5. Matroids and the greedy algorithm

Let E be a finite nonempty set and denote by $\mathcal{P}(E)$ the set of all subsets of E. A **hereditary system** M on E consists of a nonempty subset $\mathbf{I}_M \subseteq \mathcal{P}(E)$ such that for all $X \in \mathbf{I}_M$, we have $Y \in \mathbf{I}_M$ for all $Y \subseteq X$.

The elements of $\mathbf{I}_M$ are the **independent sets** of M. The subsets of E in $\mathbf{D}_M := \mathcal{P}(E) - \mathbf{I}_M$ are **dependent**.

A **base** is a maximal independent set; the set of all bases in M is denoted by $\mathbf{B}_M$. A **circuit** is a minimal dependent set; the set of all circuits in M is denoted by $\mathbf{C}_M$.

A **loop** is a circuit of size 1. **Parallel elements** are distinct non-loops that form a circuit of size 2.

The **rank** of a subset $X \subseteq E$ is the maximum size of an independent set in it. The **rank function** r_M is defined by

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

A hereditary system M on E is determined by any one of $\mathbf{I}_M$, $\mathbf{B}_M$, $\mathbf{D}_M$, $\mathbf{C}_M$, r_M since each determines all the others.

Matroids are a subclass of hereditary systems whose study was initiated in the 1930s by Whitney, Birkhoff, MacLane, and van der Waerden.

Examples of matroids and hereditary systems

1. Let V be a vector space and let $E \subseteq V$ be a finite set of vectors. The **vectorial matroid** on E is the hereditary system whose independent sets are the subsets $X \subseteq E$ that are linearly independent in V.

2. A hereditary system expressible as a vectorial matroid is a **linear matroid** (or a **representable matroid**). A linear matroid that admits representation over GF(2) is a **binary matroid**. Similarly, a linear matroid representable over GF(3) is a **ternary matroid**.

3. The **column matroid** $M(A)$ of a matrix A is the vectorial matroid defined by the columns of A.

4. Let $|E| = n$. The **uniform matroid** $U_{k,n}$ of rank k is the hereditary system whose bases are the k-subsets of E. The **free matroid** is the uniform matroid of rank n.

5. The **cycle matroid** $M(G)$ of a graph G is the hereditary system on $E(G)$ whose circuits are the cycles of G. A hereditary system that is $M(G)$ for some G is a **graphic matroid**.

6. The **bond matroid** (or **cocycle matroid**) $M^*(G)$ of a graph G is the hereditary system on $E(G)$ whose circuits are the bonds of G. (Recall that a **bond** is a minimal set of edges in G whose removal increases the number of components.)

7. Let $A_1, \ldots, A_m \subseteq E$. Define a bipartite graph G with bipartition $\{1, \ldots, m\} \dot\cup E$ as follows: for all $i \in \{1, \ldots, m\}$ and $e \in E$ we have $i \leftrightarrow e$ if and only if $e \in A_i$.
The **transversal matroid** associated with $A_1, \ldots, A_m$ is the hereditary system on E where $X \subseteq E$ is independent if and only if there exists a matching in G that saturates all the vertices in X.

8. Let $A_1, \ldots, A_m$ be a partition of E. The associated **partition matroid** is the hereditary system on E where $X \subseteq E$ is independent if and only if $|X \cap A_i| \leq 1$ for all $i \in \{1, \ldots, m\}$.

9. Let G be a graph. A set $X \subseteq V(G)$ is independent if no two vertices in X are adjacent in G. This defines a hereditary system on $V(G)$. (This system is not in general a matroid.)

10. Let G be a bipartite graph. A set $X \subseteq E(G)$ is independent if it is a matching in G. This defines a hereditary system on $E(G)$. (This system is the intersection of two matroids, but not in general a matroid.)

Outline

This lecture gives a brief introduction to matroids.

1. Definition of a matroid, properties of matroids.
2. Matroids and optimization: the greedy algorithm.
3. Duality in matroids.
4. Restriction, contraction.

Sources for this lecture

The material for this lecture has been prepared with the help of [Wes, Section 8.2] and [Jun, Chapter 5]. Two excellent references to matroid theory are [Oxl] and [Wel].

[Oxl] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.

[Wel] D. J. A. Welsh, *Matroid Theory*, Academic Press [Harcourt Brace Jovanovich, Publishers], London, 1976.

