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 $\mathrm{Conv}(\{x_1, \ldots, x_n\})$.

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

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

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

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

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

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

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 $x - c + b \in A$. □

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 $\dim(\text{Aff}(C))$. 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.

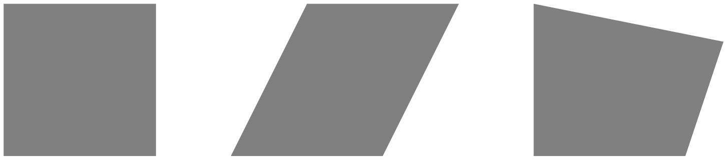


FIGURE 1.1.2. The first two polytopes are affinely isomorphic to each other, but not to the third. This is because affine functions preserve parallel lines and the first two have two sets of parallel lines, but the last one has none.

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 [6, 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 $y \in \text{rb}(C)$ because $y_n \in \text{Aff}(C)$ as $S_n \subseteq \text{Aff}(C)$. □

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 $\text{Aff}(F) \subseteq \text{Aff}(C)$, this implies that $\text{Aff}(F) = \text{Aff}(C)$. 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 $\text{ri}(F)$ is a nonempty open subset of $\mathbb{R}^d$. Therefore $\text{ri}(F) \subseteq \text{ri}(C)$ implies $\text{ri}(F) \subseteq \text{ri}(C)$. 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 $\text{ri}(\text{Conv}(x, y)) \cap F' \neq \emptyset$. 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 $F' \cap \text{ri}(\text{Conv}(x, y)) \neq \emptyset$. 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 $z \in F_{a,c} \cap \text{ri}(\text{Conv}(x, y))$. 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.

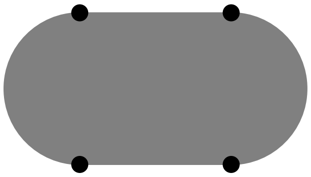


Figure 1.2.3. All of the faces of the above convex set $C \subset \mathbb{R}^2$ are exposed, aside from the four extreme points indicated by black dots. To see this, note that the tangent line to C at any one of these points will intersect along the entire edge that it lies on.

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 $H_1, \dots, H_n \subset \mathbb{R}^d$. 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*

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

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

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

Proof. Let $a_1, \dots, a_n \in (\mathbb{R}^d)^*$ and $c_1, \dots, c_n \in \mathbb{R}$ 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 $x \in \text{ri}(\text{Conv}(y, z))$. By our hypothesis, there exists $i \in I$ such that $a_i y < c_i$. Since $a_i x = c_i$ and $x \in \text{ri}(\text{Conv}(y, z))$, 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 $i \notin I$, $x \in \text{ri}(P \cap A)$. Therefore, there exist $y, z \in P \cap A$ such that $x \in \text{ri}(\text{Conv}(y, z))$. This implies that x is not an extreme point of P. □

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 $x_1, \dots, x_k$. Theorem 1.11 then implies that $P = \text{Conv}\{x_1, \dots, x_k\}$. □

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 $a \in C^*$). □

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. □

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. □

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

Problem 1.2: Prove that $x \in \operatorname{Aff}(x_1, \ldots, x_n)$ if and only if

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

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

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

Problem 1.3: 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 1.4: 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 1.5: 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 1.6: 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 1.7: Prove the unproven parts of Theorem 1.15.

Problem 1.8: Let $P, Q \subseteq \mathbb{R}^d$ be convex sets. Prove that $(P + Q)^* = P^* \cap Q^*$.

Problem 1.9: 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.

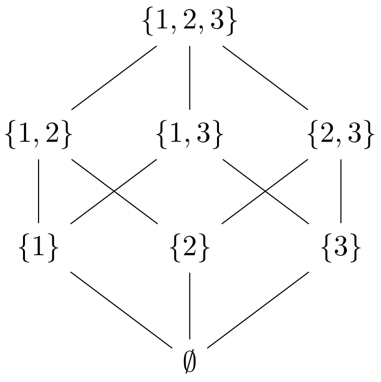


FIGURE 2.1.1. The boolean lattice B_3 is the set of all subsets of $\{1, 2, 3\}$, partially ordered by inclusion. Its order diagram is shown in this figure. This lattice is both atomic and coatomic.

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.

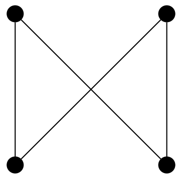


Figure 2.1.2. The order diagram of a poset that is not a lattice.

Lower bounds and ***greatest lower bounds*** are defined analogously. Least upper bounds and greatest lower bounds are unique (see Problem 2.1). 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 2.4.

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 2.2). 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

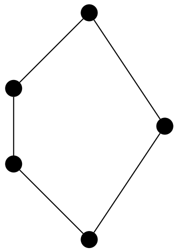


FIGURE 2.2.3. A lattice that is not graded.

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. □

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 $x \in \operatorname{ri}(\operatorname{Conv}(y, z))$. 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 $0 \in \operatorname{ri}(P)$ 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 $c \in \operatorname{ri}(\operatorname{Conv}(a, b)) \cap F'$. 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 $0 \in \operatorname{ri}(P)$. 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 $F \mapsto F'$. □

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 $\dim(P) - 1$. □

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.*

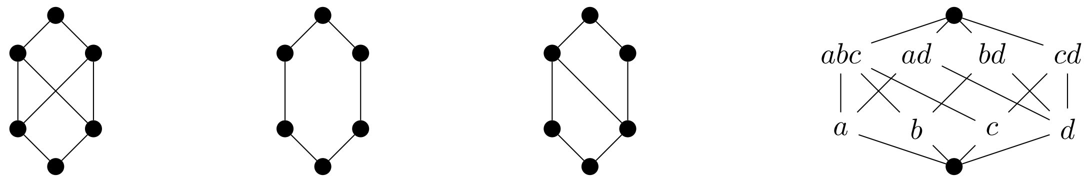
Proof. Let $P \subseteq \mathbb{R}^d$ be a polytope and let F be a face. Since the face lattice of a polytope is coatomic with facets as the coatoms (c.f. Theorem 2.3), there exist facets $F_1, \ldots, F_k$ such that $F = F_1 \cap \cdots \cap F_k$. Let $a_1, \ldots, a_k \in (\mathbb{R}^d)^*$ and $b_1, \ldots, b_k \in \mathbb{R}$ 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. □

3. Exercises

Problem 2.1: Show that least upper bounds and greatest lower bounds in a poset are unique.

Problem 2.2: Prove that every finite lattice has a $\hat{0}$ and $\hat{1}$.

Problem 2.3: For each of the following posets, determine which are lattices. Among those that are, determine which are atomic and/or coatomic.



Problem 2.4: 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 2.5: 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). □

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 $\text{Conv}(u, v)$ 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 $\dim(\text{Aff}(N)) \leq d-2$. Then $\dim(\text{Aff}(N \cup \{v\})) \leq d-1$. Let Q be as in Lemma 2.9. Since Q lies in the intersection of $\text{Aff}(N \cup \{v\})$ 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 $\dim(Q) = d-1$. □

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. □

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 $v_1, \dots, v_{d-1}$. By induction on dimension, there exists a path in F' from u' to w' and since $v_1, \dots, v_{d-1}$ are not in F', this path also does not contain any of these vertices. Thus the graph $G \setminus \{v_1, \dots, v_{d-1}\}$ is connected.

Case 2: There is no proper face of P containing $v_1, \dots, v_{d-1}$. Fix an extreme point v_0 of P, distinct from $v_1, \dots, v_{d-1}$. Then there exists a hyperplane $H = \{x \in \mathbb{R}^d : ax = c\}$ containing $v_0, \dots, v_{d-1}$. 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 $F \cap \{v_1, \dots, v_{d-1}\}$ and $F' \cap \{v_1, \dots, v_{d-1}\}$ are at most $d-2$. By induction on dimension, the graphs of F and F' are both connected even after removing $v_1, \dots, v_{d-1}$. Given a vertex $v \neq v_i$ for all $i = 0, \dots, d-1$, 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'. □

TODO: change to argument that doesn't require LP stuff, see WhatsApp messages from Louis

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 $S \subsetneq \text{Aff}(P)$ 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 [8, Chapter 4].

CHAPTER 4

Matroid fundamentals

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.

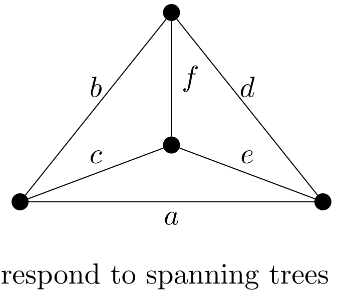
Definition 4.2: Let A be a matrix whose columns are indexed by a set E. The matroid associated to A, denoted $\mathcal{M}(A)$, is $(E, \mathcal{I})$ where $S \subseteq E$ is in $\mathcal{I}$ if and only if the submatrix of A obtained by restricting to the columns indexed by S has linearly independent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

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

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. □

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 $e_1, \dots, e_n$ 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. □

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. □

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). □

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. □

3. The lattice of flats of a matroid

Definition 4.16: Let M be a matroid on ground set E with closure operator σ. A set $S \subseteq E$ is a ***flat*** or a ***closed set*** if $S = \sigma(S)$. The ***lattice of flats of*** M, denoted $\mathcal{L}(M)$, is the set of flats of M, partially ordered by inclusion.

Proposition 4.17: *Let M be a matroid on ground set E with closure operator σ. Then $\mathcal{L}(M)$ is a lattice. The meet and join operations are as follows*

$$F_1 \wedge F_2 := F_1 \cap F_2 \qquad \text{and} \qquad F_1 \vee F_2 := \sigma(F_1 \cup F_2).$$

PROOF. It follows from the closure axioms that $F_1 \cap F_2$ is a flat of M since

$$\sigma(F_1 \cap F_2) \subseteq \sigma(F_1) \cap \sigma(F_2) = F_1 \cap F_2 \subseteq \sigma(F_1 \cap F_2)$$

and so this must be the inclusion-wise maximal flat contained in F_1 and F_2. Similarly, $\sigma(F_1 \cup F_2)$ is by definition the inclusion-wise minimal flat containing both F_1 and F_2. □

Definition 4.18: A lattice $\mathcal{L}$ is ***geometric*** if it is atomic and graded with a rank function ρ satisfying the following for all $x, y \in \mathcal{L}$

$$\rho(x \vee y) + \rho(x \wedge y) \leq \rho(x) + \rho(y).$$

Proposition 4.19: *Let M be a matroid with rank function ρ. Then $\mathcal{L}(M)$ is a geometric lattice with rank function $F \mapsto \rho(F)$.*

PROOF. Let σ be the closure operator of M and let E be the ground set. Atoms of $\mathcal{L}(M)$ are the flats of the form $\sigma(x)$ for $x \in E$. Given a flat F of M and a maximal independent subset I of F, $F = \sigma(I)$. Thus F is the join of the $\sigma(x)$ as x ranges over I. So $\mathcal{L}(M)$ is atomic.

We now show that $\mathcal{L}(M)$ is graded with the desired rank function. The inequality in Definition 4.18 will then follow immediately from submodularity of ρ. Let $\mathcal{I}$ be the set of independent subsets of M. Given any $S \subseteq E$, the pair $(S, \{I \in \mathcal{I} : I \subseteq S\})$ is a matroid. Thus by induction on $|E|$, it suffices to show that the length of any maximal chain in $\mathcal{L}(M)$ is $\rho(E)$. Indeed, let

$$\emptyset = F_0 \subsetneq F_1 \subsetneq \cdots \subsetneq F_r = E$$

be a maximal chain in $\mathcal{L}(M)$. For $i = 1, \ldots, r$, fix some $x \in F_i \setminus F_{i-1}$. Then $\{x_1, \ldots, x_r\}$ is an independent set. Otherwise, if i is the minimal i such that $\{x_1, \ldots, x_i\}$ is not independent, then $x_i \in \sigma(x_1, \ldots, x_{i-1}) \subseteq F_{i-1}$. This implies $r \leq \rho(E)$. There exists an independent set of M with $\rho(E)$ elements so if $r < \rho(E)$, then the third independence axiom implies that there exists $y \in E \setminus \{x_1, \ldots, x_r\}$ such that $\{x_1, \ldots, x_r, y\}$ is independent. But as $F_r = E$ is a flat, this would imply $y \notin E$, a contradiction. □

Theorem 4.20: *A lattice $\mathcal{L}$ is geometric if and only if there exists a matroid M such that $\mathcal{L}$ is isomorphic to $\mathcal{L}(M)$.*

PROOF. We already saw that $\mathcal{L}(M)$ is a geometric lattice for any matroid M so assume $\mathcal{L}$ is a geometric lattice. If $\hat{0} = \hat{1}$ in $\mathcal{L}$, then take $M = U_{0,0}$. Otherwise, $\mathcal{L}$ has a nonempty set E of atoms and let r be the rank function of $\mathcal{L}$. Define the function $\rho : 2^E \to \mathbb{Z}$ as follows

$$\rho(S) := r\left(\bigvee_{e \in S} e\right).$$

We show that ρ is the rank function of a matroid M by verifying the conditions of Proposition 4.12. Indeed, the first condition follows immediately. If $S \subseteq T$ then the join of the elements in T is an upper bound for the join of the elements in S so $\rho(S) \leq \rho(T)$. Submodularity of ρ follows immediately from the inequality in Definition 4.18 for r.

