Geometric Combinatorics

Daniel Irving Bernstein

Contents

CHAPTER 1

Convexity and polytopes

1. Convexity basics

A linear combination of elements in a set $S \subseteq \mathbb{R}^d$ is an expression of the form

$$\sum_{i=1}^{n} t_i x_i$$

where each $x_i \in S$. Such a linear combination is called an ***affine combination*** if $\sum_i t_i = 1$, a ***conic combination*** if $t_i \geq 0$ for each i, and a ***convex combination*** if it is conic and affine. The set of all linear, affine, conic, and convex combinations of a set S will be denoted $\mathbb{R}S, \mathrm{Aff}(S), \mathbb{R}_{\geq 0}(S)$, and $\mathrm{Conv}(S)$. In words, we will refer to them as the linear span, the affine hull, the conic hull, and the convex hull of S.

Let us explore the geometric significance of these concepts when $S = \{x, y\}$ consists of two distinct points. When neither x nor y is the origin, the linear hull of S is the unique plane containing x, y and the origin. The affine hull of S is the unique line in $\mathbb{R}^d$ containing x and y and the convex hull of S is the line segment between x and y. The conic hull of S is the union of all rays from the origin through a point in the convex hull of x and y.

One says that $S \subseteq \mathbb{R}^d$ is a ***linear subspace*** when $S = \mathbb{R}(S)$, an ***affine subspace*** when $S = \mathrm{Aff}(S)$, a ***cone*** when $S = \mathbb{R}_{\geq 0}(S)$, and ***convex*** when $S = \mathrm{Conv}(S)$.

A ***V-polytope*** is the convex hull of a finite set of points, i.e. a set of the form $\mathrm{Conv}(\{x_1, \dots, x_n\})$.

FIGURE 1.1.1. The square is a polytope. The disc is convex, but not a polytope.

A ***halfspace*** is a set of the form $\{x \in \mathbb{R}^d : ax \leq c\}$ where $a \in (\mathbb{R}^d)^*$ and $c \in \mathbb{R}$. An ***H-polyhedron*** is an intersection of finitely many halfspaces. An ***H-polytope*** is a bounded H-polyhedron. We will see in Section 3 that every V-polytope is an H-polytope and vice versa.

We now give several examples of polytopes.

(1) **Simplices:** Fix an integer $d \geq 1$ and for each $1 \leq i \leq n$ define $e_i \in \mathbb{R}^d$ to be the i^{th} standard basis vector in $\mathbb{R}^d$. We define the ***standard simplices*** as follows

$$\begin{aligned}\Delta_{d-1} :&= \mathrm{Conv}\{e_1, \dots, e_d\} \\ &= \{x \in \mathbb{R}^d : \sum_{i=1}^{d} x_i = 1; 0 \leq x_i \forall i = 1, \dots, d\}.\end{aligned}$$

(2) **Cubes:** Given $d \geq 1$, define the ***standard d-dimensional cube*** by

$$\begin{aligned} C_d &:= \operatorname{Conv}(\{+1,-1\}^d) \\ &= \{x \in \mathbb{R}^d : -1 \leq x_i \leq 1 \forall i = 1, \ldots, d\}. \end{aligned}$$

(3) **Cross polytopes:** Given $d \geq 1$, define the ***standard d-dimensional cross polytope*** by

$$\begin{aligned} C_d^* &:= \operatorname{Conv}\{e_1, -e_1, e_2, -e_2, \ldots, e_d, -e_d\} \\ &= \{x \in \mathbb{R}^d : \sum_{i=1}^d |x_i| \leq 1\}. \end{aligned}$$

Perhaps the most fundamental quantity one can associate to a geometric object is its dimension. We would like a precise way to quantify the dimension of a polytope that is easy to work with. Linear spaces are just about the only thing in mathematics that have an obvious definition of their dimension, which is the size of a basis. The following lemma says that each affine space is uniquely associated to a linear space. We will then define the dimension of an affine space to be the dimension of the associated linear space. Then, with this at our disposal, we will define the dimension of a polytope to be the dimension of its affine hull. Given two subsets $S_1, S_2 \subseteq \mathbb{R}^d$, the ***(Minkowski) sum*** of S_1 and S_2, denoted $S_1 + S_2$, is defined to be

$$S_1 + S_2 := \{x + y : x \in S_1, y \in S_2\}.$$

Lemma 1.1: *Let $A \subseteq \mathbb{R}^d$ be an affine subspace. Then there exists a unique linear subspace $L \subseteq \mathbb{R}^d$ such that $A = L + \{b\}$ where b is an arbitrary element of A.*

Proof. Let $b \in A$ and define $L := A + \{-b\}$. We must show that L is indeed a linear subspace and that it does not depend on our choice of b. Indeed, let $x_1, x_2 \in A$ so that $x_1 - b$ and $x_2 - b$ are arbitrary elements of L. Their sum is $(x_1 + x_2 - b) - b$, which is also an element of L as $x_1 + x_2 - b$ is an affine combination of elements in A and is therefore in A itself. Now, let $x \in A$ and $t \in R$. Then $t(x - b) = tx + (1-t)b - b$ which is in L since $tx + (1-t)b \in A$. Our choice of L does not depend on b since $x - c \in L$ for any $c \in A$ since $x - c = (x - c + b) - b$ and $x - c + b \in A$. $\square$

The ***dimension*** of an affine subspace $A \subseteq \mathbb{R}^d$ is the size of a basis of the linear space $\{x - b \in \mathbb{R}^d : x \in A\}$ where $b \in A$. We denote this by $\dim(A)$. The dimension of a convex set $C \subseteq \mathbb{R}^d$ is $\dim(\operatorname{Aff}(C))$. Two convex sets $P \in \mathbb{R}^d$ and $Q \in \mathbb{R}^e$ are ***affinely isomorphic*** if there exists an affine function $f : \mathbb{R}^d \to \mathbb{R}^e$ that is a bijection between P and Q. The polytopes in Figure 1.1.2 suggest that the notion of affine isomorphism is too strong for combinatorics since all three polytopes are, in a sense that we will make precise soon, "combinatorially equivalent" in the sense that they both have four edges and four vertices.

2. The relative boundary of a convex set

The interesting combinatorics of a convex set happens on its relative boundary, a topological notion we will recall soon. In particular, the relative boundary of a convex set is made up of lower-dimensional convex sets, called *faces*, that form a partially ordered set under inclusion. Since we are focusing on relative boundaries, we will often restrict our consideration to closed convex sets.

FIGURE 1.1.2. The first two polytopes are affinely isomorphic to each other, but not to the third. This is because affine functions preserve parallel lines and the first two have two sets of parallel lines, but the last one has none.

We now recall the relevant topological notions. Let $S \subseteq \mathbb{R}^d$ be a set. We say that S is ***closed*** if it is closed under taking convergent sequences, i.e. if $x_1, x_2, \dots \in S$ and $x_n \to x$, then $x \in S$. We say that S is ***open*** if $\mathbb{R}^d \setminus S$ is closed, or equivalently, if S is a union of open balls. The ***interior*** of S is the union of all open sets contained in S and the ***closure*** of S is the intersection of all closed sets containing S. The ***boundary*** of S is the relative complement of the interior of S in the closure of S. The ***relative interior*** (resp. closure, boundary) of a convex set $C \subseteq \mathbb{R}^d$ is the interior (resp. closure, boundary) of C in the induced topology on $\mathrm{Aff}(C)$.

Definition 1.2: Let $C \subseteq \mathbb{R}^d$ be closed and convex. A subset $F \subseteq C$ is a ***face*** of C if

(1) F is closed,
(2) F is convex, and
(3) given $x, y \in C$, if $\mathrm{ri}(\mathrm{Conv}(x, y)) \cap F \neq \emptyset$, then $x, y \in F$.

A face is called an ***extreme point*** if it has dimension 0, an ***edge*** if it has dimension 1 (or sometimes, in the case of cones, an extreme ray), and a ***facet*** if it has dimension $\dim(C) - 1$. A face is ***proper*** if it is neither C nor $\emptyset$.

Example 1.3: Every boundary point on a ball in $\mathbb{R}^d$ is an extreme point and these are the only proper faces. The set of proper faces of a polygon consists of its edges and vertices. An affine space has no proper faces. The only proper face of the halfspace $\{x \in \mathbb{R}^d : ax \geq c\}$ is its boundary hyperplane, namely $\{x \in \mathbb{R}^d : ax = c\}$.

Lemma 1.4: *Let $C \subseteq \mathbb{R}^d$ be convex of dimension at least 1. Then $\mathrm{ri}(C)$ is nonempty.*

PROOF. Let k denote the dimension of C and let $x_1, \dots, x_{k+1}$ affinely span $\mathrm{Aff}(C)$. Consider the function $f : \Delta_k \to C$ given by

$$\sum_{i=1}^{k+1} t_i e_i \mapsto \sum_{i=1}^{k+1} t_i x_i.$$

Then f is continuous and injective. Since Δ_k is compact, $f(\Delta_k)$ is homeomorphic to Δ_k [1, Theorem 26.6]. Since $\frac{1}{k}\sum_{i=1}^{k+1} e_i \in \mathrm{ri}(\Delta_k)$, $f(\Delta_k)$, and therefore C, has nonempty relative interior. □

Proposition 1.5: *If $C \subseteq \mathbb{R}^d$ is closed and convex and $F \subset C$ is a proper face, then $F \subseteq \mathrm{rb}(C)$.*

PROOF. Let $y \in F$ and let $x \in C \setminus F$. For $n = 1, 2, \dots$, define

$$S_n := \{ty + (1-t)x : 0 \leq t \leq 1 + 1/n\}.$$

Since F is a face of C and S_n is a line segment whose interior intersects F, there exists a point $y_n \in S_n \setminus C$. Then, $y_n \to y$ as $n \to \infty$. But this implies $y \in \mathrm{rb}(C)$ because $y_n \in \mathrm{Aff}(C)$ as $S_n \subseteq \mathrm{Aff}(C)$. □

Proposition 1.6: *Let $C \subseteq \mathbb{R}^d$ be closed and convex. If F is a proper face of C, then $\dim(F) < \dim(C)$.*

PROOF. Since $F \subseteq C$, $\dim(F) \leq \dim(C)$. Assume for the sake of contradiction that $\dim(F) = \dim(C)$. Since $\mathrm{Aff}(F) \subseteq \mathrm{Aff}(C)$, this implies that $\mathrm{Aff}(F) = \mathrm{Aff}(C)$. Passing to this affine hull if necessary, we may assume without loss of generality that $\dim(C) = d$. Since $\dim(F) = d$, Lemma 1.4 implies that $\mathrm{ri}(F)$ is a nonempty open subset of $\mathbb{R}^d$. Therefore $\mathrm{ri}(F) \subseteq \mathrm{ri}(C)$ implies $\mathrm{ri}(F) \subseteq \mathrm{ri}(C)$. But this contradicts Lemma 1.5. □

Proposition 1.7: *Let C be closed and convex and let $F \subseteq C$ be a face. Then:*

(1) *every face of F is a face of C, and*
(2) *every face of C contained in F is a face of C.*

PROOF. Let F' be a face of F. Let $x, y \in C$ be such that $\mathrm{ri}(\mathrm{Conv}(x, y)) \cap F' \neq \emptyset$. Then $x, y \in F$ since F is a face of C. This implies $x, y \in F'$ as F' is a face of F. So F' is a face of C.

