Chapter 7

Polytopes, Resultants, and Equations

In this chapter we will examine some interesting recently-discovered connections between polynomials, resultants, and the geometry of the convex polytopes determined by the exponent vectors of the monomials appearing in polynomials.

§1 Geometry of Polytopes

A set C in $\mathbb{R}^n$ is said to be *convex* if it contains the line segment connecting any two points in C. If a set is not itself convex, its *convex hull* is the smallest convex set containing it. We will use the notation $\text{Conv}(S)$ to denote the convex hull of $S \subset \mathbb{R}^n$.

More explicitly, all the points in Conv(S) may be obtained by forming a particular set of linear combinations of the elements in S. In Exercise 1 below, you will prove the following proposition.

(1.1) Proposition. *Let S be a subset of $\mathbb{R}^n$. Then*

$$\text{Conv}(S) = \{\lambda_1 s_1 + \cdots + \lambda_m s_m : s_i \in S,\ \lambda_i \geq 0,\ \textstyle\sum_{i=1}^m \lambda_i = 1\}.$$

Linear combinations of the form $\lambda_1 s_1 + \cdots + \lambda_m s_m$, where $s_i \in S$, $\lambda_i \geq 0$, and $\sum_{i=1}^m \lambda_i = 1$ are called *convex combinations*.

Exercise 1.

a. Show that if $S = \{s_1, s_2\}$ then the set of convex combinations is the straight line segment from s_1 to s_2 in $\mathbb{R}^n$. Deduce that Proposition (1.1) holds in this case.

b. Using part a, show that the set of all convex combinations

$$\{\lambda_1 s_1 + \cdots + \lambda_m s_m : s_i \in S,\ \lambda_i \geq 0,\ \textstyle\sum_{i=1}^m \lambda_i = 1\}.$$

is a convex subset of $\mathbb{R}^n$ for every S. Also show that this set contains S.

c. Show that if C is any convex set containing S, then C also contains the set of part b. Hint: One way is to use induction on the number of terms in the sum.
d. Deduce Proposition (1.1) from parts b and c.

By definition, a *polytope* is the convex hull of a *finite* set in $\mathbb{R}^n$. If the finite set is $\mathcal{A} = \{m_1, \ldots, m_l\} \subset \mathbb{R}^n$, then the corresponding polytope can be expressed as

$$\text{Conv}(\mathcal{A}) = \{\lambda_1 m_1 + \cdots + \lambda_l m_l : \lambda_i \geq 0,\ \textstyle\sum_{i=1}^{l} \lambda_i = 1\}.$$

In low dimensions, polytopes are familiar figures from geometry:

- A polytope in $\mathbb{R}$ is a line segment.
- A polytope in $\mathbb{R}^2$ is a line segment or a convex polygon.
- A polytope in $\mathbb{R}^3$ is a line segment, a convex polygon lying in a plane, or a three-dimensional polyhedron.

As these examples suggest, every polytope Q has a well-defined *dimension*. A careful definition of $\dim Q$ will be given in the exercises at the end of the section. For more background on convex sets and polytopes, the reader should consult [Zie]. Fig. 7.1 below shows a three-dimensional polytope.

For another example, let $\mathcal{A} = \{(0,0), (2,0), (0,5), (1,1)\} \subset \mathbb{R}^2$. Here, $\text{Conv}(\mathcal{A})$ is the triangle with vertices $(0,0)$, $(2,0)$, and $(0,5)$ since

$$(1,1) = \tfrac{3}{10}(0,0) + \tfrac{1}{2}(2,0) + \tfrac{1}{5}(0,5) \tag{1.2}$$

is a convex combination of the other three points in $\mathcal{A}$.

For us, the most important polytopes will be convex hulls of sets of points with *integer* coordinates. These are sometimes called *lattice polytopes*. Thus a lattice polytope is a set of the form $\text{Conv}(\mathcal{A})$, where $\mathcal{A} \subset \mathbb{Z}^n$ is finite. An example of special interest to us is when $\mathcal{A}$ consists of all exponent vectors

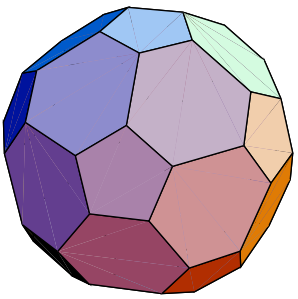

FIGURE 7.1. A three-dimensional polytope

appearing in a collection of monomials. The polytope $Q = \mathrm{Conv}(\mathcal{A})$ will play a *very* important role in this chapter.

Exercise 2. Let $\mathcal{A}_d = \{m \in \mathbb{Z}^n_{\geq 0} : |m| \leq d\}$ be the set of exponent vectors of *all* monomials of total degree at most d.

a. Show that the convex hull of $\mathcal{A}_d$ is the polytope

$$Q_d = \{(a_1, \dots, a_n) \in \mathbb{R}^n : a_i \geq 0,\ \textstyle\sum_{i=1}^n a_i \leq d\}.$$

Draw a picture of $\mathcal{A}_d$ and Q_d when $n = 1, 2, 3$ and $d = 1, 2, 3$.

b. A *simplex* is defined to be the convex hull of $n+1$ points $m_1, \dots, m_{n+1}$ such that $m_2 - m_1, \dots, m_{n+1} - m_1$ are a basis of $\mathbb{R}^n$. Show that the polytope Q_d of part a is a simplex.

A polytope $Q \subset \mathbb{R}^n$ has an n-dimensional volume, which is denoted $\mathrm{Vol}_n(Q)$. For example, a polygon Q in $\mathbb{R}^2$ has $\mathrm{Vol}_2(Q) > 0$, but if we regard Q as lying in the xy-plane in $\mathbb{R}^3$, then $\mathrm{Vol}_3(Q) = 0$.

From multivariable calculus, we have

$$\mathrm{Vol}_n(Q) = \int \cdots \int_Q 1\, dx_1 \cdots dx_n,$$

where $x_1, \dots, x_n$ are coordinates on $\mathbb{R}^n$. Note that Q has positive volume if and only if it is n-dimensional. A simple example is the unit cube in $\mathbb{R}^n$, which is defined by $0 \leq x_i \leq 1$ for all i and clearly has volume 1.

Exercise 3. Let's compute the volume of the simplex Q_d from Exercise 2.

a. Prove that the map $\phi : \mathbb{R}^n \to \mathbb{R}^n$ defined by

$$\phi(x_1, \dots, x_n) = (1 - x_1, x_1(1 - x_2), x_1x_2(1 - x_3), \dots, x_1 \cdots x_{n-1}(1 - x_n))$$

maps the unit cube $C \subset \mathbb{R}^n$ defined by $0 \leq x_i \leq 1$ to the simplex Q_1. Hint: Use a telescoping sum to show $\phi(C) \subset Q_1$. Be sure to prove the opposite inclusion.

b. Use part a and the change of variables formula for n-dimensional integrals to show that

$$\mathrm{Vol}_n(Q_1) = \int \cdots \int_C x_1^{n-1} x_2^{n-2} \cdots x_{n-1}\, dx_1 \cdots dx_n = \frac{1}{n!}.$$

c. Conclude that $\mathrm{Vol}_n(Q_d) = d^n/n!$.

Polytopes have special subsets called its *faces*. For example, a 3-dimensional polytope in $\mathbb{R}^3$ has:

- faces, which are polygons lying in planes,
- edges, which are line segments connecting certain pairs of vertices, and
- vertices, which are points.

In the general theory, all of these will be called faces. To define a face of an arbitrary polytope $Q \subset \mathbb{R}^n$, let ν be a nonzero vector in $\mathbb{R}^n$. An

affine hyperplane is defined by an equation of the form $m \cdot \nu = -a$ (the minus sign simplifies certain formulas in §3 and §4—see Exercise 3 of §3 and Proposition (4.6)). If

$$a_Q(\nu) = -\min_{m \in Q}(m \cdot \nu), \tag{1.3}$$

then we call the equation

$$m \cdot \nu = -a_Q(\nu)$$

a *supporting hyperplane* of Q, and we call ν an *inward pointing normal*. Fig. 7.2 below shows a polytope $Q \subset \mathbb{R}^2$ with two supporting hyperplanes (lines in this case) and their inward pointing normals.

In Exercise 13 at the end of the section, you will show that a supporting hyperplane has the property that

$$Q_\nu = Q \cap \{m \in \mathbb{R}^n : m \cdot \nu = -a_Q(\nu)\} \neq \emptyset,$$

and, furthermore, Q lies in the half-space

$$Q \subset \{m \in \mathbb{R}^n : m \cdot \nu \geq -a_Q(\nu)\}.$$

We call $Q_\nu = Q \cap \{m \in \mathbb{R}^n : m \cdot \nu = -a_Q(\nu)\}$ the *face of Q determined by ν*. Fig. 7.2 illustrates two faces, one a vertex and the other an edge.

Exercise 4. Draw a picture of a cube in $\mathbb{R}^3$ with three supporting hyperplanes which define faces of dimensions 0, 1, and 2 respectively. Be sure to include the inward pointing normals in each case.

Every face of Q is a polytope of dimension less than $\dim Q$. *Vertices* are faces of dimension 0 (i.e., points) and *edges* are faces of dimension 1. If Q has dimension n, then *facets* are faces of dimension $n-1$. Assuming

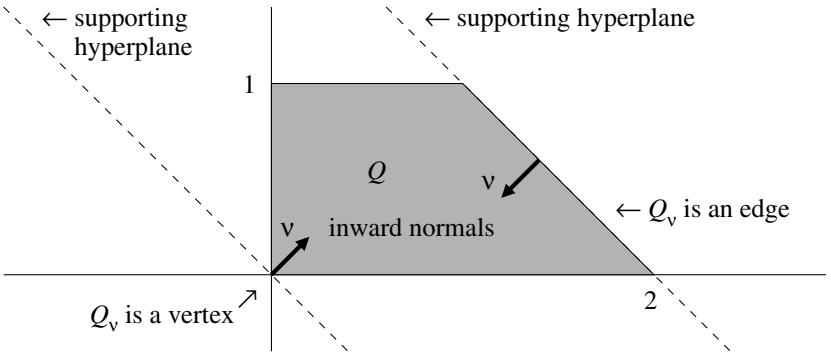

FIGURE 7.2. Supporting hyperplanes, inward normals, and faces

$Q \subset \mathbb{R}^n$, a facet lies on a unique supporting hyperplane and hence has a unique inward pointing normal (up to a positive multiple). In contrast, faces of lower dimension lie in infinitely many supporting hyperplanes. For example, the vertex at the origin in Fig 7.2 is cut out by infinitely many lines through the origin.

We can characterize an n-dimensional polytope $Q \subset \mathbb{R}^n$ in terms of its facets as follows. If $\mathcal{F} \subset Q$ is a facet, we just noted that the inward normal is determined up to a positive constant. Suppose that Q has facets $\mathcal{F}_1, \dots, \mathcal{F}_N$ with inward pointing normals $\nu_1, \dots, \nu_N$ respectively. Each facet $\mathcal{F}_j$ has a supporting hyperplane defined by an equation $m \cdot \nu_j = -a_j$ for some a_j. Then one can show that the polytope Q is given by

$$Q = \{m \in \mathbb{R}^n : m \cdot \nu_j \geq -a_j \text{ for all } j = 1, \dots, N\}. \tag{1.4}$$

In the notation of (1.3), note that $a_j = a_Q(\nu_j)$.

Exercise 5. How does (1.4) change if we use an *outward* normal for each facet?

When Q is a lattice polytope, we can rescale the inward normal $\nu_{\mathcal{F}}$ of a facet $\mathcal{F}$ so that $\nu_{\mathcal{F}}$ has integer coordinates. We can also assume that the coordinates are relatively prime. In this case, we say the $\nu_{\mathcal{F}}$ is *primitive*. It follows that $\mathcal{F}$ has a *unique* primitive inward pointing normal $\nu_{\mathcal{F}} \in \mathbb{Z}^n$. For lattice polytopes, we will always assume that the inward normals have this property.

Exercise 6. For the lattice polygon Q of Fig. 7.2, find the inward pointing normals. Also, if e_1, e_2 are the standard basis vectors for $\mathbb{R}^2$, then show that the representation (1.4) of Q is given by the inequalities

$$m \cdot e_1 \geq 0, \quad m \cdot e_2 \geq 0, \ m \cdot (-e_2) \geq -1, \quad m \cdot (-e_1 - e_2) \geq -2.$$

Exercise 7. Let $e_1, \dots, e_n$ be the standard basis of $\mathbb{R}^n$.

a. Show that the simplex $Q_d \subset \mathbb{R}^n$ of Exercise 2 is given by the inequalities

$$m \cdot \nu_0 \geq -d, \text{ and } m \cdot \nu_j \geq 0, \ j = 1, \dots, n,$$

where $\nu_0 = -e_1 - \cdots - e_n$ and $\nu_j = e_j$ for $j = 1, \dots, n$.

b. Show that the square $Q = \text{Conv}(\{(0,0), (1,0), (0,1), (1,1)\}) \subset \mathbb{R}^2$ is given by the inequalities

$$m \cdot \nu_1 \geq 0, \ m \cdot \nu_2 \geq -1, \ m \cdot \nu_3 \geq 0, \text{ and } m \cdot \nu_4 \geq -1,$$

where $e_1 = \nu_1 = -\nu_2$ and $e_2 = \nu_3 = -\nu_4$. A picture of this appears in Fig. 7.3 on the next page (with shortened inward normals for legibility).

One of the themes of this chapter is that there is very deep connection between lattice polytopes and polynomials. To describe the connection, we

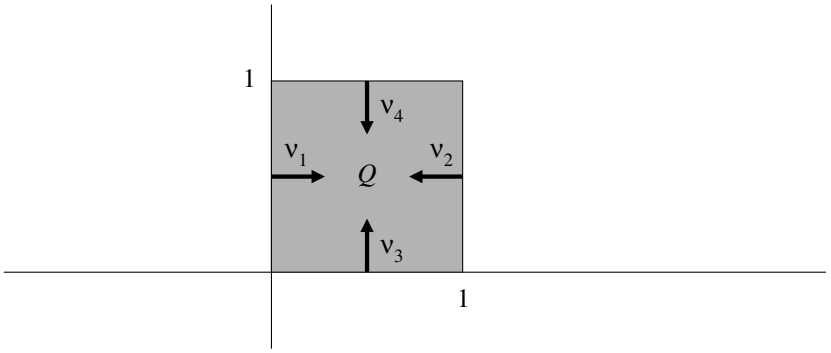

FIGURE 7.3. The unit square

will use the following notation. Let $f \in \mathbb{C}[x_1, \ldots, x_n]$ (or, more generally, in $k[x_1, \ldots, x_n]$ for any field of coefficients), and write

$$f = \sum_{\alpha \in \mathbb{Z}^n_{\geq 0}} c_\alpha x^\alpha.$$

The *Newton polytope* of f, denoted $\mathrm{NP}(f)$, is the lattice polytope

$$\mathrm{NP}(f) = \mathrm{Conv}(\{\alpha \in \mathbb{Z}^n_{\geq 0} : c_\alpha \neq 0\}).$$

In other words, the Newton polytope records the "shape" or "sparsity structure" of a polynomial—it tells us which monomials appear with nonzero coefficients. The actual values of the coefficients do not matter, however, in the definition of $\mathrm{NP}(f)$.

For example, any polynomial of the form

$$f = axy + bx^2 + cy^5 + d$$

with $a, b, c, d \neq 0$ has Newton polytope equal to the triangle

$$Q = \mathrm{Conv}(\{(1,1), (2,0), (0,5), (0,0)\}).$$

In fact, (1.2) shows that polynomials of this form with $a = 0$ would have the same Newton polytope.

Exercise 8. What is the Newton polytope of a 1-variable polynomial $f = \sum_{i=0}^m c_i x^i$, assuming that $c_m \neq 0$, so that the degree of f is exactly m? Are there special cases depending on the other coefficients?

Exercise 9. Write down a polynomial whose Newton polytope equals the polytope Q_d from Exercise 2. Which coefficients *must be* non-zero to obtain $\mathrm{NP}(f) = Q_d$? Which can be zero?

We can also go the other way, from exponents to polynomials. Suppose we have a finite set of exponents $\mathcal{A} = \{\alpha_1, \ldots, \alpha_l\} \subset \mathbb{Z}^n_{\geq 0}$. Then let $L(\mathcal{A})$ be the set of all polynomials whose terms *all* have exponents in $\mathcal{A}$. Thus

$$L(\mathcal{A}) = \{c_1 x^{\alpha_1} + \cdots + c_l x^{\alpha_l} : c_i \in \mathbb{C}\}.$$

Note that $L(\mathcal{A})$ is a vector space over $\mathbb{C}$ of dimension l (= the number of elements in $\mathcal{A}$).

Exercise 10.
a. If $f \in L(\mathcal{A})$, show that $\mathrm{NP}(f) \subset \mathrm{Conv}(\mathcal{A})$. Give an example to show that equality need not occur.
b. Show that there is a union of proper subspaces $W \subset L(\mathcal{A})$ such that $\mathrm{NP}(f) = \mathrm{Conv}(\mathcal{A})$ for all $f \in L(\mathcal{A}) \setminus W$. This means that $\mathrm{NP}(f) = \mathrm{Conv}(\mathcal{A})$ holds for a *generic* $f \in L(\mathcal{A})$.

Exercise 11. If $\mathcal{A}_d$ is as in Exercise 2, what is $L(\mathcal{A}_d)$?

Finally, we conclude this section with a slight generalization of the notion of monomial and polynomial. Since the vertices of a lattice polytope can have *negative entries*, it will be useful to have the corresponding algebraic objects. This leads to the notion of a polynomial whose terms can have negative exponents.

Let $\alpha = (a_1, \ldots, a_n) \in \mathbb{Z}^n$ be an integer vector. The corresponding *Laurent monomial* in variables $x_1, \ldots, x_n$ is

$$x^\alpha = x_1^{a_1} \cdots x_n^{a_n}.$$

For example, x^2y^{-3} and $x^{-2}y^3$ are Laurent monomials in x and y whose product is 1. More generally, we have

$$x^\alpha \cdot x^\beta = x^{\alpha+\beta} \text{ and } x^\alpha \cdot x^{-\alpha} = 1$$

for all $\alpha, \beta \in \mathbb{Z}^n$. Finite linear combinations

$$f = \sum_{\alpha \in \mathbb{Z}^n} c_\alpha x^\alpha$$

of Laurent monomials are called *Laurent polynomials*, and the collection of all Laurent polynomials forms a commutative ring under the obvious sum and product operations. We denote the ring of Laurent polynomials with coefficients in a field k by $k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$. See Exercise 15 below for another way to understand this ring.

The definition of the Newton polytope goes over unchanged to Laurent polynomials; we simply allow vertices with negative components. Thus any Laurent polynomial $f \in k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ has a Newton polytope $\mathrm{NP}(f)$, which again is a lattice polytope. Similarly, given a finite set $\mathcal{A} \subset \mathbb{Z}^n$, we get the vector space $L(\mathcal{A})$ of Laurent polynomials with exponents in $\mathcal{A}$. Although the introduction of Laurent polynomials might seem unmotivated

at this point, they will prove to be very useful in the theory developed in this chapter.

Additional Exercises for §1

Exercise 12. This exercise will develop the theory of affine subspaces. An *affine subspace* $A \subset \mathbb{R}^n$ is a subset with the property that

$$s_1, \dots, s_m \in A \Longrightarrow \textstyle\sum_{i=1}^m \lambda_i s_i \in A \text{ whenever } \sum_{i=1}^m \lambda_i = 1.$$

Note that we do not require that $\lambda_i \geq 0$. We also need the following definition: given a subset $S \subset \mathbb{R}^n$ and a vector $v \in \mathbb{R}^n$, the *translate of S by v* is the set $v + S = \{v + s : s \in S\}$.

a. If $A \subset \mathbb{R}^n$ is an affine subspace and $v \in A$, prove that the translate $-v + A$ is a subspace of $\mathbb{R}^n$. Also show that $A = v + (-v + A)$, so that A is a translate of a subspace.
b. If $v, w \in A$, prove that $-v + A = -w + A$. Conclude that an affine subspace is a translate of a *unique* subspace of $\mathbb{R}^n$.
c. Conversely, if $W \subset \mathbb{R}^n$ is a subspace and $v \in \mathbb{R}^n$, then show that the translate $v + W$ is an affine subspace.
d. Explain how to define the *dimension* of an affine subspace.

Exercise 13. This exercise will define the dimension of a polytope $Q \subset \mathbb{R}^n$. The basic idea is that the $\dim Q$ is the dimension of the smallest affine subspace containing Q.

a. Given any subset $S \subset \mathbb{R}^n$, show that

$$\mathrm{Aff}(S) = \{\lambda_1 s_1 + \cdots + \lambda_m s_m : s_i \in S,\ \textstyle\sum_{i=1}^m \lambda_i = 1\}$$

is the smallest affine subspace containing S. Hint: Use the strategy outlined in parts b, c and d of Exercise 1.
b. Using the previous exercise, explain how to define the dimension of a polytope $Q \subset \mathbb{R}^n$.
c. If $\mathcal{A} = \{m_1, \dots, m_l\}$ and $Q = \mathrm{Conv}(\mathcal{A})$, prove that $\dim Q = \dim W$, where $W \subset \mathbb{R}^n$ is the subspace spanned by $m_2 - m_1, \dots, m_l - m_1$.
d. Prove that a simplex in $\mathbb{R}^n$ (as defined in Exercise 2) has dimension n.

Exercise 14. Let $Q \subset \mathbb{R}^n$ be a polytope and $\nu \in \mathbb{R}^n$ be a nonzero vector.

a. Show that $m \cdot \nu = 0$ defines a subspace of $\mathbb{R}^n$ of dimension $n - 1$ and that the affine hyperplane $m \cdot \nu = -a$ is a translate of this subspace. Hint: Use the linear map $\mathbb{R}^n \to \mathbb{R}$ given by dot product with ν.
b. Explain why $\min_{m \in Q}(m \cdot \nu)$ exists. Hint: Q is closed and bounded, and $m \mapsto m \cdot \nu$ is continuous.
c. If $a_Q(\nu)$ is defined as in (1.3), then prove that the intersection

$$Q_\nu = Q \cap \{m \in \mathbb{R}^n : m \cdot \nu = -a_Q(\nu)\}$$

is nonempty and that

$$Q \subset \{m \in \mathbb{R}^n : m \cdot \nu \geq -a_Q(\nu)\}.$$

Exercise 15. There are several ways to represent the ring of Laurent polynomials in $x_1, \ldots, x_n$ as a quotient of a polynomial ring. Prove that

$$\begin{aligned} k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}] &\cong k[x_1, \ldots, x_n, t_1, \ldots, t_n]/\langle x_1 t_1 - 1, \ldots, x_n t_n - 1\rangle \\ &\cong k[x_1, \ldots, x_n, t]/\langle x_1 \cdots x_n t - 1\rangle. \end{aligned}$$

Exercise 16. This exercise will study the translates of a polytope. The translate of a set in $\mathbb{R}^n$ is defined in Exercise 12.

a. If $\mathcal{A} \subset \mathbb{R}^n$ is a finite set and $v \in \mathbb{R}^n$, prove that $\mathrm{Conv}(v + \mathcal{A}) = v + \mathrm{Conv}(\mathcal{A})$.
b. Prove that a translate of a polytope is a polytope.
c. If a polytope Q is represented by the inequalites (1.4), what are the inequalities defining $v + Q$?