It remains to show that $\mathcal{L}(M)$ and $\mathcal{L}$ are isomorphic as posets. Indeed, define $f : \mathcal{L} \to \mathcal{L}(M)$ by $X \mapsto \{e \in E : e \leq X\}$. To see that $f(X)$ is indeed a flat of M for each $X \in \mathcal{L}$, let σ denote the closure operator of M and let $y \in \sigma(f(X))$. Then $\rho(f(X) \cup y) = \rho(f(X))$, so

$$r\left(\bigvee_{e \leq X} e\right) = r\left(y \vee \bigvee_{e \leq X} e\right).$$

Combining this with the fact that $y \vee \bigvee_{e \leq X} e \geq \bigvee_{e \leq X} e$ in $\mathcal{L}$ gives us that $y \vee \bigvee_{e \leq X} e = \bigvee_{e \leq X} e$ i.e. that $y \leq X$ in $\mathcal{L}$. So $f(X)$ is indeed a flat of M. By construction, $X \leq Y$ implies $f(X) \subseteq f(Y)$. Since $\mathcal{L}$ is atomic, f is one-to-one.

We now show that f is onto. Let F be a flat of M and define $X \in \mathcal{L}$ by $X := \bigvee_{e \in F} e$. We claim that $F = f(X)$. Let $e \in F$. Then $e \leq X$ in $\mathcal{L}$ so $F \subseteq f(X)$. Now let $g \in f(X)$ i.e. $g \leq X$ in $\mathcal{L}$. This implies that $g \vee X = X$ in $\mathcal{L}$ so $r(g \vee X) = r(X)$ and therefore that $\rho(g \cup F) = \rho(F)$. Since F is a flat, this implies $g \in F$ so we now have $f(X) \subseteq F$ and therefore equality. □

Definition 4.21: A matroid is ***simple*** if it has no loops or parallel elements. Given a matroid M, the ***simplification of*** M is the matroid obtained from M by deleting all loops and all but one element from each parallel class.

Definition 4.22: A ***hyperplane*** of a matroid M on ground set E with rank function ρ is a flat with rank $\rho(E) - 1$.

Matroids can be axiomatized in terms of their hyperplanes (c.f. Problem 5.3).

CHAPTER 5

Visualizing matroids

1. Matroids of rank three

Proposition 5.1: *Let $E \subset \mathbb{R}^d$ be a finite set. The subsets of E that are affinely independent are the independent sets of a matroid.*

Proof. Let A be the matrix obtained from E by adding a new coordinate to each element of E and setting it equal to 1. Then a subset of E is affinely independent if and only if the corresponding columns of A are linearly independent. □

Proposition 5.2: *Let E be a finite set of size at least 3. Let Λ be a collection of proper subsets of E, each of size at least 3 such that given $L_1, L_2 \in \Lambda$, $|L_1 \cap L_2| \leq 1$. Let Λ' consists of the pairs of points in E that are not in any element of Λ. Then $\mathcal{H} := \Lambda \cup \Lambda'$ is the set of hyperplanes of a matroid of rank 3.*

Proof. We verify the hyperplane axioms (c.f. Problem 5.3). The first two axioms follow immediately from our assumptions. For the third, let $L_1, L_2 \in \mathcal{H}$ with $L_1 \neq L_2$ and let $e \notin L_1 \cup L_2$. We split into three cases.

Case 1: $L_1, L_2 \in \Lambda'$:

Case 2: $L_1, L_2 \in \Lambda$:

Case 3: $L_1 \in \Lambda$ and $L_2 \in \Lambda'$: □

(1) Non-fano matroid
(2) Fano matroid

Proposition 5.3: *Let M be a matroid of rank 3, representable over a field $\mathbb{F}$, such that every line of the non-fano matroid is dependent in M. Then M is the fano matroid if the characteristic of $\mathbb{F}$ is 2 and the non-fano matroid otherwise. In particular, the fano matroid is representable only over fields of characteristic two and the non-fano matroid is representable only over fields of characteristic other than two.*

Proposition 5.4: *Let M be a matroid on ground set E and let $S \subset E$ be a circuit and a hyperplane of E. Let $\mathcal{B}$ be the set of bases of M. Then $\mathcal{B} \cup S$ is the set of bases of a matroid.*

Proof. First note that the cardinality of S is the rank in M of E, i.e. the cardinality of any basis. Let B be a basis of M. For the two cases $B_1 = B, B_2 = S$ and $B_1 = S, B_2 = B$, we must show that for all $x \in B_1 \setminus B_2$, there exists a $y \in B_2 \setminus B_1$ such that $B_1 \cup y \setminus x$ is a basis of M. In the first case, since S is a hyperplane, $S \cup x$ contains a basis. Since $|S| = |B|$, this basis is obtained by removing a single element of $S \setminus x$. In the second case, since S is a circuit, $S \setminus x$ is independent for any $x \in S$. Since $|B| = |S|$, there exists some $y \in B$ such that $S \setminus x \cup y$ is independent in M, i.e. a basis of M. □

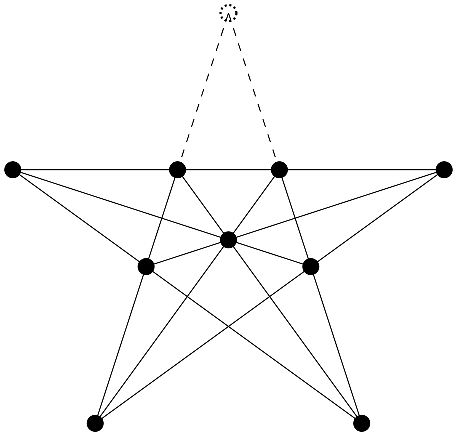


FIGURE 5.2.1. A matroid of rank three that is representable over $\mathbb{R}$ but not $\mathbb{Q}$. This is often called the "Perles matroid." The dotted point, along with the four points along the outside, are the vertices of a regular pentagon.

2. Projective geometry

Definition 5.5: Given a field $\mathbb{F}$, the ***d-dimensional projective space over*** $\mathbb{F}$, denoted $\mathbb{P}^d(\mathbb{F})$, is the vector space $\mathbb{F}^{d+1}\setminus\{0\}$ modulo the equivalence relation $x \sim y$ if $x = \lambda y$ for some $\lambda \in \mathbb{F}\setminus\{0\}$. When $\mathbb{F}$ is clear from context or not important we will write $\mathbb{P}^d$ instead of $\mathbb{P}^d(\mathbb{F})$.

We will often refer to $\mathbb{F}^d$ as ***d-dimensional affine space***. Given a point $x \in \mathbb{F}^{d+1} \setminus \{0\}$, we let $[x]$ denote its corresponding point in $\mathbb{P}^d$, i.e. its equivalence class modulo $\sim$. Since the pairwise ratios of the coordinates of x determine $[x]$, a point $[x]$ in $\mathbb{P}^d(\mathbb{F})$ is often written out as $[x_0 : x_1 : \cdots : x_d]$. For $i = 0, \ldots, d$, define

$$A_i := \{[x] \in \mathbb{P}^d : x_i \neq 0\}.$$

Then each $[x] \in A_i$ has a unique equivalence class (under $\sim$) representative $\hat{x}$ with $x_i = 1$, so we may identify A_i with the affine space $\mathbb{F}^d$ via the map $[x] \mapsto (\hat{x}_j : j \neq i)$. Since each element of $\mathbb{P}^d$ lies in some A_i, we could have alternatively constructed $\mathbb{P}^d$ by gluing together $d+1$ copies of $\mathbb{F}^d$ in a particular way. If $T : \mathbb{F}^{d+1} \to \mathbb{F}^{d+1}$ is linear, then the map $[x] \mapsto [Tx]$ is well-defined. With this in mind, we define a ***projective transformation*** to be a map $\mathbb{P}^d \to \mathbb{P}^d$ of the form $[x] \mapsto [Tx]$ where $T : \mathbb{F}^{d+1} \to \mathbb{F}^{d+1}$ is an invertible linear map. Since we can naturally identify $\mathbb{F}^d$ with A_0, we will view affine space as a subset of projective space, thinking of $\mathbb{P}^n \setminus A_0$ as "points at infinity."

TODO

- Define projective equivalence for point configurations in $\mathbb{P}^n$
- Projective equivalence implies combinatorial equivalence
- Give conditions for converse to hold
- Write special case for $d = 2$ and use to prove that the Perles matroid is not $\mathbb{Q}$-realizable

3. Exercises

Problem 5.1: Describe the rank function and closure operator of a graphic matroid in graph-theoretic terms.

Problem 5.2: 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 5.3: 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 $H_1, H_2 \in \mathcal{H}$ are distinct and $e \notin H_1 \cup H_2$, then there exists $H \in \mathcal{H}$ such that $H \supseteq (H_1 \cap H_2) \cup e$.

Problem 5.4: Define A as follows and determine whether or not the lattice of flats of $\mathcal{M}(A)$ is coatomic

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 2 \end{pmatrix} \in \mathbb{R}^{3\times 4}.$$

Problem 5.5: Theorem 4.20 says that the natural map from matroids to geometric lattices is onto. Is it one to one? Either prove that it is, or give an example of two different matroids with the same geometric lattice.

Problem 5.6: Prove that $U_{2,n}$ is representable over a field with q elements if and only if $q \geq n-1$.

CHAPTER 6

Matroid duality and minors

1. Duality basics

Proposition 6.1: *Let M be a matroid on ground set E and define $\mathcal{C}^*$ by*

$$\mathcal{C}^* = \{E \setminus H : H is a hyperplane of M\}.$$

Then $\mathcal{C}^*$ is the set of circuits of a matroid.

Proof. The above is equivalent to showing that the hyperplanes $\mathcal{H}$ of matroid satisfy the following properties

(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 $H_1, H_2 \in \mathcal{H}$ are distinct and $e \notin H_1 \cup H_2$, then there exists $H \in \mathcal{H}$ such that $H \supseteq (H_1 \cap H_2) \cup e$.

The first property follows from the fact that $\rho(H) = \rho(E) - 1$ for all $H \in \mathcal{H}$. The second property follows from the fact that $\rho(H \cup \{x\}) = \rho(E)$ for every $x \notin H$. For the third property, note that $\rho(H_1 \cap H_2) \leq \rho(E) - 2$ so $\rho(\{e\} \cup (H_1 \cap H_2)) \leq \rho(E) - 1$ and is therefore contained in a hyperplane. □

Definition 6.2: Let M be a matroid. The matroid with circuit set $\mathcal{C}^*$ as in Proposition 6.1 is called the ***dual*** of M and is denoted M^*.

Gadgets associated to M^* are associated to M as well, and we use the same name but with the prefix "co" attached. For example, the circuits of M^* are called the ***cocircuits*** of M. We define cospanning etc. sets similarly.

Example 6.3: The cocircuits of the graphic matroid of a graph are the minimal edge subsets whose removal increases the number of connected components.

Proposition 6.4: *Let M be a matroid. Then the coindependent sets of M are the complements of the spanning sets of M and the cobases of M are the complements of the bases of M.*

Proof. The second statement follows immediately from the first. Let M be a matroid on ground set E and let $S \subseteq E$. The first claim now follows from the following chain of equivalences: S is spanning iff S is not contained in a hyperplane of M iff $E \setminus S$ does not contain a cocircuit iff $E \setminus E$ is coindependent. □

Corollary 6.5: *Let M be a matroid. Then $M^{**} = M$.*

2. Duals of representable matroids

We begin by establishing some matrix notation. For any integer $r \geq 1$, the $r \times r$ identity matrix is denoted I_r. Let A be a matrix whose columns are indexed by E. For any $S \subseteq E$, A_S denotes the column submatrix of A on column set S.

Lemma 6.6: *Let M be a rank-r matroid on ground set E with $|E| = n$. If M is representable over a field $\mathbb{F}$, then (up to reordering columns) there exists a matrix $D \in \mathbb{F}^{r\times(n-r)}$ such that $M = \mathcal{M}(A)$ where*

$$A = \begin{pmatrix} I_r & D \end{pmatrix}.$$

Proof. Let A be such that $M = \mathcal{M}(A)$. Then A has rank r. By removing all but r linearly independent rows, we may assume without loss of generality that A has r rows. By reordering columns if necessary, we may also assume that the first r columns of A are linearly independent. Since elementary row operations do not affect the matroid of a matrix, we may row-reduce A to get it into the desired form. □

Theorem 6.7: *Let M be representable over a field $\mathbb{F}$. Then M^* is representable over $\mathbb{F}$.*

Proof. Let $A \in \mathbb{F}^{r\times n}$ be an $\mathbb{F}$-representation of M as in Lemma 6.6 and define

$$B := \begin{pmatrix} -D^T & I_{n-r} \end{pmatrix}.$$

Let S be a subset of r columns of A. Observe that the column submatrix of A indexed by S has determinant that is plus or minus the column submatrix of B indexed by $\{1, \ldots, n\} \setminus S$. The theorem now follows from Proposition 6.4. □

3. Matroid minors and graphic duals

Definition 6.8: Given a matroid $M = (E, \mathcal{I})$ and $e \in E$, define the ***deletion of*** e ***in*** M, denoted $M \setminus e$, to be the matroid on ground set $e \setminus E$ with independent sets

$$\{I \in \mathcal{I} : e \notin I\}$$

and the ***contraction of*** e ***in*** M by $M/e := (M^* \setminus e)^*$. A matroid N is a ***minor*** of M if and only if N can be obtained from M by a sequence of deletions and contractions. A minor is ***proper*** if this sequence is nonempty.