Properties of matroids

There are a number of equivalent ways to define a matroid.

A hereditary system M on E is a **matroid** if it satisfies any of the following nine properties:

(I) **augmentation** — if $I_1, I_2 \in \mathbf{I}$ and $|I_2| > |I_1|$, then $I_1 + e \in \mathbf{I}$ for some $e \in I_2 - I_1$;

(U) **uniformity** — for every $X \subseteq E$, the maximal independent subsets of X have the same size;

(B) **base exchange** — if $B_1, B_2 \in \mathbf{B}$, then for all $e \in B_1 - B_2$ there exists a $f \in B_2 - B_1$ such that $B_1 - e + f \in \mathbf{B}$;

(R) **submodularity** — $r(X \cap Y) + r(X \cup Y) \leq r(X) + r(Y)$ for all $X, Y \subseteq E$;

(A) **weak absorption** — $r(X) = r(X + e) = r(X + f)$ implies $r(X + e + f) = r(X)$ whenever $X \subseteq E$ and $e, f \in E$;

(A') **strong absorption** — if $X, Y \subseteq E$ and $r(X + e) = r(X)$ for all $e \in Y$, then $r(X \cup Y) = r(X)$.

(C) **weak elimination** — if $C_1, C_2 \in \mathbf{C}$ are distinct and $x \in C_1 \cap C_2$, then $(C_1 \cup C_2) - x$ contains a circuit;

(J) **induced circuits** — if $I \in \mathbf{I}$ and $e \in E$, then $I + e$ contains at most one circuit;

(G) **greedy algorithm** — for any nonnegative weight function on E, the greedy algorithm outputs an independent set of the maximum total weight.

The greedy algorithm

Input: A hereditary system M on E, a nonnegative weight function $w : E \to \mathbb{R}$.

Output: A maximal independent subset of E.

Iteration: Starting with $X = \emptyset$, repeatedly augment X with an $e \in E - X$ of the maximum possible weight such that $X + e \in \mathbf{I}$. Output X and halt when no augmentation can be performed.

Property G shows that matroids are precisely the hereditary systems for which the greedy algorithm outputs a maximum-weight independent set *regardless* of the weight function w.

Theorem A.42 *For a hereditary system M on E, the properties* I, U, B, R, A, A', C, J, G *are equivalent.*

Proof: For the full proof, see [Wes, p. 355–357]. We prove only the equivalence of I, R, C, J, G, I.

(I $\Rightarrow$ R) Let $X, Y \subseteq E$. Let I_1 be a maximum independent set in $X \cap Y$ and let I_2' be a maximum independent set in $X \cup Y$. Clearly, $|I_2'| \geq |I_1|$. Using I to augment I_1 with elements of I_2', we obtain $I_2 \in \mathbf{I}$ such that $I_1 \subseteq I_2$ and $|I_2| = |I_2'|$. Since $I_1 \subseteq I_2 \cap X$, $I_1 \subseteq I_2 \cap Y$, and I_1 is maximum in $X \cap Y$, we have

$$r(X \cap Y) + r(X \cup Y) = |I_1| + |I_2| = |I_2 \cap X| + |I_2 \cap Y| \leq r(X) + r(Y).$$

Since X, Y were arbitrary, R holds.

(R $\Rightarrow$ C) Let C_1, C_2 be distinct circuits and let $x \in C_1 \cap C_2$. Because C_1, C_2 are circuits, $r(C_1) = |C_1| - 1$ and $r(C_2) = |C_2| - 1$. To reach a contradiction, suppose $(C_1 \cup C_2) - x$ is independent. Then, $r((C_1 \cup C_2) - x) = |C_1 \cup C_2| - 1$. Since C_1, C_2 are distinct, we have $C_1 \cap C_2 \in \mathbf{I}$ and hence $r(C_1 \cap C_2) = |C_1 \cap C_2|$. By R, we obtain

$$|C_1 \cap C_2| + |C_1 \cup C_2| - 1 \leq |C_1| + |C_2| - 2,$$

which is a contradiction since $|C_1 \cap C_2| + |C_1 \cup C_2| = |C_1| + |C_2|$ for any two sets C_1, C_2. Thus, $(C_1 \cup C_2) - x$ is dependent and must hence contain a circuit.