Exercise 17. If $f \in k[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ is a Laurent polynomial and $\alpha \in \mathbb{Z}^n$, how is $\mathrm{NP}(x^\alpha f)$ related to $\mathrm{NP}(f)$? Hint: See the previous exercise.

§2 Sparse Resultants

The multipolynomial resultant $\mathrm{Res}_{d_1,\ldots,d_n}(F_1, \ldots, F_n)$ discussed in Chapter 3 is a *very* large polynomial, partly due to the size of the input polynomials $F_1, \ldots, F_n$. They have *lots* of coefficients, especially as their total degree increases. In practice, when people deal with polynomials of large total degree, they rarely use all of the coefficients. It's much more common to encounter *sparse polynomials*, which involve only exponents lying in a finite set $\mathcal{A} \subset \mathbb{Z}^n$. This suggests that there should be a corresponding notion of *sparse resultant*.

To begin our discussion of sparse resultants, we return to the implicitization problem introduced in §2 of Chapter 3. Consider the surface parametrized by the equations

$$\begin{aligned} x &= f(s,t) = a_0 + a_1 s + a_2 t + a_3 st \\ y &= g(s,t) = b_0 + b_1 s + b_2 t + b_3 st \\ z &= h(s,t) = c_0 + c_1 s + c_2 t + c_3 st, \end{aligned} \tag{2.1}$$

where $a_0, \ldots, c_3$ are constants. This is sometimes called a *bilinear surface parametrization*. We will assume

$$\det \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \neq 0 \tag{2.2}$$

In Exercise 7 at the end of the section, you will show that this condition rules out the trivial case when (2.1) parametrizes a plane.

Our goal is to find the implicit equation of (2.1). This means finding a polynomial $p(x, y, z)$ such that $p(x, y, z) = 0$ if and only if x, y, z are given by (2.1) for some choice of s, t. In Proposition (2.6) of Chapter 3, we used the resultant

$$p(x, y, z) = \mathrm{Res}_{2,2,2}(F - xu^2, G - yu^2, H - zu^2) \tag{2.3}$$

to find the implicit equation, where F, G, H are the homogenization of f, g, h with respect to u. Unfortunately, this method fails for the case at hand.

Exercise 1. Show that the resultant (2.3) vanishes identically when F, G, H come from homogenizing the polynomials in (2.1). Hint: You already did a special case of this in Exercise 2 of Chapter 3, §2.

The remarkable fact is that although the multipolynomial resultant from Chapter 3 fails, a *sparse resultant* still exists in this case. In Exercise 2 below, you will show that the implicit equation for (2.1) is given by the determinant

$$p(x, y, z) = \det \begin{pmatrix} a_0 - x & a_1 & a_2 & a_3 & 0 & 0 \\ b_0 - y & b_1 & b_2 & b_3 & 0 & 0 \\ c_0 - z & c_1 & c_2 & c_3 & 0 & 0 \\ 0 & a_0 - x & 0 & a_2 & a_1 & a_3 \\ 0 & b_0 - y & 0 & b_2 & b_1 & b_3 \\ 0 & c_0 - x & 0 & c_2 & c_1 & c_3 \end{pmatrix}. \tag{2.4}$$

Expanding this 6×6 determinant, we see that $p(x, y, z)$ is a polynomial of total degree 2 in x, y and z.

Exercise 2.

a. If x, y, z are as in (2.1), show that the determinant (2.4) vanishes. Hint: Consider the system of equations obtained by multiplying each equation of (2.1) by 1 and s. You should get 6 equations in the 6 "unknowns" $1, s, t, st, s^2, st^2$. Notice the similarity with Proposition (2.10) of Chapter 3.

b. Next assume (2.4) vanishes. We want to prove the existence of s, t such that (2.1) holds. As a first step, let A be the matrix of (2.4) and explain why we can find a nonzero column vector $v = (\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5, \alpha_6)^T$ (T denotes transpose) such that $Av = 0$. Then use (2.2) to prove that $\alpha_1 \neq 0$. Hint: Write out $Av = 0$ explicitly and use the first three equations. Then use the final three.

c. If we take the vector v of part b and multiply by $1/\alpha_1$, we can write v in the form $v = (1, s, t, \alpha, \beta, \gamma)$. Explain why it suffices to prove that $\alpha = st$.

d. Use (2.2) to prove $\alpha = st$, $\beta = s^2$ and $\gamma = s\alpha$. This will complete the proof that the implicit equation of (2.1) is given by (2.4). Hint: In the equations $Av = 0$, eliminate $a_0 - x, b_0 - y, c_0 - z$.
e. Explain why the above proof gives a linear algebra method to find s, t for a given point (x, y, z) on the surface. This solves the *inversion problem* for the parametrized surface. Hint: In the notation of part b, you will show that $s = \alpha_2/\alpha_1$ and $t = \alpha_3/\alpha_1$.

A goal of this section is to explain why a resultant like (2.4) can exist even though the standard multipolynomial resultant (2.3) vanishes identically. The basic reason is that although the equations (2.1) are quadratic in s, t, they do *not* use all monomials of total degree ≤ 2 in s, t. The *sparse resultant* works like the multipolynomial resultant of §2, except that we restrict the exponents occurring in the equations.

For simplicity, we will only treat the special case when all of the equations have exponents lying in the same set, leaving the general case for §6. We will also work exclusively over the field $\mathbb{C}$ of complex numbers. Thus, suppose that the variables are $t_1, \dots, t_n$, and fix a finite set $\mathcal{A} = \{m_1, \dots, m_l\} \subset \mathbb{Z}^n$ of exponents. Since negative exponents can occur, we will use the Laurent polynomials

$$f = a_1 t^{m_1} + \cdots + a_l t^{m_l} \in L(\mathcal{A}),$$

as defined in §1. Given $f_0, \dots, f_n \in L(\mathcal{A})$, we get $n + 1$ equations in n unknowns $t_1, \dots, t_n$:

$$\begin{aligned} f_0 &= a_{01} t^{m_1} + \cdots + a_{0l} t^{m_l} = 0 \\ &\vdots \\ f_n &= a_{n1} t^{m_1} + \cdots + a_{nl} t^{m_l} = 0. \end{aligned} \tag{2.5}$$

In seeking solutions of these equations, the presence of negative exponents means that we should consider only *nonzero* solutions of (2.5). We will use the notation

$$\mathbb{C}^* = \mathbb{C} \setminus \{0\}$$

for the set of nonzero complex numbers.

The sparse resultant will be a polynomial in the coefficents a_{ij} which vanishes precisely when we can find a "solution" of (2.5). We put "solution" in quotes because although the previous paragraph suggests that solutions should lie in $(\mathbb{C}^*)^n$, the situation is actually more complicated. For instance, the multipolynomial resultants from Chapter 3 use homogeneous polynomials, which means that the "solutions" lie in projective space. The situation for sparse resultants is similar, though with a twist: a "solution" of (2.5) need not lie in $(\mathbb{C}^*)^n$, but the space where it does lie need not be $\mathbb{P}^n$. For example, we will see in §3 that for equations like (2.1), the "solutions" lie in $\mathbb{P}^1 \times \mathbb{P}^1$ rather than $\mathbb{P}^2$.

To avoid the problem of where the solutions lie, we will take a conservative approach and initially restrict the solutions to lie in $(\mathbb{C}^*)^n$. Then, in (2.5), the coefficients give a point $(a_{ij}) \in \mathbb{C}^{(n+1)\times l}$, and we consider the subset

$$Z_0(\mathcal{A}) = \{(a_{ij}) \in \mathbb{C}^{(n+1)\times l} : (2.5) \text{ has a solution in } (\mathbb{C}^*)^n\}.$$

Since $Z_0(\mathcal{A})$ might not be a variety in $\mathbb{C}^{(n+1)l}$, we use the following fact:

- (Zariski Closure) Given a subset $S \subset \mathbb{C}^m$, there is a smallest affine variety $\overline{S} \subset \mathbb{C}^m$ containing S. We call $\overline{S}$ the *Zariski closure* of S.

(See, for example, [CLO], §4 of Chapter 4.) Then let $Z(\mathcal{A}) = \overline{Z_0(\mathcal{A})}$ be the Zariski closure of $Z_0(\mathcal{A})$.

The sparse resultant will be the equation defining $Z(\mathcal{A}) \subset \mathbb{C}^{(n+1)l}$. To state our result precisely, we introduce a variable u_{ij} for each coefficient a_{ij}. Then, for a polynomial $P \in \mathbb{C}[u_{ij}]$, we let $P(f_0, \dots, f_n)$ denote the number obtained by replacing each variable u_{ij} with the corresponding coefficient a_{ij} from (2.5). We can now state the basic existence result for the sparse resultant.

(2.6) Theorem. *Let $\mathcal{A} \subset \mathbb{Z}^n$ be a finite set, and assume that* $\mathrm{Conv}(\mathcal{A})$ *is an n-dimensional polytope. Then there is an irreducible polynomial* $\mathrm{Res}_{\mathcal{A}} \in \mathbb{Z}[u_{ij}]$ *such that for $(a_{ij}) \in \mathbb{C}^{(n+1)l}$, we have*

$$(a_{ij}) \in Z(\mathcal{A}) \Longleftrightarrow \mathrm{Res}_{\mathcal{A}}(a_{ij}) = 0.$$

In particular, if (2.5) has a solution with $t_1, \dots, t_n \in \mathbb{C}^*$, then

$$\mathrm{Res}_{\mathcal{A}}(f_0, \dots, f_n) = 0.$$

PROOF. See [GKZ], Chapter 8. □

The sparse resultant or $\mathcal{A}$-resultant is the polynomial $\mathrm{Res}_{\mathcal{A}}$. Notice that $\mathrm{Res}_{\mathcal{A}}$ is determined uniquely up to $\pm$ since it is irreducible in $\mathbb{Z}[u_{ij}]$. The condition that the convex hull of $\mathcal{A}$ has dimension n is needed to ensure that we have the right number of equations in (2.5). Here is an example of what can happen when the convex hull has strictly lower dimension.

Exercise 3. Let $\mathcal{A} = \{(1,0),(0,1)\} \subset \mathbb{Z}^2$, so that $f_i = a_{i1}t_1 + a_{i2}t_2$ for $i = 0, 1, 2$. Show that rather than one condition for $f_1 = f_2 = f_3 = 0$ to have a solution, there are three. Hint: See part b of Exercise 1 from Chapter 3, §2.

We next show that the multipolynomial resultant from Chapter 3 is a special case of the sparse resultant. For $d > 0$, let

$$\mathcal{A}_d = \{m \in \mathbb{Z}^n_{\geq 0} : |m| \leq d\}.$$

Also consider variables $x_0, \dots, x_n$, which will be related to $t_1, \dots, t_n$ by $t_i = x_i/x_0$ for $1 \leq i \leq n$. Then we homogenize the f_i from (2.5) in the

usual way, defining

$$F_i(x_0,\dots,x_n) = x_0^d f_i(t_1,\dots,t_n) = x_0^d f_i(x_1/x_0,\dots,x_n/x_0) \tag{2.7}$$

for $0 \le i \le n$. This gives $n+1$ homogeneous polynomials F_i in the $n+1$ variables $x_0,\dots,x_n$. Note that the F_i all have total degree d.

(2.8) Proposition. *For $\mathcal{A}_d = \{m \in \mathbb{Z}^n_{\ge 0} : |m| \le d\}$, we have*

$$\mathrm{Res}_{\mathcal{A}_d}(f_0,\dots,f_n) = \pm \mathrm{Res}_{d,\dots,d}(F_0,\dots,F_n),$$

where $\mathrm{Res}_{d,\dots,d}$ is the multipolynomial resultant from Chapter 3.

PROOF. If (2.5) has a solution $(t_1,\dots,t_n) \in (\mathbb{C}^*)^n$, then $(x_0,\dots,x_n) = (1,t_1,\dots,t_n)$ is a nontrivial solution of $F_0 = \cdots = F_n = 0$. This shows that $\mathrm{Res}_{d,\dots,d}$ vanishes on $Z_0(\mathcal{A}_d)$. By the definition of Zariski closure, it must vanish on $Z(\mathcal{A}_d)$. Since $Z(\mathcal{A}_d)$ is defined by the irreducible equation $\mathrm{Res}_{\mathcal{A}_d} = 0$, the argument of Proposition (2.10) of Chapter 3 shows that $\mathrm{Res}_{d,\dots,d}$ is a multiple of $\mathrm{Res}_{\mathcal{A}_d}$. But $\mathrm{Res}_{d,\dots,d}$ is an irreducible polynomial by Theorem (2.3) of Chapter 3, and the desired equality follows. □

Because $\mathcal{A}_d = \{m \in \mathbb{Z}^n_{\ge 0} : |m| \le d\}$ gives *all* exponents of total degree at most d, the multipolynomial resultant $\mathrm{Res}_{d,\dots,d}$ is sometimes called the *dense* resultant, in contrast to the *sparse* resultant $\mathrm{Res}_{\mathcal{A}}$.

We next discuss the structure of the polynomial $\mathrm{Res}_{\mathcal{A}}$ in more detail. Our first question concerns its total degree, which is determined by the convex hull $Q = \mathrm{Conv}(\mathcal{A})$. The intuition is that as Q gets larger, so does the sparse resultant. As in §1, we measure the size of Q using its volume $\mathrm{Vol}_n(Q)$. This affects the degree of $\mathrm{Res}_{\mathcal{A}}$ as follows.

(2.9) Theorem. *Let $\mathcal{A} = \{m_1,\dots,m_l\}$, and assume that every element of $\mathbb{Z}^n$ is an integer linear combination of $m_2 - m_1,\dots,m_l - m_1$. Then, if we fix i between 0 and n, $\mathrm{Res}_{\mathcal{A}}$ is homogeneous in the coefficients of each f_i of degree $n!\,\mathrm{Vol}_n(Q)$, where $Q = \mathrm{Conv}(\mathcal{A})$. This means that*

$$\mathrm{Res}_{\mathcal{A}}(f_0,\dots,\lambda f_i,\dots,f_n) = \lambda^{n!\,\mathrm{Vol}_n(Q)}\mathrm{Res}_{\mathcal{A}}(f_0,\dots,f_n).$$

Furthermore, the total degree of $\mathrm{Res}_{\mathcal{A}}$ is $(n+1)!\,\mathrm{Vol}_n(Q)$.

PROOF. The first assertion is proved in [GKZ], Chapter 8. As we observed in Exercise 1 of Chapter 3, §3, the final assertion follows by considering $\mathrm{Res}_{\mathcal{A}}(\lambda f_0,\dots,\lambda f_n)$. □

For an example of Theorem (2.9), note that $\mathcal{A}_d = \{m \in \mathbb{Z}^n_{\ge 0} : |m| \le d\}$ satisfies the hypothesis of the theorem, and its convex hull has volume $d^n/n!$ by Exercise 3 of §1. Using Proposition (2.8), we conclude that $\mathrm{Res}_{d,\dots,d}$ has degree d^n in F_i. This agrees with the prediction of Theorem (3.1) of Chapter 3.

We can also explain how the hypothesis of Theorem (2.9) relates to Theorem (2.6). If the $m_i - m_1$ span over $\mathbb{Z}$, they also span over $\mathbb{R}$, so that the convex hull $Q = \text{Conv}(\mathcal{A})$ has dimension n by Exercise 13 of §1. Thus Theorem (2.9) places a stronger condition on $\mathcal{A} \subset \mathbb{Z}^n$ than Theorem (2.6). The following example shows what can go wrong if the $m_i - m_1$ don't span over $\mathbb{Z}$.

Exercise 4. Let $\mathcal{A} = \{0, 2\} \subset \mathbb{Z}$, so that $\text{Vol}_1(\text{Conv}(\mathcal{A})) = 2$.

a. Let $f_0 = a_{01} + a_{02}t^2$ and $f_1 = a_{11} + a_{12}t^2$. If the equations $f_0 = f_1 = 0$ have a solution in $(\mathbb{C}^*)^2$, show that $a_{01}a_{12} - a_{02}a_{11} = 0$.

b. Use part a to prove $\text{Res}_{\mathcal{A}}(f_0, f_1) = a_{01}a_{12} - a_{02}a_{11}$.

c. Explain why the formula of part b does not contradict Theorem (2.9).

Using Theorem (2.9), we can now determine some sparse resultants using the methods of earlier sections. For example, suppose $\mathcal{A} = \{(0,0), (1,0), (0,1), (1,1)\} \subset \mathbb{Z}^2$, and consider the equations

$$\begin{aligned} f(s,t) &= a_0 + a_1 s + a_2 t + a_3 st = 0 \\ g(s,t) &= b_0 + b_1 s + b_2 t + b_3 st = 0 \\ h(s,t) &= c_0 + c_1 s + c_2 t + c_3 st = 0. \end{aligned} \tag{2.10}$$

The exercise below will show that that in this case, the sparse resultant is given by a determinant:

$$\text{Res}_{\mathcal{A}}(f,g,h) = \pm \det \begin{pmatrix} a_0 & a_1 & a_2 & a_3 & 0 & 0 \\ b_0 & b_1 & b_2 & b_3 & 0 & 0 \\ c_0 & c_1 & c_2 & c_3 & 0 & 0 \\ 0 & a_0 & 0 & a_2 & a_1 & a_3 \\ 0 & b_0 & 0 & b_2 & b_1 & b_3 \\ 0 & c_0 & 0 & c_2 & c_1 & c_3 \end{pmatrix} \tag{2.11}$$

Exercise 5. As above, let $\mathcal{A} = \{(0,0), (1,0), (0,1), (1,1)\}$.

a. Adapt the argument of Exercise 2 to show that if (2.10) has a solution in $(\mathbb{C}^*)^2$, then the determinant in (2.11) vanishes.

b. Adapt the argument of Proposition (2.10) of Chapter 3 to show that $\text{Res}_{\mathcal{A}}$ divides the determinant in (2.11).

c. By comparing degrees and using Theorem (2.9), show that the determinant is an integer multiple of $\text{Res}_{\mathcal{A}}$.

d. Show that the integer is ± 1 by computing the determinant when $f = 1 + st$, $g = s$ and $h = t$.

It follows that the implicitization problem (2.1) can be solved by setting

$$p(x,y,z) = \text{Res}_{\mathcal{A}}(f - x, g - y, h - z), \tag{2.12}$$

where $\mathcal{A}$ is as above. Comparing this to (2.3), we see from Proposition (2.8) that $\text{Res}_{2,2,2}$ corresponds to $\mathcal{A}_2 = \mathcal{A} \cup \{(2,0), (0,2)\}$. The convex hull of

$\mathcal{A}_2$ is strictly larger than the convex hull of $\mathcal{A}$. This explains why our earlier attempt failed—the convex hull was too big!

We also have the following sparse analog of Theorem (3.5) discussed in Chapter 3.

(2.13) Theorem. *When $\mathcal{A}$ satisfies the hypothesis of Theorem (2.9), the resultant $\operatorname{Res}_{\mathcal{A}}$ has the following properties:*

a. *If $g_i = \sum_{i=0}^{n} b_{ij} f_j$, where (b_{ij}) is an invertible matrix, then*

$$\operatorname{Res}_{\mathcal{A}}(g_0, \dots, g_n) = \det(b_{ij})^{n!\operatorname{Vol}(Q)} \operatorname{Res}_{\mathcal{A}}(f_0, \dots, f_n).$$

b. *Given indices $1 \le k_0 \le \cdots \le k_n \le l$, the* **bracket** $[k_0 \dots k_n]$ *is defined to be the determinant*

$$[k_0 \dots k_n] = \det(u_{i,k_j}) \in \mathbb{Z}[u_{ij}].$$

Then $\operatorname{Res}_{\mathcal{A}}$ is a polynomial in the brackets $[k_0 \dots k_n]$.

Proof. See [GKZ], Chapter 8. As explained in the proof of Theorem (3.5) of Chapter 3, the second part follows from the first. In §4, we will prove that $n!\operatorname{Vol}(Q)$ is an integer since Q is a lattice polytope. □

Exercise 6. As in Exercise 5, let $\mathcal{A} = \{(0,0), (1,0), (0,1), (1,1)\}$. Then prove that

$$\operatorname{Res}_{\mathcal{A}}(f, g, h) = [013][023] - [012][123]. \tag{2.14}$$

Hint: Expand the determinant (2.11) three times along certain well-chosen rows and columns.

The answer to Exercise 6 is more interesting than first meets the eye. Label the points in $\mathcal{A} = \{(0,0), (1,0), (0,1), (1,1)\}$ as $0, 1, 2, 3$, corresponding to the subscripts of the coefficients in (2.10). Then the brackets appearing in (2.14) correspond to the two ways of dividing the square $Q = \operatorname{Conv}(\mathcal{A})$ into triangles. This is illustrated in Fig. 7.4 on the next page, where the figure on the left corresponds to [013][023], and the one on the right to [012][123].

The amazing fact is that this is no accident! In general, when we express $\operatorname{Res}_{\mathcal{A}}$ as a polynomial in the brackets $[k_0 \dots k_n]$, there is a very deep relationship between certain terms in this polynomial and triangulations of the polytope $Q = \operatorname{Conv}(\mathcal{A})$. The details can be found in [KSZ]. See also [Stu4] for some nice examples.

Many of the other properties of multipolynomial resultants mentioned in §3 and §4 have sparse analogs. We refer the reader to [GKZ, Chapter 8] and [PS2] for further details.

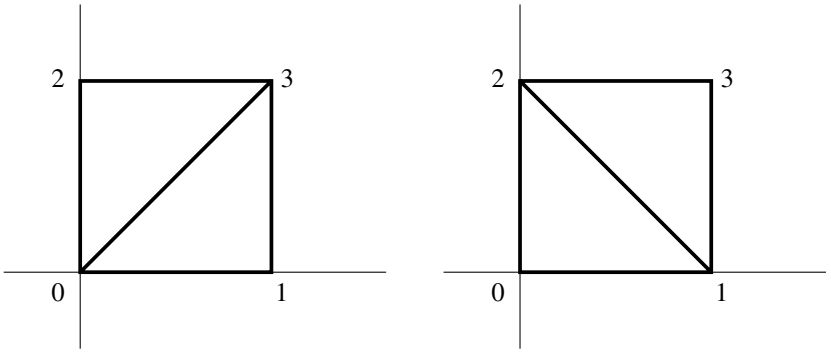

FIGURE 7.4. Triangulations of the unit square

Our account of sparse resultants is by no means complete, and in particular, we have the following questions:

- When $\mathrm{Res}_{\mathcal{A}}(f_0, \ldots, f_n)$ vanishes, the equations (2.5) should have a solution, but where? In §3, we will see that *toric varieties* provide a natural answer to this question.
- What happens when the polynomials in (2.5) have exponents not lying in the same set $\mathcal{A}$? We will explore what happens in §6.
- How do we compute $\mathrm{Res}_{\mathcal{A}}(f_0, \ldots, f_n)$? We will (very briefly) sketch one method in §6 and give references to other methods in the literature.
- What are sparse resultants good for? We've used them for implicitization in (2.12), and applications to solving equations will be covered in §6. A brief discussion of applications to geometric modeling, computational geometry, vision and molecular structure can be found in [Emi2].