Proposition 6.9: *Let $M = (E, \mathcal{I})$ be a matroid and let $e \in E$. If e is a loop or a coloop then $M/e = M \setminus e$. Otherwise:*

1. *the independent sets of M/e are all sets of the form $I \setminus e$ where $I \cup \{e\} \in \mathcal{I}$, and*
2. *the circuits of M/e are all sets of the form*
   (a) *C where C is a circuit of M not containing e, or*
   (b) *$C \setminus \{e\}$ where C is a circuit of M containing e.*

Proposition 6.10: *Let M be a matroid. If M is representable over a field $\mathbb{F}$ then any minor of M is also representable over $\mathbb{F}$. If M is graphic, then so is any minor of M.*

Proof. Assume M is representable over $\mathbb{F}$. Then $M \setminus e$ is as well because a representation for M becomes a representation for $M \setminus e$ by removing the column indexed by e. Representability of M/e now follows from Theorem 6.7.

Now assume $M = \mathcal{M}(G)$ for a graph $G = (V, E)$ and let $e \in E$. Removing e from G gives a graph representing $M \setminus e$. If e is a loop or a coloop of M then $M/e = M \setminus e$. Assume e is neither a loop nor a coloop of M. Let V/e be the set obtained from V by removing the vertices u, v of e and replacing them with a single vertex $w \notin V$ and let E/e be the set obtained from E by removing e and for each $f \in E$ incident to u or v, replacing u and v with w. Define the graph $G/e := (V/e, E/e)$. Then $M/e = \mathcal{M}(G/e)$. □

The dual of a graphic matroid need not be graphic which is why we had to use a different strategy to prove Proposition 6.10 in the graphic case. In particular, the following is true.

Proposition 6.11: *Let G be the complete graph K_5 or the complete bipartite graph $K_{3,3}$ and let $M = \mathcal{M}(G)$. Then M^* is not graphic.*

Proof. We do the case $G = K_5$ leaving $K_{3,3}$ as an exercise. Assume that $M^* = \mathcal{M}(G)$ for some graph G. If G is disconnected, we may glue connected components together along single vertices without affecting cycles, and therefore the matroid structure. We will thus without loss of generality assume G is connected.

Since $\mathcal{M}(K_5)$ has rank 4 and 10 elements, its dual has rank 6 and 10 elements. So G has 10 edges, and since it is connected, it has 7 vertices. If every vertex of G has degree at least 3 then G has at least $10 * 3/2 = 15 > 10$ edges. So G must have a vertex of degree 2, incident to edges e, f. This implies that $\{e, f\}$ is a cocircuit of $\mathcal{G}$ and therefore a circuit of $\mathcal{M}(K_5)$. This is a contradiction as K_5 does not have parallel edges. □

Theorem 6.12: *Let G be a graph. Then $\mathcal{M}(G)^*$ is graphic if and only if G is planar.*

Proof sketch. If G is planar, then $\mathcal{M}(G)^*$ is the matroid of the planar dual of G. If G is not planar, then G a graph minor isomorphic to K_5 or $K_{3,3}$ (this is a deep theorem that is outside the scope of this text). Propositions 6.10 and 6.11 then imply that $\mathcal{M}(G)^*$ is not graphic. □

Let B be a basis of a matroid M on ground set E. Then for every $e \in E \setminus B$, there exists a unique circuit $C_M(B, e)$ contained in $B \cup \{e\}$ which we call the ***fundamental circuit of** e **with respect to** B*. Note that $e \in C_M(B, e)$.

Theorem 6.13: *Let M be a matroid on ground set E. Then M is representable over $\mathbb{F}_2$ if and only if M does not have a minor isomorphic to $U_{2,4}$.*

Proof. The matroid $U_{2,4}$ is not representable over $\mathbb{F}_2$ (c.f. Problem 5.6). Proposition 6.10 thus implies that any matroid with $U_{2,4}$ as a minor is not representable over $\mathbb{F}_2$.

Now assume that M is not representable over $\mathbb{F}_2$. In light of Proposition 6.10 we may assume without loss of generality that every proper minor of M is representable over $\mathbb{F}_2$. In particular, we can assume that M has no one- nor two-element cocircuits. Thus if ρ is the rank function of M, then $\rho(E) = \rho(E \setminus \{e, f\})$ for all $e, f \in E$.

Let $A = \begin{pmatrix} I_r & D \end{pmatrix}$ be an $\mathbb{F}_2$-representation of $M \setminus \{e, f\}$ as in Lemma 6.6. Since $M \setminus e$ and $M \setminus f$ are both binary, there exist $v_f, v_e \in \mathbb{F}_2^r$ such that $M \setminus e$ is represented by $\begin{pmatrix} I_r & D & v_f \end{pmatrix}$ and $M \setminus f$ by $\begin{pmatrix} I_r & D & v_e \end{pmatrix}$. Let M' be the matroid on the columns of $\begin{pmatrix} I_r & D & v_e & v_f \end{pmatrix}$. Then $M \setminus e = M' \setminus e$ and $M \setminus f = M' \setminus f$. Let $Z \subseteq E$ be a minimal subset that is independent in one of M, M' but not the other. Then $x, y \in Z$ and Z is a circuit in whichever M, M' independence fails. So let M_i denote whichever has Z as an independent set and M_c whichever has Z as a circuit.

We claim that if J is independent in M_i containing Z then $J = \{e, f\}$. Before proving this claim, we show how it implies the desired result. It follows from our claim that $Z = \{e, f\}$ since

$\{e, f\} \subseteq Z \subseteq J = \{x, y\}$. It then follows that the rank of M_i is 2 since some basis of M_i contains Z as it is independent and the only independent set of M_i containing Z is $\{e, f\}$ by our claim. We now know that $M_i, M_c, M_i \setminus \{e, f\}$ and $M_c \setminus \{e, f\}$ have rank 2 and thus M_i and M_c have at least four elements. Since M is simple and equal to either M_i or M_c, $M = U_{2,n}$ for some $n \geq 4$. If $n > 4$ then deleting $n - 4$ elements yields a minor isomorphic to $U_{2,4}$ which is not $\mathbb{F}_2$-representable. But M was assumed to have no proper minor that was not $\mathbb{F} - 2$-representable so $M = U_{2,4}$.

Now we prove the claim. Suppose the claim fails, i.e. that J is independent in M_i containing Z and that $S := J \setminus \{x, y\} \neq \emptyset$. Then S is independent in $M_i \setminus \{e, f\}$ and $M_c \setminus \{e, f\}$ and therefore in M_i, M_c. Thus the matroids $N_i := M_i/S$ and $N_c := M_c/S$ have the same rank. Since each of N_i, N_c is a proper minor either of M', which is $\mathbb{F}_2$-representable, or of M which has $\mathbb{F}_2$-representable proper minors, N_i and N_c are both $\mathbb{F}_2$-representable. Then $\{e, f\}$ is dependent in N_c and independent in N_i so $N_c \neq N_i$. However, $N_i \setminus \{e\} = N_c \setminus \{e\}$ and $N_i \setminus \{f\} = N_c \setminus \{f\}$ so $N_i \setminus \{e, f\} = N_c \setminus \{e, f\}$.

Now let B be a basis of this matroid. Then B is also a basis of N_i and N_c. Indeed, since N_i and N_c have the same rank, B can only fail to be a basis for one if it fails to be a basis for both. In this case, since B fails to be a basis for N_i, then the rank of $N_i \setminus \{e, f\}$ is strictly less than the rank of N_i (and thus the rank of N_c) thus implying that $\{e, f\}$ contains a cocircuit of N_i and N_c, contradicting our assumption that M has no cocircuit of size one or two. Since $N_i \setminus \{e\} = N_c \setminus \{e\}$ and $N_i \setminus \{f\} = N_c \setminus \{f\}$, $C_{N_i}(B, g) = C_{N_c}(B, g)$ for every g in the common ground set of N_i and N_c that does not lie in B. Since N_i and N_c are binary, this implies that $N_i = N_c$ (to see this, think about constructing a representation of either over F_2 given the fundamental circuits with respect to B). But we already saw that $N_i \neq N_c$, so this is a contradiction thus proving our claim. □

4. Exercises

Problem 6.1: Given a matroid M on ground set E and a basis B, prove that for each $e \in E \setminus B$, there exists a unique circuit in $B \cup \{e\}$. Use this to prove that for any connected graph G with spanning tree T, for each $e \in T$ (this is not a typo), there exists a unique minimal cut of G whose only edge in common with T is e.

Problem 6.2: Let $A \in \mathbb{F}^{r \times n}$ have rank r and let $B \in \mathbb{F}^{(n-r) \times n}$ have rank $n - r$ and assume that $AB^T = 0$. Show that there exists a nonzero $\lambda \in \mathbb{F}$ such that for any $S \subseteq E$ of size r, if A_S denotes the column-submatrix of A on columns indexed by S and $B_{\{1,\ldots,n\} \setminus S}$ denotes the column-submatrix of B on columns indexed by $\{1, \ldots, n\} \setminus S$, then $\det(A_S) = \lambda \det(B_{\{1,\ldots,n\} \setminus S})$.

Problem 6.3: Prove Proposition 6.9 and describe the rank function, closure operator, and lattice of flats of M/e.

Problem 6.4: Prove that $\mathcal{M}(K_{3,3})^*$ is not graphic.

Problem 6.5: Prove directly, without using matroid duality, that M/e is representable over a field $\mathbb{F}$ whenever M is [hint: obtain a representation of M/e from a representation of M by projecting all columns not corresponding to e onto the hyperplane orthogonal to e].

CHAPTER 7

Oriented matroids

1. Ordered fields

Definition 7.1: An ***ordered field*** consists of a field $\mathbb{F}$ and a set $P \subseteq \mathbb{F}$ called ***positive elements*** satisfying the following properties:

(1) $-1 \notin P$,
(2) $x + y \in P$ and $xy \in P$ whenever $x, y \in P$,
(3) $x^2 \in P$ for all $x \in \mathbb{F}$, and
(4) $x \in P$ or $-x \in P$ for all $x \in \mathbb{F}$, i.e. $\mathbb{F} = P \cup (-P)$.

As the name suggests, every ordered field comes naturally equipped with a total order. More specifically, one can define an order $\leq$ by $x \leq y$ if and only if $y - x \in P$. The quintessential example of an ordered field is $\mathbb{R}$ or any of its subfields.

Proposition 7.2: *Let $\mathbb{F}$ be an ordered field with positive elements P. Then:*

(1) $1 \in P$,
(2) $P \cap (-P) = \{0\}$, *and*
(3) *if $\mathbb{K} \subseteq \mathbb{F}$ is a subfield then $\mathbb{K}$ is also ordered with positive elements $P \cap \mathbb{K}$.*

Proof. The first claim follows from ordered field axioms (1) and (4) and the third claim is immediate. Ordered field axiom (4) and the fact that $0 = -0$ holds in any field implies that $0 \in P \cap (-P)$. For the sake of contradiction, let $x \in P \cap (-P)$ and assume $x \neq 0$. Axiom (3) then implies $\frac{1}{x^2} \in P$ and since $-x \in P$, (2) implies $-\frac{1}{x} \in P$. Since $x \in P$, this would imply $-1 \in P$ contradicting (1). □

Given an ordered field $\mathbb{F}$ with positive elements P, the ***sign*** of $x \in \mathbb{F}$ is defined as follows

$$\operatorname{sign}(x) := \begin{cases} + & \text{if } x \notin (-P) \\ - & \text{if } x \notin P \\ 0 & \text{if } x = 0. \end{cases}$$

Given $v \in \mathbb{F}^n$, we define $\operatorname{sign}(v) \in \{+, -, 0\}^n$ by $\operatorname{sign}(v)_i := \operatorname{sign}(v_i)$. The ***support*** of some $\sigma \in \{+, -, 0\}^n$ is the subset $S \subseteq \{1, \ldots, n\}$ such that $\sigma_i \neq 0$ if and only if $i \in S$. Given a matrix $A \in \mathbb{F}^{r \times n}$, the ***signed vectors*** of A is the set

$$\{\operatorname{sign}(v) : Av = 0\}$$

and the ***signed circuits*** of A are the signed covectors of minimal nonempty support. The set of signed circuits of a matrix is highly structured. Their supports must satisfy the circuit axioms for a matroid, but even more is true and this motivates the definition of an oriented matroid, which we will provide in the next section.

2. Oriented matroid axiomatics

Let F be a field or the set $\{+,-,0\}$ and let E be a finite set. We use the notation S^E to denote the set of functions $E \to F$ which one should think of as the set of vectors with coordinates indexed by E whose coordinates take values in F. Given $x \in F^E$, the ***support of*** x, denoted $\operatorname{supp}(x)$, is the subset $S \subseteq E$ satisfying $x_e = 0$ if and only if $e \in S$.