(C $\Rightarrow$ J) Let $I \in \mathbf{I}$, $e \in E$. To reach a contradiction, suppose C_1, C_2 are distinct circuits in $I + e$. Since $I \in \mathbf{I}$, we have $e \in C_1$ and $e \in C_2$. Hence $e \in C_1 \cap C_2$, so C implies $(C_1 \cup C_2) - e$ contains a circuit. But this cannot happen because $(C_1 \cup C_2) - e \subseteq I$.

(J $\Rightarrow$ G) For an arbitrary weight function w, let I be the set output by the greedy algorithm on input M, w. Let I^* be a maximum-weight independent set for which $|I \cap I^*|$ is as large as possible. We prove that $I = I^*$. By the structure of the algorithm, we cannot have $I \subsetneq I^*$. To reach a contradiction, let $e \in I - I^*$ be the first element outside I^* selected by the greedy algorithm. By the choice of I^*, $I^* + e \in \mathbf{D}$. Thus, $I^* + e$ contains a unique circuit C by J. We have $C - I \neq \emptyset$ since $I \in \mathbf{I}$. Let $f \in C - I$. Since $I^* + e$ contains no other circuit, $I^* + e - f \in \mathbf{I}$. Since I^* has the maximum weight, $w(f) \geq w(e)$. By the choice of e, $w(e) \geq w(f)$. Thus, $w(e) = w(f)$ and $I^* + e - f$ and I^* have the same weight. But this contradicts the choice of I^* because $|I^* \cap I| < |(I^* + e - f) \cap I|$. Consequently, $I = I^*$.

(G $\Rightarrow$ I) Let $I_1, I_2 \in \mathbf{I}$ with $|I_2| > |I_1| = k$. Define a weight function w on E by

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

When started with input M, w, the greedy algorithm selects first all the elements of I_1, thus obtaining an independent set of weight $k(k+2)$. Since $w(I_2) \geq (k+1)^2 > k(k+2) = w(I_1)$, the set I_1 is not a maximum-weight independent set. So, by G there must exist an $e \in I_2 - I_1$ such that $I_1 + e \in \mathbf{I}$. $\square$

The span function

The **span function** of a hereditary system M on E is the function $\sigma_M : \mathcal{P}(E) \to \mathcal{P}(E)$ defined for all $X \subseteq E$ by

$$\sigma_M(X) := X \cup \{e \in E \ : \ Y + e \in \mathbf{C}_M \text{ for some } Y \subseteq X\}.$$

Examples:

1. In a vectorial matroid M, $\sigma_M(X)$ consists of all vectors in E that lie in the vector subspace spanned by the vectors in X.
2. In a cycle matroid $M(G)$, $\sigma_M(X)$ consists of all edges in $E(G)$ whose endpoints are connected by a path consisting only of edges in X.

Properties of the span function

The span function σ of a hereditary system M on E has the following properties.

(s1) $X \subseteq \sigma(X)$ (σ is **expansive**);

(s2) $X \subseteq Y$ implies $\sigma(X) \subseteq \sigma(Y)$ (σ is **order-preserving**);

(s3) $e \notin \sigma(X)$ and $e \in \sigma(X+f)$ imply $f \in \sigma(X+e)$ (**Steinitz exchange**).

To see that property (s3) holds, observe that $e \in \sigma(X+f)$ implies that $X+e+f$ contains a cycle C with $e \in C$. Since $e \notin \sigma(X)$, $f \in C$. Thus, C gives $f \in \sigma(X+e)$.

Matroids and the span function

Each of the following four conditions P, S, T, C' on σ is necessary and sufficient for a hereditary system M to be a matroid.

(P) **incorporation** — $r(X) = r(\sigma(X))$ for all $X \subseteq E$;

(S) **idempotence** — $\sigma(\sigma(X)) = \sigma(X)$ for all $X \subseteq E$;

(T) **transitivity of dependence** — if $e \in \sigma(X)$ and $X \subseteq \sigma(Y)$, then $e \in \sigma(Y)$;

(C') **strong elimination** — whenever $C_1, C_2 \in \mathbf{C}$, $e \in C_1 \cap C_2$, and $f \in (C_1 - C_2) \cup (C_2 - C_1)$, there exists a $C \in \mathbf{C}$ such that $f \in C \subseteq (C_1 \cup C_2) - e$.

(For a proof of this claim, see [Wes, p. 359].)