We should also mention that besides sparse resultants, some other types of resultants have been studied in recent years. For example:

- The paper [BEM1] defines a notion of resultant which works for any unirational variety. (A projective variety is *unirational* if there is a surjective rational map from $\mathbb{P}^n$ to the variety.)
- When a unirational variety is a blow-up of $\mathbb{P}^n$, the resultant of [BEM1] is called a *residual resultant*. This is studied in [BEM2] when the center of the blow-up is a complete intersection, and [Bus] considers what happens when the center is a local complete intersection in $\mathbb{P}^2$.
- In a different direction, consider polynomials whose Newton polytopes are rectangles with smaller rectangles cut out of each corner. Because we cut out rectangles, we are not using all lattice points in the convex hull. Some interesting formulas for these resultants are given in [ZG] and [Chi].

Additional Exercises for §2

Exercise 7. Let B be the 3×3 matrix in (2.2). In this exercise, we will show that the parametrization (2.1) lies in a plane $\alpha x + \beta y + \gamma z = \delta$ if and only if $\det(B) = 0$.

a. First, if the parametrization lies in the plane $\alpha x+\beta y+\gamma z = \delta$, then show that $Bv = 0$, where $v = (\alpha, \beta, \gamma)^t$. Hint: If a polynomial in s, t equals zero for all values of s and t, then the coefficients of the polynomial must be zero.

b. Conversely, if $\det(B) = 0$, then we can find a nonzero column vector $v = (\alpha, \beta, \gamma)^t$ such that $Bv = 0$. Show that $\alpha x + \beta y + \gamma z = \delta$ for an appropriately chosen δ.

Exercise 8. Given $\mathcal{A} = \{m_1, \dots, m_l\} \subset \mathbb{Z}^n$ and $v \in \mathbb{Z}^n$, let $v + \mathcal{A} = \{v + m_1, \dots, v + m_l\}$. Explain why $\mathrm{Res}_{\mathcal{A}} = \mathrm{Res}_{v+\mathcal{A}}$. Hint: Remember that in defining the resultant, we only use solutions of the equations (2.5) with $t_1, \dots, t_n \in \mathbb{C}^*$.

Exercise 9. For $\mathcal{A} = \{(0,0), (1,0), (0,1), (1,1), (2,0)\}$, compute $\mathrm{Res}_{\mathcal{A}}$ using the methods of Exercise 5. Hint: Let the variables be s, t, and let the equations be $f = g = h = 0$ with coefficients $a_0, \dots, c_4$. Multiply each of the three equations by $1, s, t$. This will give you a 9×9 determinant. The tricky part is finding polynomials f, g, h such that the determinant is ± 1. See part d of Exercise 5.

Exercise 10. This exercise will explore the *Dixon resultant* introduced by Dixon in 1908. See Section 2.4 of [Stu4] for some nice examples. Let

$$\mathcal{A}_{l,m} = \{(a, b) \in \mathbb{Z}^2 : 0 \le a \le l,\ 0 \le b \le m\}.$$

Note that $\mathcal{A}_{l,m}$ has $(l + 1)(m + 1)$ elements. Let the variables be s, t. Our goal is to find a determinant formula for $\mathrm{Res}_{\mathcal{A}_{l,m}}$.

a. Given $f, g, h \in L(\mathcal{A}_{l,m})$, we get equations $f = g = h = 0$. Multiplying these equations by $s^a t^b$ for $(a, b) \in \mathcal{A}_{2l-1,m-1}$, show that you get a system of $6lm$ equations in the $6lm$ "unknowns" $s^a t^b$ for $(a, b) \in \mathcal{A}_{3l-1,2m-1}$. Hint: For $l = m = 1$, this is *exactly* what you did in Exercise 1.

b. If A is the matrix of part a, conclude that $\det(A) = 0$ whenever $f = g = h = 0$ has a solution $(s, t) \in (\mathbb{C}^*)^2$. Also show that $\det(A)$ has total degree $2lm$ in the coefficients of f, and similarly for g and h.

c. What is the volume of the convex hull of $\mathcal{A}_{l,m}$?

d. Using Theorems (2.6) and (2.9), show that $\det(A)$ is a constant multiple of $\mathrm{Res}_{\mathcal{A}_{l,m}}$.

e. Show that the constant is ± 1 by considering $f = 1 + s^l t^m$, $g = s^l$ and $h = t^m$. Hint: In this case, A has $4lm$ rows with only one nonzero entry. Use this to reduce to a $2lm \times 2lm$ matrix.

§3 Toric Varieties

Let $\mathcal{A} = \{m_1, \dots, m_l\} \subset \mathbb{Z}^n$, and suppose that

$$f_i = a_{i1}t^{m_1} + \cdots + a_{il}t^{m_l}, \qquad i = 0, \dots, n$$

are $n+1$ Laurent polynomials in $L(\mathcal{A})$. The basic question we want to answer in this section is: *If* $\operatorname{Res}_{\mathcal{A}}(f_0, \dots, f_n) = 0$*, where do the equations*

$$f_0 = \cdots = f_n = 0 \tag{3.1}$$

have a solution? In other words, what does it mean for the resultant to vanish?

For $\mathcal{A}_d = \{m \in \mathbb{Z}^n_{\geq 0} : |M| \leq d\}$, we know the answer. Here, we homogenize $f_0, \dots, f_n$ as in (2.7) to get $F_0, \dots, F_n$. Proposition (2.8) implies

$$\operatorname{Res}_{\mathcal{A}_d}(f_0, \dots, f_n) = \operatorname{Res}_{d,\dots,d}(F_0, \dots, F_n),$$

and then Theorem (2.3) of Chapter 3 tells us

$$\operatorname{Res}_{d,\dots,d}(F_0, \dots, F_n) = 0 \Longleftrightarrow \begin{cases} F_0 = \cdots = F_n = 0 \\ \text{has a nontrivial solution.} \end{cases} \tag{3.2}$$

Recall that a *nontrivial* solution means $(x_0, \dots, x_n) \neq (0, \dots, 0)$, i.e., a solution in $\mathbb{P}^n$. Thus, by going from $(\mathbb{C}^*)^n$ to $\mathbb{P}^n$ and changing to homogeneous coordinates in (3.1), we get a space where the vanishing of the resultant means that our equations have a solution.

To understand what happens in the general case, suppose that $\mathcal{A} = \{m_1, \dots, m_l\} \subset \mathbb{Z}^n_{\geq 0}$, and assume that $Q = \operatorname{Conv}(\mathcal{A})$ has dimension n. Then consider the map

$$\phi_{\mathcal{A}} : (\mathbb{C}^*)^n \longrightarrow \mathbb{P}^{l-1}$$

defined by

$$\phi_{\mathcal{A}}(t_1, \dots, t_n) = (t^{m_1}, \dots, t^{m_l}). \tag{3.3}$$

Note that $(t^{m_1}, \dots, t^{m_l})$ is never the zero vector since $t_i \in \mathbb{C}^*$ for all i. Thus $\phi_{\mathcal{A}}$ is defined on all of $(\mathbb{C}^*)^n$, though the image of $\phi_{\mathcal{A}}$ need not be a subvariety of $\mathbb{P}^{l-1}$. Then the *toric variety* $X_{\mathcal{A}}$ is the Zariski closure of the image of $\phi_{\mathcal{A}}$, i.e.,

$$X_{\mathcal{A}} = \overline{\phi_{\mathcal{A}}\big((\mathbb{C}^*)^n\big)} \subset \mathbb{P}^{l-1}.$$

Toric varieties are an important area of research in algebraic geometry and feature in many applications. The reader should consult [GKZ] or [Stu2] for an introduction to toric varieties. There is also a more abstract theory of toric varieties, as described in [Ful]. See [Cox4] for an elementary introduction.

For us, the key fact is that the equations $f_i = a_{i1}t^{m_1} + \cdots + a_{il}t^{m_l} = 0$ from (3.1) extend naturally to $X_{\mathcal{A}}$. To see how this works, let $u_1, \dots, u_l$

be homogeneous coordinates on $\mathbb{P}^{l-1}$. Then consider the linear function $L_i = a_{i1}u_1 + \cdots + a_{il}u_l$, and notice that $f_i = L_i \circ \phi_{\mathcal{A}}$. However, L_i is not a function on $\mathbb{P}^{l-1}$ since $u_1, \ldots, u_l$ are homogeneous coordinates. But the equation $L_i = 0$ still makes sense on $\mathbb{P}^{l-1}$ (be sure you understand why), so in particular, $L_i = 0$ makes sense on $X_{\mathcal{A}}$. Since L_i and f_i have the same coefficients, we can write $\mathrm{Res}_{\mathcal{A}}(L_0, \ldots, L_n)$ instead of $\mathrm{Res}_{\mathcal{A}}(f_0, \ldots, f_n)$. Then we can characterize the vanishing of the resultant as follows.

(3.4) Theorem.

$$\mathrm{Res}_{\mathcal{A}}(L_0, \ldots, L_n) = 0 \Longleftrightarrow \begin{cases} L_0 = \cdots = L_n = 0 \\ \textit{has a solution in } X_{\mathcal{A}}. \end{cases}$$

Proof. See Proposition 2.1 of Chapter 8 of [GKZ]. This result is also discussed in [KSZ]. □

This theorem tells us that the resultant vanishes if and only if (3.1) has a solution in the toric variety $X_{\mathcal{A}}$. From a more sophisticated point of view, Theorem (3.4) says that $\mathrm{Res}_{\mathcal{A}}$ is closely related to the *Chow form* of $X_{\mathcal{A}}$.

To get a better idea of what Theorem (3.4) means, we will work out two examples. First, if $\mathcal{A}_d = \{m \in \mathbb{Z}^n_{\geq 0} : |m| \leq d\}$, let's show that $X_{\mathcal{A}_d} = \mathbb{P}^n$. Let $x_0, \ldots, x_n$ be homogeneous coordinates on $\mathbb{P}^n$, so that by Exercise 19 of Chapter 3, §4, there are $N = \binom{d+n}{n}$ monomials of total degree d in $x_0, \ldots, x_n$. These monomials give a map

$$\Phi_d : \mathbb{P}^n \longrightarrow \mathbb{P}^{N-1}$$

defined by $\Phi_d(x_0, \ldots, x_n) = (\ldots, x^\alpha, \ldots)$, where we use all monomials x^α of total degree d. In Exercise 6 at the end of the section, you will show that Φ_d is well-defined and one-to-one. We call Φ_d the *Veronese map*. The image of Φ_d is a variety by the following basic fact.

- (Projective Images) Let $\Psi : \mathbb{P}^n \to \mathbb{P}^{N-1}$ be defined by $\Psi(x_0, \ldots, x_n) = (h_1, \ldots, h_N)$, where the h_i are homogeneous of the same degree and don't vanish simultaneously on $\mathbb{P}^n$. Then the image $\Psi(\mathbb{P}^n) \subset \mathbb{P}^{N-1}$ is a variety.

(See §5 of Chapter 8 of [CLO].) For $t_1, \ldots, t_n \in \mathbb{C}^*$, observe that

$$\Phi_d(1, t_1, \ldots, t_n) = \phi_{\mathcal{A}_d}(t_1, \ldots, t_n), \tag{3.5}$$

where $\phi_{\mathcal{A}_d}$ is from (3.3) (see Exercise 6). Thus $\Phi_d(\mathbb{P}^n)$ is a variety containing $\phi_{\mathcal{A}_d}\big((\mathbb{C}^*)^n\big)$, so that $X_{\mathcal{A}_d} \subset \Phi_d(\mathbb{P}^n)$. Exercise 6 will show that equality occurs, so that $X_{\mathcal{A}_d} = \Phi_d(\mathbb{P}^n)$. Finally, since Φ_d is one-to-one, $\mathbb{P}^n$ can be identified with its image under Φ_d (we are omitting some details here), and we conclude that $X_{\mathcal{A}_d} = \mathbb{P}^n$. It follows from Theorem (3.4) that for homogeneous polynomials $F_0, \ldots, F_n$ of degree d,

$$\mathrm{Res}_{d,\ldots,d}(F_0, \ldots, F_n) = 0 \Longleftrightarrow \begin{cases} F_0 = \cdots = F_n = 0 \\ \text{has a solution in } \mathbb{P}^n. \end{cases}$$

Thus we recover the characterization of $\mathrm{Res}_{d,\dots,d}$ given in (3.2).

For a second example, you will show in the next exercise that $\mathbb{P}^1 \times \mathbb{P}^1$ is the toric variety where the equations (2.10) have a solution when the resultant vanishes.

Exercise 1. Let $\mathcal{A} = \{(0,0),(1,0),(0,1),(1,1)\}$. Then $\phi_{\mathcal{A}}(s,t) = (1,s,t,st) \in \mathbb{P}^3$ and $X_{\mathcal{A}}$ is the Zariski closure of the image of $\phi_{\mathcal{A}}$. A formula for $\mathrm{Res}_{\mathcal{A}}$ is given in (2.11).

a. Let the coordinates on $\mathbb{P}^1 \times \mathbb{P}^1$ be (u,s,v,t), so that (u,s) are homogeneous coordinates on the first $\mathbb{P}^1$ and (v,t) are homogeneous coordinates on the second. Show that the *Segre map* $\Phi : \mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^3$ defined by $\Phi(u,s,v,t) = (uv, sv, ut, st)$ is well-defined and one-to-one.
b. Show that the image of Φ is $X_{\mathcal{A}}$ and explain why this allows us to identify $\mathbb{P}^1 \times \mathbb{P}^1$ with $X_{\mathcal{A}}$.
c. Explain why the "homogenizations" of f, g, h from (2.10) are

$$\begin{aligned} F(u,s,v,t) &= a_0uv + a_1sv + a_2ut + a_3st = 0 \\ G(u,s,v,t) &= b_0uv + b_1sv + b_2ut + b_3st = 0 \\ H(u,s,v,t) &= c_0uv + c_1sv + c_2ut + c_3st = 0, \end{aligned} \tag{3.6}$$

and then prove that $\mathrm{Res}_{\mathcal{A}}(F,G,H) = 0$ if and only if $F = G = H = 0$ has a solution in $\mathbb{P}^1 \times \mathbb{P}^1$. In Exercises 7 and 8 at the end of the section, you will give an elementary proof of this assertion.

Exercise 1 can be restated as saying that $\mathrm{Res}_{\mathcal{A}}(F,G,H) = 0$ if and only if $F = G = H = 0$ has a *nontrivial* solution (u,s,v,t), where nontrivial now means $(u,s) \neq (0,0)$ and $(v,t) \neq (0,0)$. This is similar to (3.2), except that we "homogenized" (3.1) in a different way, and "nontrivial" has a different meaning.

Our next task is to show that there is a systematic procedure for homogenizing the equations (3.1). The key ingredient will again be the polytope $Q = \mathrm{Conv}(\mathcal{A})$. In particular, we will use the facets and inward normals of Q, as defined in §1. If Q has facets $\mathcal{F}_1, \dots, \mathcal{F}_N$ with inward pointing normals $\nu_1, \dots, \nu_N$ respectively, each facet $\mathcal{F}_j$ lies in the supporting hyperplane defined by $m \cdot \nu_j = -a_j$, and according to (1.4), the polytope Q is given by

$$Q = \{m \in \mathbb{R}^n : m \cdot \nu_j \geq -a_j \text{ for all } j = 1, \dots, N\}. \tag{3.7}$$

As usual, we assume that $\nu_j \in \mathbb{Z}^n$ is the unique primitive inward pointing normal of the facet $\mathcal{F}_j$.

We now explain how to homogenize the equations (3.1) in the general case. Given the representation of Q as in (3.7), we introduce new variables $x_1, \dots, x_N$. These "facet variables" are related to $t_1, \dots, t_n$ by the substitution

$$t_i = x_1^{\nu_{1i}} x_2^{\nu_{2i}} \cdots x_N^{\nu_{Ni}}, \qquad i = 1, \dots, n \tag{3.8}$$

where ν_{ji} is the ith coordinate of ν_j. Then the "homogenization" of $f(t_1, \dots, t_n)$ is

$$F(x_1, \dots, x_n) = \left(\prod_{j=1}^N x_j^{a_j}\right) f(t_1, \dots, t_n), \tag{3.9}$$

where each t_i is replaced with (3.8). Note the similarity with (2.7). The homogenization of the monomial t^m will be denoted $x^{\alpha(m)}$. An explicit formula for $x^{\alpha(m)}$ will be given below.

Since the inward normals ν_j can have negative coordinates, negative exponents can appear in (3.8). Nevertheless, the following lemma shows that $x^{\alpha(m)}$ has no negative exponents in the case we are interested in.

(3.10) Lemma. *If $m \in Q$, then $x^{\alpha(m)}$ is a monomial in $x_1, \dots, x_N$ with nonnegative exponents.*

PROOF. Write $m \in \mathbb{Z}^n$ as $m = \sum_{i=1}^n a_i e_i$. Since $\nu_{ji} = \nu_j \cdot e_i$, (3.8) implies

$$t^m = x_1^{m\cdot\nu_1} x_2^{m\cdot\nu_2} \cdots x_N^{m\cdot\nu_N}, \tag{3.11}$$

from which it follows that

$$\begin{aligned} x^{\alpha(m)} &= \left(\prod_{j=1}^N x_j^{a_j}\right) x_1^{m\cdot\nu_1} x_2^{m\cdot\nu_2} \cdots x_N^{m\cdot\nu_N} \\ &= x_1^{m\cdot\nu_1+a_1} x_2^{m\cdot\nu_2+a_2} \cdots x_N^{m\cdot\nu_N+a_N}. \end{aligned}$$

Since $m \in Q$, (3.7) implies that the exponents of the x_j are ≥ 0. □

Exercise 2. Give a careful proof of (3.11).

Exercise 3. If we used $+a_j$ rather than $-a_j$ in the description of $Q = \mathrm{Conv}(\mathcal{A})$ in (3.7), what effect would this have on (3.9)? This explains the minus signs in (3.7): they give a nicer homogenization formula.

From the equations (3.1), we get the homogenized equations

$$\begin{aligned} F_0 &= a_{01}x^{\alpha(m_1)} + \cdots + a_{0l}x^{\alpha(m_l)} = 0 \\ &\vdots \\ F_n &= a_{n1}x^{\alpha(m_1)} + \cdots + a_{nl}x^{\alpha(m_l)} = 0, \end{aligned}$$

where F_i is the homogenization of f_i. Notice that Lemma (3.10) applies to these equations since $m_i \in \mathcal{A} \subset Q$ for all i. Also note that $F_0, \dots, F_n$ and $f_0, \dots, f_n$ have the same coefficients, so we can write the resultant as $\mathrm{Res}_{\mathcal{A}}(F_0, \dots, F_n)$.

Exercise 4.

a. For $\mathcal{A}_d = \{m \in \mathbb{Z}^n_{\geq 0} : |m| \leq d\}$, let the facet variables be $x_0, \dots, x_n$, where we use the labelling of Exercise 3. Show that $t_i = x_i/x_0$ and that the homogenization of $f(t_1, \dots, t_n)$ is given precisely by (2.7).

b. For $\mathcal{A} = \{(0,0),(1,0),(0,1),(1,1)\}$, the convex hull $Q = \text{Conv}(\mathcal{A})$ in $\mathbb{R}^2$ is given by the inequalities

$$m \cdot \nu_s \geq 0,\ m \cdot \nu_u \geq -1,\ m \cdot \nu_t \geq 0,\ \text{and } m \cdot \nu_v \geq -1,$$

where $e_1 = \nu_s = -\nu_u$ and $e_2 = \nu_t = -\nu_v$. As indicated by the labelling of the facets, the facet variables are u, s, v, t. This is illustrated in Fig. 7.5 on the next page. Show that the homogenization of (2.10) is precisely the system of equations (3.6).

Our final task is to explain what it means for the equations $F_0 = \cdots = F_n = 0$ to have a "nontrivial" solution. We use the *vertices* of polytope Q for this purpose. Since Q is the convex hull of the finite set $\mathcal{A} \subset \mathbb{Z}^n$, it follows that every vertex of Q lies in $\mathcal{A}$, i.e., the vertices are a special subset of $\mathcal{A}$. This in turn gives a special collection of homogenized monomials which will tell us what "nontrivial" means. The precise definitions are as follows.

(3.12) Definition. Let $x_1, \ldots, x_N$ be facet variables for $Q = \text{conv}(\mathcal{A})$.
a. If $m \in \mathcal{A}$ is a vertex of Q, then we say that $x^{\alpha(m)}$ is a *vertex monomial*.
b. A point $(x_1, \ldots, x_N) \in \mathbb{C}^N$ is *nontrivial* if $x^{\alpha(m)} \neq 0$ for at least one vertex monomial.

Exercise 5.
a. Let $\mathcal{A}_d$ and $x_0, \ldots, x_n$ be as in Exercise 4. Show that the vertex monomials are $x_0^d, \ldots, x_n^d$, and conclude that $(x_0, \ldots, x_n)$ is nontrivial if and only if $(x_0, \ldots, x_n) \neq (0, \ldots, 0)$.
b. Let $\mathcal{A}$ and u, s, v, t be as in Exercise 4. Show that the vertex monomials are uv, ut, sv, st, and conclude that (u, s, v, t) is nontrivial if and only if $(u, s) \neq (0, 0)$ and $(v, t) \neq (0, 0)$.

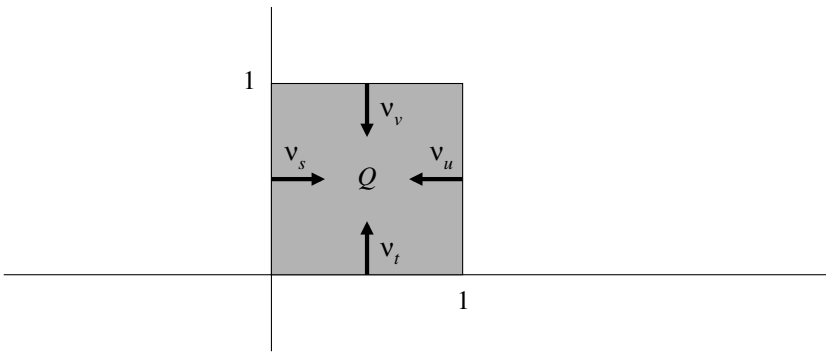

FIGURE 7.5. Facet normals of the unit square

Exercises 4 and 5 show that the homogenizations used in (2.7) and (3.6) are special cases of a theory that works for any set $\mathcal{A}$ of exponents. Once we have the description (3.7) of the convex hull of $\mathcal{A}$, we can read off everything we need, including the facet variables, how to homogenize, and what nontrivial means.

We now come to the main result of this section, which uses the facet variables to give necessary and sufficient conditions for the vanishing of the resultant.

(3.13) Theorem. *Let $\mathcal{A} = \{m_1, \dots, m_l\} \subset \mathbb{Z}^n_{\geq 0}$ be finite, and assume that $Q = \operatorname{Conv}(\mathcal{A})$ is n-dimensional. If $x_1, \dots, x_N$ are the facet variables, then the homogenized system of equations*

$$\begin{aligned} F_0 &= a_{01}x^{\alpha(m_1)} + \cdots + a_{0l}x^{\alpha(m_l)} = 0 \\ &\vdots \\ F_n &= a_{n1}x^{\alpha(m_1)} + \cdots + a_{nl}x^{\alpha(m_l)} = 0 \end{aligned}$$

has a nontrivial solution in $\mathbb{C}^N$ if and only if $\operatorname{Res}_{\mathcal{A}}(F_0, \dots, F_n) = 0$.