Now let F' be a face of C contained in F. Let $x, y \in F$ with $F' \cap \mathrm{ri}(\mathrm{Conv}(x, y)) \neq \emptyset$. Since F' is a face of C, this implies $x, y \in F'$. So F' is a face of C. □

Lemma 1.8: *Let $C \subseteq \mathbb{R}^d$ be closed and convex, let $a \in (\mathbb{R}^d)^*$, let $c \in \mathbb{R}$, and assume $ax \leq c$ for all $x \in C$. The set*

$$F_{a,c} := \{x \in C : ax = c\}$$

is a face of C.

PROOF. Let $x, y \in C$ and assume that there exists $z \in F_{a,c} \cap \mathrm{ri}(\mathrm{Conv}(x, y))$. Let $t \in [0, 1]$ such that $z = tx + (1 - t)y$. Then

$$c = az = tax + (1 - t)ay.$$

Since $ax \geq c$ and $ay \geq c$, this implies $ax = ay = c$, i.e. that $x, y \in F_{a,c}$. □

A face F of a closed convex set $C \subseteq \mathbb{R}^d$ is called ***exposed*** if $F = F_{a,c}$ as in Lemma 1.8. The geometric interpretation of an exposed face is as follows. If $ax \leq c$ for all $x \in C$, then the hyperplane $\{x \in \mathbb{R}^d : ax = c\}$ lies tangent to C. The intersection of this hyperplane with C is the face $F_{a,c}$. A convex set may have faces that are not exposed - see Figure 1.2.3, for example. That said, we will eventually see that all faces of a polytope are exposed so we will not spend much time talking about non-exposed faces.

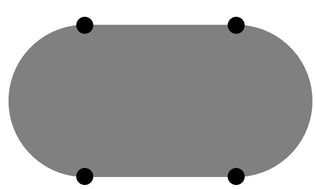


FIGURE 1.2.3. All of the faces of the above convex set $C \subset \mathbb{R}^2$ are exposed, aside from the four extreme points indicated by black dots. To see this, note that the tangent line to C at any one of these points will intersect along the entire edge that it lies on.

We now come to the first big theorem in convexity theory: the hyperplane separation theorem. There are various similar theorems that go by the same name and we will stick with the one that has the exact level of generality we need. The second homework guides you through a proof of this theorem. A proof will be added to these notes after that assignment is turned in.

Theorem 1.9 (Hyperplane separation theorem)**:** *Given a convex $C \subset \mathbb{R}^n$ and a point $y \in \mathbb{R}^d \backslash C$, there exists $a \in (\mathbb{R}^n)^*$ and $b \in \mathbb{R}$ such that $ax \leq b$ for all $x \in C$ and $ay \geq b$.*

The geometric content of Theorem 1.9 is as follows: given a convex set $C \subseteq \mathbb{R}^d$ and a point $y \notin C$, there exists a hyperplane H containing C in one of its two half-spaces and y in the other. When $y \notin \mathrm{rb}(C)$, H can be chosen so that neither C nor $\{y\}$ intersects H, and C and y lie on opposite sides of this hyperplane. When $y \in \mathrm{rb}(C)$, H will contain y and be tangent to C. The hyperplane separation theorem allows us to close an important circle of ideas that will allow us to move away from topological considerations. In particular, we have the following theorem.

Theorem 1.10: *Let $C \subseteq \mathbb{R}^d$ be closed and convex. Then $\mathrm{rb}(C)$ is the union of its proper faces.*

Proof. Proposition 1.5 implies that the union of the proper faces of C is contained in $\mathrm{rb}(C)$. It therefore suffices to let $x \in \mathrm{rb}(C)$ and find a proper face of C containing x. By restricting to $\mathrm{Aff}(C)$ if necessary, we may assume that $\dim(C) = d$. Since $\mathrm{ri}(C)$ is convex, Theorem 1.9 implies that there exists $a \in (\mathbb{R}^d)^*$ and $c \in \mathbb{R}$ such that $ax = c$ and $ay \leq c$ for all $y \in C$. Lemma 1.8 implies that $F_{a,c} := \{y \in C : ay = c\}$ is a face of C and it is clear that this contains x. The dimension of $F_{a,c}$ is at most $d-1$ and since $\dim(C) = d$ and $F_{a,c} \neq \emptyset$, $F_{a,c}$ is proper. □

The following theorem is often known as the Minkowski-Carathéodory theorem.

Theorem 1.11: *Let $C \subset \mathbb{R}^d$ be a compact, convex set of dimension k. Then for each $x \in C$, there exist extreme points $x_1, \ldots, x_{k+1}$, not necessarily distinct, such that $x \in \mathrm{Conv}(x_1, \ldots, x_{k+1})$. Moreover, one such x_i may be chosen arbitrarily.*

Proof. We induct on k. When $k = 0$, C is a single point and the theorem follows. Now assume $k \geq 1$ and let $x \in C$. If $x \in \mathrm{rb}(C)$, then Theorem 1.10 implies that there exists a face F such that $x \in F$. Proposition 1.6 implies that $\dim(F) < k$ so we are done by induction.

Now suppose $x \in \mathrm{ri}(C)$ and let x_{k+1} be an extreme point of C. Compactness of C implies that $\mathrm{Aff}\{x, x_{k+1}\} \cap C = \mathrm{Conv}\{x_{k+1}, y\}$ where $y \in \mathrm{rb}(C)$. Theorem 1.10 implies that there exists a face F of C with $y \in F$ and Proposition 1.6 implies that $\dim(F) < k$. Since $x \in \mathrm{ri}(C)$, the definition of a face implies that $x_{k+1} \notin F$. The inductive hypothesis implies that $y \in \mathrm{Conv}\{x_1, \ldots, x_k\}$ for extreme points $x_1, \ldots, x_k$ of F. Proposition 1.7 implies that $x_1, \ldots, x_k$ are also extreme points of C. Since $x \in \mathrm{Conv}\{x_{k+1}, y\}$ and $y \in \mathrm{Conv}\{x_1, \ldots, x_k\}$, we have that $x \in \mathrm{Conv}\{x_1, \ldots, x_{k+1}\}$. □

3. Duality and the main theorem of polytopes

The goal of this section is to prove the main theorem of polytopes, i.e. that H-polytopes are V-polytopes and vice-versa. We will do this by first showing that every H-polytope is a V-polytope. Once we have this, we will will introduce convex duality which will enable us to prove the other direction.

Each hyperplane $H \subseteq \mathbb{R}^d$ defines two halfspaces which we will denote H^+ and H^-. There is a choice to be made as to which halfspace is which, but when H is given explicitly as

$$H := \{x \in \mathbb{R}^d : ax = c\},$$

we define

$$H^+ := \{x \in \mathbb{R}^d : ax \leq c\} \qquad \text{and} \qquad \{x \in \mathbb{R}^d : ax \geq c\}.$$

Using this notation, each H-polytope can be written as

$$\bigcap_{i=1}^{n} H_i^+ \tag{1}$$

for hyperplanes $H_1, \ldots, H_n \subset \mathbb{R}^d$. The following lemma characterizes the extreme points of an H-polytope.

Lemma 1.12: *Let P be an H-polytope as in* (1)*, let $x \in P$, and define*

$$I := \{i \in \{1, \ldots, n\} : x \in H_i\}.$$

Then x is an extreme point of P if and only if

$$\{x\} = \bigcap_{i \in I} H_i. \tag{2}$$

Proof. Let $a_1, \ldots, a_n \in (\mathbb{R}^d)^*$ and $c_1, \ldots, c_n \in \mathbb{R}$ such that $H_i^+ = \{a_i x \leq c_i\}$. Assume (2). Let $y, z \in \mathbb{R}^d$ with $y, z \neq x$ and $y \in P$ such that $x \in \operatorname{ri}(\operatorname{Conv}(y, z))$. By our hypothesis, there exists $i \in I$ such that $a_i y < c_i$. Since $a_i x = c_i$ and $x \in \operatorname{ri}(\operatorname{Conv}(y, z))$, it follows that $a_i z > c_i$ so $z \notin P$.

Now assume (2) fails and define $A := \bigcap_{i \in I} H_i$. Then $P \cap A$ is an H-polytope in A which we can write as $P \cap A = \{y \in A : a_i y \leq c_i \text{ for all } i \notin I\}$. We claim that $P \cap A$ is at least one-dimensional. Indeed, $P \cap A$ has the same dimension as A (which is at least one) since otherwise $P \cap A$ would lie in a hyperplane of A and so there would be some $i \notin I$ such that $a_i y = c_i$ for all $y \in P \cap A$. But $x \in P \cap A$, so this would imply $i \in I$, a contradiction. Since $a_i x < c_i$ for all $i \notin I$, $x \in \operatorname{ri}(P \cap A)$. Therefore, there exist $y, z \in P \cap A$ such that $x \in \operatorname{ri}(\operatorname{Conv}(y, z))$. This implies that x is not an extreme point of P. $\square$

Corollary 1.13: *Every H-polytope is a V-polytope.*

Proof. Let P be an H-polytope. Lemma 1.12 implies that P has finitely many extreme points $x_1, \ldots, x_k$. Theorem 1.11 then implies that $P = \operatorname{Conv}\{x_1, \ldots, x_k\}$. $\square$

We now develop the theory of convex duality. This will enable us to use Corollary 1.13 in order to prove its converse.