More terminology

The **spanning sets** of a hereditary system M on E are the sets $X \subseteq E$ for which $\sigma(X) = E$.

The **closed sets** (or **flats** or **subspaces**) are the sets $X \subseteq E$ such that $\sigma(X) = X$.

The **hyperplanes** are the maximal proper closed subsets of E.

The **supbases S** of M are the sets $X \subseteq E$ that contain a base.

The **hypobases H** of M are the maximal subsets containing no base.

The dual of a hereditary system

Duality in matroids generalizes the notion of duality in plane graphs.

Let M be a hereditary system on E. The **dual** of M, denoted by M^*, is the hereditary system on E where $X \subseteq E$ is independent if and only if $\bar{X} := E - X$ contains a base of M (i.e. $\bar{X} \in \mathbf{S}$).

M^* is well-defined because

$$X_1 \subseteq X_2 \text{ if and only if } \bar{X}_2 \subseteq \bar{X}_1. \qquad (*)$$

We write $\mathbf{I}^*$ for the independent sets of M^*, $\mathbf{B}^*$ for the bases of M^*, $\mathbf{C}^*$ for the circuits of M^*, and so on. A set in $\mathbf{I}^*$ is **coindependent** in M. Similarly, the sets in $\mathbf{B}^*$ and $\mathbf{C}^*$ are the **cobases** and **cocircuits** of M.

Duality

By $(*)$, a maximal independent set in M^* is the complement of a minimal set that contains a base of M (i.e. the minimal set *is* a base of M). In other words, the bases of M^* are the complements of bases in M. This gives the first two equalities below. The other equalities can be obtained from $(*)$ using analogous arguments.

$$\mathbf{B}^* = \{\bar{B} \ : \ B \in \mathbf{B}\}, \qquad \mathbf{B} = \{\bar{B} \ : \ B \in \mathbf{B}^*\};$$
$$\mathbf{I}^* = \{\bar{S} \ : \ S \in \mathbf{S}\}, \qquad \mathbf{S}^* = \{\bar{I} \ : \ I \in \mathbf{I}\};$$
$$\mathbf{C}^* = \{\bar{H} \ : \ H \in \mathbf{H}\}, \qquad \mathbf{H}^* = \{\bar{C} \ : \ C \in \mathbf{C}\}.$$

In particular, $(M^*)^* = M$.

Duality in matroids: preliminaries

Lemma A.9 *If M is a matroid, then the supbases are the spanning sets, and the hypobases are the hyperplanes.*

Proof: We prove only the first claim, the latter claim is left as an exercise. Any base $B \subseteq E$ of M is clearly a spanning set (any $e \in E - B$ occurs by definition in a circuit $C \subseteq B + e$). For the converse, let $X \subset E$ be spanning, i.e. $\sigma(X) = E$. By incorporation, $r(X) = r(\sigma(X)) = r(E)$. By uniformity, all bases have the same size $r(E)$. Thus, X contains a base. □

We require the following dual base exchange property to prove that M^* is a matroid if M is a matroid.

Lemma A.10 *If M is a matroid and $B_1, B_2 \in \mathbf{B}$, then for each $e \in B_2 - B_1$ there exists an $f \in B_1 - B_2$ such that $B_1 + e - f$ is a base.*

Proof: Since B_1 is a base, there exists a unique circuit $C \subseteq B_1 + e$. Now, $C - B_2$ must be nonempty because otherwise $C \subseteq B_2$. Let $f \in C - B_2$. Since C is the unique circuit in $B_1 + e$, $B_1 + e - f$ is independent and hence a base by uniformity. □

Duality in matroids

Theorem A.43 *The dual of a matroid M on E is a matroid with rank function $r^*(X) = |X| - (r(E) - r(\bar{X}))$.*

Proof: We prove first that the dual satisfies the base exchange property. Let $B_1, B_2 \in \mathbf{B}^*$ be distinct and let $e \in B_1 - B_2$. By duality, $\bar{B}_1, \bar{B}_2 \in \mathbf{B}$ and $e \in \bar{B}_2 - \bar{B}_1$. Since M is a matroid, Lemma A.10 shows that there exists an $f \in \bar{B}_1 - \bar{B}_2$ (i.e. $f \in B_2 - B_1$) such that $\bar{B}_1 + e - f \in \mathbf{B}$ (i.e. $B_1 - e + f \in \mathbf{B}^*$). Thus, the base exchange property holds for M^*.

