of $X$ |
|---|---|
| **Uniform** $U_{r,n}$ | $X$ if $\lvert X\rvert < r$, and $E$ if $\lvert X\rvert \geq r$. |
| **Linear** | All represented columns lying in the linear span of the columns in $X$. |
| **Graphic** | $X$ together with every edge whose endpoints lie in one component of $(V,X)$. |
| **Partition** | If $\lvert X \cap P_i\rvert \geq q_i$, add all of $P_i$; otherwise leave $X \cap P_i$ unchanged. |

**Common pitfall.** $\mathrm{cl}(\varnothing)$ need not be empty: it is exactly the set of loops. Thus $\varnothing$ need not be a flat. Matroid closure is also not topological closure; in general $\mathrm{cl}(X \cup Y) \neq \mathrm{cl}(X) \cup \mathrm{cl}(Y)$.

**Flats can also be axiomatized.** For a family $\mathcal{F} \subseteq 2^E$, let $\mathrm{Cov}(F)$ be the flats that cover $F$. The family $\mathcal{F}$ is the flat family of a finite matroid exactly when: $E \in \mathcal{F}$; intersections of members of $\mathcal{F}$ lie in $\mathcal{F}$; and, for each $F \in \mathcal{F}$, the sets $G \setminus F$ with $G \in \mathrm{Cov}(F)$ partition $E \setminus F$. Closure is recovered as the intersection of all flats containing the given set.

### 5.2 Loops, parallelism, and coloops

The structural descriptions now line up:

$$\begin{aligned} e \text{ is a loop} &\iff \{e\} \text{ is a circuit} \iff e \in \mathrm{cl}(\varnothing) \iff e \text{ lies in no base;} \\ e, f \text{ are parallel nonloops} &\iff \{e, f\} \text{ is a circuit} \iff f \in \mathrm{cl}(\{e\}); \\ e \text{ is a coloop} &\iff e \text{ lies in every base} \iff e \text{ lies in no circuit.} \end{aligned}$$

## 6 Duality and cocircuits

Duality exchanges choosing with omitting.

**Definition 6.1** (Dual matroid)**.** For a matroid $M$ on $E$, define $M^*$ by

$$\mathcal{B}(M^*) = \{E \setminus B : B \in \mathcal{B}(M)\}.$$

The basis axioms show that this is a matroid, called the *dual* of $M$. Clearly $(M^*)^* = M$.

**Proposition 6.2** (Dual rank formula)**.** *For every $X \subseteq E$,*

$$r_{M^*}(X) = |X| - r_M(E) + r_M(E \setminus X).$$

*Proof.* An independent subset of $X$ in $M^*$ lies in $E \setminus B$ for some base $B$ of $M$. Hence

$$r_{M^*}(X) = |X| - \min_{B \in \mathcal{B}(M)} |B \cap X|.$$

Every base uses at least $r_M(E) - r_M(E \setminus X)$ elements of $X$, and equality is attained by extending a basis of $E \setminus X$ to a base of $M$. $\square$

**Definition 6.3.** A *cocircuit* of $M$ is a circuit of $M^*$. Equivalently, cocircuits are the complements of hyperplanes of $M$. A *coloop* of $M$ is a loop of $M^*$.

For a graph, cocircuits of $M(G)$ are the *bonds*: inclusion-minimal nonempty edge cuts. If a connected plane graph (with a fixed embedding) has dual graph $G^*$, then $M(G)^* \cong M(G^*)$. Also

$$U_{r,n}^* = U_{n-r,n}.$$

**Theorem 6.4** (Circuit–cocircuit orthogonality)**.** *If $C$ is a circuit and $D$ is a cocircuit of a matroid, then*

$$|C \cap D| \neq 1.$$

*Proof.* Suppose $C \cap D = \{e\}$. Since $D$ is a cocircuit, $H = E \setminus D$ is a hyperplane and hence a flat. Now $C - e \subseteq H$, while the circuit property gives $e \in \mathrm{cl}(C - e)$. Therefore

$$e \in \mathrm{cl}(C - e) \subseteq \mathrm{cl}(H) = H,$$

contradicting $e \in D$. $\square$

**Parity is a binary phenomenon.** For an arbitrary matroid, a circuit and a cocircuit are only guaranteed not to intersect in exactly one element. In a binary matroid, every circuit–cocircuit intersection has even cardinality, which is strictly stronger.

**Running example.** In the running graph, $D = \{a, b\}$ is the bond isolating vertex 2, hence a cocircuit. It meets the triangle $\{a, b, e\}$ in two elements and is disjoint from $\{c, d, e\}$, consistent with orthogonality.

# 7 Deletion, contraction, and minors

**Definition 7.1** (Restriction and deletion)**.** For $A \subseteq E$, the restriction $M|A$ has ground set $A$ and independent sets $\{I \in \mathcal{I}(M) : I \subseteq A\}$. Deleting $A$ means restricting to the complement:

$$M \setminus A = M|(E \setminus A).$$

Thus $r_{M \setminus A}(X) = r_M(X)$ for $X \subseteq E \setminus A$.

**Definition 7.2** (Contraction)**.** For $A \subseteq E$, the contraction $M/A$ has ground set $E \setminus A$ and rank function

$$r_{M/A}(X) = r_M(X \cup A) - r_M(A), \qquad X \subseteq E \setminus A.$$

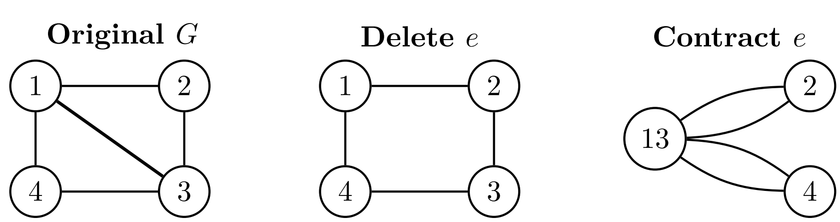
Equivalently, if $B_A$ is a basis of $A$, then $I \subseteq E \setminus A$ is independent in $M/A$ exactly when $I \cup B_A$ is independent in $M$.

A *minor* is obtained by a sequence of deletions and contractions. These operations commute on disjoint sets, and duality swaps them:

$$(M \setminus A)^* = M^*/A, \qquad (M/A)^* = M^* \setminus A.$$

The circuits of $M \setminus A$ are the circuits of $M$ disjoint from $A$. The circuits of $M/A$ are the inclusion-minimal nonempty sets among $C \setminus A$, where $C$ ranges over circuits of $M$.

For a graph, matroid deletion and contraction agree with graph deletion and contraction (with the usual handling of loops and parallel edges).




For the running example, $M \setminus e$ is the four-cycle matroid, while $M/e$ has two parallel pairs $\{a, b\}$ and $\{c, d\}$.

**Direct sums.** If $M_1, M_2$ have disjoint ground sets, their direct sum has

$$\mathcal{I}(M_1 \oplus M_2) = \{I_1 \cup I_2 : I_i \in \mathcal{I}(M_i)\}, \qquad r_{M_1 \oplus M_2}(X) = r_{M_1}(X \cap E_1) + r_{M_2}(X \cap E_2).$$

Circuits stay inside one summand, and $(M_1 \oplus M_2)^* = M_1^* \oplus M_2^*$.

## References

[1] J. Oxley, *Matroid Theory*, 2nd ed., Oxford University Press, 2011.

[2] A. Schrijver, *Combinatorial Optimization: Polyhedra and Efficiency*, Springer, 2003.

[3] D. J. A. Welsh, *Matroid Theory*, Academic Press, 1976.