Definition 1.14: Let $C \subseteq \mathbb{R}^d$. The ***(polar) dual*** C^* of C is

$$C^* := \{a \in (\mathbb{R}^d)^* : ax \leq 1 \text{ for all } x \in C\}.$$

We pause to note two things about our definition of duality. In particular, C need not be convex, and C^* lives in the dual of the vector space that contains C. Using the natural isomorphism between a vector space and its double dual, we may view C and C^{**} as subsets of the same space.

Theorem 1.15: *Let $C \subseteq \mathbb{R}^d$. Then*

(1) *C^* is closed and convex*
(2) *If $D \subseteq \mathbb{R}^d$ and $C \subseteq D$, then $D^* \subseteq C^*$*
(3) $C \subseteq C^{**}$
(4) $0 \in C^*$

(5) *If* $0 \in \mathrm{ri}(C)$ *then* C^* *is compact.*
(6) *If* $C \subseteq \mathbb{R}^d$ *is convex, compact, and d-dimensional, then* $C^{**} = C$.

Proof. We will prove (6), leaving (1) through (5) as an exercise. We know from (3) that $C \subseteq C^{**}$, so it suffices to show that if $x \notin C$ then $x \notin C^{**}$. Theorem 1.9 implies that there exists $a \in (\mathbb{R}^d)^*$ and $c \in \mathbb{R}$ such that $ay \leq c$ for all $y \in C$ and $ax \geq c$. Since C is closed, we can choose a, c so that $ax > c$. We may also assume that $c \neq 0$, since if $c = 0$, then a, ε satisfy the desired conditions for small $\varepsilon > 0$. Compactness of C implies that the functional a achieves a maximum α on C and since $0 \in C$, we know $\alpha \geq 0$. This implies $c > 0$ and therefore that $\frac{1}{c}ax > 1$. But this shows that $x \notin C^{**}$ since $\frac{1}{c}ay \leq 1$ for all $y \in C$ (i.e. that $a \in C^*$). $\square$

Lemma 1.16: *Let* $P \subset \mathbb{R}^d$ *be a d-dimensional V-polytope with* $0 \in \mathrm{ri}(P)$. *Then* P^* *is a d-dimensional H-polytope and* $0 \in \mathrm{ri}(P^*)$.

Proof. We already know from Theorem 1.15 that P^* is compact so it suffices to show that P^* is an intersection of finitely many half-spaces and that $0 \in \mathrm{ri}(P^*)$. Assume $P = \mathrm{Conv}\{v_1, \ldots, v_k\}$. If $a \in P^*$ then $av_i \leq 1$ for $i = 1, \ldots, k$. Conversely, if $av_i \leq 1$ for all i and $x \in P$, then since $x = \sum_{i=1}^k t_i v_i$ with $\sum_{i=1}^k t_i = 1$, we have

$$ax = \sum_{i=1}^{k} t_i a v_i \leq \sum_{i=1}^{k} t_i = 1$$

and therefore $a \in P^*$.

Now we argue that P^* is full-dimensional with 0 in its interior. The inequalities $av_i \leq 1$ are satisfied strictly for $a = 0$ and therefore for all a in a small open neighborhood of 0. Thus 0 is in the interior of P^*. Since P^* has a nonempty (non-relative) interior, P^* is full-dimensional. $\square$

Theorem 1.17 (Main theorem of polytopes)**:** *Every H-polytope is a V-polytope and vice versa.*

Proof. In light of Corollary 1.13, it suffices to show that every V-polytope is an H-polytope. Indeed, let $P \subset \mathbb{R}^d$ be a V-polytope. By passing to $\mathrm{Aff}(P)$ and translating if necessary, we may assume that P is full-dimensional and that $0 \in \mathrm{ri}(P)$. Now, Lemma 1.16 and Corollary 1.13 together tell us that P^* is a V-polytope. Applying Lemma 1.16 once more tells us that P^{**} is an H-polytope. Theorem 1.15 then tells us that $P = P^{**}$ so that P is an H-polytope as well. $\square$

Theorem 1.17 has earned its title as the main theorem of polytopes because many fundamental properties of polytopes are easy to prove using one of the two equivalent notions and hard using the other. Consider for example the following proposition, which has a very short proof in light of Theorem 1.17, but would otherwise be much harder if we were stuck with only one of V or H descriptions.

Proposition 1.18: *Let* $P, Q \subseteq \mathbb{R}^d$ *be polytopes. Then* $P + Q$ *and* $P \cap Q$ *are polytopes.*

Proof. Since P and Q are polytopes, we can write $P = \mathrm{Conv}\{v_1, \ldots, v_n\}$ and $Q = \{u_1, \ldots, u_m\}$. We immediately see that $P + Q \supseteq \mathrm{Conv}\{v_i + u_j : i = 1, \ldots, n; j = 1, \ldots m\}$. To see that this containment is not strict, let $x + y \in P + Q$. Then we have

$$x + y = \sum_{i=1}^{n} t_i v_i + \sum_{j=1}^{m} s_j v_j.$$

Since $\sum_{j=1}^m s_j = \sum_{i=1}^n t_i = 1$, we can rewrite the above as

$$\sum_{i=1}^n t_i \left(\sum_{j=1}^m s_j\right) v_i + \sum_{j=1}^m s_j \left(\sum_{i=1}^n t_i\right) u_j = \sum_{i=1}^n \sum_{j=1}^m t_i s_j (v_i + u_j)$$

thus showing equality.

Now we switch to an H-description. We can write

$$P = \bigcap_{i=1}^n H_i^+ \qquad \text{and} \qquad \bigcap_{j=1}^m G_j^+$$

where H_i, G_j are hyperplanes. Then $P \cap Q$ is just

$$P \cap Q = \bigcap_{i=1}^n H_i^+ \cap \bigcap_{j=1}^m G_j^+$$

which represents $P \cap Q$ as an H-polytope. □

4. Exercises

Problem 1: Show that every compact convex set has an extreme point. Give an example of a non-compact convex set with an extreme point.

Problem 2: Prove that $x \in \operatorname{Aff}(x_1, \ldots, x_n)$ if and only if

$$\begin{pmatrix} 1 \\ x \end{pmatrix} \in \mathbb{R} \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \end{pmatrix}$$

and that $x \in \operatorname{Conv}(x_1, \ldots, x_n)$ if and only if

$$\begin{pmatrix} 1 \\ x \end{pmatrix} \in \mathbb{R}_{\geq 0} \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_n \end{pmatrix}$$

Problem 3: Let $X, Y \subseteq \mathbb{R}^d$ with $|X| = |Y| = d+1$. Assume X, Y are each affinely independent sets. Prove that $\operatorname{Conv}(X)$ and $\operatorname{Conv}(Y)$ are affinely isomorphic.

Problem 4: Prove that $p_1, \ldots, p_n \in \mathbb{R}^d$ are affinely independent if and only if there do not exist $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$, not all zero, such that

$$\sum_{i=1}^n \lambda_i p_i = 0 \qquad \text{and} \qquad \sum_{i=1}^n \lambda_i = 0.$$

Problem 5: Let $P, Q \subset \mathbb{R}^2$ be two-dimensional polytopes (i.e. polygons). For each of the following statements, either prove that they are true, or provide a counterexample.

(1) If P and Q have the same number of edges, then they are affinely isomorphic.
(2) If P and Q have the same number of edges, then they are combinatorially isomorphic.
(3) If P and Q are both triangles, then they are affinely isomorphic.
(4) If P is a square and Q is a parallelogram, then P and Q are affinely isomorphic. Begin by convincing yourself that it makes no difference if you assume that the vertices of P are $\{0,1\}^2$ and that $(0,0)$ is a vertex of Q.

Problem 6: Prove that $\dim(\mathrm{Conv}\{v_1, \ldots, v_n\}) = \mathrm{rank}(\hat{V}) - 1$ where

$$\hat{V} = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ v_1 & v_2 & \ldots & v_n \end{pmatrix}$$

Problem 7: Prove the unproven parts of Theorem 1.15.

Problem 8: Let $P, Q \subseteq \mathbb{R}^d$ be convex sets. Prove that $(P + Q)^* = P^* \cap Q^*$.

Problem 9: Prove that the standard cube is indeed dual to the standard cross-polytope, as the notation suggests.

CHAPTER 2

The face lattice

1. Preliminaries on partially ordered sets

A ***partially ordered set***, or ***poset***, is a pair $(S, \leq)$ consisting of a set S and relation $\leq$ on S satisfying the following properties:

(1) Reflexivity: let $x \in S$. Then $x \leq x$.
(2) Transitivity: let $x, y, z \in S$ such that $x \leq y$ and $y \leq z$. Then $x \leq z$.
(3) Anti-symmetry: let $x, y \in S$. If $x \leq y$ and $y \leq x$, then $x = y$.

Given a poset $(S, \leq)$ and $x, y \in S$, we use the notation $x < y$ to mean $x \leq y$ and $x \neq y$. Two posets $(S_1, \leq_1)$ and $(S_2, \leq_2)$ are ***isomorphic*** if there exists a bijection $\phi : S_1 \to S_2$ such that for all $x, y \in S_1$, $x \leq_1 y$ if and only if $\phi(x) \leq_2 \phi(y)$. If $x < y$ and $x \leq z \leq y$ implies $z = x$ or $z = y$, then we say that x ***covers*** y and denote this by $x \lessdot y$. A partial order satisfying the additional proper that $x \leq y$ or $y \leq x$ for all $x, y \in S$ is called a ***total order***. When S is finite, we can represent $(S, \leq)$ using an ***order diagram***. This is a directed graph G whose vertices correspond to elements of S and has an arc $x \to y$ whenever $x \lessdot y$. When drawing an order diagram, the convention is to draw things so that all arcs are oriented up, and then not put arrows on the edges.