Proof: (continued) Let $X \subseteq E$ and let Y be a maximal coindependent set in X, i.e. $\bar{Y}$ is a minimal superset of $\bar{X}$ that contains a base. Since $\bar{Y}$ contains only those elements outside $\bar{X}$ that are necessary to augment a maximal independent set in $\bar{X}$ to a base, we have

$$|\bar{Y}| - |\bar{X}| = r(\bar{Y}) - r(\bar{X}) = r(E) - r(\bar{X}).$$

(Note that maximal independent sets in $\bar{X}$ have the same size by uniformity.) Thus, $|X| + |\bar{X}| = |Y| + |\bar{Y}|$ implies

$$r^*(X) = r^*(Y) = |Y| = |X| - (r(E) - r(\bar{X})).$$

□

Theorem A.44 *For any graph G, the dual of the cycle matroid $M(G)$ is the bond matroid $M^*(G)$.*

Proof: We prove that the cocircuits of the cycle matroid $M(G)$ are the bonds of G, which by definition are the circuits of $M^*(G)$. A cocircuit is a minimal set intersecting every base of $M(G)$, i.e., a minimal set of edges that intersects every maximal spanning forest of G.

A set $X \subseteq E(G)$ that intersects every maximal spanning forest of G also has the property that the deletion of X from G increases the number of components in G (otherwise there would exist a maximal spanning forest that does not intersect X). Conversely, a set $X \subseteq E(G)$ whose deletion increases the number of components must intersect every maximal spanning forest of G (a maximal spanning forest consists of spanning trees for each component of G). □

Restriction, contraction

Let M be a hereditary system on E and let $F \subseteq E$.

The **restriction** of M to F, denoted by $M|F$, is the hereditary system on F defined by

$$\mathbf{I}_{M|F} = \{X \in \mathbf{I}_M \ : \ X \subseteq F\}.$$

The **contraction** of M to F, denoted by $M.F$, is the hereditary system on F defined by

$$\mathbf{S}_{M.F} = \{X \subseteq F : \ X \cup \bar{F} \in \mathbf{S}_M\}.$$

Alternatively, we say that $M|F$ is the hereditary system obtained from M by **deleting** $\bar{F}$. Similarly, $M.F$ is obtained from M by **contracting** $\bar{F}$.

Duality of restriction and contraction

Theorem A.45 *For hereditary systems, restriction and contraction are dual operations: $(M.F)^* = M^*|F$ and $(M|F)^* = M^*.F$.*

Proof: For the first claim, observe that

$$\begin{aligned}
\mathbf{I}_{(M.F)^*} &= \{X \subseteq F \ : \ F - X \in \mathbf{S}_{M.F}\} \\
&= \{X \subseteq F \ : \ (F - X) \cup (E - F) \in \mathbf{S}_M\} \\
&= \{X \subseteq F \ : \ E - X \in \mathbf{S}_M\} \\
&= \{X \subseteq F \ : \ X \in \mathbf{I}_{M^*}\} \\
&= \mathbf{I}_{M^*|F}.
\end{aligned}$$

The first claim and $M^{**} = M$ imply the second claim because $(M|F)^* = (M^{**}|F)^* = (M^*.F)^{**} = M^*.F$. □

Theorem A.46 *If M is a matroid, then both $M|F$ and $M.F$ are matroids, and their rank functions are*

$$r_{M|F}(X) = r_M(X), \qquad r_{M.F}(X) = r_M(X \cup \bar{F}) - r_M(\bar{F}).$$

Proof: The augmentation property of M is passed on to $M|F$. Thus, $M|F$ is a matroid and its rank function is clearly as claimed. Because $M^*|F$ is a matroid, also $M.F = (M^*|F)^*$ is a matroid. By Theorem A.43,

$$\begin{aligned}
r_{(M^*|F)^*}(X) &= |X| - (r_{M^*|F}(F) - r_{M^*|F}(F - X)) \\
&= |X| - r_{M^*}(F) + r_{M^*}(F - X) \\
&= |X| - |F| + r_M(E) - r_M(E - F) \\
&\quad + |F - X| - r_M(E) + r_M(E - (F - X)) \\
&= r_M(X \cup \bar{F}) - r_M(\bar{F}).
\end{aligned}$$

□