Proof. Let $U \subset \mathbb{C}^N$ consist of all nontrivial points, and notice that $(\mathbb{C}^*)^N \subset U$. Then consider the map Φ defined by

$$\Phi(x_1, \dots, x_N) = (x^{\alpha(m_1)}, \dots, x^{\alpha(m_l)}).$$

Since the vertex monomials appear among the $x^{\alpha(m_i)}$, we see that $\Phi(x_1, \dots, x_N) \neq (0, \dots, 0)$ when $(x_1, \dots, x_N) \in U$. Thus Φ can be regarded as a map $\Phi : U \to \mathbb{P}^{l-1}$. By Theorem (3.4), it suffices to prove that the image of Φ is the toric variety $X_{\mathcal{A}}$. To prove this, we will use the following properties of the map Φ:

(i) $\Phi(U)$ is a variety in $\mathbb{P}^{l-1}$.
(ii) $\Phi\big((\mathbb{C}^*)^N\big)$ is precisely $\phi_{\mathcal{A}}\big((\mathbb{C}^*)^n\big)$.

Assuming (i) and (ii), we see that $\phi_{\mathcal{A}}\big((\mathbb{C}^*)^n\big) \subset \Phi(U)$, and since $\Phi(U)$ is a variety, we have $X_{\mathcal{A}} \subset \Phi(U)$. Then the argument of part d of Exercise 6 shows that $X_{\mathcal{A}} = \Phi(U)$, as desired.

The proofs of (i) and (ii) are rather technical and use results from [BC] and [Cox1]. Since Theorem (3.13) has not previously appeared in the literature, we will include the details. What follows is for experts only!

For (i), note that [Cox1] implies that Φ factors

$$U \to X_Q \to \mathbb{P}^{l-1},$$

where X_Q is the abstract toric variety determined by Q (see [Ful], §1.5). By Theorem 2.1 of [Cox1], $U \to X_Q$ is a categorical quotient, and in fact, the proof shows that it is a universal categorical quotient (because $\mathbb{C}$ has characteristic 0—see Theorem 1.1 of [FM]). A universal categorical quotient is surjective by §0.2 of [FM], so that $U \to X_Q$ is surjective. This

shows that $\Phi(U)$ is the image of $X_Q \to \mathbb{P}^{l-1}$. Since X_Q is a projective variety, a generalization of the Projective Images principle used earlier in this section implies that the image of $X_Q \to \mathbb{P}^{l-1}$ is a variety. We conclude that $\Phi(U)$ is a variety in $\mathbb{P}^{l-1}$.

For (ii), first observe that the restriction of Φ to $(\mathbb{C}^*)^N$ factors

$$(\mathbb{C}^*)^N \xrightarrow{\psi} (\mathbb{C}^*)^n \xrightarrow{\phi_{\mathcal{A}}} \mathbb{P}^{l-1}$$

where ψ is given by (3.8) and $\phi_{\mathcal{A}}$ is given by (3.3). To prove this, note that by the proof of Lemma (3.11), we can write

$$x^{\alpha(m)} = \left(\prod_{j=1}^N x_j^{a_j}\right) t^m,$$

provided we use ψ to write t^m in terms of $x_0, \dots, x_N$. It follows that

$$\Phi(x_0, \dots, x_N) = \left(\prod_{j=1}^N x_j^{a_j}\right) \phi_{\mathcal{A}}\big(\psi(x_0, \dots, x_N)\big).$$

Since we are working in projective space, we conclude that $\Phi = \phi_{\mathcal{A}} \circ \psi$.

Using Remark 8.8 of [BC], we can identify ψ with the restriction of $U \to X_Q$ to $(\mathbb{C}^*)^N$. It follows from [Cox1] (especially the discussion following Theorem 2.1) that ψ is onto, and it follows that

$$\Phi\big((\mathbb{C}^*)^N\big) = \phi_{\mathcal{A}}\big(\psi\big((\mathbb{C}^*)^N\big)\big) = \phi_{\mathcal{A}}\big((\mathbb{C}^*)^n\big),$$

which completes the proof of the theorem. □

The proof of Theorem (3.13) shows that the map $\Phi : U \to X_{\mathcal{A}}$ is surjective, which allows us to think of the facet variables as "homogeneous coordinates" on $X_{\mathcal{A}}$. However, for this to be useful, we need to understand when two points $P, Q \in U$ correspond to the same point in $X_{\mathcal{A}}$. In nice cases, there is a simple description of when this happens (see Theorem 2.1 of [Cox1]), but in general, things can be complicated. We should also mention that facet variables and toric varieties have proved to be useful in geometric modeling. See, for example, [CoxKM], [Kra], and [Zub].

There is a *lot* more that one can say about sparse resultants and toric varieties. In Chapter 8, we will discover a different use for toric varieties when we study combinatorial problems arising from magic squares. Toric varieties are also useful in studying solutions of sparse equations, which we will discuss in §5, and the more general sparse resultants defined in §6 also have relations to toric varieties. But before we can get to these topics, we first need to learn more about polytopes.

Additional Exercises for §3

Exercise 6. Consider the Veronese map $\Phi_d : \mathbb{P}^n \to \mathbb{P}^{N-1}$, $N = \binom{n+d}{d}$, as in the text.

a. Show that Φ_d is well-defined. This has two parts: first, you must show that $\Phi_d(x_0, \dots, x_n)$ doesn't depend on which homogeneous coordinates

you use, and second, you must show that $\Phi_d(x_0, \dots, x_n)$ never equals the zero vector.

b. Show that Φ_d is one-to-one. Hint: If $\Phi_d(x_0, \dots, x_n) = \Phi_d(y_0, \dots, y_n)$, then for some μ, $\mu x^\alpha = y^\alpha$ for all $|\alpha| = d$. Pick i such that $x_i \neq 0$ and let $\lambda = y_i/x_i$. Then show that $\mu = \lambda^d$ and $y_j = \lambda x_j$ for all j.

c. Prove (3.5).

d. Prove that $\Phi_d(\mathbb{P}^n)$ is the Zariski closure of $\phi_{\mathcal{A}_d}\big((\mathbb{C}^*)^n\big)$ in $\mathbb{P}^{N-1}$. In concrete terms, this means the following. Let the homogeneous coordinates on $\mathbb{P}^{N-1}$ be $u_1, \dots, u_N$. If a homogeneous polynomial $H(u_1, \dots, u_N)$ vanishes on $\phi_{\mathcal{A}_d}\big((\mathbb{C}^*)^n\big)$, then prove that H vanishes on $\Phi_d(\mathbb{P}^n)$. Hint: Use (3.5) to show that $x_0 \dots x_n H \circ \Phi_d$ vanishes identically on $\mathbb{P}^n$. Then argue that $H \circ \Phi_d$ must vanish on $\mathbb{P}^n$.

Exercise 7. Let $\mathcal{A}$ and F, G, H be as in Exercise 1. In this exercise and the next, you will give an elementary proof that $\operatorname{Res}_{\mathcal{A}}(F, G, H) = 0$ if and only if $F = G = H = 0$ has a nontrivial solution (u, s, v, t), meaning $(u, s) \neq (0, 0)$ and $(v, t) \neq (0, 0)$.

a. If $F = G = H = 0$ has a nontrivial solution (u, s, v, t), show that the determinant in (2.11) vanishes. Hint: Multiply the equations by u and s to get 6 equations in the 6 "unknowns" $u^2v, usv, u^2t, ust, s^2v, s^2t$. Show that the "unknowns" can't all vanish simultaneously.

b. For the remaining parts of the exercise, assume that the determinant (2.11) vanishes. We will find a nontrivial solution of the equations $F = G = H = 0$ by considering 3×3 submatrices (there are four of them) of the matrix

$$\begin{pmatrix} a_0 & a_1 & a_2 & a_3 \\ b_0 & b_1 & b_2 & b_3 \\ c_0 & c_1 & c_2 & c_3 \end{pmatrix}.$$

One of the 3×3 submatrices appears in (2.2), and if its determinant doesn't vanish, show that we can find a solution of the form $(1, s, 1, t)$. Hint: Adapt the argument of Exercise 2 of §2.

c. Now suppose instead that

$$\det \begin{pmatrix} a_0 & a_2 & a_3 \\ b_0 & b_2 & b_3 \\ c_0 & c_2 & c_3 \end{pmatrix} \neq 0.$$

Show that we can find a solution of the form $(u, 1, 1, t)$.

d. The matrix of part b has two other 3×3 submatrices. Show that we can find a nontrivial solution if either of these has nonvanishing determinant.

e. Conclude that we can find a nontrivial solution whenever the matrix of part b has rank 3.

f. If the matrix has rank less than three, explain why it suffices to show that the equations $F = G = 0$ have a nontrivial solution. Hence we

are reduced to the case where H is the zero polynomial, which will be considered in the next exercise.

Exercise 8. Continuing the notation of the previous exercise, we will show that the equations $F = G = 0$ always have a nontrivial solution. Write the equations in the form

$$\begin{aligned}(a_0u + a_1s)v + (a_2u + a_3s)t &= 0\\ (b_0u + b_1s)v + (b_2u + b_3s)t &= 0,\end{aligned}$$

which is a system of two equations in the unknowns v, t.

a. Explain why we can find $(u_0, s_0) \neq (0, 0)$ such that

$$\det\begin{pmatrix} a_0u_0 + a_1s_0 & a_2u_0 + a_3s_0\\ b_0u_0 + b_1s_0 & b_2u_0 + b_3s_0\end{pmatrix} = 0.$$

b. Given (u_0, s_0) from part a, explain why we can find $(v_0, t_0) \neq (0, 0)$ such that (u_0, s_0, v_0, t_0) is a nontrivial solution of $F = G = 0$.

Exercise 9. In Exercise 8 of §2, you showed that $\mathrm{Res}_{\mathcal{A}}$ is unchanged if we translate $\mathcal{A}$ by a vector $v \in \mathbb{Z}^n$. You also know that if Q is the convex hull of $\mathcal{A}$, then $v + Q$ is the convex hull of $v + \mathcal{A}$ by Exercise 16 of §1.

a. If Q is represented as in (3.7), show that $v + Q$ is respresented by the inequalities $m \cdot \nu_j \geq -a_j + v \cdot \nu_j$.
b. Explain why $\mathcal{A}$ and $v + \mathcal{A}$ have the same facet variables.
c. Consider $m \in Q$. Show that the homogenization of t^m with respect to $\mathcal{A}$ is equal to the homogenization of t^{v+m} with respect to $v + \mathcal{A}$. This says that the homogenized equations in Theorem (3.13) are unchanged if we replace $\mathcal{A}$ with $v + \mathcal{A}$.

Exercise 10. Let $x_1, \ldots, x_N$ be facet variables for $Q = \mathrm{Conv}(\mathcal{A})$. We say that two monomials x^α and x^β have the same $\mathcal{A}$-*degree* if there is $m \in \mathbb{Z}^n$ such that

$$\beta_j = \alpha_j + m \cdot \nu_j$$

for $j = 1, \ldots, N$.

a. Show that the monomials $x^{\alpha(m)}$, $m \in Q$, have the same $\mathcal{A}$-degree. Thus the polynomials in Theorem (3.13) are $\mathcal{A}$-*homogeneous*, which means that all terms have the same $\mathcal{A}$-degree.
b. If $\mathcal{A}_d$ and $x_0, \ldots, x_n$ are as in part a of Exercise 4, show that two monomials x^α and x^β have the same $\mathcal{A}_d$-degree if and only if they have the same total degree.
c. If $\mathcal{A}$ and u, s, v, t are as in part b of Exercise 4, show that two monomials $u^{a_1}s^{a_2}v^{a_3}t^{a_4}$ and $u^{b_1}s^{b_2}v^{b_3}t^{b_4}$ have the same $\mathcal{A}$-degree if and only if $a_1 + a_2 = b_1 + b_2$ and $a_3 + a_4 = b_3 + b_4$.

Exercise 11. This exercise will explore the notion of "nontrivial" given in Definition (3.12). Let $m \in Q = \text{Conv}(\mathcal{A})$, and let $x_1, \dots, x_N$ be the facet variables. We define the *reduced monomial* $x_{red}^{\alpha(m)}$ to be the monomial obtained from $x^{\alpha(m)}$ by replacing all nonzero exponents by 1.

a. Prove that

$$x_{red}^{\alpha(m)} = \prod_{m \notin \mathcal{F}_j} x_j.$$

Thus $x_{red}^{\alpha(m)}$ is the product of those facet variables corresponding to the facets *not* containing m. Hint: Look at the proof of Lemma (3.10) and remember that $m \in \mathcal{F}_j$ if and only if $m \cdot \nu_j = -a_j$.

b. Prove that $(x_1, \dots, x_N)$ is nontrivial if and only if $x_{red}^{\alpha(m)} \neq 0$ for at least one vertex $m \in Q$.

c. Prove that if $m \in Q \cap \mathbb{Z}^n$ is arbitrary, then $x^{\alpha(m)}$ is divisible by some reduced vertex monomial. Hint: The face of Q of smallest dimension containing m is the intersection of those facets $\mathcal{F}_j$ for which $m \cdot \nu_j = -a_j$. Then let m' be a vertex of Q lying in this face.

d. As in the proof of Theorem (3.13), let $U \subset \mathbb{C}^N$ be the set of nontrivial points. If $(x_1, \dots, x_n) \notin U$, then use parts b and c to show that $(x_1, \dots, x_n)$ is a solution of the homogenized equations $F_0 = \cdots = F_n = 0$ in the statement of Theorem (3.13). Thus the points in $\mathbb{C}^N - U$ are "trivial" solutions of our equations, which explains the name "nontrivial" for the points of U.

Exercise 12. Let $\mathcal{A} = \{(0,0), (1,0), (0,1), (1,1), (2,0)\}$. In Exercise 9 of §2, you showed that $\text{Res}_{\mathcal{A}}(f, g, h)$ was given by a certain 9×9 determinant. The convex hull of $\mathcal{A}$ is pictured in Fig. 7.2, and you computed the inward normals to be $e_1, e_2, -e_2, -e_1 - e_2$ in Exercise 6 of §1. Let the corresponding facet variables be x_1, x_2, x_3, x_4.

a. What does it mean for (x_1, x_2, x_3, x_4) to be nontrivial? Try to make your answer as nice as possible. Hint: See part b of Exercise 5.

b. Write down explicitly the homogenizations F, G, H of the polynomials f, g, h from Exercise 9 of §2.

c. By combining parts a and b, what is the condition for $\text{Res}_{\mathcal{A}}(F, G, H)$ to vanish?

Exercise 13. In Exercise 10 of §2, you studied the Dixon resultant $\text{Res}_{\mathcal{A}_{l,m}}$, where $\mathcal{A}_{l,m} = \{(a, b) \in \mathbb{Z}^2 : 0 \leq a \leq l,\ 0 \leq b \leq m\}$.

a. Draw a picture of $\text{Conv}(\mathcal{A}_{l,m})$ and label the facets using the variables u, s, v, t (this is similar to what you did in part b of Exercise 4).

b. What is the homogenization of $f \in L(\mathcal{A}_{l,m})$?

c. What does it mean for (u, s, v, t) to be nontrivial?

d. What is the toric variety $X_{\mathcal{A}_{l,m}}$? Hint: It's one you've seen before!

e. Explain how the Dixon resultant can be formulated in terms of *bihomogeneous polynomials*. A polynomial $f \in k[u, s, v, t]$ is bihomogeneous of

degree (l, m) if it is homogeneous of degree l as a polynomial in u, s and homogeneous of degree m as a polynomial in v, t.

§4 Minkowski Sums and Mixed Volumes

In this section, we will introduce some important constructions in the theory of convex polytopes. Good general references for this material are [BoF], [BZ], [Ewa] and [Lei]. [Ful] and [GKZ] also contain brief expositions. Throughout, we will illustrate the main ideas using the Newton polytopes (see §1) of the following polynomials:

$$\begin{aligned} f_1(x, y) &= ax^3y^2 + bx + cy^2 + d \\ f_2(x, y) &= exy^4 + fx^3 + gy. \end{aligned} \tag{4.1}$$

We will assume that the coefficients $a, \ldots, g$ are all non-zero in $\mathbb{C}$.

There are two operations induced by the vector space structure in $\mathbb{R}^n$ that form new polytopes from old ones.

(4.2) Definition. Let P, Q be polytopes in $\mathbb{R}^n$ and let $\lambda \geq 0$ be a real number.

a. The *Minkowski sum* of P and Q, denoted $P + Q$, is

$$P + Q = \{p + q : p \in P \text{ and } q \in Q\},$$

where $p + q$ denotes the usual vector sum in $\mathbb{R}^n$.

b. The polytope λP is defined by

$$\lambda P = \{\lambda p : p \in P\},$$

where λp is the usual scalar multiplication on $\mathbb{R}^n$.

For example, the Minkowski sum of the Newton polytopes $P_1 = \mathrm{NP}(f_1)$ and $P_2 = \mathrm{NP}(f_2)$ from (4.1) is a convex heptagon with vertices $(0, 1), (3, 0), (4, 0), (6, 2), (4, 6), (1, 6)$, and $(0, 3)$. In Fig. 7.6, P_1 is indicated by dashed lines, P_2 by bold lines, and the Minkowski sum $P_1 + P_2$ is shaded.

Exercise 1. In Fig. 7.6, show that the Minkowski sum $P_1 + P_2$ can be obtained by placing a copy of P_1 at every point of P_2. Illustrate your answer with a picture. This works because P_1 contains the origin.

Exercise 2. Let

$$\begin{aligned} f_1 &= a_{20}x^2 + a_{11}xy + a_{02}y^2 + a_{10}x + a_{01}y + a_{00} \\ f_2 &= b_{30}x^3 + b_{21}x^2y + b_{12}xy^2 + b_{03}y^3 + b_{20}x^2 + \cdots + b_{00} \end{aligned}$$

be general ("dense") polynomials of total degrees 2 and 3 respectively. Construct the Newton polytopes $P_i = \mathrm{NP}(f_i)$ for $i = 1, 2$ and find the Minkowski sum $P_1 + P_2$.

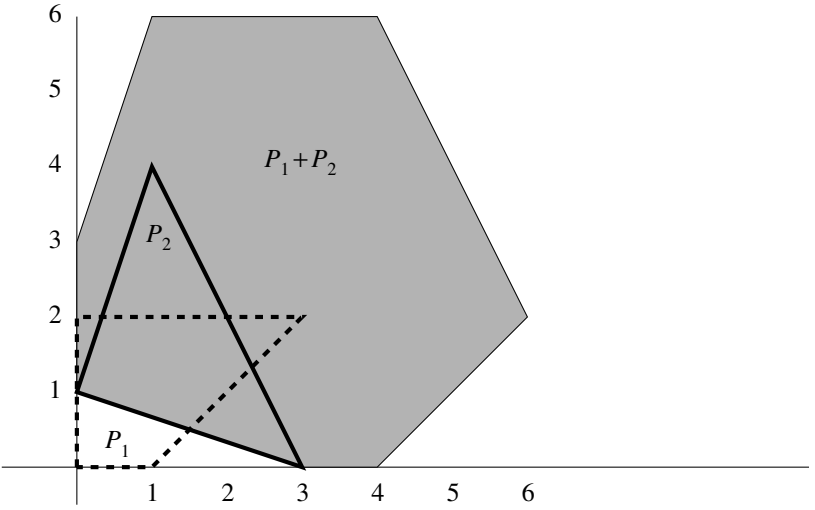

FIGURE 7.6. Minkowski sum of polytopes

Exercise 3.

a. Show that if $f_1, f_2 \in \mathbb{C}[x_1, \ldots, x_n]$ and $P_i = \mathrm{NP}(f_i)$, then $P_1 + P_2 = \mathrm{NP}(f_1 \cdot f_2)$.
b. Show in general that if P_1 and P_2 are polytopes, then their Minkowski sum $P_1 + P_2$ is also convex. Hint: If $P_i = \mathrm{Conv}(\mathcal{A}_i)$, where $\mathcal{A}_i$ is finite, what finite set will give $P_1 + P_2$?
c. Show that a Minkowski sum of lattice polytopes is again a lattice polytope.
d. Show that $P + P = 2\,P$ for any polytope P. How does this generalize?

Given finitely many polytopes $P_1, \ldots, P_l \subset \mathbb{R}^n$, we can form their Minkowski sum $P_1 + \cdots + P_l$, which is again a polytope in $\mathbb{R}^n$. In §1, we learned about the *faces* of a polytope. A useful fact is that faces of the Minkowski sum $P_1 + \cdots + P_l$ are themselves Minkowski sums. Here is a precise statement.

(4.3) Proposition. *Let $P_1, \ldots, P_r \subset \mathbb{R}^n$ be polytopes in $\mathbb{R}^n$, and let $P = P_1 + \cdots + P_r$ be their Minkowski sum. Then every face P' of P can be expressed as a Minkowski sum*

$$P' = P'_1 + \cdots + P'_r,$$

where each P'_i is a face of P_i.

PROOF. By §1, there is a nonzero vector $\nu \in \mathbb{R}^n$ such that

$$P' = P_\nu = P \cap \{m \in \mathbb{R}^n : m \cdot \nu = -a_P(\nu)\}.$$

In Exercise 12 at the end of the section, you will show that

$$P_\nu = (P_1 + \cdots + P_r)_\nu = (P_1)_\nu + \cdots + (P_r)_\nu,$$

which will prove the proposition. □

Exercise 4. Verify that Proposition (4.3) holds for each facet of the Minkowski sum $P_1 + P_2$ in Fig. 7.6.

We next show how to compute the volume of an n-dimensional lattice polytope P using its facets. As in §1, each facet $\mathcal{F}$ of P has a unique primitive inward pointing normal $\nu_\mathcal{F} \in \mathbb{Z}^n$. If the supporting hyperplane of $\mathcal{F}$ is $m \cdot \nu_\mathcal{F} = -a_\mathcal{F}$, then the formula (1.4) for P can be stated as

$$P = \bigcap_\mathcal{F} \{m \in \mathbb{R}^n : m \cdot \nu_\mathcal{F} \geq -a_\mathcal{F}\}, \tag{4.4}$$

where the intersection is over all facets $\mathcal{F}$ of P. Recall also that in the notation of (1.3), $a_\mathcal{F} = a_P(\nu_\mathcal{F})$.

Let $\nu_\mathcal{F}^\perp$ denote the $(n-1)$-dimensional subspace defined by $m \cdot \nu_\mathcal{F} = 0$. Then $\nu_\mathcal{F}^\perp \cap \mathbb{Z}^n$ is closed under addition and scalar multiplication by integers. One can prove that $\nu_\mathcal{F}^\perp \cap \mathbb{Z}^n$ is a *lattice of rank* $n-1$, which means there are $n-1$ vectors $w_1, \ldots, w_{n-1} \in \nu_\mathcal{F}^\perp \cap \mathbb{Z}^n$ such that every element of $\nu_\mathcal{F}^\perp \cap \mathbb{Z}^n$ is a unique linear combination of $w_1, \ldots, w_{n-1}$ with *integer* coefficients. We call $w_1, \ldots, w_{n-1}$ a *basis* of $\nu_\mathcal{F}^\perp \cap \mathbb{Z}^n$. The existence of $w_1, \ldots, w_{n-1}$ follows from the fundamental theorem on discrete subgroups of Euclidean spaces. Using $w_1, \ldots, w_{n-1}$, we get the set

$$\mathcal{P} = \{\lambda_1 w_1 + \cdots + \lambda_{n-1} w_{n-1} : 0 \leq \lambda_i \leq 1\},$$

which is the called a *fundamental lattice parallelotope* of the lattice $\nu_\mathcal{F}^\perp \cap \mathbb{Z}^n$.