Example 2.1: The subsets of $\{1, 2, \ldots, n\}$ form a partially ordered set when ordered by inclusion. We denote this poset by B_n and call it a ***boolean lattice***. Given $S, T \subseteq \{1, \ldots, n\}$, $S \lessdot T$ if and only if $S \subseteq T$ with $|T \setminus S| = 1$. The order diagram of B_3 is shown in Figure 2.1.1.

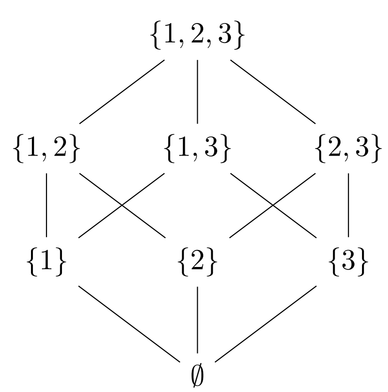


FIGURE 2.1.1. The boolean lattice B_3 is the set of all subsets of $\{1, 2, 3\}$, partially ordered by inclusion. Its order diagram is shown in this figure. This lattice is both atomic and coatomic.

Given a poset $(S, \leq)$ and $x, y, z \in S$, we say that z is an ***upper bound*** of x, y if $z \geq x$ and $z \geq y$ and a ***least upper bound*** if additionally $z \leq w$ for any other upper bound w of x, y.

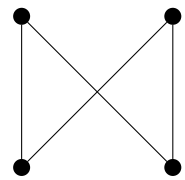


FIGURE 2.1.2. The order diagram of a poset that is not a lattice.

Lower bounds and ***greatest lower bounds*** are defined analogously. Least upper bounds and greatest lower bounds are unique (see Problem 1). If every pair $x, y \in S$ have both a least upper bound and greatest lower bound, then $(S, \leq)$ is called a ***lattice***. Not every poset is a lattice - see Figure 2.1.2.

When $(S, \leq)$ is a lattice, we denote the least upper bound of x, y by $x \vee y$ and call it their ***join***, and the greatest lower bound by $x \wedge y$ and call it the ***meet***. Unsurprisingly, boolean lattices are indeed lattices and the join of two elements is their union and the meet is their intersection. The meet and join operations of any lattice each satisfy an associative law and together satisfy two absorption laws. In fact, these two algebraic axioms are enough to completely characterize lattices - see Problem 4.

Associativity of the meet and join operations allows us to extend them to arbitrary sets. In particular, one can define

$$\bigvee_{i=1}^{n} x_i := x_1 \vee x_2 \vee \cdots \vee x_n \qquad \text{and} \qquad \bigwedge_{i=1}^{n} x_i := x_1 \wedge x_2 \wedge \cdots \wedge x_n$$

for arbitrary finite sets. These operations can also be extended to infinite sets, but we will not encounter any.

An element x of a poset $(S, \leq)$ is called a ***one-hat*** if $x \geq y$ for all $y \in S$ and a ***zero-hat*** if $x \leq y$ for all $y \in S$. We denote these symbolically by $\hat{1}$ and $\hat{0}$ and every finite lattice has one of each (Problem 2). When $(S, \leq)$ has a $\hat{0}$, elements covering $\hat{0}$ are called ***atoms*** and when it has a $\hat{1}$, elements covered by $\hat{1}$ are called ***coatoms***. A lattice is ***atomic*** if every non-$\hat{0}$ element can be expressed as a join of atoms and ***coatomic*** if every non-$\hat{1}$ element can be expressed as a meet of coatoms. Boolean lattices B_n are both atomic and coatomic for all n. Every finite total order is a lattice, but if it has four or more elements, then it is neither atomic nor coatomic.

In the next section, we will define a partially ordered set that one can associate to any convex set, then show that in the case of polytopes, this poset is a lattice that is both atomic and coatomic. The meet operation will be relatively easy to work with, but the join operation less so. For this reason, we will need the following lemma that will enable us to assert the existence of a join operation without having to work with it explicitly.

Lemma 2.2: *Let $(S, \leq)$ be a finite poset with a $\hat{1}$ such that every pair of elements has a greatest lower bound. Then every pair of elements has a least upper bound so $(S, \leq)$ is a lattice.*

PROOF. Let $x, y \in S$ and define T to be the set of all upper bounds of x, y, i.e.

$$T := \{z \in S : z \geq x \text{ and } z \geq y\}.$$

Since $(S, \leq)$ contains a $\hat{1}$, T is nonempty. Since S, and therefore T, is finite and each pair of elements in T contains a greatest lower bound in S, there exist a greatest lower bound $w \in S$ of T. Since x and y are both lower bounds of T, $x \leq w$ and $y \leq w$. In other words $w \in T$, i.e. w

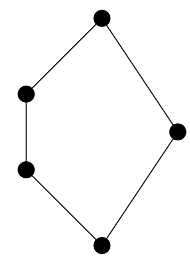


FIGURE 2.2.3. A lattice that is not graded.

is an upper bound of x and y. Since T is the set of all upper bounds of x and y, this implies w is the least upper bound of x and y. $\square$

2. The face lattice of a polytope

For each convex set $C \subseteq \mathbb{R}^d$, we let $\mathcal{F}(C)$ denote the set of all faces of C, partially ordered by inclusion. We call $\mathcal{F}(C)$ the ***face poset of*** C, and when C is a polytope, the ***face lattice of*** C. As we shall soon see, our use of the word "lattice" is justified. Face lattices are a fundamental concept in the study of polytopes because they allow us to rigorously define the notion of combinatorial equivalence of polytopes. In particular, two polytopes are ***combinatorially equivalent*** if they have isomorphic face lattices.

The main goal of this section is to prove Theorem 2.3, a structure theorem for the face lattice of a polytope. In order to do so, we must introduce a few more poset terms. Given a poset $(S, \leq)$ and $x, y \in S$ satisfying $x \leq y$, we define the ***interval between*** x, y to be

$$[x, y] := \{z \in S : x \leq z \leq y\}.$$

The ***opposite*** of a poset $(S, \leq)$, is the poset $(S, \preceq)$ where $x \preceq y$ if and only if $y \leq x$. A finite lattice is ***graded*** if every maximal totally ordered subset has the same cardinality. In a graded lattice $(P, \leq)$, we define the ***rank function*** $r : S \to \mathbb{N}$ of $(P, \leq)$ recursively by

$$r(x) := \begin{cases} 0 & \text{if } x = \hat{0} \\ r(y) + 1 & \text{if } y \lessdot x. \end{cases}$$

This is well-defined because $(S, \leq)$ is graded. The ***rank*** of a graded lattice is the rank of $\hat{1}$. The boolean lattice B_n is graded of rank n and the rank of each $S \subseteq \{1, \ldots, n\}$ is $|S|$. See Figure 2.2.3 for an example of a lattice that is not graded.

Theorem 2.3: *Let $P \subseteq \mathbb{R}^d$ be a k-dimensional polytope. Then:*

(1) *$\mathcal{F}(P)$ is an atomic and coatomic graded lattice of rank $k+1$*
(2) *The rank function of $\mathcal{F}(P)$ is given by $F \mapsto \dim(F) + 1$*
(3) *Given $F, G \in \mathcal{F}(P)$ with $F \subseteq G$, $[F, G]$ is the face lattice of a polytope of dimension $\dim(G) - \dim(F) - 1$*
(4) *The opposite poset of $\mathcal{F}(P)$ is $\mathcal{F}(P^*)$.*

We will break Theorem 2.3 and its proof into several smaller lemmas.

Lemma 2.4: *Let $C \subseteq \mathbb{R}^d$ be convex. For any pair F_1, F_2 of faces of C, $F_1 \cap F_2$ is a face of C.*

Proof. Let F_1, F_2 be faces of C and let $F := F_1 \cap F_2$ Let $x \in F$ and let $y, z \in C$ such that $x \in \mathrm{ri}(\mathrm{Conv}(y, z))$. Since F_1 is a face, this implies $y, z \in F_1$ and similarly for F_2. So $y, z \in F$ and therefore F is a face of C. □

Lemma 2.5: *Each polytope has finitely many faces, each of which is itself a polytope.*

Proof. Let $P \subseteq \mathbb{R}^d$ be a polytope and let $F \subseteq P$ be a face. Proposition 1.7 implies that every extreme point of F is an extreme point of P. Lemma 1.12 implies that P, and therefore F, has only finitely many extreme points. Theorem 1.11 implies that F is the convex hull of these finitely many extreme points, i.e. is a polytope. This argument also shows that the number of faces of P is bounded above by 2^k where k is the number of extreme points of P. In particular, the number of faces of P is finite. □

Proposition 2.6: *Let $P \subseteq \mathbb{R}^d$ be a polytope. Then $\mathcal{F}(P)$ is a finite atomic lattice. Moreover, given $F_1, F_2 \in \mathcal{F}(P)$, $F_1 \wedge F_2 = F_1 \cap F_2$.*

Proof. That $\mathcal{F}(P)$ is a finite lattice with meet operation given by intersection is an immediate consequence of Lemmas 2.4, 2.5, and 2.2, and that $F_1 \cap F_2$ is the maximal face of P contained in both F_1 and F_2.

We now argue that $\mathcal{F}(P)$ is atomic. Since the atoms of $\mathcal{F}(P)$ are the extreme points of P, it suffices to show that each face F of P is the minimal face containing all of its extreme points. Theorem 1.11 implies that F is the convex hull of its extreme points. Since the convex hull of a set S is the minimal convex set containing S, this implies that F is the minimal subset of P containing all of its extreme points. Since F is a face, this implies that F is moreover the minimal face of P with this property.

Since $\mathcal{F}(P)$ is an atomic lattice with finitely many atoms, $\mathcal{F}(P)$ is finite. □

Lemma 2.7: *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional polytope with $0 \in \mathrm{ri}(P)$ so that P^* is a polytope (c.f. Lemma 1.16). For each face F of P, define*

$$F' := \{a \in P^* : ax = 1 \text{ for all } x \in F\}.$$

Then the following hold:

(1) *F' is a face of P^*,*
(2) *the map $F \mapsto F'$ is a bijection, and*
(3) *if F, G are faces of P with $F \subseteq G$, then $G' \subseteq F'$.*

Proof. Let $a, b \in (\mathbb{R}^d)^*$ so that there exists $c \in \mathrm{ri}(\mathrm{Conv}(a, b)) \cap F'$. Assume $a \in P^*$. Then $ax \leq 1$ for all $x \in P$. If $a \notin F'$, then there exists $x \in F$ such that $ax < 1$. But since $cx = 1$ and $c = ta + (1-t)b$ for some $0 \leq t \leq 1$, this would imply $bx > 1$ and therefore that $b \notin P^*$. So F' is a face of P^*.