Given a finite set E and sign vectors $\sigma, \tau \in \{+,-,0\}^E$, the ***composition*** $\sigma \circ \tau$ is the sign vector defined by

$$(\sigma \circ \tau)_e := \begin{cases} \sigma_i & \text{if } \sigma_i \neq 0 \\ \tau_i & \text{otherwise.} \end{cases}$$

Note that if $v, w \in \mathbb{F}^E$ and if $\varepsilon > 0$ is sufficiently small, then

$$\operatorname{sign}(v + \varepsilon w) = \operatorname{sign}(v) + \operatorname{sign}(w).$$

Given an oriented matroid $\mathcal{O} = (E, \mathcal{C})$, the ***signed vectors of*** $\mathcal{O}$ is the set

$$\{\eta \in \{+,-,0\}^E : \eta = \sigma \circ \tau \text{ for some } \sigma, \tau \in \mathcal{C}\}.$$

Definition 7.3: An ***oriented matroid*** $\mathcal{O} = (E, \mathcal{V})$ consists of a finite set E, called the ***ground set*** and a set $\mathcal{V} \subset \{+,-,0\}^E$ called the ***signed vectors*** satisfying

(1) the all-zeros vector is in $\mathcal{V}$,
(2) if $\sigma \in \mathcal{V}$ then $-\sigma \in \mathcal{V}$,
(3) if $\sigma, \tau \in \mathcal{V}$, then $\sigma \circ \tau \in \mathcal{V}$, and
(4) given $\sigma, \tau \in \mathcal{V}$ with $\sigma \neq -\tau$ and $e \in \operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau)$ with $\sigma_e = -\tau_e$, there exists $\eta \in \mathcal{V}$ such that
   (a) $\eta_e = 0$,
   (b) if $\eta_f = +$ then $\sigma_f = +$ or $\tau_f = +$,
   (c) if $\eta_f = -$ then $\sigma_f = -$ or $\tau_f = -$,
   (d) if $\sigma_f, \tau_f \in \{+, 0\}$, not both zero, then $\eta_f = +$, and
   (e) if $\sigma_f, \tau_f \in \{-, 0\}$, not both zero, then $\eta_f = -$.

Proposition 7.4: *Let $\mathbb{F}$ be an ordered field and let $A \in \mathbb{F}^{r \times n}$. If E denotes the column set of A and $\mathcal{V}$ is the signed vectors, then $\mathcal{O} = (E, \mathcal{V})$ is an oriented matroid.*

Proof. For any matrix A, it is true that $A0 = 0$ and that if $Ax = 0$ then $A(-x) = 0$. Thus the first two axioms are satisfied. Now let x, y be such that $Ax = Ay = 0$. Then $\operatorname{sign}(x) \circ \operatorname{sign}(y) = \operatorname{sign}(x + \varepsilon y)$ for $\varepsilon > 0$ sufficently small so the third axiom is satisfied. For the fourth axiom, assume that $e \in \operatorname{supp}(x) \cap \operatorname{supp}(y)$ and that $\operatorname{sign}(x)_e = -\operatorname{sign}(y)_e$. Define

$$z := x + \frac{|x_e|}{|y_e|} y.$$

Then $\operatorname{sign}(z)$ satisfies the desired conditions for $\sigma = \operatorname{sign}(x)$ and $\tau = \operatorname{sign}(y)$. □

The oriented matroid defined from a matrix A with entries in an ordered field as in Proposition 7.4 is denoted $\mathcal{O}(A)$. If $\mathcal{O} = \mathcal{O}(A)$ for some $\mathbb{F}$-matrix A, then $\mathcal{O}$ is said to be ***$\mathbb{F}$-representable***.

Define the relation $\preceq$ on $\{+,-,0\}^E$ by $\sigma \preceq \tau$ if $\sigma_e = +$ implies $\tau_e = +$ and $\sigma_e = -$ implies $\tau_e = -$. Then $\preceq$ is symmetric, transitive, and anti-symmetric i.e. a partial order.

Proposition 7.5: *Let $\mathcal{O} = (E, \mathcal{V})$ be an oriented matroid. Given $\sigma \in \mathcal{V}$, there exist signed circuits $\tau^1, \ldots, \tau^k$ such that $\sigma = \tau^1 \circ \cdots \circ \tau^k$.*

Proof. Let $\{\tau^1, \ldots, \tau^k\}$ be the set of all signed circuits satisfying $\tau \prec \sigma$. For each $i = 1, \ldots, k$ and each $e \in E$, either $\tau^i_e = \sigma_e$ or $\tau^i_e = 0$. Therefore $\tau^1 \circ \cdots \circ \tau^k \prec \sigma$. It now suffices to show that for each $e \in \operatorname{supp}(\sigma)$, there exists some circuit $\tau \prec \sigma$ satisfying $\tau_e = \sigma_e$. So let $e \in \operatorname{supp}(\sigma)$ and let $\tau \in \mathcal{V}$ have minimal support such that $\tau \preceq \sigma$ and $\tau_e \neq 0$. If for all $f \in \operatorname{supp}(\sigma)$ we have either $\tau_f = 0$ or $\tau_f = \sigma_f$ Otherwise, signed vector axiom (4) applied to τ and σ at f contradicts our minimality assumption. □

Proposition 7.6: *Let $\mathcal{O} = (E, \mathcal{V})$ be an oriented matroid with signed circuits $\mathcal{C}$. Then $\operatorname{supp}(\mathcal{C}) := \{\operatorname{supp}(\sigma) : \sigma \in \mathcal{C}\}$ is the circuit set of a matroid.*

Proof. That $\operatorname{supp}(\mathcal{C})$ satisfies the first two circuit axioms is immediate from the fact that the all-zero signed vector is not a signed circuit, and that signed circuits are support-minimal. We now show that $\operatorname{supp}(\mathcal{C})$ satisfies the third. Indeed, let $\sigma, \tau \in \mathcal{C}$ with $e \in \operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau)$. Then signed vector axiom (4) implies there exists some $\rho \in \mathcal{V}$ such that $\operatorname{supp}(\rho) \subseteq \operatorname{supp}(\sigma) \cup \operatorname{supp}(\tau) \setminus \{e\}$. Proposition 7.5 implies that $\rho = \eta_1 \circ \cdots \circ \eta_k$ for $\eta_1, \ldots, \eta_k \in \mathcal{C}$. Then $\operatorname{supp}(\eta_1)$ certifies that the desired axiom is satisfied. □

Given an oriented matroid $\mathcal{O}$, we write $\mathcal{M}(\mathcal{O})$ to denote the matroid from Proposition 7.6.

Proposition 7.7: *Let $\mathcal{O}$ be an oriented matroid and let $\mathbb{F}$ be an ordered field. If $\mathcal{O}$ is $\mathbb{F}$-realizable, then so is $\mathcal{M}(\mathcal{O})$.*

Proof. If $\mathcal{O} = \mathcal{O}(A)$ for some matrix A, then $\mathcal{M}(\mathcal{O}) = \mathcal{M}(A)$. □

3. Duality

Given sign vectors $\sigma, \tau \in \{+, -, 0\}^E$ we say that σ and τ are ***orthogonal*** and write $\sigma \cdot \tau = 0$ if either $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau) = 0$, or if there exist $e, f \in \operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau)$ such that $\sigma_e = \tau_e$ and $\sigma_f = -\tau_f$. Given an oriented matroid $\mathcal{O} = (E, \mathcal{V})$, the ***dual oriented matroid*** $\mathcal{O}*$ is the pair $(E, \mathcal{V}^*)$ where

$$\mathcal{V}^* := \{\sigma \in \{+, -, 0\} : \sigma \cdot \tau = 0 \text{ for all } \tau \in \mathcal{V}\}.$$

Proposition 7.8: *Let $\mathbb{F}$ be an ordered field and let $A \in \mathbb{F}^{r \times n}$ have rank r. Let $B \in \mathbb{F}^{(n-r) \times n)}$ have rank $n - r$ and assume $AB^T = 0$. Then $\mathcal{O}(A)^* = \mathcal{O}(B)$.*

Proposition 7.9: *Let $\mathcal{O} := (E, \mathcal{V})$ be an oriented matroid. Then $\mathcal{O}^*$ is also an oriented matroid.*

Proof. Vector axioms (1) and (2) are simple to verify for $\mathcal{O}^*$. For axioms (3) and (4), let $\sigma, \tau \in \mathcal{V}^*$ and $\eta \in \mathcal{V}$. If $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\eta) \neq \emptyset$ then let $e, f \in \operatorname{supp}(\sigma) \cap \operatorname{supp}(\eta)$ be such that $\sigma_e = \eta_e$ and $\sigma_f = -\eta_f$. Then $(\sigma \circ \tau) \cdot \eta = 0$ since in this case $(\sigma \circ \tau)_e = \sigma_e$ and $(\sigma \circ \tau)_f = \sigma_f$. On the other hand, if $\operatorname{supp}(\sigma) \cap \operatorname{supp}(\eta) = \emptyset$ then $\operatorname{supp}(\sigma \circ \tau) \cap \operatorname{supp}(\eta) = \operatorname{supp}(\tau) \cap \operatorname{supp}(\eta)$ and so $(\sigma \circ \tau) \cdot \eta = 0$ since $\tau \cdot \eta = 0$. Therefore vector axiom (3) holds for $\mathcal{V}^*$.

Now assume $e \in \operatorname{supp}(\sigma) \cap \operatorname{supp}(\tau)$ such that $\sigma_e = -\tau_e$. Consider the set $S \subseteq \mathcal{V}^*$ consisting of elements η such that $\eta_e = 0$, $\eta_f = +$ whenever one of σ_f, τ_f is $+$ and neither is $-$, and similarly for $-$, and $\eta_f = 0$ if $\sigma_f = \tau_f = 0$. By construction, every element of S satisfies the desired properties for vector axiom (4). Assume for the sake of contradiction that for each $\eta \in S$ there exists $\rho \in \mathcal{V}$ such that $\eta \cdot \rho \neq 0$. TODO FINISH □

Proposition 7.10: *Let $\mathcal{O}$ be an oriented matroid. Then $\mathcal{O}^{**} = \mathcal{O}$.*

Proof. It follows from the definition of a dual oriented matroid that if σ is a signed vector of $\mathcal{O}$, then it is also a signed vector of $\mathcal{O}^{**}$. Therefore, in light of Proposition 7.5, it suffices to show that every signed circuit of $\mathcal{O}^{**}$ is a signed circuit of $\mathcal{O}$. Let σ be a signed circuit of $\mathcal{O}^{**}$. Then $\operatorname{supp}(\sigma)$ is a circuit of $\mathcal{M}(\mathcal{O})$ since each (non-oriented) matroid is isomorphic to its double dual. So there exists a signed circuit τ of $\mathcal{O}$ with the same support as σ. This implies that τ is also a vector of $\mathcal{O}^{**}$. If $\tau \neq \pm\sigma$, then we can apply axiom (4) in $\mathcal{O}^{**}$ to obtain a signed vector ρ of $\mathcal{O}^{**}$ such that $\operatorname{supp}(\rho) \subsetneq \operatorname{supp}(\sigma)$. This contradicts that σ is a signed circuit of $\mathcal{O}^{**}$. □

The oriented matroid of a matrix $A \in \mathbb{F}^{r\times n}$ only depends on the linear space spanned by the rows of A. In particular, $\mathcal{O}(A) = \{\operatorname{sign}(x) : yx = 0 \text{ for all } y = zA, z \in (\mathbb{R}^r)^*\}$. It then follows from Proposition 7.10 that $\mathcal{O}^*(A) = \{\operatorname{sign}(x) : x = zA, z \in (\mathbb{R}^r)^*\}$.

As with ordinary matroids, we use the prefix "co" when talking about objects associated dual oriented matroids. In particular, the signed circuits and signed vectors of $\mathcal{O}^*$ are called the ***signed cocircuits*** and ***signed covectors*** of $\mathcal{O}^*$.