If S is subset of $\mathbb{R}^n$ lying in any affine hyperplane, we can define the Euclidean volume $\mathrm{Vol}_{n-1}(S)$. In particular, we can define $\mathrm{Vol}_{n-1}(\mathcal{F})$. However, we also need to take the volume of the fundamental lattice parallelotope $\mathcal{P}$ into account. This leads to the following definition.

(4.5) Definition. The *normalized volume* of the facet $\mathcal{F}$ of the lattice polytope P is given by

$$\mathrm{Vol}'_{n-1}(\mathcal{F}) = \frac{\mathrm{Vol}_{n-1}(\mathcal{F})}{\mathrm{Vol}_{n-1}(\mathcal{P})},$$

where $\mathcal{P}$ is a fundamental lattice parallelotope for $\nu_\mathcal{F}^\perp \cap \mathbb{Z}^n$.

This definition says that the normalized volume is the usual volume scaled so that the fundamental lattice parallelotope has volume 1. In

Exercise 13, you will show that this definition is independent of which fundamental lattice parallelotope we use. We should also mention the following nice formula:

$$\mathrm{Vol}_{n-1}(\mathcal{P}) = ||\nu_{\mathcal{F}}||,$$

where $||\nu_{\mathcal{F}}||$ is the Euclidean length of the vector $\nu_{\mathcal{F}}$. We omit the proof since we will not use this result.

For example, let $P_2 = \mathrm{NP}(f_2) = \mathrm{Conv}(\{(1,4),(3,0),(0,1)\})$ be the Newton polytope of the polynomial f_2 from (4.1). For the facet

$$\mathcal{F} = \mathrm{Conv}(\{(3,0),(0,1)\}),$$

we have $\nu_{\mathcal{F}} = (1,3)$, and the line containing $\mathcal{F}$ is $x + 3y = 3$. It is easy to check that $(3,0)$ and $(0,1)$ are as close together as any pair of integer points in the line $x + 3y = 3$, so the line segment from $(3,0)$ to $(0,1)$ is a translate of the fundamental lattice parallelotope. It follows that

$$\mathrm{Vol}'_1(\mathcal{F}) = 1.$$

Notice that the usual Euclidean length of $\mathcal{F}$ is $\sqrt{10}$. In general, the normalized volume differs from the Euclidean volume.

Exercise 5. Let $P_2 = \mathrm{NP}(f_2)$ be as above.

a. Show that for the facet $\mathcal{G} = \mathrm{Conv}(\{(3,0),(1,4)\})$, we have $\nu_{\mathcal{G}} = (-2,-1)$ and $\mathrm{Vol}'_1(\mathcal{G}) = 2$.
b. Finally, for the facet $\mathcal{H} = \mathrm{Conv}(\{(0,1),(1,4)\})$, show that $\nu_{\mathcal{H}} = (3,-1)$ and $\mathrm{Vol}'_1(\mathcal{H}) = 1$.

Our main reason for introducing the normalized volume of a facet is the following lovely connection between the n-dimensional volume of a polytope and the $(n-1)$-dimensional normalized volumes of its facets.

(4.6) Proposition. *Let P be a lattice polytope in $\mathbb{R}^n$, and assume that P is represented as in (4.4). Then*

$$\mathrm{Vol}_n(P) = \frac{1}{n}\sum_{\mathcal{F}} a_{\mathcal{F}}\,\mathrm{Vol}'_{n-1}(\mathcal{F}),$$

where the sum is taken over all facets of P.

Proof. See [BoF], [Lei] or [Ewa], Section IV.3. The formula given in these sources is not specifically adapted to lattice polytopes, but with minor modifications, one gets the desired result. Note also that this proposition explains the minus sign used in the equation $m \cdot \nu_{\mathcal{F}} \geq -a_{\mathcal{F}}$ of a supporting hyperplane. □

For an example of Proposition (4.6), we will compute the area of the polytope $P_2 = \mathrm{NP}(f_2)$ of Exercise 5. First note that if we label the facet

normals $\nu_{\mathcal{F}} = (1,3)$, $\nu_{\mathcal{G}} = (-2,-1)$ and $\nu_{\mathcal{H}} = (3,-1)$ as above, then P_2 is defined by

$$m \cdot \nu_{\mathcal{F}} \geq 3,\ m \cdot \nu_{\mathcal{G}} \geq -6,\ \text{and } m \cdot \nu_{\mathcal{H}} \geq -1.$$

It follows that $a_{\mathcal{F}} = -3$, $a_{\mathcal{G}} = 6$ and $a_{\mathcal{H}} = 1$. Applying Proposition (4.6), the area of P_2 is given by

$$\text{Vol}_2(P_2) = (1/2)(-3 \cdot 1 + 6 \cdot 2 + 1 \cdot 1) = 5. \tag{4.7}$$

You should check that this agrees with the result obtained from the elementary area formula for triangles.

Exercise 6. Show that the area of the polytope $P_1 = \text{NP}(f_1)$ for f_1 from (4.1) is equal to 4, by first applying Proposition (4.6), and then checking with an elementary area formula.

Proposition (4.6) enables us to prove results about volumes of lattice polytopes using induction on dimension. Here is a nice example which is relevant to Theorem (2.13).

(4.8) Proposition. *If $P \subset \mathbb{R}^n$ is a lattice polytope, then $n!\,\text{Vol}_n(P)$ is an integer.*

PROOF. The proof is by induction on n. Then case $n = 1$ is obvious, so we may assume inductively that the result is true for lattice polytopes in $\mathbb{R}^{n-1}$. By Proposition (4.6), we get

$$n!\,\text{Vol}_n(P) = \sum_{\mathcal{F}} a_{\mathcal{F}} \cdot (n-1)!\,\text{Vol}'_{n-1}(\mathcal{F}).$$

Note that $a_{\mathcal{F}}$ is an integer. If we can show that $(n-1)!\,\text{Vol}'_{n-1}(\mathcal{F})$ is an integer, the proposition will follow.

A basis $w_1, \ldots, w_{n-1}$ of the lattice $\nu_{\mathcal{F}}^{\perp} \cap \mathbb{Z}^n$ gives $\phi : \nu_{\mathcal{F}}^{\perp} \cong \mathbb{R}^{n-1}$ which carries $\nu_{\mathcal{F}}^{\perp} \cap \mathbb{Z}^n \subset \nu_{\mathcal{F}}^{\perp}$ to the usual lattice $\mathbb{Z}^{n-1} \subset \mathbb{R}^{n-1}$. Since the fundamental lattice polytope $\mathcal{P}$ maps to $\{(a_1, \ldots, a_{n-1}) : 0 \leq a_i \leq 1\}$ under ϕ, it follows easily that

$$\text{Vol}'_{n-1}(S) = \text{Vol}_{n-1}(\phi(S)),$$

where Vol_{n-1} is the usual Euclidean volume in $\mathbb{R}^{n-1}$. By translating $\mathcal{F}$, we get a lattice polytope $\mathcal{F}' \subset \nu_{\mathcal{F}}^{\perp}$, and then $\phi(\mathcal{F}') \subset \mathbb{R}^{n-1}$ is a lattice polytope in $\mathbb{R}^{n-1}$. Since

$$(n-1)!\,\text{Vol}'_{n-1}(\mathcal{F}) = (n-1)!\,\text{Vol}'_{n-1}(\mathcal{F}') = (n-1)!\,\text{Vol}_{n-1}(\phi(\mathcal{F}')),$$

we are done by our inductive assumption. □

Our next result concerns the volumes of linear combinations of polytopes formed according to Definition (4.2).

(4.9) Proposition. *Consider any collection $P_1, \dots, P_r$ of polytopes in $\mathbb{R}^n$, and let $\lambda_1, \dots, \lambda_r \in \mathbb{R}$ be nonnegative. Then*

$$\mathrm{Vol}_n(\lambda_1 P_1 + \cdots + \lambda_r P_r)$$

is a homogeneous polynomial function of degree n in the λ_i.

PROOF. The proof is by induction on n. For $n = 1$, the $P_i = [\ell_i, r_i]$ are all line segments in $\mathbb{R}$ (possibly of length 0 if some $\ell_i = r_i$). The linear combination $\lambda_1 P_1 + \cdots + \lambda_r P_r$ is the line segment $[\sum_i \lambda_i \ell_i, \sum_i \lambda_i r_i]$, whose length is clearly a homogeneous linear function of the λ_i.

Now assume the proposition has been proved for all combinations of polytopes in $\mathbb{R}^{n-1}$, and consider polytopes P_i in $\mathbb{R}^n$ and $\lambda_i \geq 0$. The polytope $Q = \lambda_1 P_1 + \cdots + \lambda_r P_r$ depends on $\lambda_1, \dots, \lambda_r$, but as long as $\lambda_i > 0$ for all i, the Q's all have the *same* set of inward pointing facet normals (see Exercise 14 at the end of the section). Then, using the notation of (1.3), we can write the formula of Proposition (4.6) as

$$\mathrm{Vol}_n(Q) = \sum_{\nu} a_Q(\nu) \mathrm{Vol}'_{n-1}(Q_\nu), \tag{4.10}$$

where the sum is over the set of common inward pointing facet normals ν. In this situation, the proof of Proposition (4.3) tells us that

$$Q_\nu = \lambda_1 (P_1)_\nu + \cdots + \lambda_r (P_r)_\nu.$$

By the induction hypothesis, for each ν, the volume $\mathrm{Vol}'_{n-1}(Q_\nu)$ in (4.10) is a homogeneous polynomial of degree $n-1$ in $\lambda_1, \dots, \lambda_r$ (the details of this argument are similar to what we did in Proposition (4.8)).

Turning to $a_Q(\nu)$, we note that by Exercise 12 at the end of the section,

$$a_Q(\nu) = a_{\lambda_1 P_1 + \cdots + \lambda_r P_r}(\nu) = \lambda_1 a_{P_1}(\nu) + \cdots + \lambda_r a_{P_r}(\nu).$$

Since ν is independent of the λ_i, it follows that $a_Q(\nu)$ is a homogeneous linear function of $\lambda_1, \dots, \lambda_r$. Multiplying $a_Q(\nu)$ and $\mathrm{Vol}'_{n-1}(Q_\nu)$, we see that each term on the right hand side of (4.10) is a homogeneous polynomial function of degree n, and the proposition follows. □

When $r = n$, we can single out one particular term in the polynomial $\mathrm{Vol}_n(\lambda_1 P_1 + \cdots + \lambda_n P_n)$ that has special meaning for the whole collection of polytopes.

(4.11) Definition. The n-dimensional *mixed volume* of a collection of polytopes $P_1, \dots, P_n$, denoted

$$MV_n(P_1, \dots, P_n),$$

is the coefficient of the monomial $\lambda_1 \cdot \lambda_2 \cdots \lambda_n$ in $\mathrm{Vol}_n(\lambda_1 P_1 + \cdots + \lambda_n P_n)$.

Exercise 7.

a. If P_1 is the unit square $\mathrm{Conv}(\{(0,0),(1,0),(0,1),(1,1)\})$ and P_2 is the triangle $\mathrm{Conv}(\{(0,0),(1,0),(1,1)\})$, show that

$$\mathrm{Vol}_2(\lambda_1 P_1 + \lambda_2 P_2) = \lambda_1^2 + 2\lambda_1\lambda_2 + \tfrac{1}{2}\lambda_2^2,$$

and conclude that $MV_2(P_1, P_2) = 2$.

b. Show that if $P_i = P$ for all i, then the mixed volume is given by

$$MV_n(P, P, \ldots, P) = n!\,\mathrm{Vol}_n(P).$$

Hint: First generalize part d of Exercise 3 to prove $\lambda_1 P + \cdots + \lambda_n P = (\lambda_1 + \cdots + \lambda_n)\,P$, and then determine the coefficient of $\lambda_1\lambda_2\cdots\lambda_n$ in $(\lambda_1 + \cdots + \lambda_n)^n$.

The basic properties of the n-dimensional mixed volume are given by the following theorem.

(4.12) Theorem.

a. *The mixed volume $MV_n(P_1, \ldots, P_n)$ is invariant if the P_i are replaced by their images under a volume-preserving transformation of $\mathbb{R}^n$ (for example, a translation).*

b. *$MV_n(P_1, \ldots, P_n)$ is symmetric and linear in each variable.*

c. *$MV_n(P_1, \ldots, P_n) \geq 0$. Furthermore, $MV_n(P_1, \ldots, P_n) = 0$ if one of the P_i has dimension zero (i.e., if P_i consists of a single point), and $MV_n(P_1, \ldots, P_n) > 0$ if every P_i has dimension n.*

d. *The mixed volume of any collection of polytopes can be computed as*

$$MV_n(P_1, \ldots, P_n) = \sum_{k=1}^{n} (-1)^{n-k} \sum_{\substack{I \subset \{1,\ldots,n\} \\ |I| = k}} \mathrm{Vol}_n\Big(\sum_{i \in I} P_i\Big),$$

where $\sum_{i\in I} P_i$ is the Minkowski sum of polytopes.

e. *For all collections of lattice polytopes $P_1, \ldots, P_n$,*

$$MV_n(P_1, \ldots, P_n) = \sum_{\nu} a_{P_1}(\nu)\, MV'_{n-1}((P_2)_\nu, \ldots, (P_n)_\nu),$$

where $a_{P_1}(\nu)$ is defined in (1.3) and the sum is over all primitive vectors $\nu \in \mathbb{Z}^n$ such that $(P_i)_\nu$ has dimension ≥ 1 for $i = 2, \ldots, n$. The notation $MV'_{n-1}((P_2)_\nu, \ldots, (P_n)_\nu)$ on the right stands for the normalized mixed volume *analogous to the normalized volume in Definition (4.5):*

$$MV'_{n-1}((P_2)_\nu, \ldots, (P_n)_\nu) = \frac{MV_{n-1}((P_2)_\nu, \ldots, (P_n)_\nu)}{\mathrm{Vol}_{n-1}(\mathcal{P})},$$

where $\mathcal{P}$ is a fundamental lattice parallelotope in the hyperplane $\nu^\perp$ orthogonal to ν.

Proof. Part a follows directly from the definition of mixed volumes, as does part b. We leave the details to the reader as Exercise 15 below.

The nonnegativity assertion of part c is quite deep, and a proof can be found in [Ful], Section 5.4. This reference also proves positivity when the P_i all have dimension n. If P_i has dimension zero, then adding the term $\lambda_i P_i$ merely translates the sum of the other terms in $\lambda_1 P_1 + \cdots + \lambda_n P_n$ by a vector whose length depends on λ_i. The volume of the resulting polytope does not change, so that $\mathrm{Vol}_n(\lambda_1 P_1 + \cdots + \lambda_n P_n)$ is independent of λ_i. Hence the coefficient of $\lambda_1 \cdot \lambda_2 \cdots \lambda_n$ in the expression for the volume must be zero.

For part d, see [Ful], Section 5.4. Part e is a generalization of the volume formula given in Proposition (4.6) and can be deduced from that result. See Exercises 16 and 17 below. Proofs may also be found in [BoF], [Lei] or [Ewa], Section IV.4. Note that by part b of the theorem, only ν with $\dim (P_i)_\nu > 0$ can yield non-zero values for $MV'_{n-1}((P_2)_\nu, \ldots, (P_n)_\nu)$. □

For instance, let's use Theorem (4.12) to compute the mixed volume $MV_2(P_1, P_2)$ for the Newton polytopes of the polynomials from (4.1). In the case of two polytopes in $\mathbb{R}^2$, the formula of part d reduces to:

$$MV_2(P_1, P_2) = -\mathrm{Vol}_2(P_1) - \mathrm{Vol}_2(P_2) + \mathrm{Vol}_2(P_1 + P_2).$$

Using (4.7) and Exercise 5, we have $\mathrm{Vol}_2(P_1) = 4$ and $\mathrm{Vol}_2(P_2) = 5$. The Minkowski sum $P_1 + P_2$ is the heptagon pictured in Fig. 7.6 above. Its area may be found, for example, by subdividing the heptagon into four trapezoids bounded by the horizontal lines $y = 0, 1, 2, 3, 6$. Using that subdivision, we find

$$\mathrm{Vol}_2(P_1 + P_2) = 3 + 11/2 + 23/4 + 51/4 = 27.$$

The mixed volume is therefore

$$MV_2(P_1, P_2) = -4 - 5 + 27 = 18. \tag{4.13}$$

Exercise 8. Check the result of this computation using the formula of part e of Theorem (4.12). Hint: You will need to compute $a_{P_1}(\nu_\mathcal{F})$, $a_{P_1}(\nu_\mathcal{G})$ and $a_{P_1}(\nu_\mathcal{H})$, where $\nu_\mathcal{F}, \nu_\mathcal{G}, \nu_\mathcal{H}$ are the inward normals to the facets $\mathcal{F}, \mathcal{G}, \mathcal{H}$ of P_2.

In practice, computing the mixed volume $MV_n(P_1, \ldots, P_n)$ using the formulas given by parts d and e of Theorem (4.12) can be very time consuming. A better method, due to Sturmfels and Huber [HuS1] and Canny and Emiris [EC], is given by the use of a *mixed subdivision* of the Minkowski sum $P_1 + \cdots + P_n$. A brief description of mixed subdivisions will be given in §6, where we will also give further references and explain how to obtain software for computing mixed volumes.

Exercise 9. Let $P_1, \ldots, P_n$ be lattice polytopes in $\mathbb{R}^n$.
a. Prove that the mixed volume $MV_n(P_1, \ldots, P_n)$ is an integer.

b. Explain how the result of part a generalizes Proposition (4.8). Hint: Use Exercise 7.

We should remark that there are several different conventions in the literature concerning volumes and mixed volumes. Some authors include an extra factor of $1/n!$ in the definition of the mixed volume, so that $MV_n(P, \ldots, P)$ will be exactly equal to $\mathrm{Vol}_n(P)$. When this is done, the right side of the formula from part d of Theorem (4.12) acquires an extra $1/n!$. Other authors include the extra factor of $n!$ in the definition of Vol_n itself (so that the "volume" of the n-dimensional simplex is 1). In other words, care should be taken in comparing the formulas given here with those found elsewhere!

Additional Exercises for §4

Exercise 10. Let $P_1, \ldots, P_r$ be polytopes in $\mathbb{R}^n$. This exercise will show that the dimension of $\lambda_1 P_1 + \cdots + \lambda_r P_r$ is independent of the the λ_i, provided all $\lambda_i > 0$.

a. If $\lambda > 0$ and $p_0 \in P$, show that $(1-\lambda)p_0 + \mathrm{Aff}(\lambda P + Q) = \mathrm{Aff}(P + Q)$. This uses the affine subspaces discussed in Exercises 12 and 13 of §1. Hint: $(1-\lambda)p_0 + \lambda p + q = \lambda(p+q) - \lambda(p_0+q) + p_0 + q$.

b. Conclude that $\dim(\lambda P + Q) = \dim(P + Q)$.

c. Prove that $\dim(\lambda_1 P_1 + \cdots + \lambda_r P_r)$ is independent of the the λ_i, provided all $\lambda_i > 0$.

Exercise 11. Let $m \cdot \nu = -a_P(\nu)$ be a supporting hyperplane of $P = \mathrm{Conv}(\mathcal{A})$, where $\mathcal{A} \subset \mathbb{R}^n$ is finite. Prove that

$$P_\nu = \mathrm{Conv}(\{m \in \mathcal{A} : m \cdot \nu = -a_P(\nu)\}).$$

Exercise 12. Let $a_P(\nu) = -\min_{m \in P}(m \cdot \nu)$ be as in (1.3).

a. Show that $(\lambda P)_\nu = \lambda P_\nu$ and $a_{\lambda P}(\nu) = \lambda a_P(\nu)$.

b. Show that $(P+Q)_\nu = P_\nu + Q_\nu$ and $a_{P+Q}(\nu) = a_P(\nu) + a_Q(\nu)$.

c. Conclude that $(\lambda_1 P_1 + \cdots + \lambda_r P_r)_\nu = \lambda_1 (P_1)_\nu + \cdots + \lambda_r (P_r)_\nu$ and $a_{\lambda_1 P_1 + \cdots + \lambda_r P_r}(\nu) = \lambda_1 a_{P_1}(\nu) + \cdots + \lambda_r a_{P_r}(\nu)$.

Exercise 13. Let $\nu^\perp$ be the hyperplane orthogonal to a nonzero vector $\nu \in \mathbb{Z}^n$, and let $\{w_1, \ldots, w_{n-1}\}$ and $\{w'_1, \ldots, w'_{n-1}\}$ be any two bases for the lattice $\nu^\perp \cap \mathbb{Z}^n$.

a. By expanding the w'_i in terms of the w_j, show that there is an $(n-1) \times (n-1)$ integer matrix $A = (a_{ij})$ such that $w'_i = \sum_{i=1}^{n-1} a_{ij} w_j$ for all $i = 1, \ldots, n-1$.

b. Reversing the roles of the two lattice bases, deduce that A is invertible, and A^{-1} is also an integer matrix.

c. Deduce from part b that $\det(A) = \pm 1$.

d. Show that in the coordinate system defined by $w_1, \ldots, w_{n-1}$, A defines a volume preserving transformation from $\nu^\perp$ to itself. Explain why this shows that any two fundamental lattice parallelotopes in $\nu^\perp$ have the same $(n-1)$-dimensional volume.

Exercise 14. Fix polytopes $P_1, \ldots, P_r$ in $\mathbb{R}^n$ such that $P_1 + \cdots + P_r$ has dimension n. Prove that for any positive reals $\lambda_1, \ldots, \lambda_r$, the polytopes $\lambda_1 P_1 + \cdots + \lambda_r P_r$ all have the *same* inward pointing facet normals. Illustrate your answer with a picture. Hint: If ν is an inward pointing facet normal for $P_1 + \cdots + P_r$, then $(P_1 + \cdots + P_r)_\nu$ has dimension $n-1$. This implies that $(P_1)_\nu + \cdots + (P_r)_\nu$ has dimension $n-1$ by Exercise 12. Now use Exercise 10.

Exercise 15.

a. Using Definition (4.11), show that the mixed volume $MV_n(P_1, \ldots, P_n)$ is invariant under all permutations of the P_i.

b. Show that the mixed volume is linear in each variable:

$$MV_n(P_1, \ldots, \lambda P_i + \mu P_i', \ldots, P_n) = \lambda MV_n(P_1, \ldots, P_i, \ldots, P_n) + \mu MV_n(P_1, \ldots, P_i', \ldots, P_n)$$

for all $i = 1, \ldots, n$, and all $\lambda, \mu \geq 0$ in $\mathbb{R}$. Hint: When $i = 1$, consider the polynomial representing $\mathrm{Vol}_n(\lambda P_1 + \lambda' P_1' + \lambda_2 P_2 + \cdots + \lambda_n P_n)$ and look at the coefficients of $\lambda\lambda_2 \cdots \lambda_n$ and $\lambda'\lambda_2 \cdots \lambda_n$.