For the second claim, note that we can apply this construction to the faces of P^*. In particular, $(F')' = F$ and so the map $F \mapsto F'$ is injective. By the same logic, the same map applied to the faces of P^* is injective. Since P and P^* have finitely many faces by Lemma 2.5, this implies that the map $F \mapsto F'$ is a bijection.

The third claim is immediate. □

Corollary 2.8: *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional polytope with $0 \in \mathrm{ri}(P)$. Then $\mathcal{F}(P^*)$ is the opposite poset of $\mathcal{F}(P)$ and so $\mathcal{F}(P)$ is coatomic.*

Lemma 2.9: *Let $P \subseteq \mathbb{R}^d$ be a polytope and let $v \in P$ be an extreme point. Proposition 2.11 implies that there exists $a \in (\mathbb{R}^d)^*$ and $c \in \mathbb{R}$ such that $ax \leq c$ for all $x \in P$ and $\{v\} = \{x \in P : ax = c\}$. Let $c_0 < c$ such that $ax \leq c_0$ for all extreme points of P aside from v. Define*

$$H := \{x \in \mathbb{R}^d : ax = c_0\} \qquad \text{and} \qquad Q := P \cap H.$$

Then $\mathcal{F}(Q)$ is isomorphic to the interval $[v, P]$ in $\mathcal{F}(P)$.

Proof. For each face F of P containing v, define $F' := F \cap H$. We claim that F' is a face of Q. Indeed, Proposition 2.11 implies that there exist $a_1 \in (\mathbb{R}^d)^*$ and $c_1 \in \mathbb{R}$ such that $F = P \cap H_1$ where $H_1 = \{x \in \mathbb{R}^d : a_1 x = c_1\}$ and $a_1 x \leq c_1$ for all $x \in P$ and therefore for all $x \in Q$. Then $H_1 \cap H$ is a hyperplane in H and since $F' = Q \cap (H_1 \cap H)$ we then have that F' is a face of Q.

The map $F \mapsto F'$ is inclusion preserving, so if we show that it is a bijection, then it is the desired poset isomorphism from the interval $[v, P]$ in $\mathcal{F}(P)$ to $\mathcal{F}(Q)$. Given $G \in \mathcal{F}(Q)$, define

$$\hat{G} := P \cap \operatorname{Aff}(G \cup \{v\}).$$

We claim that $\hat{G}$ is a face of P. Indeed, Proposition 2.11 implies that there exist $a_2 \in (\mathbb{R}^d)^*$ and $c_2 \in \mathbb{R}$ such that $G = \{x \in Q : a_2 x = c_2\}$ and $a_2 x \leq c_2$ for all $x \in Q$. Additionally, for all $\lambda \in \mathbb{R}$, the following inequality holds with equality at G

$$(a_2 + \lambda a)x \leq c_2 + \lambda c_0 \qquad \text{for all} \qquad x \in Q. \tag{3}$$

Define $\lambda_0 := (c_2 - a_2 v)/(c - c_0)$. The inequality in (3) becomes an equality at $x = v$ when we set $\lambda = \lambda_0$. Given an extreme point $v' \neq v$ of $P \cap \operatorname{Aff}(G \cup \{v\})$ then $av' < c_0$ and $av = c > c_0$ so

$$v'' := \frac{(av - c_0)v' + (c_0 - av')v}{av - av'} \in P \cap H = Q.$$

Therefore, we have $(a_2 + \lambda_0 a)v'' \leq c_2 + \lambda_0 c_0$. Since (3) is an equality at v when $\lambda = \lambda_0$, this implies $(a_2 + \lambda_0 a)v' = c_2 + \lambda_0 c_0$. Thus setting $\lambda = \lambda_0$ makes (3) hold for all extreme points of P and therefore for all of P. Thus $\operatorname{Aff}(G \cup \{v\}) \cap P = \{x \in P : (a_2 + \lambda_0 a)x \leq c_2 + \lambda_0 c_0\}$ is indeed a face of P.

The proof is now complete by noting that the map $G \mapsto \hat{G}$ is the inverse of $F \mapsto F'$. $\square$

Proposition 2.10: *Let $P \subseteq \mathbb{R}^d$ be a polytope. Then*

1. *given $F, G \in \mathcal{F}(P)$ with $F \leq G$, the interval $[F, G]$ is isomorphic to a face lattice of a polytope of dimension $\dim(G) - \dim(F) - 1$, and*
2. *$\mathcal{F}(P)$ is graded with rank function $r(F) = \dim(F) + 1$.*

Proof. Given any face G of P, it follows from Proposition 1.7 and Lemma 2.5 that the interval $[\emptyset, G]$ is isomorphic to $\mathcal{F}(G)$. So to prove the first claim, it now suffices to show that the interval $[F, P]$ of $\mathcal{F}(P)$ is isomorphic to the face lattice of a polytope for any face F of P. This is clearly true for $F = \emptyset$ or when $\dim(P) = -1$, i.e. when $P = \emptyset$. Let v be any vertex of P. Then $[v, P]$ is the face lattice of a polytope by Lemma 2.9. Therefore, so is $[F, P]$ for any face F of P by induction on $\dim(P)$.

Now, let $\emptyset = F_{-1} \subsetneq F_0 \subsetneq \cdots \subsetneq F_k = P$ be a maximal totally ordered subset of $\mathcal{F}(P)$. The second claim now follows by induction on dimension since $[F_0, P]$ is the face lattice of a poset of dimension $\dim(P) - 1$. $\square$

With Proposition 2.10, we have now finished the proof of Theorem 2.3. We end this section with an important implication.

Proposition 2.11: *Every face of a polytope is exposed.*

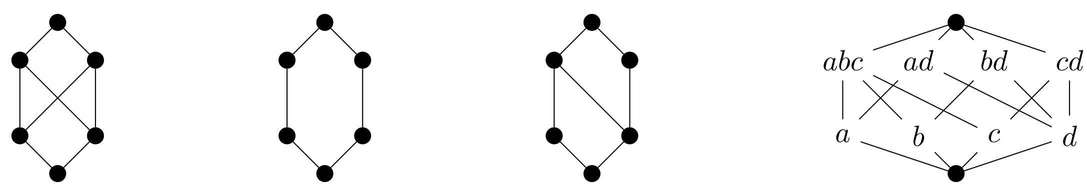
Proof. Let $P \subseteq \mathbb{R}^d$ be a polytope and let F be a face. Since the face lattice of a polytope is coatomic with facets as the coatoms (c.f. Theorem 2.3), there exist facets $F_1, \ldots, F_k$ such that $F = F_1 \cap \cdots \cap F_k$. Let $a_1, \ldots, a_k \in (\mathbb{R}^d)^*$ and $b_1, \ldots, b_k \in \mathbb{R}$ such that $a_i x \leq b_i$ holds for all $x \in P$ and $F_i = \{x \in P : a_i x = b_i\}$. Then whenever $x \in P$, we have $(a_1 + \cdots + a_k)x \leq b_1 + \ldots b_k$. Moreover $F = \{x \in P_i : (a_1 + \cdots + a_k)x = b_1 + \ldots b_k\}$ and therefore F is an exposed face. $\square$

3. Exercises

Problem 1: Show that least upper bounds and greatest lower bounds in a poset are unique.

Problem 2: Prove that every finite lattice has a $\hat{0}$ and $\hat{1}$.

Problem 3: For each of the following posets, determine which are lattices. Among those that are, determine which are atomic and/or coatomic.



Problem 4: An ***algebraic lattice*** consists of a set S and two binary operations $\vee$ and $\wedge$ satisfying the following two axioms:

(1) $x \vee (y \vee z) = (x \vee y) \vee z$ and $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ for all $x, y, z \in S$ (associativity)
(2) $x \vee (x \wedge y) = x$ and $x \wedge (x \vee y)$ for all $x, y \in S$ (absorption).

Show that if $(S, \leq)$ is a lattice with join and meet operations $\vee$ and $\wedge$, then $(S, \vee, \wedge)$ is an algebraic lattice. Then, show that if $(S, \vee, \wedge)$ is an algebraic lattice, then there exists a partial order $\leq$ on S that is a lattice with meet and join operations $\vee$ and $\wedge$.

Problem 5: Define a partial order $\prec$ on $\mathbb{N}$ by $x \prec y$ if and only if for all primes p, if p^n divides x, then p^n divides y.

(1) Show that $(\mathbb{N}, \prec)$ is a lattice.
(2) Does $(\mathbb{N}, \prec)$ have a $\hat{0}$ and/or a $\hat{1}$? If applicable, determine its atoms/coatoms.
(3) Is $(\mathbb{N}, \prec)$ atomic and/or coatomic?
(4) Show that $(\mathbb{N}, \prec)$ is isomorphic to the poset $(S, \subseteq)$ where S is the set of all finite multisets with elements in $\mathbb{N}$, partially ordered by inclusion.

CHAPTER 3

Graphs of polytopes

1. General polytopes

Lemma 3.1: *Let $P \subseteq \mathbb{R}^d$ be a polytope. Then*

(1) *the set of points in P maximizing a linear functional $a \in (\mathbb{R}^d)^*$ is a face of P, and*
(2) *for every proper face F of P, there exists a linear functional maximized exactly at F.*

Proof. Since P is compact, we can define $c := \max_{x \in P} ax$. Then $ax \leq c$ for all $x \in P$ so $P \cap \{x \in \mathbb{R}^d : ax = c\}$ is a face of P and this is precisely where a is maximized. The second claim is a restatement of the fact that all faces of a polytope are exposed (c.f. Proposition 2.11). $\square$

Given a polytope $P \subseteq \mathbb{R}^d$, the ***graph of*** P is the graph $G(P)$ whose vertices are the extreme points of P that has an edge between vertices u and v if and only if $\mathrm{Conv}(u, v)$ is a face of P. Given a linear functional $a \in (\mathbb{R}^d)^*$, define $G_a(P)$ to be the partially directed graph obtained from $G(P)$ directing an edge between u and v from u to v whenever $au < av$.