4. Low rank

Just as with ordinary matroids, we can represent oriented matroids of rank three pictorially using lines and dots. We will focus exclusively on the representable case. So let $A \in \mathbb{R}^{d\times n}$. We will think of the columns of A as points in d-dimensional space. If none of the columns are zero, we can pick a linear functional $f \in (\mathbb{R}^d)^*$ such that $fa \neq 0$ for each column a of A. Then, we associate A with the point configuration

$$\{\frac{a}{fa} : a \text{ is a column of } A\}$$

and label those for which $fa > 0$ "positive" and those for which $fa < 0$ "negative." This new point configuration lies in the affine hyperplane $\{x \in \mathbb{R}^d : fx = 1\}$ which we view simply as $\mathbb{R}^{d-1}$. We will color the positive points black and the negative ones white. For example, let A be the following matrix

$$A = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}$$

and denote its columns by $a_1, \dots, a_6$. Let e_1, e_2, e_3 be the standard basis of $\mathbb{R}^3$ with dual basis e_1^*, e_2^*, e_3^*. Define $f := e_1^* + e_2^* - 5e_3^*$. Then the positive points are a_1, a_2, a_4 and the negative points are a_3, a_5, a_6. Normalizing by f gives the new point configuration

$$\begin{pmatrix} 1 & \frac{1}{2} & -\frac{1}{3} & 0 & 0 & 0 \\ 0 & \frac{1}{2} & -\frac{1}{3} & 1 & -\frac{1}{4} & 0 \\ 0 & 0 & -\frac{1}{3} & 0 & -\frac{1}{4} & -\frac{1}{5} \end{pmatrix}.$$

We drop the third row to get a point configuration in $\mathbb{R}^2$. We now draw this, coloring the positive points black and the negative ones white to get the picture in Figure 7.4.1. These pictures give us a simple interpretation of the signed circuits of the resulting oriented matroid. Let σ be a signed circuit and let τ obtained from σ by negating every entry on a negative point. Then, the convex hull of the negative points in τ must intersect the convex hull of the positive points in τ and removing any nonzero point of τ destroys this property. Conversely, given disjoint subsets A and B of points whose convex hulls intersect, and are minimal with respect to this property, let τ be the sign vector that is positive on A and negative on B. Let σ be obtained from τ

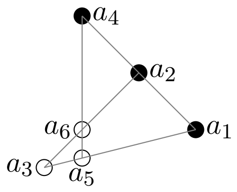


FIGURE 7.4.1. Two-dimensional picture of a rank-three oriented matroid

by negating all the negative points. Then σ is a signed circuit of the oriented matroid. For example, from Figure 7.4.1, we can see that e.g. the following are signed circuits of $\mathcal{O}(A)$

$$(+-0+00) \qquad (+-00+-) \qquad (000+-+).$$

We can also read off the signed cocircuits from such a picture. In particular, for each pair of points $e, f \in E$ let $l \in (\mathbb{R}^d)^*$ and $c \in \mathbb{R}$ be such that $l(e) = l(f) = c$. Define a sign vector $\tau \in \{+,-,0\}^E$ by $\tau_g = 0$ of $l(g) = c$, $\tau_g = +$ if $l(g) > c$ and $\tau_g = -$ if $l(g) < c$. This computation can be done just using the picture by looking at each line through at least two points, setting the points on the line to zero, and setting the points on one side positive and the other negative. Then define σ to be obtained from τ by negating all entries corresponding to negative points in the picture. In this case, σ is a signed cocircuit of $\mathcal{O}$. This enables us to e.g. read off the following signed cocircuits from Figure 7.4.1

$$(+00--0) \qquad (0++++0) \qquad (0+0+0-).$$

5. Gale diagrams of polytopes

Oriented matroids give us a way to construct and visualize polytopes in more than three dimensions, as long as they don't have too many vertices. The main result of this section will be a construction of an eight-dimensional polytope with twelve vertices that is not combinatorially equivalent to any polytope with rational vertices.

Given an oriented matroid $\mathcal{O}$ and an ordered field $\mathbb{F}$, we say that $\mathcal{O}$ is ***$\mathbb{F}$-realizable*** if there exists a matrix $A \in \mathbb{F}^{d\times n}$ such that $\mathcal{O} = \mathcal{O}(A)$.

Definition 7.11: Let $P \subseteq \mathbb{R}^d$ be a d-dimensional polytope with vertex set $\{v_1, \dots, v_n\}$. The ***oriented matroid of*** P, denoted $\mathcal{O}(P)$, is $\mathcal{O}(A)$ where $A \in \mathbb{R}^{(d+1)\times n}$ is defined as follows

$$A := \begin{pmatrix} 1 & 1 & \dots & 1 \\ v_1 & v_2 & \dots & v_n \end{pmatrix}.$$

We say that an oriented matroid $\mathcal{O}$ is ***acyclic*** if it has no positive circuit and ***totally cyclic*** it has no positive cocircuit. These are dual notions: $\mathcal{O}$ is acyclic if and only if $\mathcal{O}^*$ is totally cyclic.

Theorem 7.12: *Let $\mathcal{O}$ be an oriented matroid. Then there exists a polytope P such that $\mathcal{O} = \mathcal{O}(P)$ if and only if*

(1) *$\mathcal{O}$ is $\mathbb{R}$-representable,*
(2) *$\mathcal{O}$ is acyclic, and*
(3) *every circuit of $\mathcal{O}$ has at least two positive elements.*

In this case P has n vertices and dimension $r-1$ where r is the rank of $\mathcal{O}$ and n is the size of its ground set.

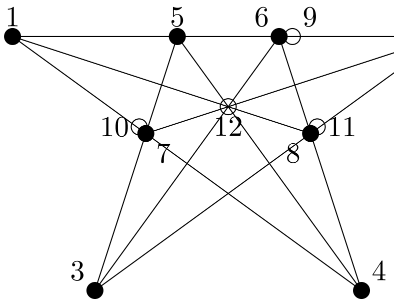


FIGURE 7.5.2. The Gale diagram of an 8-dimensional polytope with 12 vertices that has a non-rational vertex.

PROOF. TODO □

Given a matrix $A \in \mathbb{R}^{d \times n}$ of rank d, we say that $B \in \mathbb{R}^{(n-d) \times n}$ is a ***Gale dual of*** A if it has rank $(n-d)$ and if $AB^T = 0$. In this case we may also say that A and B are ***Gale duals***. Note that if A and B are Gale duals, then $\mathcal{O}(A)^* = \mathcal{O}(B)$. We say that B is a ***Gale diagram*** of a polytope P if $\mathcal{O}(B) = \mathcal{O}(P)^*$. Theorem 7.12 gives us the following characterization of Gale diagrams of polytopes as a corollary.

Corollary 7.13: *Let $B \in \mathbb{R}^{(n-d-1) \times d}$ have rank $n-d-1$. Then B is the Gale diagram of a polytope P if and only if $\mathcal{O}(B)$ is totally cyclic and every cocircuit has at least two positive elements. In this case, P has n vertices and dimension d.*

Given a matrix $B \in \mathbb{R}^{(n-d-1) \times d}$ of rank $n-d-1$ satisfying the conditions of Corollary 7.13, we let $\mathcal{P}(B)$ denote the polytope with Gale diagram B.

Proposition 7.14: *Let $\mathbb{F}$ be an ordered field and let $A \in \mathbb{F}^{d \times n}$ with columns $a_1, \ldots, a_n$. Then σ is a signed covector of $\mathcal{O}(A)$ if and only if there exists $b \in (\mathbb{F}^d)^*$ such that*

(1) *$ba_i = 0$ if $\sigma_i = 0$,*
(2) *$ba_i < 0$ if $\sigma_i = -$, and*
(3) *$ba_i > 0$ if $\sigma_i = +$.*

PROOF. Let $B \in \mathbb{F}^{(n-d) \times d}$ have rank $n-d$ such that $AB^T = 0$. Then $\mathcal{O}(A)^* = \mathcal{O}(B)$ by Proposition 7.8. Then σ is a signed vector of $\mathcal{O}(B)$, and therefore a signed covector of $\mathcal{O}(A)$, if and only if there exists some $x \in \mathbb{F}^n$ such that $Bx = 0$ and $\operatorname{sign}(x) = \sigma$. Our assumptions on A, B imply that the columns of A^T are a basis of $\ker(B)$. Thus $x = A^T y$ for some $y \in \mathbb{R}^d$. The desired b is then y^T. □

Proposition 7.15: *Let $P, Q \subseteq \mathbb{R}^d$ be polytopes of dimension d. If P and Q are combinatorially equivalent, then $\mathcal{O}(P)$ and $\mathcal{O}^*(P)$ have the same positive cocircuits.*

PROOF. This follows immediately from Proposition 7.14 and the fact that all faces of a polytope are exposed (Proposition 2.11). □

Example 7.16: TODO: insert example of two combinatorially equivalent polytopes with different oriented matroids

Theorem 7.17: *Let $\mathcal{O}$ be as in Figure 7.5.2. Then*

(1) *$\mathcal{O}$ is the Gale diagram of an 8-dimensional polytope P,*
(2) *any $\mathbb{R}$-representable oriented matroid $\hat{\mathcal{O}}$ of rank 3 with the same positive circuits as $\mathcal{O}$ has $\mathcal{M}(\hat{\mathcal{O}}) = \mathcal{M}(\mathcal{O})$, and*
(3) *any polytope combinatorially equivalent to P has a non-rational vertex.*

Proof. Corollary 7.13 implies that the first claim follows once we verify that $\mathcal{O}$ has no positive cocircuit, and that every cocircuit has at least two positive elements. This can be done by checking the lines in Figure 7.5.2. For the second claim, let $\mathcal{O}'$ be an oriented matroid with the same positive circuits as $\mathcal{O}$ and let B be a matrix such that $\mathcal{O}(B) = \mathcal{O}'$. Then $\mathcal{M}(\mathcal{O}')$ has no rank-zero flats aside from the empty set. Then the rank-one flats of $\mathcal{M}(\mathcal{O}')$ are precisely those of $\mathcal{M}(\mathcal{O})$ (in particular note that those with two elements are $\{6,9\}, \{7,10\}, \{8,11\}$ since these are the only two-element positive circuits). The following are all positive circuits of $\mathcal{O}$ and therefore of $\mathcal{O}'$

1,2,9	1,8,12	1,4,10	2,5,9	2,7,12
2,3,11	3,5,10	3,6,12	4,5,12	4,6,11.

Thus the rank-two flats of $\mathcal{M}(\mathcal{O})$ with three or more elements also have rank two in $\mathcal{M}(\mathcal{O})$. Since B has rank three, its only rank-three flat is the whole ground set. Thus $\mathcal{M}(\mathcal{O}) = \mathcal{M}(\mathcal{O}')$ since they have the same lattice of flats, the same parallel elements, and no loops. Since $\mathcal{M}(\mathcal{O}') \setminus \{9, 10, 11\}$ is matroid given in Figure 5.2.1, it is not representable over $\mathbb{Q}$. Proposition 6.10 then implies that $\mathcal{M}(\mathcal{O}')$ is also not representable over $\mathbb{Q}$ and Proposition 7.7 implies that neither is $\mathcal{O}'$. Thus the second claim is proven.

Now let P' be a polytope that is combinatorially equivalent to P. Proposition 7.15 and the second claim imply that the oriented matroid of any Gale diagram of P' is not $\mathbb{Q}$-representable. In particular, if the columns of A are the vertices of P' and B is a Gale diagram of P', then $AB^T = 0$ and therefore A has an irrational entry. Thus P is not combinatorially equivalent to any polytope with rational vertices. □

CHAPTER 8

Algebraic matroids

1. Field theory preliminaries

Given fields $\mathbb{K}$ and $\mathbb{F}$, we say that $\mathbb{K}$ is a ***field extension of*** $\mathbb{F}$ if $\mathbb{F} \subseteq \mathbb{K}$. We notate this by $\mathbb{K}/\mathbb{F}$. Given a field extension $\mathbb{K}/\mathbb{F}$ and $S \subseteq \mathbb{K}$, we let $\mathbb{F}(S)$ denote the minimal subfield of $\mathbb{K}$ containing $\mathbb{F}$ and S. If $\mathbf{x}$ is a set of indeterminates then $\mathbb{F}[\mathbf{x}]$ denotes the polynomial ring with coefficients in $\mathbb{F}$ and indeterminate set $\mathbf{x}$. Unless otherwise stated, $\mathbf{x}$ will denote the set $\{x_1, \dots, x_n\}$. Given $\mathbb{K}/\mathbb{F}$ and $S \subseteq \mathbb{K}$, one says that S is ***(algebraically) independent over*** $\mathbb{F}$ if $f(s_1, \dots, s_n) \neq 0$ for all $s_1, \dots, s_n \in S$ and $f \in \mathbb{F}[\mathbf{x}]$; otherwise, one says that S is ***(algebraically) dependent over*** $\mathbb{F}$. We will abuse notation and say that $s \in \mathbb{K}$ is (in)dependent over $\mathbb{F}$ to mean that $\{s\}$ is. A field extension $\mathbb{K}/\mathbb{F}$ is ***algebraic*** if s is algebraically dependent over $\mathbb{F}$ for all $s \in \mathbb{K}$.

Lemma 8.1: *Let $\mathbb{K}/\mathbb{F}$ be a field extension. A given $s \in \mathbb{K}$ is algebraically dependent over $\mathbb{F}$ if and only if $\mathbb{F}(s)/\mathbb{F}$ is finite dimensional as an $\mathbb{F}$-vector space. If $\mathbb{K}/\mathbb{F}$ is finite-dimensional as an $\mathbb{F}$-vector space then it is algebraic.*

Proof. Let $s \in \mathbb{K}$. If $\mathbb{F}(s)$ is d-dimensional as an $\mathbb{F}$-vector space then $\{1, s, \dots, s^n\}$ is linearly dependent over $\mathbb{F}$. In other words, there exist $f_0, \dots, f_n \in \mathbb{F}$ such that $f_0 + f_1 s + \cdots + f_n s^n = 0$. Define $f := f_0 + f_1 x + \cdots + f_n x^n \in \mathbb{F}[\mathbf{x}]$. Then $f(s) = 0$ so s is algebraically dependent over $\mathbb{F}$.