Exercise 16. In this exercise, we will consider several additional properties of mixed volumes. Let P, Q be polytopes in $\mathbb{R}^n$.

a. If $\lambda, \mu \geq 0$ are in $\mathbb{R}$, show that $\mathrm{Vol}_n(\lambda P + \mu Q)$ can be expressed in terms of mixed volumes as follows:

$$\frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} \lambda^k \mu^{n-k} MV_n(P, \ldots, P, Q, \ldots, Q),$$

where in the term corresponding to k, P is repeated k times and Q is repeated $n-k$ times in the mixed volume. Hint: By Exercise 7, $n!\,\mathrm{Vol}_n(\lambda P + \mu Q) = MV_n(\lambda P + \mu Q, \ldots, \lambda P + \mu Q)$.

b. Using part a, show that $MV_n(P, \ldots, P, Q)$ (which appears in the term containing $\lambda^{n-1}\mu$ in the formula of part a) can also be expressed as

$$(n-1)! \lim_{\mu \to 0^+} \frac{\mathrm{Vol}_n(P + \mu Q) - \mathrm{Vol}_n(P)}{\mu}.$$

Exercise 17. In this exercise, we will use part b of Exercise 16 to prove part e of Theorem (4.12). Replacing Q by a translate, we may assume that the origin is one of the vertices of Q.

a. Show that the Minkowski sum $P + \mu Q$ can be decomposed into: a subpolytope congruent to P, prisms over each facet $\mathcal{F}$ of P with height equal

to $\mu \cdot a_Q(\nu) \geq 0$, where $\nu = \nu_{\mathcal{F}}$, and other polyhedra with n-dimensional volume bounded above by a constant times μ^2.

b. From part a, deduce that

$$\mathrm{Vol}_n(P + \mu Q) = \mathrm{Vol}_n(P) + \mu \sum_{\nu} a_Q(\nu)\mathrm{Vol}'_{n-1}(P_\nu) + O(\mu^2).$$

c. Using part b of Exercise 16, show that

$$MV_n(P, \dots, P, Q) = (n-1)! \sum_{\nu} a_Q(\nu)\mathrm{Vol}'_{n-1}(P_\nu),$$

where the sum is over the primitive inward normals ν to the facets of P.

d. Now, to prove part e of Theorem (4.12), substitute

$$P = \lambda_2 P_2 + \cdots + \lambda_n P_n$$

and $Q = P_1$ into the formula of part c and use Exercises 7 and 15.

Exercise 18. Given polytopes $P_1, \dots, P_r$ in $\mathbb{R}^n$, this exercise will show that *every* coefficient of the polynomial representing

$$\mathrm{Vol}_n(\lambda_1 P_1 + \cdots + \lambda_r P_r)$$

is given by an appropriate mixed volume (up to a constant). We will use the following notation. If $\alpha = (i_1, \dots, i_r) \in \mathbb{Z}^r_{\geq 0}$ satisfies $|\alpha| = n$, then λ^α is the usual monomial in $\lambda_1, \dots, \lambda_r$, and let $\alpha! = i_1! i_2! \cdots i_r!$. Also define

$$MV_n(P; \alpha) = MV_n(P_1, \dots, P_1, P_2, \dots, P_2, \dots, P_r, \dots, P_r),$$

where P_1 appears i_1 times, P_2 appears i_2 times, $\dots$, P_r appears i_r times. Then prove that

$$\mathrm{Vol}_n(\lambda_1 P_1 + \cdots + \lambda_r P_r) = \sum_{|\alpha|=n} \frac{1}{\alpha!} MV_n(P; \alpha)\lambda^\alpha.$$

Hint: Generalize what you did in part a of Exercise 16.

§5 Bernstein's Theorem

In this section, we will study how the geometry of polytopes can be used to predict the *number* of solutions of a general system of n polynomial (or Laurent polynomial) equations $f_i(x_1, \dots, x_n) = 0$. We will also indicate how these results are related to a particular class of numerical root-finding methods called *homotopy continuation methods*.

Throughout the section, we will use the following system of equations to illustrate the main ideas:

$$\begin{aligned} 0 &= f_1(x, y) = ax^3y^2 + bx + cy^2 + d \\ 0 &= f_2(x, y) = exy^4 + fx^3 + gy, \end{aligned} \tag{5.1}$$

where the coefficients $a, \ldots, g$ are in $\mathbb{C}$. These are the same polynomials used in §4. We want to know how many solutions these equations have. We will begin by studying this question using the methods of Chapters 2 and 3, and then we will see that the mixed volume discussed in §4 has an important role to play. This will lead naturally to Bernstein's Theorem, which is the main result of the section.

Let's first proceed as in §1 of Chapter 2 to find the solutions of (5.1). Since different choices of $a, \ldots, g$ could potentially lead to different numbers of solutions, we will initially treat the coefficients $a, \ldots, g$ in (5.1) as symbolic parameters. This means working over the field $\mathbb{C}(a, \ldots, g)$ of rational functions in $a, \ldots, g$. Using a *lex* Gröbner basis to eliminate y, it is easy to check that the reduced Gröbner basis for the ideal $\langle f_1, f_2 \rangle$ in the ring $\mathbb{C}(a, \ldots, g)[x, y]$ has the form

$$\begin{aligned} 0 &= y + p_{17}(x) \\ 0 &= p_{18}(x), \end{aligned} \tag{5.2}$$

where $p_{17}(x)$ and $p_{18}(x)$ are polynomials in x alone, of degrees 17 and 18 respectively. The coefficients in p_{17} and p_{18} are rational functions in $a, \ldots, g$. Gröbner basis theory tells us that we can transform (5.2) back into our original equations (5.1), and vice versa. These transformations will also have coefficients in $\mathbb{C}(a, \ldots, g)$.

Now assign numerical values in $\mathbb{C}$ to $a, \ldots, g$. We claim that for "most" choices of $a, \ldots, g \in \mathbb{C}$, (5.1) is still equivalent (5.2). This is because transforming (5.1) into (5.2) and back involves a finite number of elements of $\mathbb{C}(a, \ldots, g)$. If we pick $a, \ldots, g \in \mathbb{C}$ so that none of the denominators appearing in these elements vanish, then our transformations will still work for the chosen numerical values of $a, \ldots, g$. In fact, for most choices, (5.2) remains a Gröbner basis for (5.1)—this is related to the idea of *specialization* of a Gröbner basis, which is discussed in Chapter 6, §3 of [CLO], especially Exercises 7–9.

The equivalence of (5.1) and (5.2) for most choices of $a, \ldots, g \in \mathbb{C}$ can be stated more geometrically as follows. Let $\mathbb{C}^7$ denote the affine space consisting of all possible ways of choosing $a, \ldots, g \in \mathbb{C}$, and let P be the product of all of the denominators appearing in the transformation of (5.1) to (5.2) and back. Note that $P(a, \ldots, g) \neq 0$ implies that all of the denominators are nonvanishing. Thus, (5.1) is equivalent to (5.2) for all coefficients $(a, \ldots, g) \in \mathbb{C}^7$ such that $P(a, \ldots, g) \neq 0$. As defined in §5 of Chapter 3, this means that the two systems of equations are equivalent *generically*. We will make frequent use of the term "generic" in this section.

Exercise 1. Consider the equations (5.1) with symbolic coefficients.

a. Using Maple or another computer algebra system, compute the exact form of the Gröbner basis (5.2) and identify explicitly a polynomial P such that if $P(a, \ldots, g) \neq 0$, then (5.1) is equivalent to a system of the

form (5.2). Hint: One can transform (5.1) into (5.2) using the division algorithm. Going the other way is more difficult. The Maple package described in the section on Maple in Appendix D of [CLO] can be used for this purpose.

b. Show that there is another polynomial P' such that if $P'(a, \dots, g) \neq 0$, then the solutions lie in $(\mathbb{C}^*)^2$, where as usual $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

Since (5.2) clearly has at most 18 distinct solutions in $\mathbb{C}^2$, the same is true generically for (5.1). Exercise 8 will show that for generic $(a, \dots, g)$, p_{18} has *distinct* solutions, so that (5.1) has precisely 18 solutions in the generic case. Then, using part b of Exercise 1, we conclude that generically, (5.1) has 18 solutions, all of which lie in $(\mathbb{C}^*)^2$. This will be useful below.

We next turn to §5 of Chapter 3, where we learned about Bézout's Theorem and solving equations via resultants. Since the polynomials f_1 and f_2 have total degree 5, Bézout's Theorem predicts that (5.1) should have at most $5 \cdot 5 = 25$ solutions in $\mathbb{P}^2$. If we homogenize these equations using a third variable z, we get

$$\begin{aligned} 0 &= F_1(x, y) = ax^3y^2 + bxz^4 + cy^2z^3 + dz^5 \\ 0 &= f_2(x, y) = exy^4 + fx^3z^2 + gyz^4. \end{aligned}$$

Here, solutions come in two flavors: affine solutions, which are the solutions of (5.1), and solutions "at ∞", which have $z = 0$. Assuming $ae \neq 0$ (which holds generically), it is easy to see that the solutions at ∞ are $(0, 1, 0)$ and $(1, 0, 0)$. This, combined with Bézout's Theorem, tells us that (5.1) has at most 23 solutions in $\mathbb{C}^2$.

Why do we get 23 instead of 18, which is the actual number? One way to resolve this discrepancy is to realize that the solutions $(0, 1, 0)$ and $(1, 0, 0)$ at ∞ have *multiplicities* (in the sense of Chapter 4) bigger than 1. By computing these multiplicities, one can prove that there are 18 solutions. However, it is more important to realize that by Bézout's Theorem, *generic* equations $f_1 = f_2 = 0$ of total degree 5 in x, y have 25 solutions in $\mathbb{C}^2$. The key point is that the equations in (5.1) are *not* generic in this sense—a typical polynomial $f(x, y)$ of total degree 5 has 21 terms, while those in (5.1) have far fewer. In the terminology of §2, we have *sparse* polynomials—those with fixed Newton polytopes—and what we're looking for is a *sparse* Bézout's Theorem. As we will see below, this is precisely what Bernstein's Theorem does for us.

At this point, the reader might be confused about our use of the word "generic". We just finished saying that the equations (5.1) aren't generic, yet in our discussion of Gröbner bases, we showed that generically, (5.1) has 18 solutions. This awkwardness is resolved by observing that *generic is always relative to a particular set of Newton polytopes*. To state this more precisely, suppose we fix finite sets $\mathcal{A}_1, \dots, \mathcal{A}_l \subset \mathbb{Z}^n$. Each $\mathcal{A}_i$ gives the set

$L(\mathcal{A}_i)$ of Laurent polynomials

$$f_i = \sum_{\alpha \in \mathcal{A}_i} c_{i,\alpha} x^\alpha.$$

Note that we can regard each $L(\mathcal{A}_i)$ as an affine space with the coefficients $c_{i,\alpha}$ as coordinates. Then we can define generic as follows.

(5.3) Definition. A property is said to *hold generically* for Laurent polynomials $(f_1, \dots, f_l) \in L(\mathcal{A}_1) \times \cdots \times L(\mathcal{A}_l)$ if there is a nonzero polynomial in the coefficients of the f_i such that the property holds for all $f_1, \dots, f_l$ for which the polynomial is nonvanishing.

This definition generalizes Definition (5.6) from Chapter 3. Also observe that by Exercise 10 of §1, the Newton polytope $NP(f_i)$ of a generic $f_i \in L(\mathcal{A}_i)$ satisfies $NP(f_i) = \text{Conv}(\mathcal{A}_i)$. Thus we can speak of *generic polynomials with fixed Newton polytopes*. In particular, for polynomials of total degree 5, Bézout's Theorem deals with generic relative to the Newton polytope determined by *all* monomials $x^i y^j$ with $i + j \leq 5$, while for (5.1), generic means relative to the Newton polytopes of f_1 and f_2. The difference in Newton polytopes explains why there is no conflict between our various uses of the term "generic".

One also could ask if resultants can help solve (5.1). This was discussed in §5 of Chapter 3, where we usually assumed our equations had no solutions at ∞. Since (5.1) does have solutions at ∞, standard procedure suggests making a random change of coordinates in (5.1). With high probability, this would make all of the solutions affine, but it would destroy the sparseness of the equations. In fact, it should be clear that rather than the classical multipolynomial resultants of Chapter 3, we want to use the sparse resultants of §2 of this chapter. Actually, we need something slightly more general, since §2 assumes that the Newton polytopes are all equal, which is not the case for (5.1). In §6 we will learn about more general sparse resultants which can be used to study (5.1).

The above discussion leads to the first main question of the section. Suppose we have Laurent polynomials $f_1, \dots, f_n \in \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]$ such that $f_1 = \cdots = f_n = 0$ have finitely many solutions in $(\mathbb{C}^*)^n$. Then we want to know if there is a way to predict an upper bound on the number of solutions of $f_1 = \cdots = f_n = 0$ in $(\mathbb{C}^*)^n$ that is more refined than the Bézout Theorem bound $\deg(f_1) \cdot \deg(f_2) \cdots \deg(f_n)$. Ideally, we want a bound that uses only information about the forms of the polynomials f_i themselves. In particular, we want to *avoid* computing Gröbner bases and studying the ring $A = \mathbb{C}[x_1, \dots, x_n]/\langle f_1, \dots, f_n \rangle$ as in Chapter 2, if possible.

To see how mixed volumes enter the picture, let P_1 and P_2 denote the Newton polytopes of the polynomials f_1, f_2 in (5.1). Referring back to equation (4.13) from the previous section, note that the *mixed volume* of

these polytopes satisfies

$$MV_2(P_1, P_2) = 18,$$

which agrees with the number of solutions of the system (5.1) for generic choices of the coefficients. Surely this is no coincidence! As a further test, consider instead two generic polynomials of total degree 5. Here, the Newton polytopes are both the simplex $Q_5 \subset \mathbb{R}^2$ described in Exercise 2 of §1, which has volume $\mathrm{Vol}_2(Q_5) = 25/2$ by Exercise 3 of that section. Using Exercise 7 of §4, we conclude that

$$MV_2(Q_5, Q_5) = 2\,\mathrm{Vol}_2(Q_5) = 25,$$

so that again, the mixed volume predicts the number of solutions.

Exercise 2. More generally, polynomials of total degrees $d_1, \dots, d_n$ in $x_1, \dots, x_n$ have Newton polytopes given by the simplices $Q_{d_1}, \dots, Q_{d_n}$ respectively. Use the properties of mixed volume from §4 to prove that

$$MV_n(Q_{d_1}, \dots, Q_{d_n}) = d_1 \cdots d_n,$$

so that the general Bézout bound is the mixed volume of the appropriate Newton polytopes.

The main result of this section is a theorem of Bernstein relating the number of solutions to the mixed volume of the Newton polytopes of the equations. A slightly unexpected fact is that the theorem predicts the numbers of solutions in $(\mathbb{C}^*)^n$ rather than in $\mathbb{C}^n$. We will explain why at the end of the section.

(5.4) Theorem (Bernstein's Theorem). *Given Laurent polynomials $f_1, \dots, f_n$ over $\mathbb{C}$ with finitely many common zeroes in $(\mathbb{C}^*)^n$, let $P_i = \mathrm{NP}(f_i)$ be the Newton polytope of f_i in $\mathbb{R}^n$. Then the number of common zeroes of the f_i in $(\mathbb{C}^*)^n$ is bounded above by the mixed volume $MV_n(P_1, \dots, P_n)$. Moreover, for generic choices of the coefficients in the f_i, the number of common solutions is exactly $MV_n(P_1, \dots, P_n)$.*

Proof. We will sketch the main ideas in Bernstein's proof, and indicate how $MV_n(P_1, \dots, P_n)$ solutions of a generic system can be found. However, proving that this construction finds *all* the solutions of a generic system in $(\mathbb{C}^*)^n$ requires some additional machinery. Bernstein uses the theory of Puiseux expansions of algebraic functions for this; a more geometric understanding is obtained via the theory of projective toric varieties. We will state the relevant facts here without proof. For this and other details of the proof, we will refer the reader to [Ber] (references to other proofs will be given below).

The proof is by induction on n. For $n = 1$, we have a single Laurent polynomial $f(x) = 0$ in one variable. After multiplying by a suitable Laurent

monomial x^a, we obtain a polynomial equation

$$0 = \hat{f}(x) = x^a f(x) = c_m x^m + c_{m-1}x^{m-1} + \cdots + c_0, \tag{5.5}$$

where $m \geq 0$. Multiplying by x^a does not affect the solutions of $f(x) = 0$ in $\mathbb{C}^*$. By the Fundamental Theorem of Algebra, we see that both (5.5) and the original equation $f = 0$ have m roots (counting multiplicity) in $\mathbb{C}^*$ provided $c_m c_0 \neq 0$. Furthermore, as explained in Exercise 8 at the end of the section, $\hat{f}$ has distinct roots when $c_0, \ldots, c_m$ are generic. Thus, generically, $f = 0$ has m distinct roots in $\mathbb{C}^*$. However, the Newton polytope $P = \mathrm{NP}(f)$ is a translate of $\mathrm{NP}(\hat{f})$, which is the interval $[0, m]$ in $\mathbb{R}$. By Exercise 7 of §4, the mixed volume $MV_1(P)$ equals the length of P, which is m. This establishes the base case of the induction.

The induction step will use the geometry of the Minkowski sum $P = P_1 + \cdots + P_n$. The basic idea is that for each primitive inward pointing facet normal $\nu \in \mathbb{Z}^n$ of P, we will deform the equations $f_1 = \cdots = f_n = 0$ by varying the coefficients until some of them are zero. Using the induction hypothesis, we will show that in the limit, the number of solutions of the deformed equations is given by

$$a_{P_1}(\nu)\, MV'_{n-1}((P_2)_\nu, \ldots, (P_n)_\nu), \tag{5.6}$$

where $a_{P_1}(\nu)$ is defined in (1.3) and $MV'_{n-1}((P_2)_\nu, \ldots, (P_n)_\nu)$ is the normalized $(n-1)$-dimensional mixed volume defined in Theorem (4.12). We will also explain how each of these solutions contributes a solution to our original system. Adding up these solutions over all facet normals ν of P gives the sum

$$\sum_\nu a_{P_1}(\nu)\, MV'_{n-1}((P_2)_\nu, \ldots, (P_n)_\nu) = MV_n(P_1, \ldots, P_n), \tag{5.7}$$

where the equality follows from Theorem (4.12). To complete the induction step, we would need to show that the total number of solutions of the original system in $(\mathbb{C}^*)^n$ is generically equal to, and in any case no larger than, the sum given by (5.7). The proof is beyond the scope of this book, so we will not do this. Instead, we will content ourselves with showing explicitly how each facet normal ν of P gives a deformation of the equations $f_1 = \cdots = f_n = 0$ which in the limit has (5.6) as its generic number of solutions.

To carry out this strategy, let $\nu \in \mathbb{Z}^n$ be the primitive inward pointing normal to a facet of P. As usual, the facet is denoted P_ν, and we know from §4 that

$$P_\nu = (P_1)_\nu + \cdots + (P_n)_\nu,$$

where $(P_i)_\nu$ is the face (not necessarily a facet) of the Newton polytope $P_i = \mathrm{NP}(f_i)$ determined by ν. By §1, $(P_i)_\nu$ is the convex hull of those α minimizing $\nu \cdot \alpha$ among the monomials x^α from f_i. In other words, if the face $(P_i)_\nu$ lies in the hyperplane $m \cdot \nu = -a_{P_i}(\nu)$, then for all exponents α

of f_i, we have

$$\alpha \cdot \nu \geq -a_{P_i}(\nu),$$

with equality holding if and only if $\alpha \in (P_i)_\nu$. This means that f_i can be written

$$f_i = \sum_{\nu\cdot\alpha=-a_{P_i}(\nu)} c_{i,\alpha}x^\alpha \quad + \sum_{\nu\cdot\alpha>-a_{P_i}(\nu)} c_{i,\alpha}x^\alpha. \tag{5.8}$$

Before we can deform our equations, we first need to change f_1 slightly. If we multiply f_1 by $x^{-\alpha}$ for some $\alpha \in P_1$, then we may assume that there is a nonzero constant term c_1 in f_1. This means $0 \in P_1$, so that $a_{P_1}(\nu) \geq 0$ by the above inequality. As noted in the base case, changing f_1 in this way affects neither the solutions of the system in $(\mathbb{C}^*)^n$ nor the mixed volume of the Newton polytopes.

We also need to introduce some new coordinates. In Exercise 9 below, you will show that since ν is primitive, there is an invertible $n \times n$ integer matrix B such that ν is its first row and its inverse is also an integer matrix. If we write $B = (b_{ij})$, then consider the coordinate change

$$x_j \mapsto \prod_{i=1}^{n} y_i^{-b_{ij}}. \tag{5.9}$$

This maps x_j to the Laurent monomial in the new variables $y_1, \ldots, y_n$ whose exponents are the integers appearing in the jth column of the matrix $-B$. (The minus sign is needed because ν is an inward pointing normal.) Under this change of coordinates, it is easy to check that the Laurent monomial x^α maps to the Laurent monomial $y^{-B\alpha}$, where $B\alpha$ is the usual matrix multiplication, regarding α as a column vector. See Exercise 10 below.

If we apply this coordinate change to f_i, note that a monomial x^α appearing in the first sum of (5.8) becomes

$$y^{-B\alpha} = y_1^{a_{P_i}(\nu)} y_2^{\beta_2} \cdots y_n^{\beta_n}$$

(for some integers $\beta_2, \ldots, \beta_n$) since $\nu \cdot \alpha = -a_{P_i}(\nu)$ and ν is the first row of B. Similarly, a monomial x^α in the second sum of (5.8) becomes

$$y^{-B\alpha} = y_1^{\beta_1} y_2^{\beta_2} \cdots y_n^{\beta_n}, \quad \beta_1 < a_{P_i}(\nu).$$

It follows from (5.8) that f_i transforms into a polynomial of the form

$$g_{i\nu}(y_2, \ldots, y_n) y_1^{a_{P_i}(\nu)} + \sum_{j<a_{P_i}(\nu)} g_{ij\nu}(y_2, \ldots, y_n) y_1^j.$$

Note also that the Newton polytope of $g_{i\nu}(y_2, \ldots, y_n)$ is equal to the image under the linear mapping defined by the matrix B of the face $(P_i)_\nu$.