Lemma 3.2: *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional polytope and let v be an extreme point of P. Then there exist neighbors $u_1, \ldots, u_d$ of v in $G(P)$ that are affinely independent.*

Proof. Let N denote the set of neighbors of v in $G(P)$ and assume for the sake of contradiction that $\dim(\mathrm{Aff}(N)) \leq d-2$. Then $\dim(\mathrm{Aff}(N \cup \{v\})) \leq d-1$. Let Q be as in Lemma 2.9. Since Q lies in the intersection of $\mathrm{Aff}(N \cup \{v\})$ and a hyperplane H not containing v, this implies that $\dim(Q) \leq d-2$. But Lemma 2.9 and Theorem 2.3 together imply $\dim(Q) = d-1$. $\square$

Theorem 3.3: *Let $P \subseteq \mathbb{R}^d$ be a d-dimensional polytope and let $a \in (\mathbb{R}^d)^*$ not equal to zero. Let G be the graph of P with edges directed according to increasing a. Let F be the face of P where a is maximized and let v be an extreme point of P not in F. Then there exists a directed path in G from v to a point in F.*

Proof. Let v be an extreme point of P and let $u_1, \ldots, u_k$ be the neighbors of v in G. Since P is d-dimensional $k \geq d$. If none of the edges vu_i are directed towards u_i, then $av \geq au_i$ for each i. If v is not in F, then there exists a vertex w of P such that $av < aw$. For each $t \in (0, 1]$, the point $v_t := (1-t)v + tw$ satisfies $av < av_t$. But there must exist some v_t in the hyperplane spanned by some d-subset of v's neighbors. This gives a contradiction. $\square$

Theorem 3.4 (Balinski 1961)**:** *Let G be the graph of a d-dimensional polytope. Then G is d-connected.*

Proof. Let P be a polytope. Since the graph of P is invariant under affine isomorphism, we may assume that P is full-dimensional. Let $v_1, \ldots, v_{d-1}$ be vertices of G, i.e. extreme points of P. We consider two cases.

Case 1: There exists a proper face F of P containing $v_1, \ldots, v_{d-1}$. By Lemma 3.1, there exists $a \in (\mathbb{R}^d)^*$ maximized at F. Direct the edges of G according to $-a$ and let F' be the face of P where $-a$ is maximized. Let u, w be vertices of G. The simplex algorithm gives us directed paths from u to u' and w to w' where u' and w' lie in F'. Since they move in the direction of increasing $-a$, i.e. decreasing a, these paths will not contain $v_1, \ldots, v_{d-1}$. By induction on dimension, there exists a path in F' from u' to w' and since $v_1, \ldots, v_{d-1}$ are not in F', this path also does not contain any of these vertices. Thus the graph $G \setminus \{v_1, \ldots, v_{d-1}\}$ is connected.

Case 2: There is no proper face of P containing $v_1, \ldots, v_{d-1}$. Fix an extreme point v_0 of P, distinct from $v_1, \ldots, v_{d-1}$. Then there exists a hyperplane $H = \{x \in \mathbb{R}^d : ax = c\}$ containing $v_0, \ldots, v_{d-1}$. Let F, F' be the faces of P that respectively maximize and minimize a. Since F, F' are proper faces of P, the cardinality of $F \cap \{v_1, \ldots, v_{d-1}\}$ and $F' \cap \{v_1, \ldots, v_{d-1}\}$ are at most $d-2$. By induction on dimension, the graphs of F and F' are both connected even after removing $v_1, \ldots, v_{d-1}$. Given a vertex $v \neq v_i$ for all $i = 0, \ldots, d-1$, if $av \geq c$ then the simplex algorithm applied to $-a$ gives us a path from v to F', and if $av \leq c$ then the simplex algorithm applied to a gives us a path from v to F'. Finally, we the simplex algorithm also gives us paths from v_0 to both F and F'. □

2. Graphs of three-dimensional polytopes

Definition 3.5: A graph G is planar if it can be embedded as a topological space into $\mathbb{R}^2$. Stated simply, it means that you can draw it without crossing edges.

Proposition 3.6: *Let P be a three-dimensional polytope. Then $G(P)$ is planar, three-connected, and simple.*

PROOF. Let P be a three-dimensional polytope. Three-connectedness of $G(P)$ follows from Theorem 3.4. Simplicity of $G(P)$ follows from Theorem 2.3. We now prove that $G(P)$ is planar. Let $S \subseteq \mathrm{Aff}(P)$ be a 2-sphere around P. Project the vertices and edges of P radially to S. This gives an embedding of $G(P)$ onto S. Let $p \in S$ be a point not on this graph. Since a punctured sphere is homeomorphic to a plane, this means that $G(P)$ can be embedded in the plane, i.e. is planar. □

The converse of Proposition 3.6 is also true. For a proof, see [2, Chapter 4].

CHAPTER 4

Matroids

1. Basic definitions

Definition 4.1: A matroid $\mathcal{M}$ consists of a finite set E, called the ***ground set***, and a collection $\mathcal{I}$ of subsets of E, called ***independent sets*** satisyfing the following three axioms:

(1) the empty set is independent, i.e. $\emptyset \in \mathcal{I}$,
(2) subsets of independent sets are independent, i.e. if $I \in \mathcal{I}$ and $J \subset I$ then $J \in \mathcal{I}$, and
(3) if $I, J \in \mathcal{I}$ such that $|I| < |J|$, then there exists $e \in J \setminus I$ such that $I \cup \{e\} \in \mathcal{I}$.

The ***bases of*** $\mathcal{M}$ are the maximal independent sets, the ***spanning sets of*** $\mathcal{M}$ are the subsets of E that contain a basis. The ***dependent sets of*** $\mathcal{M}$ are the subsets of E that are not independent and the ***circuits of*** M are the inclusion-minimal dependent sets.

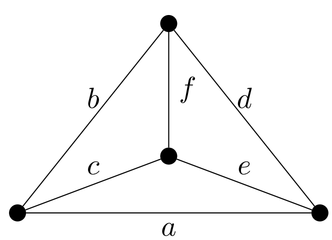
Definition 4.2: Let A be a matrix whose columns are indexed by a set E. The matroid associated to A, denoted $\mathcal{M}(A)$, is $(E, \mathcal{I})$ where $S \subseteq E$ is in $\mathcal{I}$ if and only if the submatrix of A obtained by restricting to the columns indexed by S has linearly independent columns.

What are the circuits of $\mathcal{M}(A)$ in general?

Here's an example. Let A be the following matrix over any field, with columns a, b, c, d, e, f.

$$\begin{array}{cc} & \begin{array}{cccccc} a & b & c & d & e & f \end{array} \\ A := & \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ -1 & 0 & 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & -1 & 0 & 1 \end{pmatrix} \end{array}$$

There are 16 bases, including e.g. $\{a, b, c\}$ There are 7 circuits including e.g. $\{a, b, d\}$. In fact, there is a very natural bijection between the columns of this matrix, and the six edges of the complete graph on 4 vertices. In particular, this bijection is given by the edge labeling as follows:



Under this bijection, bases correspond to spanning trees and circuits correspond to cycles.

Definition 4.3: Let G be a graph with edge set E. The matroid associated to G, denoted $\mathcal{M}(G)$, is the matroid on ground set E whose circuits are the simple cycles of G.

Proposition 4.4: *Let A be a matrix with entries in a field $\mathbb{F}$. Then $\mathcal{M}(A)$ is a matroid.*

PROOF. The hard part is to prove that $\mathcal{M}(A)$ satisfies the third axiom. Let I, J be independent subsets of columns of A so that $|I| < |J|$. If $I \cup \{e\}$ were dependent for all $e \in J$, then the linear span of I and $I \cup J$ would be the same. Thus the linear span of J would have dimension at most $|I|$. But J is linearly independent, so its linear span has dimension $|J| > |I|$, a contradiction. $\square$

Definition 4.5: Let $\mathbb{F}$ be a field and let M be a matroid. We say that M is ***representable over*** $\mathbb{F}$ means that there exists a matrix A with entries in $\mathbb{F}$ such that $M = \mathcal{M}(A)$. We say that M is graphic if there exists a graph G such that $M = \mathcal{M}(G)$.

Given a field $\mathbb{F}$ and a finite set E, we let $\mathbb{F}^E$ denote a vector space with a choice of basis that is in bijection with E. Given another finite set V, we let $\mathbb{F}^{V\times E}$ denote the set of matrices whose rows are indexed by V and whose columns are indexed by E.

Proposition 4.6: *Let G be a graph. Then $\mathcal{M}(G)$ is representable over every field.*

PROOF. Let V and E denote the vertex and edge set of G and let $\mathbb{F}$ be a field. Fix an orientation on the edges of G and let A denote its directed incidence matrix over $\mathbb{F}$. In other words, $A \in \mathbb{F}^{V\times E}$ is the matrix whose v, e entry is given over $\mathbb{F}$ as follows

$$a_{v,e} := \begin{cases} 0 & \text{if } e \text{ is a loop or is not incident to } v \\ 1 & \text{if } e \text{ is incident to } v \text{ and directed towards } v \\ -1 & \text{if } e \text{ is incident to } v \text{ and directed away from } v. \end{cases}$$

We now show that $\mathcal{M}(A) = \mathcal{M}(G)$. Let $D \subseteq E$ be dependent in $\mathcal{M}(G)$. Then there exists $C \subset D$ that is a circuit in $\mathcal{M}(G)$. Order the elements of C as $e_1, \ldots, e_n$ so that e_i and e_{i+1} (cyclically ordered) share exactly one vertex. We say that e_i is ***positively oriented*** if it is directed toward the vertex that it shares with e_{i+1} and ***negatively oriented*** otherwise. Define $x \in \mathbb{F}^E$ by

$$x_e := \begin{cases} 0 & \text{if } e \notin C \\ 1 & \text{if } e \in C \text{ and is positively oriented} \\ -1 & \text{if } e \in C \text{ and is negatively oriented.} \end{cases}$$

Then $Ax = 0$, so C and therefore D is dependent in $\mathcal{M}(A)$.