Conversely, if s satisfies a polynomial $p \in \mathbb{F}[x]$ of degree d, then s satisfies an irreducible factor of p and so we may assume p is irreducible (over $\mathbb{F}$) without loss of generality. The $\mathbb{F}$-algebra homomorphism $\mathbb{F}[x] \to \mathbb{F}(s)$ obtained by sending x to s then has $\langle p \rangle$ as its kernel so $\mathbb{F}(s)$ contains an isomorphic copy of $\mathbb{F}[x]/\langle p \rangle$. Since p is irreducible, $\langle p \rangle$ is a maximal ideal of $\mathbb{F}[x]$ and therefore $\mathbb{F}[x]/\langle p \rangle$ is a field. But $\mathbb{F}(s)$ is the minimal subfield of $\mathbb{K}$ containing both s and $\mathbb{F}$, both of which lie in the isomorphic copy of $\mathbb{F}[x]/\langle p \rangle$, thus implying that $\mathbb{F}(s) \cong \mathbb{F}[x]/\langle p \rangle$. Finally, note that $\mathbb{F}[x]/\langle p \rangle$ is d-dimensional as an $\mathbb{F}$-vector space.

Now assume $\mathbb{K}/\mathbb{F}$ is n-dimensional for some finite n and let $s \in \mathbb{K}$. As before, the coefficients of the linear dependence among $\{1, s, s^2, \dots, s^d\}$ give the coefficients of the polynomial vanishing on s. Therefore $\mathbb{K}/\mathbb{F}$ is algebraic. □

Not all algebraic field extensions are finite dimensional. To see this define $S_n := \{(\sqrt[n]{2})O^i : 0 \leq i \leq n-1\}$ and $S := \bigcup_{n=2}^{\infty}$. Then $\mathbb{Q}(S)$ is a subfield of $\mathbb{C}$ that is algebraic over $\mathbb{Q}$, but each S_n is a $\mathbb{Q}$-linearly independent set for every n.

Lemma 8.2: *Let $\mathbb{F}/\mathbb{L}$ be an algebraic field extension and let $\mathbb{K}/\mathbb{F}$ be a (possibly non-algebraic) field extension. Then each $s \in \mathbb{K}$ is algebraic over $\mathbb{F}$ if and only it is algebraic over $\mathbb{L}$. In particular, if $\mathbb{K}/\mathbb{F}$ is algebraic then so is $\mathbb{K}/\mathbb{L}$.*

Proof. Let $s \in \mathbb{K}$. If s is algebraic over $\mathbb{L}$ then it is also algebraic over $\mathbb{F}$ since $\mathbb{L}[x]$ is a subring of $\mathbb{F}[x]$. Now assume s is algebraic over $\mathbb{F}$ and let $p \in \mathbb{F}[x]$ be irreducible such that

$p(s) = 0$. Let $c_1, \ldots, c_k$ be the coefficients of p. Then s is algebraic over the subfield $\mathbb{L}(c_1, \ldots, c_k)$ of $\mathbb{F}$. Induction on k it now suffices to show that if s is algebraic over $\mathbb{L}(c)$ for some $c \in \mathbb{F}$, then s is algebraic over $\mathbb{L}$. Since $\mathbb{F}$ and therefore c is algebraic over $\mathbb{L}$, Lemma 8.1 implies that $\mathbb{L}(c)$ is d_1-dimensional as an $\mathbb{L}$-vector space for some finite d_1. Similarly, $\mathbb{L}(c)(s)$ is d_2-dimensional as an $\mathbb{L}(c)$-vector space. This implies that $\mathbb{L}(c)(s)$ is at most $d_1 d_2$-dimensional as an $\mathbb{L}$-vector space. In particular, it is finite dimensional. Since $\mathbb{L}(s)$ is an $\mathbb{L}$-vector subspace of $\mathbb{L}(c)(s)$, it is finite dimensional as well. Lemma 8.1 now implies that s is algebraic over $\mathbb{L}$. □

Definition 8.3: A ***transcendence basis*** of a field extension $\mathbb{K}/\mathbb{F}$ is a set $S \subseteq \mathbb{K}$ such that $\mathbb{K}/\mathbb{F}(S)$ is algebraic. A field extension $\mathbb{K}/\mathbb{F}$ is ***finitely generated*** if $\mathbb{K} = \mathbb{F}(S)$ for some finite set $S \subseteq \mathbb{K}$.

Proposition 8.4: *Let $\mathbb{K}/\mathbb{F}$ be a finitely generated field extension. Then there exists a finite cardinality k such that every transcendence basis of $\mathbb{K}/\mathbb{F}$ has cardinality k.*

Proof. Since $\mathbb{K}/\mathbb{F}$ is finitely generated we may write $\mathbb{K} = \mathbb{F}(s_1, \ldots, s_n)$. Without loss of generality assume that $s_1, \ldots, s_k$ are algebraically independent over $\mathbb{K}$ and that $\{s_1, \ldots, s_k, s_{k+i}\}$ is algebraically dependent for each $i \geq 1$. Then $\mathbb{F}(s_1, \ldots, s_{k+l})$ is finite dimensional over $\mathbb{F}(s_1, \ldots, s_{k+l-1})$ for each $l \geq 1$ and therefore algebraic by Lemma 8.1. Lemma 8.2 then implies that $\mathbb{K}$ is algebraic over $\mathbb{F}(s_1, \ldots, s_k)$. Therefore $\{s_1, \ldots, s_k\}$ is a transcendence basis of $\mathbb{K}/\mathbb{F}$ since it is algebraically independent.

Now assume $T \subseteq \mathbb{K}$ is another transcendence basis and assume $|T| \geq k$ without loss of generality. We proceed by induction on $k - |\{s_1, \ldots, s_k\} \cap T|$. In the base case, where $s_i \in T$ for $1 \leq i \leq k$, we have $T = \{s_1, \ldots, s_k\}$ since $T \subseteq \mathbb{K}$ is algebraically independent. Otherwise, let $t \in T$ such that $t \neq s_i$ for all $1 \leq i \leq k$. Since $\{t, s_1, \ldots, s_k\}$ is algebraically dependent over $\mathbb{F}$ there exists a polynomial $f \in \mathbb{F}[y, x_1, \ldots, x_k]$ such that $f(t, s_1, \ldots, s_k) = 0$. Since $\{t\}$ and $\{s_1, \ldots, s_k\}$ are each algebraically independent, we may write as follows, relabeling the $s_1, \ldots, s_k$ if necessary

$$f = \sum_{i=0}^{d} f_i(t, s_2, \ldots, s_k) s_1^i$$

where $d \geq 1$ and $f_d \neq 0$. But this shows that s_1 is algebraically dependent over $\mathbb{F}(t, s_2, \ldots, s_k)$ Lemma 8.2 then implies that $\mathbb{K}/\mathbb{F}(t, s_2, \ldots, s_k)$ is algebraic. By induction, we then have $\mathbb{K}/\mathbb{F}(t_1, \ldots, t_k)$ is algebraic for some elements $t_1, \ldots, t_k$ of T. But then $T = \{t_1, \ldots, t_k\}$. □

In light of Proposition 8.4, we may define the ***transcendence degree*** of a finitely generated field extension $\mathbb{K}/\mathbb{F}$ by the size of a transcendence basis.

Proposition 8.5: *Let $\mathbb{K}/\mathbb{F}$ be a finitely generated field extension and let $E \subseteq \mathbb{K}$ be finite. Let $\mathcal{I}$ consist of the algebraically independent subsets of E. Then $(E, \mathcal{I})$ is a matroid.*

Proof. We proceed by showing that the set $\mathcal{B}$ of maximal elements of $\mathcal{I}$ satisfies the basis axioms. Each element of $\mathcal{B}$ is a transcendence basis of $\mathbb{F}(E)$ which we without loss of generality assume is equal to $\mathbb{K}$. Proposition 8.4 implies that $\mathbb{K}/\mathbb{F}$ has a transcendence basis so $\mathcal{B}$ is not empty. So let $B_1, B_2 \in \mathcal{I}$ be distinct maximal elements. Write $B_1 = \{s_1, \ldots, s_k\}$ and let $t \in B_2 \setminus B_1$. We proceed as in the proof of Proposition 8.4 to show that $\mathbb{K}$ is algebraic over $\mathbb{F}(t, s_2, \ldots, s_k)$. It now remains to show that $\{t, s_2, \ldots, s_k\}$ is algebraically independent over $\mathbb{F}$. If not, then since $\{s_2, \ldots, s_k\}$ is algebraically independent, we would have that $\mathbb{K}(t, s_2, \ldots, s_k)/\mathbb{K}(s_2, \ldots, s_k)$ is algebraic. Then Lemma 8.2 implies that $\mathbb{K}(s_1,\ldots,s_k)/\mathbb{K}(s_2,\ldots,s_k)$ is algebraic, contradicting that $\{s_1,\ldots,s_k\}$ is algebraically independent. □

Given a finite subset E of a field extension $\mathbb{K}/\mathbb{F}$, the matroid given in Proposition 8.5 is called the ***algebraic matroid of*** E. We denote it $\mathcal{M}(E)$. If $\mathcal{M}=\mathcal{M}(E)$ for some finite subset $E\subseteq\mathbb{K}/\mathbb{F}$, then we say that $\mathcal{M}$ is $\mathbb{F}$***-algebraic*** or ***algebraic over*** $\mathbb{F}$.

2. Geometry of algebraic matroids

Let $\mathbb{F}$ be a field and let $n\geq 1$. The ***variety*** of a set $F\in\mathbb{F}[x_1,\ldots,x_n]$ of polynomials is the set $V(F)\subseteq\mathbb{F}^n$ defined by

$$V(F)=\{(s_1,\ldots,s_n)\in\mathbb{F}^n : f(s_1,\ldots,s_n)=0\text{ for all }f\in F\}.$$

The ideal generated by a set $F\subseteq\mathbb{F}[\mathbf{x}]$ of polynomials is denoted $\langle F\rangle$. Passing from a set of polynomials to the ideal it generates does not change the corresponding variety - see Problem 8.3. We associate to any $S\subseteq\mathbb{F}^n$ the set of polynomials $I(S)\subseteq\mathbb{F}[x_1,\ldots,x_n]$ that vanish when evaluated at any point in S. Formally speaking we define

$$I(S):=\{f\in\mathbb{F}[\mathbf{x}] : f(s)=0\text{ for all }s\in S\}.$$

Then $I(S)$ is an ideal - see Problem 8.4. The ***Zariski closure*** of a set $S\subseteq\mathbb{F}^n$, denoted $\overline{S}$, is the variety $V(I(S))$. It is the smallest variety containing S. Given a variety $V\subseteq\mathbb{F}^n$, the ***coordinate ring of*** V is the ring

$$\mathbb{F}[V]:=\mathbb{F}[\mathbf{x}]/I(V).$$

A variety $V\subseteq\mathbb{F}^n$ is ***irreducible*** if whenever $V=V_1\cup V_2$ for varieties $V_1,V_2\subseteq\mathbb{F}^n$, either $V=V_1$ or $V=V_2$. This is equivalent to the condition that $\mathbb{F}[V]$ is an integral domain (see Problem 8.6). We will focus exclusively on irreducible varieties. This is not a major loss of generality since every variety is the union of finitely many irreducible varieties. We will skip proving this since it requires a major detour into commutative algebra, but the interested reader is advised to consult e.g. [3, Chapter 3] or [4, Chapter 8].

The ***quotient field*** of an integral domain R, denoted $K(R)$, is the minimal field containing R. Concretely, it consists of ordered pairs (a,b) modulo the equivalence relation $(a,b)\sim(c,d)$ if and only if $ad=bc$ and the ring operations are $(a,b)+(c,d)=(ad+bc,bd)$ and $(a,b)(c,d)=(ac,bd)$. The ***dimension*** of an irreducible variety $V\subseteq\mathbb{F}^n$ is defined to be the transcendence degree of the field extension $K(\mathbb{F}[V])/\mathbb{F}$.

We will now argue that this definition of dimension really captures what "dimension" intuitively means. Define an equivalence relation on $\mathbb{F}[x_1,\ldots,x_n]$ by $f\sim g$ if and only if $f(s)=g(s)$ for all $s\in\mathbb{V}$. Then $f\sim g$ if and only if $f=g+h$ for some $h\in I(V)$. In other words, elements of $\mathbb{F}[V]$ are the equivalence classes of polynomial functions on $\mathbb{F}^n$ based on the functions they define when restricted to V. It then follows that $K(\mathbb{F}[V])$ is the equivalence class of rational functions on $\mathbb{F}^n$ based on the functions they define on V. The transcendence degree of the field extension $K(\mathbb{F}[V])/\mathbb{F}$ is therefore the minimum number of rational functions $\rho_1,\ldots,\rho_k$ on V such that for all $s\in V$ where $\rho_i(s)$ has nonzero denominator for all i, if ρ is another rational function on V where $\rho(s)$ has nonzero denominator, then $\rho(s)$ is a root of a polynomial equation in one variable whose coefficients only depend on $\rho_i(s)$. TODO: insert examples

Given a finite set E and a field $\mathbb{F}$ we let $\mathbb{F}^E$ denote the vector space whose coordinates are indexed by E. The corresponding polynomial ring, whose indeterminates are indexed by E, is written $\mathbb{F}[x_e : e\in E]$. Each subset $S\subseteq E$ defines the coordinate projection $\pi_S:\mathbb{F}^E\to\mathbb{F}^S$ and the inclusion of rings $\mathbb{F}[x_e : e\in S]\hookrightarrow\mathbb{F}[x_e : e\in E]$.