Thus the equations $f_1 = \cdots = f_n = 0$ map to the new system

$$\begin{aligned}
0 &= g_{1\nu}(y_2,\dots,y_n)y_1^{a_{P_1}(\nu)} + \sum_{j<a_{P_1}(\nu)} g_{1j\nu}(y_2,\dots,y_n)y_1^j \\
0 &= g_{2\nu}(y_2,\dots,y_n)y_1^{a_{P_2}(\nu)} + \sum_{j<a_{P_2}(\nu)} g_{2j\nu}(y_2,\dots,y_n)y_1^j \\
&\vdots \\
0 &= g_{n\nu}(y_2,\dots,y_n)y_1^{a_{P_n}(\nu)} + \sum_{j<a_{P_n}(\nu)} g_{nj\nu}(y_2,\dots,y_n)y_1^j
\end{aligned} \tag{5.10}$$

under the coordinate change $x^\alpha \mapsto y^{-B\alpha}$. As above, the constant term of f_1 is denoted c_1, and we now deform these equations by substituting

$$c_1 \mapsto \frac{c_1}{t^{a_{P_1}(\nu)}}, \quad y_1 \mapsto \frac{y_1}{t}$$

in (5.10), where t is a new variable, and then multiplying the ith equation by $t^{a_{P_i}(\nu)}$. To see what this looks like, first suppose that $a_{P_1}(\nu) > 0$. This means that in the first equation of (5.10), c_1 is the $j = 0$ term in the sum. Then you can check that the deformation has the effect of leaving c_1 and the $g_{i\nu}$ unchanged, and multiplying all other terms by positive powers of t. It follows that the deformed equations can be written in the form

$$\begin{aligned}
0 &= g_{1\nu}(y_2,\dots,y_n)y_1^{a_{P_1}(\nu)} + c_1 + O(t) \\
0 &= g_{2\nu}(y_2,\dots,y_n)y_1^{a_{P_2}(\nu)} + O(t) \\
&\vdots \\
0 &= g_{n\nu}(y_2,\dots,y_n)y_1^{a_{P_n}(\nu)} + O(t),
\end{aligned} \tag{5.11}$$

where the notation $O(t)$ means a sum of terms each divisible by t.

When $t = 1$, the equations (5.11) coincide with (5.10). Also, from the point of view of our original equations $f_i = 0$, note that (5.11) corresponds to multiplying each term in the second sum of (5.8) by a positive power of t, with the exception of the constant term c_1 of f_1, which is unchanged.

Now, in (5.11), let $t \to 0$ along a general path in $\mathbb{C}$. This gives the equations

$$\begin{aligned}
0 &= g_{1\nu}(y_2,\dots,y_n)y_1^{a_{P_1}(\nu)} + c_1 \\
0 &= g_{2\nu}(y_2,\dots,y_n)y_1^{a_{P_2}(\nu)} \\
&\vdots \\
0 &= g_{n\nu}(y_2,\dots,y_n)y_1^{a_{P_n}(\nu)},
\end{aligned}$$

which, in terms of solutions in $(\mathbb{C}^*)^n$, are equivalent to

$$\begin{aligned} 0 &= g_{1\nu}(y_2,\dots,y_n)y_1^{a_{P_1}(\nu)} + c_1 \\ 0 &= g_{2\nu}(y_2,\dots,y_n) \\ &\vdots \\ 0 &= g_{n\nu}(y_2,\dots,y_n). \end{aligned} \tag{5.12}$$

It can be shown that for a sufficiently generic original system of equations, the equations $g_{2\nu} = \cdots = g_{n\nu} = 0$ in (5.12) are generic with respect to $B \cdot (P_2)_\nu, \dots, B \cdot (P_n)_\nu$. Hence, applying the induction hypothesis to the last $n-1$ equations in (5.12), we see that there are

$$MV_{n-1}(B \cdot (P_2)_\nu, \dots, B \cdot (P_n)_\nu)$$

possible solutions $(y_2,\dots,y_n) \in (\mathbb{C}^*)^{n-1}$ of these $n-1$ equations. In Exercise 11 below, you will show that

$$MV_{n-1}(B \cdot (P_2)_\nu, \dots, B \cdot (P_n)_\nu) = MV'_{n-1}((P_2)_\nu, \dots, (P_n)_\nu),$$

where MV'_{n-1} is the normalized mixed volume from Theorem (4.12).

For each $(y_2,\dots,y_n)$ solving the last $n-1$ equations in (5.12), there are $a_{P_1}(\nu)$ possible values for $y_1 \in \mathbb{C}^*$ provided $g_{1\nu}(y_2,\dots,y_n) \neq 0$ and $c_1 \neq 0$. This is true generically (we omit the proof), so that the total number of solutions of (5.12) is

$$a_{P_1}(\nu)\, MV'_{n-1}((P_2)_\nu, \dots, (P_n)_\nu),$$

which agrees with (5.6).

The next step is to prove that for each solution $(y_1,\dots,y_n)$ of (5.12), one can find parametrized solutions $(y_1(t),\dots,y_n(t))$ of the deformed equations (5.11) satisfying $(y_1(0),\dots,y_n(0)) = (y_1,\dots,y_n)$. This step involves some concepts we haven't discussed (the functions $y_i(t)$ are *not* polynomials in t), so we will not go into the details here, though the discussion following the proof will shed some light on what is involved.

Once we have the parametrized solutions $(y_1(t),\dots,y_n(t))$, we can follow them back to $t = 1$ to get solutions $(y_1(1),\dots,y_n(1))$ of (5.10). Since the inverse of the matrix B has integer entries, each of these solutions $(y_1(1),\dots,y_n(1))$ can be converted back to a unique $(x_1,\dots,x_n)$ using the inverse of (5.9) (see Exercise 10 below). It follows that the equations (5.12) give rise to (5.6) many solutions of our original equations.

This takes care of the case when $a_{P_1}(\nu) > 0$. Since we arranged f_1 so that $a_{P_1}(\nu) \geq 0$, we still need to consider what happens when $a_{P_1}(\nu) = 0$. Here, c_1 lies in the first sum of (5.8) for f_1, so that under our coordinate change, it becomes the constant term of $g_{1\nu}$. This means that instead of (5.11), the first deformed equation can be written as

$$0 = g_{1\nu}(y_2,\dots,y_n) + O(t)$$

since $a_{P_1}(\nu) = 0$ and c_1 appears in $g_{1\nu}$. Combined with the deformed equations from (5.11) for $2 \le i \le n$, the limit as $t \to 0$ gives the equations

$$0 = g_{i\nu}(y_2, \dots, y_n) y_1^{a_{P_i}(\nu)}, \quad 1 \le i \le n.$$

As before, the $(\mathbb{C}^*)^n$ solutions are the same as the solutions of the equations

$$0 = g_{i\nu}(y_2, \dots, y_n), \quad 1 \le i \le n.$$

However, one can show that $g_{1\nu}$ is generic and hence *doesn't* vanish at the solutions of $g_{2\nu} = \cdots = g_{n\nu} = 0$. This means that generically, the $t \to 0$ limit of the deformed system has *no* solutions, which agrees with (5.6).

We conclude that each facet contributes (5.6) many solutions to our original equations, and adding these up as in (5.7), we get the mixed volume $MV_n(P_1, \dots, P_n)$. This completes our sketch of the proof. □

In addition to Bernstein's original paper [Ber], there are closely related papers by Kushnirenko [Kus] and Khovanskii [Kho]. For this reason, the mixed volume bound $MV_n(P_1, \dots, P_n)$ on the number of solutions given in Theorem (5.4) is sometimes called the *BKK bound*. A geometric interpretation of the BKK bound in the context of toric varieties is given in [Ful] and [GKZ], and a more refined version can be found in [Roj3]. Also, [HuS1] and [Roj1] study the genericity conditions needed to ensure that exactly $MV_n(P_1, \dots, P_n)$ different solutions exist in $(\mathbb{C}^*)^n$. These papers use a variety of methods, including sparse elimination theory and toric varieties.

The proof we sketched for the BKK bound uses the formula

$$\sum_{\nu} a_{P_1}(\nu) \cdot MV'_{n-1}((P_2)_\nu, \dots, (P_n)_\nu) = MV_n(P_1, \dots, P_n)$$

from Theorem (4.12). If you look back at the statement of this theorem in §4, you'll see that the sum is actually taken over all facet normals ν such that $(P_2)_\nu, \dots, (P_n)_\nu$ all have dimension *at least one*. This restriction on ν relates nicely to the proof of the BKK bound as follows.

Exercise 3. In the proof of Theorem (5.4), we obtained the system (5.10) of transformed equations. Suppose that for some i between 2 and n, $(P_i)_\nu$ has dimension zero. Then show that in (5.10), the corresponding $g_{i\nu}$ consists of a single term, and conclude that in the limit (5.12) of the deformed equations, the last $n-1$ equations have *no* solutions generically.

Exercise 4. Consider the equations $f_1 = f_2 = 0$ from (5.1). In this exercise, you will explicitly construct the coordinate changes used in the proof of Bernstein's theorem.

a. Use the previous exercise to show that in this case, the vectors ν that must be considered are all among the facet normals of the polytope $P_2 = NP(f_2)$. These normals, denoted $\nu_{\mathcal{F}}$, $\nu_{\mathcal{G}}$ and $\nu_{\mathcal{H}}$, were computed

in Exercise 5 of §4 and in the discussion preceeding that exercise. Also, the mixed volume $MV_2(P_1, P_2) = 18$ was computed in (4.13).

b. Show that $a_{P_1}(\nu_{\mathcal{F}}) = 0$. Hence the term from (5.7) with $\nu = \nu_{\mathcal{F}}$ is zero.

c. For $\nu = \nu_{\mathcal{G}}$, show that

$$B = \begin{pmatrix} -2 & -1 \\ 1 & 0 \end{pmatrix}$$

has ν as first row. Also show that B^{-1} has integer entries.

d. Apply the corresponding change of variables

$$x \mapsto z^2 w^{-1}, \qquad y \mapsto z$$

to (5.1). Note that we are calling the "old" variables x, y and the "new" ones z, w rather than using subscripts. In particular, z plays the role of the variable y_1 used in the proof.

e. After substituting $d \mapsto d/t$ and $z \mapsto z/t$, multiply by the appropriate powers of t to obtain

$$\begin{aligned} 0 &= aw^{-3}z^8 + d + t^6 \cdot bw^{-1}z^2 + t^6 \cdot cz^2 \\ 0 &= (ew^{-1} + fw^{-3})z^6 + t^5 \cdot gz. \end{aligned}$$

f. Let $t \to 0$ and count the number of solutions of the deformed system. Show that this number equals $a_{P_1}(\nu_{\mathcal{G}})MV_1'(\mathcal{G})$.

g. Finally, carry out steps c–f for the facet $\mathcal{H}$ of P_2, and show we obtain 18 solutions.

Exercise 5. Use Bernstein's theorem to deduce a statement about the number of solutions in $(\mathbb{C}^*)^n$ of a generic system of Laurent polynomial equations $f_1 = \cdots = f_n = 0$ when the Newton polytopes of the f_i are all *equal*. (This was the case considered by Khovanskii in [Kho].)

Exercise 6. Use Bernstein's Theorem and Exercise 2 to obtain a version of the usual Bézout theorem. Your version will be slightly different from those discussed in §5 of Chapter 3 because of the $(\mathbb{C}^*)^n$ restriction.

While the BKK bound tells us about the number of solutions in $(\mathbb{C}^*)^n$, one could also ask about the number of solutions in $\mathbb{C}^n$. For example, for (5.1), we checked earlier that generically, these equations have $MV_2(P_1, P_2) = 18$ solutions in either $\mathbb{C}^2$ or $(\mathbb{C}^*)^2$. However, some surprising things happen if we change the equations slightly.

Exercise 7. Suppose that the equations of (5.1) are $f_1 = f_2 = 0$.

a. Show that generically, the equations $f_1 = x\, f_2 = 0$ have 18 solutions in $(\mathbb{C}^*)^2$ and 20 solutions in $\mathbb{C}^2$. Also show that

$$MV_2(\mathrm{NP}(f_1), \mathrm{NP}(x\, f_2)) = 18.$$

Hint: Mixed volume is unaffected by translation.

b. Show that generically, the equations $y\,f_1 = x\,f_2 = 0$ have 18 solutions in $(\mathbb{C}^*)^2$ and 21 solutions in $\mathbb{C}^2$. Also show that

$$MV_2(\mathrm{NP}(y\,f_1), \mathrm{NP}(x\,f_2)) = 18.$$

This exercise illustrates that multiplying f_1 and f_2 by monomials changes neither the solutions in $(\mathbb{C}^*)^2$ nor the mixed volume, while the number of solutions in $\mathbb{C}^2$ *can* change. There are also examples, not obtained by multiplying by monomials, which have more solutions in $\mathbb{C}^n$ than in $(\mathbb{C}^*)^n$ (see Exercise 13 below). The consequence is that the mixed volume is really tied to the solutions in $(\mathbb{C}^*)^n$. In general, finding the generic number of solutions in $\mathbb{C}^n$ is a more subtle problem. For some recent progress in this area, see [HuS2], [LW], [Roj1], [Roj3], and [RW]. An analysis of genericity conditions for solutions in $\mathbb{C}^n$ appears in [Roj3] and an expository account of recent work in this area (including proofs) can be found in [Roj5].

We will conclude this section with some remarks on how the BKK bound can be combined with numerical methods to actually find the solutions of equations like (5.1). First, recall that for (5.1), Bézout's Theorem gives the upper bound of 25 for the number of solutions, while the BKK bound of 18 is smaller (and gives the exact number generically). For the task of computing numerically all complex solutions of (5.1), the better upper bound 18 is useful information to have, since once we have found 18 solutions, there are no others, and whatever method we are using can terminate.

But what sort of numerical method should we use? Earlier, we discussed methods based on Gröbner bases and resultants. Now we will say a few words about numerical *homotopy continuation methods*, which give another approach to practical polynomial equation solving. The method we will sketch is especially useful for systems whose coefficients are known only in some finite precision approximations, or whose coefficients vary widely in size. Our presentation follows [VVC].

We begin with a point we did not address in the proof of Theorem (5.4): exactly *how* do we extend a solution $(y_1, \ldots, y_n)$ of (5.12) to a parametric solution $(y_1(t), \ldots, y_n(t))$ of the deformed equations (5.11)? In general, the problem is to "track" solutions of systems of equations such as (5.11) where the coefficients depend on a parameter t, and the solutions are thought of as functions of t. General methods for doing this were developed by numerical analysts independently, at about the same time as the BKK bound. See [AG] and [Dre] for general discussion of these *homotopy continuation methods*. The idea is the following. For brevity, we will write a system of equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0$$

more compactly as $f(x) = 0$. To solve $f(x) = 0$, we start with a second system $g(x) = 0$ whose solutions are known in advance. In some versions of this approach, $g(x)$ might have a simpler form than $f(x)$. In others, as

we will do below, one takes a known system which we expect has the same number of solutions as $f(x) = 0$.

Then we consider the continuous family of systems

$$0 = h(x,t) = c(1-t)g(x) + tf(x), \tag{5.13}$$

depending on a parameter t, where $c \in \mathbb{C}$ is some constant which is chosen generically to avoid possible bad special behavior.

When $t = 0$, we get the known system $g(x) = 0$ (up to a constant). Indeed, $g(x) = 0$ is often called the *start system* and (5.13) is called a *homotopy* or *continuation system*. As t changes continuously from 0 to 1 along the real line (or more generally along a path in the complex plane), suppose the rank of the Jacobian matrix of $h(x,t)$ with respect to x:

$$J(x,t) = \Big(\frac{\partial h_i}{\partial x_j}(x,t)\Big)$$

is n for all values of t. Then, by the Implicit Function Theorem, if x_0 is a solution of $g(x) = 0$, we obtain a solution curve $x(t)$ with $x(0) = x_0$ that is parametrized by algebraic functions of t. The goal is to determine the values of $x(t)$ at $t = 1$, since these will yield the solutions of the system $f(x) = 0$ we are interested in.

To find these parametrized solutions, we proceed as follows. Since we want $h(x(t),t)$ to be identically zero as a function of t, its derivative $\frac{d}{dt}h(x(t),t)$ should also vanish identically. By the multivariable chain rule, we see that the solution functions $x(t)$ satisfy

$$0 = \frac{d}{dt}h(x(t),t) = J(x(t),t)\frac{dx(t)}{dt} + \frac{\partial h}{\partial t}(x(t),t),$$

which gives a system of ordinary differential equations (ODEs):

$$J(x(t),t)\frac{dx(t)}{dt} = -\frac{\partial h}{\partial t}(x(t),t)$$

for the solution functions $x(t)$. Since we also know the initial value $x(0) = x_0$, one possible approach is to use the well-developed theory of numerical methods for ODE initial value problems to construct approximate solutions, continuing this process until approximations to the solution $x(1)$ are obtained.

Alternatively, we could apply an iterative numerical root-finding method (such as the Newton-Raphson method) to solve (5.13). The idea is to take a known solution of (5.13) for $t = 0$ and propagate it in steps of size Δt until $t = 1$. Thus, if we start with a solution $x_0 = x(0)$ for $t = 0$, we can use it as the initial guess for solving

$$h(x(\Delta t), \Delta t) = 0$$

using our given numerical method. Then, once we have $x(\Delta t)$, we use it as the initial guess for solving

$$h(x(2\Delta t), 2\Delta t) = 0$$

by our chosen method. We continue in this way until we have solved $h(x(1), 1) = 0$, which will give the desired solution. This method works because $x(t)$ is a continuous function of t, so that at the step with $t = (k + 1)\Delta t$, we will generally have fairly good estimates for initial points from the results of the previous step (i.e., for $t = k\Delta t$), provided Δt is sufficiently small.

When homotopy continuation methods were first developed, the best commonly known bound on the number of expected solutions was the Bézout theorem bound. A common choice for $g(x)$ was a random dense system with equations of the same total degrees as $f(x)$. But many polynomial systems (for instance (5.1)) have fewer solutions than general dense systems of the same total degrees! When this is true, some of the numerically generated approximate solution paths diverge to infinity as $t \to 1$. This is because the start equations $g(x) = 0$ would typically have many more solutions than the sparse system $f(x) = 0$. Much computational effort can be wasted trying to track them accurately.

As a result, the more refined BKK bound is an important tool in applying homotopy continuation methods. Instead of a random *dense* start system $g(x) = 0$, a much better choice in many cases is a randomly chosen start system for which the g_i have the *same Newton polytopes* as the corresponding f_i:

$$\mathrm{NP}(g_i) = \mathrm{NP}(f_i).$$

Of course, the solutions of $g(x) = 0$ must be determined as well. Unless solutions of some specific system with precisely these Newton polytopes is known, some work must be done to solve the start system before the homotopy continuation method can be applied. For this, the authors of [VVC] propose adapting the deformations used in the proof of Bernstein's theorem, and applying a continuation method again to determine the solutions of $g(x) = 0$. A closely related method, described in [HuS1] and [VGC], uses the mixed subdivisions to be defined in §6. Also, some interesting numerical issues are addressed in [HV]. Some other recent papers on this subject include [DKK], [Li], and [Ver2]. The software PHCpack described in [Ver1] solves systems of equations using the polynomial homotopy continuation method described here. This package is available at `http://www2.math.uic.edu/~jan/PHCpack/phcpack.html`. Other software for polynomial homotopies is described in [Li].

The geometry of polytopes provides powerful tools for understanding sparse systems of polynomial equations. The mixed volume is an efficient bound for the number of solutions, and homotopy continuation methods

give practical methods for finding the solutions. This is an active area of research, and further progress is likely in the future.

Additional Exercises for §5

Exercise 8. If $f \in \mathbb{C}[x]$ is a polynomial of degree n, its *discriminant* $\mathrm{Disc}(f)$ is defined to be the resultant

$$\mathrm{Disc}(f) = \mathrm{Res}_{n,n-1}(f, f'),$$

where f' is the derivative of f. One can show that $\mathrm{Disc}(f) \neq 0$ if and only if f has no multiple roots (see Exercises 7 and 8 of Chapter 3, §5 of [CLO]).

a. Show that the generic polynomial $f \in \mathbb{C}[x]$ has no multiple roots. Hint: It suffices to show that the discriminant is a nonzero polynomial in the coefficients of f. Prove this by writing down an explicit polynomial of degree n which has distinct roots.
b. Now let $p_{18} \in \mathbb{C}(a, \ldots, g)[x]$ be the polynomial from (5.2). To show that p_{18} has no multiple roots generically, we need to show that $\mathrm{Disc}(p_{18})$ is nonzero as a rational function of $a, \ldots, g$. Computing this discriminant would be unpleasant since the coefficients of p_{18} are so complicated. So instead, take p_{18} and make a random choice of $a, \ldots, g$. This will give a polynomial in $\mathbb{C}[x]$. Show that the discriminant is nonzero and conclude that p_{18} has no multiple roots for generic $a, \ldots, g$.

Exercise 9. Let $\nu \in \mathbb{Z}^n$ be a primitive vector (thus $\nu \neq 0$ and the entries of ν have no common factor > 1). Our goal is to find an integer $n \times n$ matrix with integer inverse and ν as its first row. For the rest of the exercise, we will regard ν as a column vector. Hence it suffices to find an integer $n \times n$ matrix with integer inverse and ν as its first column.

a. Explain why it suffices to find an integer matrix A with integer inverse such that $A\nu = \vec{e}_1$, where $\vec{e}_1 = (1, 0, \ldots, 0)^T$ is the usual standard basis vector. Hint: Multiply by A^{-1}.
b. An *integer row operation* consists of a row operation of the following three types: switching two rows, adding an integer multiple of a row to another row, and multiplying a row by ± 1. Show that the elementary matrices corresponding to integer row operations are integer matrices with integer inverses.
c. Using parts a and b, explain why it suffices to reduce ν to $\vec{e}_1$ using integer row operations.
d. Using integer row operations, show that ν can be transformed to a vector $(b_1, \ldots, b_n)^T$ where $b_1 > 0$ and $b_1 \leq b_i$ for all i with $b_i \neq 0$.
e. With $(b_1, \ldots, b_n)^T$ as in the previous step, use integer row operations to subtract multiples of b_1 from one of the nonzero entries b_i, $i > 1$, until you get either 0 or something positive and smaller than b_1.

f. By repeatedly applying steps d and e, conclude that we can integer row reduce ν to a positive multiple of $\vec{e}_1$.
g. Finally, show that ν being primitive implies that the previous step gives $\vec{e}_1$ exactly. Hint: Using earlier parts of the exercise, show that we have $A\nu = d\vec{e}_1$, where A has an integer inverse. Then use A^{-1} to conclude that d divides every entry of ν.

Exercise 10.
a. Under the coordinate change (5.9), show that the Laurent monomial x^α, $\alpha \in \mathbb{Z}^n$, maps to the Laurent monomial $y^{-B\alpha}$, where $B\alpha$ is the matrix product.
b. Show that (5.9) actually induces a one-to-one correspondence between Laurent monomials in x and Laurent monomials in y.
c. Show that (5.9) defines a one-to-one, onto mapping from $(\mathbb{C}^*)^n$ to itself. Also explain how $-B^{-1}$ gives the inverse mapping.

Exercise 11. Show that

$$MV_{n-1}(B \cdot (P_2)_\nu, \dots, B \cdot (P_n)_\nu) = MV'_{n-1}((P_2)_\nu, \dots, (P_n)_\nu),$$

where the notation is as in the proof of Bernstein's Theorem.

Exercise 12. Consider the following system of three equations in three unknowns:

$$\begin{aligned} 0 &= a_1xy^2z + b_1x^4 + c_1y + d_1z + e_1 \\ 0 &= a_2xyz^2 + b_2y^3 + c_2 \\ 0 &= a_3x^3 + b_3y^2 + c_3z. \end{aligned}$$

What is the BKK bound for the generic number of solutions in $(\mathbb{C}^*)^3$?