Now let $I \subseteq E$ be independent in $\mathcal{M}(G)$. Then the subgraph of G on edge set I is a forest. Then the submatrix B of A obtained by restricting to the columns indexed by I has linearly independent columns. Indeed, let v be a vertex of degree one in I and let e denote its incident edge. Then the row of B indexed by v has exactly one nonzero entry at column e. We can therefore remove this row and column to obtain a new matrix B' which has linearly independent columns if and only if B does. Since $I \setminus \{v\}$ is also independent in $\mathcal{M}(G)$, B' has linearly independent columns by induction on $|I|$. So I is independent in $\mathcal{M}(A)$ as well. $\square$

2. Cryptomorphism

We defined matroids in terms of their independent sets and then defined circuits in terms of independent sets. Since the circuits of a matroid determine its independents sets, we could have just as easily defined matroids in terms of their circuits and then defined independent sets to be the subsets of the ground set not containing any circuit. Proposition 4.7 makes this precise. But this isn't the end of the story. In this section, we will define several other invariants of a matroid and then show how one could have axiomatize matroids using them instead of independent sets.

It is quite pleasing that one can do this, and this phenomenon is often referred to as ***matroid cryptomorphism***.

Proposition 4.7: *Let E be a finite set and let $\mathcal{C} \subseteq 2^E$. Then there exists a matroid M with circuit set $\mathcal{C}$ if and only if*

(1) $\emptyset \notin \mathcal{C}$,
(2) *if* $C_1, C_2 \in \mathcal{C}$ *and* $C_1 \subseteq C_2$, *then* $C_1 = C_2$, *and*
(3) *given* $C_1, C_2 \in \mathcal{C}$ *are distinct and* $e \in C_1 \cap C_2$, *there exists* $C_3 \in \mathcal{C}$ *such that* $C_3 \subseteq (C_1 \cup C_2) \setminus \{e\}$.

Proof. First assume $\mathcal{C}$ is the circuit set of some matroid M. Since $\emptyset$ is independent in M, $\mathcal{C}$ satisfies the first condition and since circuits are inclusion-minimal dependent sets, the second condition is satisfied as well. To see that it satisfies the third, let $C_1, C_2 \in \mathcal{C}$ and let $e \in C_1 \cap C_2$. If $C_1 \cup C_2 \setminus \{e\}$ does not contain a circuit then it is independent. Let $f \in C_2 \setminus C_1$ and let $I \subseteq C_1 \cup C_2$ be maximal with respect to being independent and containing $C_2 \setminus \{f\}$. Since C_1 is a circuit, some $g \in C_1$ is not in I. Note that $f \neq g$. But then

$$|I| \leq |C_1 \cup C_2| - 2 < |C_1 \cup C_2 \setminus e|.$$

Applying the third independent set axiom contradicts maximality of I.

Now assume $\mathcal{C}$ satisfies the conditions of the proposition. Let $\mathcal{I}$ be the set of subsets of E that contain no member of $\mathcal{C}$. Then $\emptyset \in \mathcal{I}$ and if $J \in \mathcal{I}$ and $I \subseteq J$, then $I \in \mathcal{I}$. We now prove the third independence axiom.

Suppose that $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$. Choose $I_3 \in \mathcal{I}$ satisfying $I_3 \subseteq I_1 \cup I_2$ and $|I_3| > |I_1|$ such that $|I_1 \setminus I_3|$ is minimal. If the third independence axiom fails for I_1, I_2, then $I_1 \setminus I_3$ is nonempty so for the sake of contradiction let $e \in I_1 \setminus I_3$. For each $f \in I_3 \setminus I_1$ define $T_f := (I_3 \cup e) \setminus f$. Then $T_f \subseteq I_1 \cup I_2$ and $|I_1 \setminus T_f| < |I_1 \setminus I_3|$. Our minimality assumption then implies $T_f \notin \mathcal{I}$ so there exists $C_f \in \mathcal{C}$ contained in T_f. Then $f \notin C_f$ and since $I_3 \in \mathcal{I}$, $e \in C_f$.

Now suppose $g \in I_3 \setminus I_1$. If $C_g \cap (I_3 \setminus I_1) = \emptyset$ then $C_g \subseteq ((I_1 \cap I_3) \cup e) \setminus g \subseteq I_1$ which is a contradiction. So let $g \in C_g \cap (I_3 \setminus I_1)$. Since $h \notin C_h$, we have $C_g \neq C_h$. Since $e \in C_g \cap C_h$, there exists $C \in \mathcal{C}$ such that $C \subseteq (C_g \cup C_h) \setminus e$. But $C_g, C_h \subseteq I_3 \cup \{e\}$ so this implies $C \subseteq I_3$ contradicting $I_3 \in \mathcal{I}$. ☐

Definition 4.8: Let $M = (E, \mathcal{I})$ be a matroid. A ***basis*** of M is an inclusion-wise maximal element of $\mathcal{I}$.

Proposition 4.9: *Let $M = (E, \mathcal{I})$ be a matroid. If B_1, B_2 are bases of M, then $|B_1| = |B_2|$.*

Proof. If $|B_1| < |B_2|$ without loss of generality, then the third independence axiom implies that $B_1 \cup \{y\}$ is independent for some $y \in B_2 \setminus B_1$. But this contradicts maximality of B_1. ☐

Proposition 4.10: *Let E be a finite set and let $\mathcal{B} \subseteq 2^E$. Then there exists a matroid $M = (E, \mathcal{I})$ whose bases are the elements of $\mathcal{B}$ if and only if*

(1) $\mathcal{B}$ *is nonempty, and*
(2) *Given* $B_1, B_2 \in \mathcal{B}$ *and* $x \in B_1 \setminus B_2$, *there exists* $y \in B_2 \setminus B_1$ *such that* $(B_1 \setminus x) \cup y \in \mathcal{B}$.

Proof. First let $M = (E, \mathcal{I})$ be a matroid with basis set $\mathcal{B}$. Since $\mathcal{I}$ is nonempty, so is $\mathcal{B}$. Let $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \setminus B_2$. Since $B_1 \setminus x$ and B_2 are both independent sets, there exists $y \in B_2 \setminus B_1$ such that $B_1 \cup y$ is independent. Proposition 4.9 implies that $B_1 \cup y$ is moreover a basis.

Now assume that $\mathcal{B}$ satisfies the given properties. Define $\mathcal{I}$ to be the set of all subsets of elements of $\mathcal{B}$. We now show that that $(M, \mathcal{I})$ is a matroid. Indeed, the first basis axiom implies $\emptyset \in \mathcal{I}$ and the second independence axiom is satisfied by construction. We proceed to show the third.

We begin by claiming that all members of $\mathcal{B}$ have the same cardinality. Otherwise, let $B_1, B_2 \in \mathcal{B}$ have $|B_1| > |B_2|$ and assume $|B_1 \setminus B_2|$ is minimal with respect to this property. Let $x \in B_1 \setminus B_2$. There exists $y \in B_2 \setminus B_1$ such that $(B_1 \setminus x) \cup y \in \mathcal{B}$. But this contradicts minimality of $|B_1 \setminus B_2|$ so the claim is proven.

Now assume the third axiom fails for $(E, \mathcal{I})$ and let $I_1, I_2 \in \mathcal{I}$ satisfy $|I_1| < |I_2|$ and $I_1 \cup \{e\} \notin \mathcal{I}$ for all $e \in I_2$. Then $\mathcal{B}$ has B_1 containing I_1 and B_2 containing I_2, Assume B_2 is chosen so that $|B_2 \setminus (I_2 \cup B_1)|$ is minimal. Then

$$I_2 \setminus B_1 = I_2 \setminus I_1 \tag{4}$$

We claim that $B_2 \setminus (I_2 \cup B_1)$ is empty. Otherwise, let x lie in this set. Then there exists $y \in B_1$ such that $B_3 := (B_2 \setminus x) \cup y \in \mathcal{B}$. But then $|B_3 \setminus (I_2 \cup B_1)| < |B_2 \setminus (I_2 \cup B_1)|$ contradicting our choice of B_2. This proves our claim. It then follows from our claim and (4) that

$$B_2 \setminus B_1 = I_2 \setminus I_1. \tag{5}$$

We now claim that $B_1 \setminus (I_1 \cup B_2)$ is also empty. Again, let $x \in B_1 \setminus (I_1 \cup B_2)$ for sake of contradiction. Then there exists $y \in B_2 \setminus B_1$ such that $B_4 := (B_1 \setminus x) \cup y \in \mathcal{B}$. Then $I_1 \cup y \subseteq B_4$ so $I_1 \cup y \in \mathcal{I}$. Since $y \in B_2 \setminus B_1$, it follows from (5) that $y \in I_2 \setminus I_1$ which would contradict our assumption that the third independence axiom fails. So $B_1 \setminus (I_1 \cup B_2)$ is indeed empty. We now have the following

$$B_1 \setminus B_2 = I_1 \setminus B_2 \subseteq I_1 \setminus I_2. \tag{6}$$

Proposition 4.9 implies that $|B_1| = |B_2|$ and therefore that $|B_1 \setminus B_2| = |B_2 \setminus B_1|$. Then (5) and (6) imply that $|I_1 \setminus I_2| \geq |I_2 \setminus I_1|$ and therefore $|I_1| \geq |I_2|$, contradicting our assumption that $|I_1| < |I_2|$. This implies that $(E, \mathcal{I})$ is indeed a matroid. $\square$

Definition 4.11: Let $M = (E, \mathcal{I})$ be a matroid. The ***rank function of*** M is the function $\rho : 2^E \to \mathbb{Z}$ defined by

$$\rho(S) := \max_{\substack{I \in \mathcal{I} \\ I \subseteq S}} |I|$$

The following proposition axiomatizes matroids in terms of their rank functions. The first two properties should be relatively unsurprising. To make the third seem a little less exotic, recall that the following holds for any subsets S, T of a set E

$$|S \cup T| = |S| + |T| - |S \cap T|.$$

The third property below, called ***submodularity***, specializes to this identity on the matroid $(E, 2^E)$. The second property is called ***montonicity***.