Proposition 8.6: *Let $\mathbb{L}/\mathbb{F}$ be a field extension, let $E \subseteq \mathbb{L}$ be finite, and define $\mathbb{K} := \mathbb{F}(E)$. Then there exists an irreducible variety $V \subseteq \mathbb{F}^E$ such that*

(1) *the rank of $S \subseteq E$ in $\mathcal{M}(E)$ is the dimension of $\overline{\pi_S(V)}$,*
(2) *$\mathbb{K}$ is isomorphic to $K(\mathbb{F}[V])$, and*
(3) *$\mathcal{M}(E)$ is isomorphic to $\mathcal{M}(X)$ where $X := \{x_e : e \in E\} \subseteq K(\mathbb{F}[V])$.*

Proof. Define an $\mathbb{F}$-algebra homomorphism $\phi : \mathbb{F}[x_e : e \in E] \to \mathbb{K}$ by extending the map $x_e \mapsto e$ on generators. Letting I be the kernel of ϕ gives us an injective ring homomorphism $\mathbb{F}[x_e : e \in E]/I \to \mathbb{K}$ so we may treat $\mathbb{F}[x_e : e \in E]/I$ as a subring of $\mathbb{K}$. Since $\mathbb{K}$ is a field, this implies $\mathbb{F}[x_e : e \in E]/I$ is an integral domain. Moreover, $\mathbb{F}[x_e : e \in E]/I$ is the subring of $\mathbb{K}$ generated by $\mathbb{F}$ and E. Since $\mathbb{K}$ is generated as field by $\mathbb{F}$ and E, this implies that $K(\mathbb{F}[x_e : e \in E]/I) \cong \mathbb{K}$. Define $V := V(I)$. Then V is irreducible. For each $S \subseteq E$, the coordinate ring of $\overline{\pi_S(V)}$ is $\mathbb{F}[S]$. Therefore the dimension of $\overline{\pi_S(V)}$ is the transcendence degree of the field extension $\mathbb{F}(S)/\mathbb{F}$. This is the largest cardinality of an algebraically independent (over $\mathbb{F}$) subset of S, i.e. the rank of S in $\mathcal{M}(E)$. This proves the first claim. □

Given an irreducible variety $V \subseteq \mathbb{F}^E$, we let $\mathcal{M}(V)$ denote the algebraic matroid of $\{x_e : e \in E\}$ viewed as a subset of $K(\mathbb{F}[V])$ as a field extension of $\mathbb{F}$. Proposition 8.6 implies that the rank of $S \subseteq E$ is given by the dimension of $\overline{\pi_S(V)}$.

The ***support*** of a polynomial $f \in \mathbb{F}[x_e : e \in E]$, denoted $\operatorname{supp}(f)$, is the minimal subset $S \subseteq E$ such that $f \in \mathbb{F}[x_e : e \in S]$.

Proposition 8.7: *Let $\mathbb{K}/\mathbb{F}$ be a field extension and let $E \subseteq \mathbb{K}$ be finite. Then for each circuit C of $\mathcal{M}(E)$ there exists an irreducible polynomial $p_C\mathbb{F}[x_e : e \in E]$ with support C that vanishes under the substitution $x_e \mapsto e$. This polynomial is unique up to multiplication by nonzero elements of $\mathbb{F}$.*

Proof. TODO □

Given a finite subset $E \subseteq \mathbb{K}$ of a field extension $\mathbb{K}/\mathbb{F}$ and a circuit C of the matroid $\mathcal{M}(E)$, a polynomial p_C as in Proposition 8.7 is called a ***circuit polynomial***.

Proposition 8.8: *Let $\mathbb{K}/\mathbb{F}$ be a field extension, let $E \subseteq \mathbb{K}$ be finite and let $\mathcal{C}$ denote the set of circuits of $\mathcal{M}(E)$. For each $C \in \mathcal{C}$ fix a circuit polynomial $p_C \in \mathbb{F}[x_e : e \in E]$ and define P to be the ideal in $\mathbb{F}[x_e : e \in E]$ generated by p_C's, i.e.*

$$P := \langle p_C : C \in \mathcal{C} \rangle \subseteq \mathbb{F}[x_e : e \in E].$$

Then P is prime and $\mathcal{M}(E)$ is isomorphic to $\mathcal{M}(X)$ where $X = \{x_e : e \in E\}$, viewed as a subset of $K(\mathbb{F}[x_e : e \in E]/P)$, which is viewed as a field extension of $\mathbb{F}$.

Proof. Let I be the kernel of the $\mathbb{F}$-algebra homomorphism $\mathbb{F}[x_e : e \in E] \to \mathbb{K}$ given by $x_e \mapsto e$. Then $P \subseteq I$ and our goal is to show that this containment is moreover an equality. So for the reverse direction assume for the sake of contradiction that their exists $f \in I \setminus P$ and assume f has been chosen to have minimal support. The support of f cannot be strictly contained in a circuit C since this would contradict C being a circuit, nor can f have the support of a circuit by Proposition 8.7. If $\operatorname{supp}(f)$ does not contain a circuit, then this would imply that $\operatorname{supp}(f)$ is independent in $\mathcal{M}(E)$ but the existence of f implies that f is dependent in $\mathcal{M}(E)$, a contradiction.

The only remaining possibility is that $\operatorname{supp}(f)$ strictly contains a circuit C. Let p be a circuit polynomial for C and let $e \in C$. Then we can eliminate e from f and p to get a polynomial g

such that $\operatorname{supp}(g) \subsetneq \operatorname{supp}(f)$. Our minimality assumption on $\operatorname{supp}(f)$ implies that $g \in P$. So we have $g = h_1 f + h_2 p$. Since g and p are in P and $f \notin P$, this implies $h_1 \in P$. So then g is congruent to $h_2 p$ modulo I^2. This implies that the (images modulo I^2) of the circuit polynomials generate I/I^2. The circuit polynomials therefore generate I by Nakayama's Lemma. TODO: find a proof without Nakayama's lemma, or write up stuff about Nakayama's lemma, or make decisions about what I'm going to outsource to a commutative algebra book. □

3. Algebraic representability

Proposition 8.9: *Let $\mathbb{F}/\mathbb{L}$ be an algebraic field extension and let $\mathcal{M}$ be a matroid. Then $\mathcal{M}$ is algebraically representable over $\mathbb{F}$ if and only if it is algebraically representable over $\mathbb{L}$.*

Proof. Let $\mathbb{K}/\mathbb{F}$ and let $S \subseteq \mathbb{K}$. We will show that S is algebraically dependent over $\mathbb{F}$ if and only if it is algebraically dependent over $\mathbb{L}$. The proposition will then immediately follow. Assume S is algebraically dependent over $\mathbb{L}$. Since $\mathbb{L} \subseteq \mathbb{F}$, this implies that S is algebraically dependent over $\mathbb{F}$ too. Now assume S is algebraically dependent over $\mathbb{F}$. We may assume without loss of generality that every proper subset of S is algebraically independent over $\mathbb{F}$. Then $S \setminus s$ is algebraically dependent over $\mathbb{F}(s)$ for all $s \in S$. Induction on $|S|$ shows that S is algebraically dependent over $\mathbb{L}$ via Lemma 8.2. □

Proposition 8.10: *Let $\mathbb{F}$ be an algebraically closed field, let t be transcendental over $\mathbb{F}$, and let $\mathcal{M}$ be a matroid. Then $\mathcal{M}$ is $\mathbb{F}$-algebraically representable if and only if it is $\mathbb{F}(t)$-algebraically representable.*

Proof. TODO □

Recall that the ***characteristic*** of a field $\mathbb{F}$ is the minimum $n \geq 1$ such that $\sum_{i=1}^{n} 1 = 0$ in $\mathbb{F}$, and 0 if such an n does not exist. The characteristic of any field is either 0 or prime (see Problem 8.7). The ***prime subfield*** of a field $\mathbb{F}$ is the minimal subfield of $\mathbb{F}$. Equivalently, it is the subfield generated by 1. A field is ***prime*** if it is its own prime subfield. For each $n \geq 0$, there is at most one prime field of characteristic n. In particular, the only prime fields are $\mathbb{Q}$ and the finite fields $\mathbb{F}_p$ for p prime. The ***algebraic closure*** of a field $\mathbb{F}$ is the minimal algebraically closed field containing $\mathbb{F}$. It is nontrivial to prove that every field does have an algebraic closure (see e.g. [2, Chapter 13.4]).

Theorem 8.11: *Let $\mathcal{M}$ be a matroid and let $\mathbb{F}$ be a field. If $\mathcal{M}$ is $\mathbb{F}$-algebraically representable then $\mathcal{M}$ is $\mathbb{K}$-algebraically representable over any field $\mathbb{K}$ with the same characteristic.*

Proof. Let $\mathbb{K}/\mathbb{F}$ be a field extension and let $E \subseteq \mathbb{K}$ such that $\mathcal{M} = \mathcal{M}(E)$. For Let $\mathbb{L}$ be the prime subfield of $\mathbb{F}$. □

4. Applications

Many questions in applied algebraic geometry boil down to describing the spanning sets of a particular algebraic matroid. In this section we look at two particular examples.

4.1. Low-rank matrix completion. In a low-rank matrix completion problem, one is given access to a subset of entries of a matrix, and hopes to fill in the missing entries in a way

$$\begin{pmatrix} a & \cdot & b \\ c & d & \cdot \\ \cdot & e & f \end{pmatrix}$$

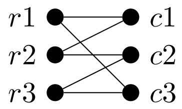


FIGURE 8.4.1. The subset of known entries of the matrix to the left correspond to the graph on the right. If a, b, c, d, e, f are sufficiently generic, then the partial matrix can be completed to rank two, but not rank one.

that minimizes rank, or that achieves a particular low rank. For example, given any partial matrix of the following form

$$\begin{pmatrix} a & b \\ c & \cdot \end{pmatrix},$$

one can fill in the missing entry so that the resulting matrix has rank one. Namely, plug in $\frac{bc}{a}$. Of course, this won't work if $a = 0$, but we can safely ignore this issue, and similar ones, by working over $\mathbb{C}$ and invoking a genericity assumption on the visible entries. In this setup, whether or not a particular partial matrix can be completed to a particular rank r depends only on which entries are observed, and not their actual values. Thus, one can ask: given an integer $r \geq 1$ and a subset E of entries of an $m \times n$ matrix – which is naturally encoded by the bipartite graph $([m], [n], E)$, see Figure 8.4.1 – can the resulting generic[1] partial matrices be completed to rank r? The subsets of entries for which the answer to this question is "yes" form the independent sets of a matroid.

Let $\mathrm{M}(m \times n, r) \subseteq \mathbb{C}^{m \times n}$ denote the set of $m \times n$ complex matrices of rank at most r. Since a matrix has rank r or less if and only if all $(r + 1) \times (r + 1)$ submatrices have zero determinant, $\mathrm{M}(m \times n, r)$ is a variety. Moreover, it is irreducible so we can talk about its algebraic matroid. The ground set of this matroid is the set of entries of an $m \times n$ matrix, which we identify with the edge set of the complete bipartite graph $K_{m,n}$. Subsets of the ground set can therefore be described as bipartite graphs on partite sets of size m and n.

Given a bipartite graph G, let $\mathbb{C}^G$ denote the vector space whose coordinates are indexed by edges of G, and let $\Omega_G : \mathbb{C}^{m \times n} \to \mathbb{C}^G$ be the map that projects a matrix M onto its entries corresponding to the edges of G. Elements of $\mathbb{C}^G$ are called ***G-partial matrices***. Given a G-partial matrix A, elements of $\Omega_G^{-1}(A)$ are called ***completions*** of A. A fundamental problem in low-rank matrix completion is to determine whether a given partial matrix $A \in \mathbb{C}^G$ has a completion to a particular rank. The following proposition tells us that assuming A is generic, whether or not A can be completed to rank r depends only on G.

Proposition 8.12: *Let $G = ([m], [n], E)$ be a bipartite graph and let $A \in \mathbb{C}^G$ be a G-partial matrix. If A is generic, then A has a completion to rank r if and only if G is independent in the algebraic matroid $\mathcal{M}(\mathrm{M}(m \times n, r))$.*

PROOF. Given any irreducible variety $V \subseteq \mathbb{C}^E$, $S \subseteq E$ is independent in $\mathcal{M}(V)$ if and only if $\dim(\pi_S(V)) = |S|$. This means that the set $\{x \in \mathbb{C}^S : x \notin \pi_S(V)\}$ is contained in a

[1] When applied algebraic geometers say "property P is satisfied by a generic point of V," it means that the set of points in V where P is ***not*** satisfied is contained in a subvariety of V. We use the word "generic" to avoid explicitly writing down what that variety is. When V is irreducible, any subvariety of V has lower dimension than V. Therefore, when $\mathbb{F} = \mathbb{C}$ or $\mathbb{R}$, if V is irreducible and a generic point of V satisfies property P, then a point randomly sampled from V with respect to a reasonable probability distribution will satisfy P with probability one.

subvariety of $\mathbb{C}^S$, and in particular, has dimension strictly less than $|S|$. Thus given any generic $x \in \mathbb{C}^S$, there exists $y \in V$ such that $\pi_S(y) = x$. The proposition is now the special case where $V = \mathrm{M}(m \times n, r)$. □

Proposition 8.12 now motivates the following general problem.

Problem 8.1: For each r, give a combinatorial description of the (independent sets of the) matroid $\mathcal{M}(\mathrm{M}(m \times n, r))$.

Problem 8.1 is open in all cases other than $r = 1$ and $r = 2$. For $r = 1$, it is relatively easy to show that $\mathcal{M}(\mathrm{M}(m \times n, 1))$ is the graphic matroid of $K_{m,n}$; we do this below.

Proposition 8.13: *The matroid $\mathcal{M}(\mathrm{M}(m \times n, 1))$ is the graphic matroid of $K_{m,n}$. In other words, a bipartite graph $G = ([m], [n], E)$ is independent in $\mathcal{M}(\mathrm{M}(m \times n, 1))$ if and only if Gis a forest.*

Proof. Assume G has no cycles. Let X be a generic G-partial matrix. By Proposition 8.12, it suffices to show that X can be completed to a rank-one matrix. Let G' be obtained from G by removing a vertex of degree zero or one; without loss of generality, assume it was the row-vertex m. Let X' be the G'-partial matrix obtained from X by removing the last row. By induction, X' can be completed to a rank-one matrix Y. If the degree of m was zero, then we can further complete X to a rank-one matrix by plugging in zeros for the entries in the last row. If the degree of m was 1, then assuming the unique known entry of the m^{th} row of X is in the first column, then multiply the $(m-1)^{\text{th}}$ row of Y by $X_{m,1}/Y_{m-1,1}$ and adjoining it to Y gives a rank-one completion of X.

Now assume G has a cycle $x_1, x_2, \ldots, x_{2k}$ (G is bipartite, so the cycle must have even length). Then $\pi_G(\mathrm{M}(m \times n, 1))$ must satisfy the equation $x_1 x_3 \cdots x_{2k-1} = x_2 x_4 \cdots x_{2k}$. In particular, $\pi_G(\mathrm{M}(m \times n, 1))$ has dimension less than the number of edges of G. □

The characterization of $\mathcal{M}(\mathrm{M}(m \times n, 2))$ is more complicated. We omit the proof, which uses tropical geometry.

Theorem 8.14 ([1, Theorem 4.4])**:** *Let $G = ([m], [n], E)$ be a bipartite graph. Then G is independent in $\mathcal{M}(\mathrm{M}(m \times n, 2))$ if and only if there exists a two-coloring of the edges of G with no monochromatic cycle, and no cycle whose edge-colors alternate.*

4.2. Rigidity theory. If one were to physically build a graph G in d-dimensional space, using rigid struts for the edges, and universal joints for the vertices (i.e. joints that the struts can move freely around) would the resulting structure be rigid, or flexible? Consider, for example, the four-cycle. If we build it in the plane as a square, then the resulting structure is flexible, since we can deform the square into a rhombus without stretching, compressing, or breaking any of the edges – see Figure 8.4.2. However, if we add a chord to the four-cycle, then it becomes rigid in the plane.

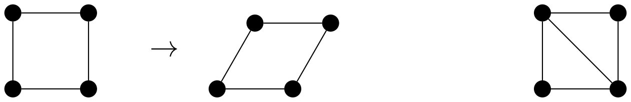


Figure 8.4.2. The four-cycle is not rigid in the plane, but becomes rigid after adding a chord.

Whether or not a graph is rigid in d-dimensional space depends not only on the combinatorics of the graph, but also on the specific positions we place the vertices. For example, we can build the four-cycle in the plane so that it becomes rigid by placing all four vertices on a line. However, just as in the matrix completion example, we can safely ignore such issues by invoking a genericity assumption. Then, every graph will either be rigid or flexible in d-dimensional space, and we can ask to characterize those that are rigid. Moreover, the graphs on a fixed number of vertices that are rigid in d-dimensional space form the spanning sets of a matroid. When $d = 1$, this is the graphic matroid of the complete graph (see if you can convince yourself of this). When $d = 2$, the independent sets of this matroid consist of graphs such that every subgraph on k vertices has at most $2k - 3$ edges. More on this later.

Consider the function $\phi_n^d : (\mathbb{R}^d)^n \to \mathbb{R}^{\binom{n}{2}}$ that sends a configuration of n points in d-dimensional space to their vector of squared pairwise distances. For example, if $d = 2$, this map would send the n points $(x_1, y_1), \ldots, (x_n, y_n)$ to the vector $((x_i - x_j)^2 + (y_i - y_j)^2)_{1 \le i < j \le n}$. The image of ϕ_n^d is subset of $\mathbb{R}^{\binom{n}{2}}$, and taking its Zariski closure in $\mathbb{C}^{\binom{n}{2}}$ (i.e. the smallest variety in $\mathbb{C}^{\binom{n}{2}}$ containing it) yields an irreducible variety CM_n^d called the ***Cayley-Menger variety of*** n ***points in*** $\mathbb{R}^d$. We can identify the coordinate indices of $\mathbb{C}^{\binom{n}{2}}$, i.e. the ground set of the matroid $\mathcal{M}(\mathrm{CM}_n^d)$, with the edges of the complete graph K_n.

Proposition 8.15: *A graph G is spanning in $\mathcal{M}(\mathrm{CM}_n^d)$ if and only if it is rigid in d-dimensional space.*

PROOF SKETCH. Given any varieties V and W and any polynomial map $f : V \to W$, the following relationship holds for generic $x \in V$

$$\dim(V) = \dim(f(V)) + \dim(f^{-1}(f(x))).$$

When $\dim(V) = \dim(f(V))$, this implies $\dim(f^{-1}(f(x))) = 0$ and since $\dim(f^{-1}(f(x))$ is a variety, this is equivalent to $\dim(f^{-1}(f(x))$ being a finite set. In particular, if $V \subseteq \mathbb{C}^E$ then $S \subseteq E$ is spanning in $\mathcal{M}(V)$ if and only if $\pi_S^{-1}(\pi_S(x)) \cap V$ is a finite set. So it remains to see that G is rigid if and only if $\pi_G^{-1}(\pi_G(x)) \cap \mathrm{CM}_n^d$ is finite for generic $x \in \mathrm{CM}_n^d$.

We now need to be more formal in our definition of rigidity. Suppose we build a graph G in $\mathbb{R}^d$ by putting the vertices at points $p^{(1)}, \ldots, p^{(n)}$. A (nontrivial) ***flex*** of G is a curve in the space of configuration of n points in $\mathbb{R}^d$, i.e. a function $\mathbf{p} : [0, 1] \to (\mathbb{R}^d)^n$, such that

(1) the curve starts at the original configuration, i.e. $\mathbf{p}(0) = (p^{(1)}, \ldots, p^{(n)})$
(2) all configurations along the curve preserve the lengths of the edges of G, i.e. for each $t \in [0, 1]$ and edge $\{i, j\}$ of G, $\|\mathbf{p}(t)^{(i)} - \mathbf{p}(t)^{(j)}\|^2 = \|\mathbf{p}(0)^{(i)} - \mathbf{p}(0)^{(j)}\|^2$, and
(3) somewhere along the curve, the framework on G actually gets deformed, i.e. for some $t \in [0, 1]$ and some ***non***-edge $\{i, j\}$ of G, $\|\mathbf{p}(t)^{(i)} - \mathbf{p}(t)^{(j)}\|^2 \ne \|\mathbf{p}(0)^{(i)} - \mathbf{p}(0)^{(j)}\|^2$.

This formalizes our intuitive notion of what it would mean to deform our particular construction of a graph. A graph is then (generically) ***rigid*** if for any generic point configuration $p^{(1)}, \ldots, p^{(n)}$, the corresponding framework on G does not have any flex.

To see that the absence of a flex of G is equivalent to the statement that $\pi_G^{-1}(\pi_G(x)) \cap \mathrm{CM}_n^d$ is generically finite, first note that if $\mathbf{p} : [0, 1] \to (\mathbb{R}^d)^n$ is a curve satisfying the second condition required for $\mathbf{p}$ to be a flex of G, then $\pi_G \circ \phi_n^d \circ \mathbf{p}([0, 1])$ is a single point y in $\pi_G(\mathrm{CM}_n^d)$, and $\pi_G^{-1}(y) \cap \mathrm{CM}_n^d$ contains $\phi_n^d \circ \mathbf{p}([0, 1])$. The curve $\mathbf{p}$ additionally satisfies the third condition if and only if $\phi_n^d \circ \mathbf{p}[0, 1])$ is one-dimensional, thus exhibiting infinitely many points in $\pi_G^{-1}(\pi_G(x)) \cap \mathrm{CM}_n^d$ for some $x \in \pi_G^{-1}(y) \cap \mathrm{CM}_n^d$. Conversely, since $\pi_G^{-1}(\pi_G(x)) \cap \mathrm{CM}_n^d$ is a variety, then if it has infinitely many points, it must contain a curve. In this case, we can find such a curve that also lies in the image of ϕ_n^d (this is me ignoring the issues that arise when passing from a semi-algebraic set to its complex Zariski closure). Such a curve is a flex. □

Proposition 8.15 motivates the following general problem: for each $d \geq 1$, find a combinatorial description of $\mathcal{M}(\mathrm{CM}_n^d)$, the algebraic matroid of the Cayley-Menger variety of n points in d-dimensional space. For $d \geq 3$, this problem is open, and has been for at least a century. The $d = 1$ case is quite simple: $\mathcal{M}(\mathrm{CM}_n^1)$ is the graphic matroid of the complete graph K_n, and you might be able to see this intuitively. There are a handful of characterizations for the $d = 2$ case; perhaps the most famous, and elegant, due to Hilda Polaczek-Geiringer, is the following

Theorem 8.16 ([7])**:** *A graph G is independent in $\mathcal{M}(\mathrm{CM}_n^d)$ if and only if every subgraph of G on k vertices has at most $2k - 3$ edges.*

Theorem 8.16 is known as ***Laman's theorem***, based on the mistaken, but previously widespread, belief that this result originated with Gerard Laman's 1970 paper [5]. Recently however, it was noticed that Hilda Pollaczek-Geiringer had actually proven this result much earlier in 1927 [7].

5. Exercises

Problem 8.2: For each of the following field extensions $\mathbb{K}/\mathbb{F}$, determine which are finite-dimensional $\mathbb{F}$-vector spaces, which are algebraic, and which are finitely generated:

(1) $\mathbb{C}/\mathbb{R}$
(2) $\mathbb{C}/\mathbb{Q}$
(3) $\overline{\mathbb{Q}}/\mathbb{Q}$ where $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$, i.e. the subfield of $\mathbb{C}$ consisting of elements that are algebraic over $\mathbb{Q}$
(4) $\mathbb{Q}(x)/\mathbb{Q}$
(5) $\mathbb{Q}(\pi)/\mathbb{Q}$
(6) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$.

Problem 8.3: Let $F \subseteq \mathbb{F}[\mathbf{x}]$. Prove that $V(F) = V(\langle F \rangle)$.

Problem 8.4: Prove that $I(S) \subseteq \mathbb{F}[\mathbf{x}]$ is an ideal for every $S \subseteq \mathbb{F}^n$.

Problem 8.5: Let For each ideal $I \subseteq \mathbb{F}[\mathbf{x}]$, define the ***radical*** of I to be

$$\sqrt{I} := \{f : f^n \in I \text{ for some } n \geq 1\}.$$

Prove that $\sqrt{I}$ is an ideal and that $V(I) = V(\sqrt{(I)})$.

Problem 8.6: Prove that a variety $V \subseteq \mathbb{F}^n$ is irreducible if and only if its coordinate ring $\mathbb{F}[V]$ is an integral domain.

Problem 8.7: Prove that the characteristic of any field is either 0 or prime.

Bibliography

[1] Daniel Irving Bernstein. Completion of tree metrics and rank 2 matrices. *Linear Algebra and its Applications*, 533:1–13, 2017.

[2] David Steven Dummit and Richard M Foote. *Abstract algebra*, volume 3. Wiley Hoboken, 2004.

[3] David Eisenbud. *Commutative algebra: with a view toward algebraic geometry*, volume 150. Springer Science & Business Media, 2013.

[4] Brendan Hassett. *Introduction to algebraic geometry.* Cambridge University Press, 2007.

[5] Gerard Laman. On graphs and rigidity of plane skeletal structures. *Journal of Engineering mathematics*, 4(4):331–340, 1970.

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

[7] Hilda Pollaczek-Geiringer. Über die gliederung ebener fachwerke. *ZAMM-Journal of Applied Mathematics and Mechanics/Zeitschrift für Angewandte Mathematik und Mechanik*, 7(1):58–72, 1927.

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