Proposition 4.12: *Let E be a finite set and let $\rho : 2^E \to \mathbb{Z}$. Then ρ is the rank function of a matroid $M = (E, \mathcal{I})$ if and only if*

(1) $0 \leq \rho(S) \leq |S|$ *for all* $S \subseteq E$
(2) *if* $S \subseteq T$ *then* $\rho(S) \subseteq \rho(T)$, *and*
(3) $\rho(S \cup T) + \rho(S \cap T) \leq \rho(S) + \rho(T)$ *for all* $S, T \subseteq E$.

Proof. First, assume that ρ is the rank function of a matroid $M = (E, \mathcal{I})$. The reader can verify that ρ satisfies the first two properties. For the third, let $S, T \subseteq E$ and let I, J' be maximum-cardinality independent subsets of $S \cap T$ and $S \cup T$. By the third independence axiom, there exists a maximum-cardinality independent subset J of $S \cup T$ that contains I. Since $J \cap S$ and $J \cap T$ are independent, we have the following

$$\begin{aligned}\rho(S) + \rho(T) &\geq |J \cap S| + |J \cap T| \\ &= |(J \cap S) \cup (J \cap T)| + |(J \cap S) \cap (J \cap T)| \\ &= |J \cap (S \cup T)| + |J \cap S \cap T| \\ &= |J| + |I| \\ &= \rho(S \cup T) + \rho(S \cap T).\end{aligned}$$

Now, assume ρ satisfies the given properties and define

$$\mathcal{C} := \{C \subseteq E : \rho(C) = \rho(C \setminus e) = |C| - 1 \text{ for all } e \in C\}.$$

We will show that $\mathcal{C}$ is the circuit set of a matroid with rank function ρ. First observe that $\emptyset \notin \mathcal{C}$ as $\rho(\emptyset) = 0$. Given $S \subseteq E$ and $e \in E$, monotonicity of ρ and the submodular inequality applied to S and $\{e\}$ gives

$$\rho(S) \leq \rho(S \cup \{e\}) \leq \rho(S) + 1. \tag{7}$$

To see the second circuit axiom, let $C_1, C_2 \in \mathcal{C}$ with $C_1 \subset C_2$. For sake of contradiction, assume $e \in C_2 \setminus C_1$. Then $\rho(C_2 \setminus e) = |C_2 \setminus e|$ and therefore (7) implies that $\rho(S) = |S|$ for all $S \subseteq C_2 \setminus e$. But this contradicts $\rho(C_1) = |C_1| - 1$.

We now show that the third circuit axiom is satisfied. If $C_1, C_2 \in \mathcal{C}$ are distinct then $\rho(C_1 \cap C_2) = |C_1 \cap C_2|$ and $\rho(C_i) = |C_i| - 1$. Since ρ is monotone and submodular, we have

$$\begin{aligned}\rho((C_1 \cup C_2) \setminus e) &\leq \rho(C_1 \cup C_2) \\ &\leq |C_1| + |C_2| - 2 - |C_1 \cap C_2| \\ &= |C_1 \cup C_2| - 2.\end{aligned}$$

The result now follows from the claim that if $S \subseteq E$ satisfies $\rho(S) = |S| - 1$ then there exists $C \subseteq S$ such that $C \in \mathcal{C}$. Indeed, let $C \subseteq S$ have minimum cardinality such that $\rho(C) = |C| - 1$. For each $e \in C$, the first property that ρ satisfies implies that $\rho(C \setminus e) \leq |C| - 1$. The claim now follows from (7). $\square$

We will use (7) again, so we state it below as a lemma.

Lemma 4.13: *Let $\rho : 2^E \to \mathbb{Z}$ be the rank function of a matroid. Then $\rho(S) \leq \rho(S \cup e) \leq \rho(S) + 1$ for all $S \subseteq E$ and $e \in E$.*

The last cryptomorphic way to define matroids that we introduce in this chapter is through their closure operators. Closure operators generalize the notion of span in a vector space. More specifically if $M = \mathcal{M}(A)$ for some matrix A, then the closure operator of M is the function that sends a subset of columns S of A to the set of columns spanned by S.

Definition 4.14: Let M be a matroid on ground set E with rank function ρ. The ***closure operator*** $\sigma : 2^E \to 2^E$ is defined by

$$\sigma(S) = \{x \in E : \rho(S) = \rho(S \cup x)\}.$$

Proposition 4.15: *Let E be a finite set and let $\sigma : 2^E \to 2^E$. Then σ is the closure operator of a matroid if and only if it satisfies the following properties:*

(1) $S \subseteq \sigma(S)$ *for all* $S \subseteq E$,
(2) $\sigma(S) \subseteq \sigma(T)$ *whenever* $S \subseteq T$,
(3) σ *is idempotent, i.e.* $\sigma(\sigma(S)) = \sigma(S)$ *for all* $S \subseteq E$, *and*
(4) *if* $S \subseteq E$ *and* $y \in \sigma(S \cup x) \setminus \sigma(S)$, *then* $x \in \sigma(S \cup y)$.

Proof. First assume that σ is the closure operator of a matroid M on ground set E with rank function ρ. It follows from the definition that σ satisfies the first property. For the second, let $x \in \sigma(S)$. The submodular inequality applied to T and $S \cup \{x\}$ gives

$$\rho(T \cup \{x\}) + \rho(S) \leq \rho(T) + \rho(S \cup \{x\}).$$

Since $\rho(S) = \rho(S \cup \{x\})$, this implies $\rho(T \cup \{x\}) \leq \rho(T)$ and monotonicity of ρ then implies $\rho(T \cup \{x\}) = \rho(T)$ i.e. that $x \in \sigma(T)$. The first two properties imply that $\sigma(S) \subseteq \sigma(\sigma(S))$. To get the reverse inclusion and therefore idempotency, let $x \in \sigma(\sigma(S))$ and note

$$\rho(S) \leq \rho(S \cup \{x\}) \leq \rho(\sigma(S) \cup \{x\}) = \rho(\sigma(S)) = \rho(S).$$

We now show the final property. Indeed, let $S \subseteq E$ and $x, y \in E$ such that $y \in \sigma(S \cup x) \setminus \sigma(S)$. Lemma 4.13 then gives the following

$$\rho(S) + 1 \geq \rho(S \cup x) = \rho(S \cup \{x, y\}) \geq \rho(S \cup y) = \rho(S) + 1$$

and therefore that $x \in \sigma(S \cup y)$.

Now assume that $\sigma : 2^E \to 2^E$ satisfies the given properties. Define

$$\mathcal{I} := \{I \subseteq E : e \notin \sigma(I \setminus e) \text{ for all } e \in I\}.$$

We now show that $\mathcal{I}$ is the independent sets of a matroid with σ as its closure operator. Indeed, $\emptyset \in \mathcal{I}$ is immediate. Now let $I \in \mathcal{I}$ and $J \subseteq I$. If $e \in J$ then $e \notin \sigma(I \setminus e) \supseteq \sigma(J \setminus e)$ so $J \in \mathcal{I}$.

We claim that if $I \in \mathcal{I}$ but $I \cup \{x\} \notin \mathcal{I}$ then $x \in \sigma(I)$. Indeed, the definition of $\mathcal{I}$ implies that there exists $y \in I \cup x$ such that $y \in \sigma((I \cup x) \setminus y)$. The claim is proven if $y = x$ so assume $y \in I$. Then the fourth closure axiom implies $x \in \sigma((I \setminus y) \cup y) = \sigma(I)$ so the claim is proven.

We now prove that $\mathcal{I}$ satisfies the third independence axiom. Assume for the sake of contradiction that there exist $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$ and $I_1 \cup x \notin \mathcal{I}$ for all $x \in I_2 \setminus I_1$. Moreover, assume I_1, I_2 have been chosen so that $|I_1 \cap I_2|$ is maximized with respect to this property. Choose $y \in I_2 \setminus I_1$. Assume that $I_1 \subseteq \sigma(I_2 \setminus y)$. Since $\sigma(I_1) \subseteq \sigma(I_2)$ and $I_2 \in \mathcal{I}$, we have $y \notin \sigma(I_1)$. But then the claim implies that $I_1 \cup y \in \mathcal{I}$ contradicting our assumptions on I_1, I_2. So there exists $t \in I_1 \setminus \sigma(I_2 \setminus y)$. Then $t \in I_1 \setminus I_2$ and the claim implies $I_2 \setminus y \cup t \in \mathcal{I}$. Our minimality assumption then implies that there exists $x \in (I_2 \setminus y \cup t) \setminus I_1$ such that $I_1 \cup x \in \mathcal{I}$. But as $t \in I_1$ this would imply $x \in I_2$ contradicting our assumption. $\square$

3. Exercises

Problem 1: Describe the rank function and closure operator of a graphic matroid in graph-theoretic terms.

Problem 2: Prove that a graph with n vertices, c connected components, and at least $n - c + 1$ edges has a cycle. Then let G be a graph with edge set E and show that its matroid $\mathcal{M}(G)$ has the following rank function

$$\rho(S) = |V(S)| - c(S)$$

where $V(S)$ denotes the set of vertices of G that are incident to some edge in S and $c(S)$ denotes the number of connected components of the graph on vertex set $V(S)$ and edge set S.

Problem 3: Let E be a finite set and let $\mathcal{H} \subseteq 2^E$. Prove that $\mathcal{H}$ is the set of hyperplanes of a matroid if and only if

(1) $E \notin \mathcal{H}$,
(2) if $H_1, H_2 \in \mathcal{H}$ with $H_1 \subseteq H_2$, then $H_1 = H_2$, and
(3) if $H_1, H_2 \in \mathcal{H}$ and $e \notin H_1 \cup H_2$, then there exists $H \in \mathcal{H}$ such that $H \supseteq (H_1 \cap H_2) \cup e$.

Bibliography

[1] James R Munkres. *Topology*, volume 2. Prentice Hall Upper Saddle River, 2000.

[2] Günter M Ziegler. *Lectures on polytopes*, volume 152. Springer Science & Business Media, 2012.