Exercise 13. Show that generically, the equations (taken from [RW])

$$\begin{aligned} 0 &= ax^2y + bxy^2 + cx + dy \\ 0 &= ex^2y + fxy^2 + gx + hy \end{aligned}$$

have 4 solutions in $(\mathbb{C}^*)^2$ and 5 solutions in $\mathbb{C}^2$.

§6 Computing Resultants and Solving Equations

The sparse resultant $\mathrm{Res}_{\mathcal{A}}(f_1, \dots, f_n)$ introduced in §2 requires that the Laurent polynomials $f_1, \dots, f_n$ be built from monomials using the same set $\mathcal{A}$ of exponents. In this section, we will discuss what happens when we allow each f_i to involve different monomials. This will lead to the *mixed sparse resultant*. We also have some unfinished business from §2, namely the problem of computing sparse resultants. For this purpose, we will introduce

the notion of a *mixed subdivision*. These will enable us not only to compute sparse resultants but also to find mixed volumes and to solve equations using the methods of Chapter 3.

We begin with a discussion of the mixed sparse resultant. Fix $n+1$ finite sets $\mathcal{A}_0, \dots, \mathcal{A}_n \subset \mathbb{Z}^n$ and consider $n+1$ Laurent polynomials $f_i \in L(\mathcal{A}_i)$. The rough idea is that the resultant

$$\operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0, \dots, f_n)$$

will measure whether or not the $n+1$ equations in n variables

$$f_0(x_1, \dots, x_n) = \cdots = f_n(x_1, \dots, x_n) = 0 \tag{6.1}$$

have a solution. To make this precise, we proceed as in §2 and let

$$Z(\mathcal{A}_0, \dots, \mathcal{A}_n) \subset L(\mathcal{A}_0) \times \cdots \times L(\mathcal{A}_n)$$

be the Zariski closure of the set of all $(f_0, \dots, f_n)$ for which (6.1) has a solution in $(\mathbb{C}^*)^n$.

(6.2) Theorem. *Assume that $Q_i = \operatorname{Conv}(\mathcal{A}_i)$ is an n-dimensional polytope for $i = 0, \dots, n$. Then there is an irreducible polynomial $\operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}$ in the coefficients of the f_i such that*

$$(f_0, \dots, f_n) \in Z(\mathcal{A}_0, \dots, \mathcal{A}_n) \iff \operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0, \dots, f_n) = 0.$$

In particular, if (6.1) has a solution $(t_1, \dots, t_n) \in (\mathbb{C}^*)^n$, then

$$\operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0, \dots, f_n) = 0.$$

This theorem is proved in Chapter 8 of [GKZ]. Note that the mixed sparse resultant includes *all* of the resultants considered so far. More precisely, the (unmixed) sparse resultant from §2 is

$$\operatorname{Res}_{\mathcal{A}}(f_0, \dots, f_n) = \operatorname{Res}_{\mathcal{A},\dots,\mathcal{A}}(f_0, \dots, f_n),$$

and the multipolynomial resultant studied in Chapter 3 is

$$\operatorname{Res}_{d_0,\dots,d_n}(F_0, \dots, F_n) = \operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0, \dots, f_n),$$

where $\mathcal{A}_i = \{m \in \mathbb{Z}^n_{\geq 0} : |m| \leq d_i\}$ and F_i is the homogenization of f_i.

We can also determine the degree of the mixed sparse resultant. In §2, we saw that the degree of $\operatorname{Res}_{\mathcal{A}}$ involves the volume of the Newton polytope $\operatorname{Conv}(\mathcal{A})$. For the mixed resultant, this role is played by the mixed volume from §4.

(6.3) Theorem. *Assume that $Q_i = \operatorname{Conv}(\mathcal{A}_i)$ is n-dimensional for each $i = 0, \dots, n$ and that $\mathbb{Z}^n$ is generated by the differences of elements in $\mathcal{A}_0 \cup \cdots \cup \mathcal{A}_n$. Then, if we fix i between 0 and n, $\operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}$ is homogeneous in the coefficients of f_i of degree $MV_n(Q_0, \dots, Q_{i-1}, Q_{i+1}, \dots, Q_n)$. Thus*

$$\operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0, \dots, \lambda f_i, \dots, f_n) = \lambda^{MV_n(Q_0,\dots,Q_{i-1},Q_{i+1},\dots,Q_n)} \operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0, \dots, f_n).$$

A proof can be found in Chapter 8 of [GKZ]. Observe that this result generalizes both Theorem (3.1) of Chapter 3 and Theorem (2.9) of this chapter. There are also more general versions of Theorems (6.2) and (6.3) which don't require that the Q_i be n-dimensional. See, for instance, [Stu3]. Exercise 9 at the end of the section gives a simple example of a sparse resultant where all of the Q_i have dimension $< n$.

We next discuss how to compute sparse resultants. Looking back at Chapter 3, recall that there were wonderful formulas for the multipolynomial case, but it general, computing these resultants was not easy. The known formulas for multipolynomial resultants fall into three main classes:

- Special cases where the resultant is given as a determinant. This includes the resultants $\mathrm{Res}_{l,m}$ and $\mathrm{Res}_{2,2,2}$ from §1 and §2 of Chapter 3.
- The general case where the resultant is given as the GCD of $n+1$ determinants. This is Proposition (4.7) of Chapter 3.
- The general case where the resultant is given as the quotient of two determinants. This is Theorem (4.9) of Chapter 3.

Do sparse resultants behave similarly? In §2 of this chapter, we gave formulas for the Dixon resultant (see (2.12) and Exercise 10 of §2). Other determinantal formulas for sparse resultants can be found in [CK1], [DE], [Khe], [SZ], and [WZ], so that the first bullet definitely has sparse analogs. We will see below that the second and third bullets also have sparse analogs.

We now introduce our main tool for computing sparse resultants. The idea is to subdivide the Minkowski sum $Q = Q_0 + \cdots + Q_n$ in a special way. We begin with what it means to subdivide a polytope.

(6.4) Definition. Let $Q \subset \mathbb{R}^n$ be a polytope of dimension n. Then a *polyhedral subdivision* of Q consists of finitely many n-dimensional polytopes $R_1, \ldots, R_s$ (the *cells* of the subdivision) such that $Q = R_1 \cup \cdots \cup R_s$ and for $i \neq j$, the intersection $R_i \cap R_j$ is a face of both R_i and R_j.

For example, Fig. 7.7 below shows three ways of dividing a square into smaller pieces. The first two are polyedral subdivisions, but the third isn't since $R_1 \cap R_2$ is not a face of R_1 (and $R_1 \cap R_3$ has a similar problem).

We next define what it means for a polyhedral subdivision to be compatible with a Minkowski sum. Suppose that $Q_1, \ldots, Q_m$ are arbitrary polytopes in $\mathbb{R}^n$.

(6.5) Definition. Let $Q = Q_1 + \cdots + Q_m \subset \mathbb{R}^n$ be a Minkowski sum of polytopes, and assume that Q has dimension n. Then a subdivision

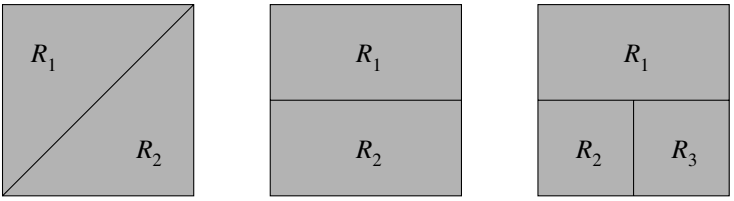

FIGURE 7.7. Subdividing the square

$R_1, \ldots, R_s$ of Q is a *mixed subdivision* if each cell R_i can be written as a Minkowski sum

$$R_i = F_1 + \cdots + F_m$$

where each F_i is a face of Q_i and $n = \dim(F_1) + \cdots + \dim(F_m)$. Furthermore, if $R_j = F_1' + \cdots + F_m'$ is another cell in the subdivision, then $R_i \cap R_j = (F_1 \cap F_1') + \cdots + (F_m \cap F_m')$.

Exercise 1. Consider the polytopes

$$P_1 = \text{Conv}((0,0),(1,0),(3,2),(0,2))$$
$$P_2 = \text{Conv}((0,1),(3,0),(1,4)).$$

The Minkowski sum $P = P_1 + P_2$ was illustrated in Fig. 7.6 of §4.
a. Prove that Fig. 7.8 on the next page gives a mixed subdivision of P.
b. Find a different mixed subdivision of P.

When we have a mixed subdivision, some of the cells making up the subdivision are especially important.

(6.6) Definition. Suppose that $R = F_1 + \cdots + F_m$ is a cell in a mixed subdivision of $Q = Q_1 + \cdots + Q_m$. Then R is called a *mixed cell* if $\dim(F_i) \leq 1$ for all i.

Exercise 2. Show that the mixed subdivision illustrated in Fig. 7.8 has three mixed cells.

As an application of mixed subdivisions, we will give a surprisingly easy formula for mixed volume. Given n polytopes $Q_1, \ldots, Q_n \subset \mathbb{R}^n$, we want to compute the mixed volume $MV_n(Q_1, \ldots, Q_n)$. We begin with a mixed subdivision of $Q = Q_1 + \cdots + Q_n$. In this situation, observe that every mixed cell R is a sum of edges (because the faces $F_i \subset Q_i$ summing to R

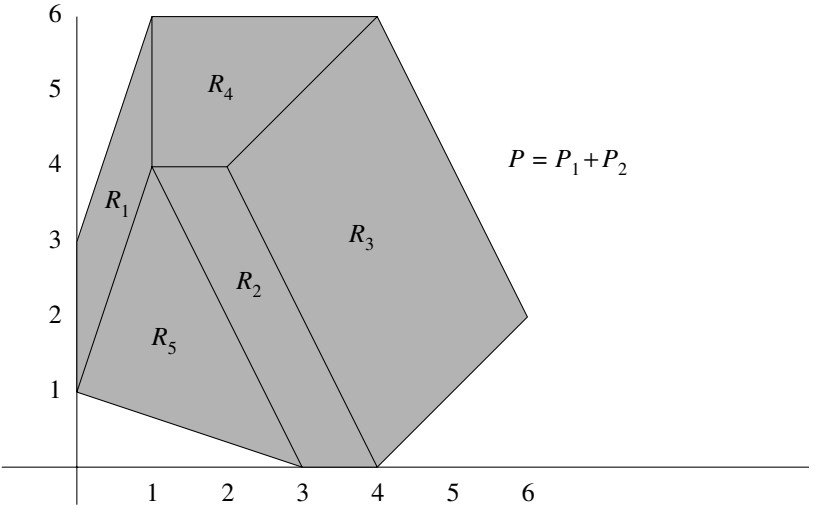

FIGURE 7.8. Mixed subdivision of a Minkowski sum

satisfy $n = \dim(F_1) + \cdots + \dim(F_n)$ and $\dim(F_i) \leq 1$). Then the mixed cells determine the mixed volume in the following simple manner.

(6.7) Theorem. *Given polytopes $Q_1, \ldots, Q_n \subset \mathbb{R}^n$ and a mixed subdivision of $Q = Q_1 + \cdots + Q_n$, the mixed volume $MV_n(Q_1, \ldots, Q_n)$ is computed by the formula*

$$MV_n(Q_1, \ldots, Q_n) = \sum_R \mathrm{Vol}_n(R),$$

where the sum is over all mixed cells R of the mixed subdivision.

PROOF. We will give the main idea of the proof and refer to [HuS1] for the details. The key observation is that mixed subdivisions behave well under scaling. More precisely, let $R_1, \ldots, R_s$ be a mixed subdivision of $Q_1 + \cdots + Q_n$, where each R_i is a Minkowski sum of faces $R_i = F_1 + \cdots + F_n$ as in Definition (6.5). If $\lambda_i > 0$ for $i = 1, \ldots, n$, then one can show that $\lambda_1 Q_1 + \cdots + \lambda_n Q_n$ has a mixed subdivision $R'_1, \ldots, R'_s$ such that

$$R'_i = \lambda_1 F_1 + \cdots + \lambda_n F_n.$$

It follows that

$$\mathrm{Vol}_n(R'_i) = \lambda_1^{\dim(F_1)} \cdots \lambda_n^{\dim(F_n)} \mathrm{Vol}_n(R_i)$$

since $n = \dim(F_1) + \cdots + \dim(F_n)$. Adding these up, we see that $\mathrm{Vol}_n(\lambda_1 Q_1 + \cdots + \lambda_n Q_n)$ is a polynomial in the λ_i and the coefficient

of $\lambda_1 \cdots \lambda_n$ is the sum of the volumes of the cells R_i where each F_i has dimension 1, that is, the mixed cells. By the definition of mixed volume, $MV_n(Q_1, \ldots, Q_n)$ is the sum of the volumes of the mixed cells. □

Although Theorem (6.7) was known in the polytope community for some time, it was first written up in [Bet] and discovered independently in [HuS1]. The latter includes formulas for computing the mixed volumes $MV_n(P, \alpha)$ from Exercise 18 of §4 in terms of certain nonmixed cells in the mixed subdivision.

One feature which makes Theorem (6.7) useful is that the volume of a mixed cell R is easy to compute. Namely, if we write $R = F_1 + \cdots + F_n$ as a sum of edges F_i and let $\vec{v}_i$ be the vector connecting the two vertices of F_i, then one can show that the volume of the cell is

$$\mathrm{Vol}_n(R) = |\det(A)|,$$

where A is the $n \times n$ matrix whose columns are the edge vectors $\vec{v}_1, \ldots, \vec{v}_n$.

Exercise 3. Use Theorem (6.7) and the above observation to compute the mixed volume $MV_2(P_1, P_2)$, where P_1 and P_2 are as in Exercise 1.

Theorem (6.7) has some nice consequences. First, it shows that the mixed volume is nonnegative, which is not obvious from the definition given in §4. Second, since all mixed cells lie inside the Minkowski sum, we can relate mixed volume to the volume of the Minkowski sum as follows:

$$MV_n(Q_1, \ldots, Q_n) \leq \mathrm{Vol}_n(Q_1 + \cdots + Q_n).$$

By [Emi1], we have a lower bound for mixed volume as well:

$$MV_n(Q_1, \ldots, Q_n) \geq n! \sqrt[n]{\mathrm{Vol}_n(Q_1) \cdots \mathrm{Vol}_n(Q_n)}.$$

Mixed volume also satisfies the *Alexandrov-Fenchel inequality*, which is discussed in [Ewa] and [Ful].

Exercise 4. Work out the inequalities displayed above for the polytopes P_1 and P_2 from Exercise 1.

All of this is very nice, except for one small detail: how do we find mixed subdivisions? Fortunately, they are fairly easy to compute in practice. We will describe briefly how this is done. The first step is to "lift" the polytopes $Q_1, \ldots, Q_n \subset \mathbb{R}^n$ to $\mathbb{R}^{n+1}$ by picking random vectors $l_1, \ldots, l_n \in \mathbb{Z}^n$ and considering the polytopes

$$\widehat{Q}_i = \{(v, l_i \cdot v) : v \in Q_i\} \subset \mathbb{R}^n \times \mathbb{R} = \mathbb{R}^{n+1}.$$

If we regard l_i as the linear map $\mathbb{R}^n \to \mathbb{R}$ defined by $v \mapsto l_i \cdot v$, then $\widehat{Q}_i$ is the portion of the graph of l_i lying over Q_i.

Now consider the polytope $\widehat{Q} = \widehat{Q}_1 + \cdots + \widehat{Q}_n \subset \mathbb{R}^{n+1}$. We say that a facet $\mathcal{F}$ of $\widehat{Q}$ is a *lower facet* if its outward-pointing normal has a *negative* t_{n+1}-coordinate, where t_{n+1} is the last coordinate of $\mathbb{R}^{n+1} = \mathbb{R}^n \times \mathbb{R}$. If the l_i are sufficiently generic, one can show that the projection $\mathbb{R}^{n+1} \to \mathbb{R}^n$ onto the first n coordinates carries the lower facets $\mathcal{F} \subset \widehat{Q}$ onto n-dimensional polytopes $R \subset Q = Q_1 + \cdots + Q_n$, and these polytopes form the cells of a mixed subdivision of Q. The theoretical background for this construction is given in [BS] and some nice pictures appear in [CE2] (see also [HuS1], [CE1] and [EC]). Mixed subdivisions arising in this way are said to be *coherent*.

Exercise 5. Let $Q_1 = \mathrm{Conv}((0,0),(1,0),(0,1))$ be the unit simplex in the plane, and consider the vectors $l_1 = (0,4)$ and $l_2 = (2,1)$. This exercise will apply the above strategy to create a coherent mixed subdivision of $Q = Q_1 + Q_2$, where $Q_2 = Q_1$.

a. Write $\widehat{Q}_1$ and $\widehat{Q}_2$ as convex hulls of sets of three points, and then express $\widehat{Q} = \widehat{Q}_1 + \widehat{Q}_2$ as the convex hull of 9 points in $\mathbb{R}^3$.
b. In $\mathbb{R}^3$, plot the points of $\widehat{Q}$ found in part a. Note that such each point lies over a point of Q.
c. Find the lower facets of $\widehat{Q}$ (there are 3 of them) and use this to determine the corresponding coherent mixed subdivision of Q. Hint: When one point lies above another, the higher point can't lie in a lower facet.
d. Show that choosing $l_1 = (1,1)$ and $l_2 = (2,3)$ leads to a different coherent mixed subdivision of Q.

It is known that computing mixed volume is #P-complete (see [Ped]). Being #P-complete is similar to being NP-complete—the difference is that NP-complete refers to a class of hard *decision* problems, while #P-complete refers to certain hard *enumerative problems*. The complexity of computing mixed volume is discussed carefully in [DGH], with some recent developments appearing in [GuS].

There are several known algorithms for computing mixed volumes and mixed subdivisions, some of which have been implemented in publicly available software. In particular, software for computing mixed volumes is available at:

- `http://www-sop.inria.fr/galaad/logiciels/emiris/soft_geo.html`, based on [EC] and described in [Emi3];
- `http://www2.math.uic.edu/~jan/PHCpack/phcpack.html`, described in [Ver1]; and
- `http://www.mth.msu.edu/~li/`, based on [GL2] and [LL].

Further references for mixed volume are [GL1], [GLW], [VGC], and the references mentioned in Section 6 of [EC].

We now return to our original question of computing the mixed sparse resultant $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}(f_0,\ldots,f_n)$. In this situation, we have $n+1$ polytopes $Q_i = \mathrm{Conv}(\mathcal{A}_i)$. Our goal is to show that a coherent mixed subdivision of

the Minkowski sum $Q = Q_0 + \cdots + Q_n$ gives a systematic way to compute the sparse resultant.

To see how this works, first recall what we did in Chapter 3. If we think of the multipolynomial resultant $\mathrm{Res}_{d_0,\dots,d_n}(F_0,\dots,F_n)$ in homogeneous terms, then the method presented in §4 of Chapter 3 goes as follows: we fixed the set of monomials of total degree $d_0 + \cdots + d_n - n$ and wrote this set as a disjoint union $S_0 \cup \cdots \cup S_n$. Then, for each monomial $x^\alpha \in S_i$, we multiplied F_i by $x^\alpha / x_i^{d_i}$. This led to the equations (4.1) of Chapter 3:

$$(x^\alpha / x_i^{d_i}) F_i = 0, \quad x^\alpha \in S_i, \quad i = 1, \dots, n.$$

Expressing these polynomials in terms of the monomials in our set gave a system of equations, and the determinant of the coefficient matrix was the polynomial D_n in Definition (4.2) of Chapter 3.

By varying this construction slightly, we got determinants $D_0, \dots, D_n$ with the following two properties:

- Each D_i is a nonzero multiple of the resultant.
- For i fixed, the degree of D_i as a polynomial in the coefficients of f_i is the same as the degree of the resultant in these coefficients.

(See §4 of Chapter 3, especially Exercise 7 and Proposition (4.6)). From here, we easily proved

$$\mathrm{Res}_{d_0,\dots,d_n} = \pm \mathrm{GCD}(D_0, \dots, D_n),$$

which is Proposition (4.7) of Chapter 3.

We will show that this entire framework goes through with little change in the sparse case. Suppose we have exponent sets $\mathcal{A}_0, \dots, \mathcal{A}_n$, and as above set $Q_i = \mathrm{Conv}(\mathcal{A}_i)$. Also assume that we have a coherent mixed subdivision of $Q = Q_0 + \cdots + Q_n$. The first step in computing the sparse resultant is to fix a set of monomials or, equivalently, a set of exponents. We will call this set $\mathcal{E}$, and we define $\mathcal{E}$ to be

$$\mathcal{E} = \mathbb{Z}^n \cap (Q + \delta),$$

where $\delta \in \mathbb{R}^n$ is a small vector chosen so that for every $\alpha \in \mathcal{E}$, there is a cell R of the mixed subdivision such that α lies in the *interior* of $R + \delta$. Intuitively, we displace the subdivision slightly so that the lattice points lie in the interiors of the cells.

The following exercise illustrates what this looks like in a particularly simple case. We will refer to this exercise several times as we explain how to compute $\mathrm{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}$.

Exercise 6. Consider the equations

$$\begin{aligned} 0 = f_0 &= a_1 x + a_2 y + a_3 \\ 0 = f_1 &= b_1 x + b_2 y + b_3 \\ 0 = f_2 &= c_1 x^2 + c_2 y^2 + c_3 + c_4 xy + c_5 x + c_6 y \end{aligned}$$

obtained by setting $z = 1$ in equations (2.9) from Chapter 3. If $\mathcal{A}_i$ is the set of exponents appearing in f_i, then $\mathrm{Res}_{\mathcal{A}_0,\mathcal{A}_1,\mathcal{A}_2}$ is the resultant $\mathrm{Res}_{1,1,2}$ considered in Proposition (2.10) of Chapter 3.

a. If we let $l_0 = (0,4)$, $l_1 = (2,1)$ and $l_2 = (5,7)$, then show that we get the coherent mixed subdivision of Q pictured in Fig. 7.9. This calculation is not easy to do by hand—you should use a program such as `qhull` (available from the Geometry Center at the University of Minnesota) to compute convex hulls.

b. If $\delta = (\epsilon, \epsilon)$ for small $\epsilon > 0$, show that $\mathcal{E}$ contains the six exponent vectors indicated by dots in Fig. 7.9. We will think of $\mathcal{E}$ as consisting of the monomials

$$x^3y,\ x^2y^2,\ x^2y,\ xy^3,\ xy^2,\ xy.$$

The reason for listing the monomials this way will soon become clear.

c. If $\delta = (-\epsilon, -\epsilon)$ for small $\epsilon > 0$, show that $\mathcal{E}$ consists of 10 exponent vectors. So different δ's can give very different $\mathcal{E}$'s!

Now that we have $\mathcal{E}$, our next task is to break it up into a disjoint union $S_0 \cup \cdots \cup S_n$. This is where the coherent mixed subdivision comes in. Each cell R of the subdivision is a Minkowski sum

$$R = F_0 + \cdots + F_n,$$

where the $F_i \subset Q_i$ are faces such that $n = \dim(F_0) + \cdots + \dim(F_n)$. Note that at least one F_i must have $\dim(F_i) = 0$, i.e., at least one F_i is a vertex. Sometimes R can be written in the above form in several ways (we will see an example below), but using the *coherence* of our mixed subdivision, we get a canonical way of doing this. Namely, R is the projection of a

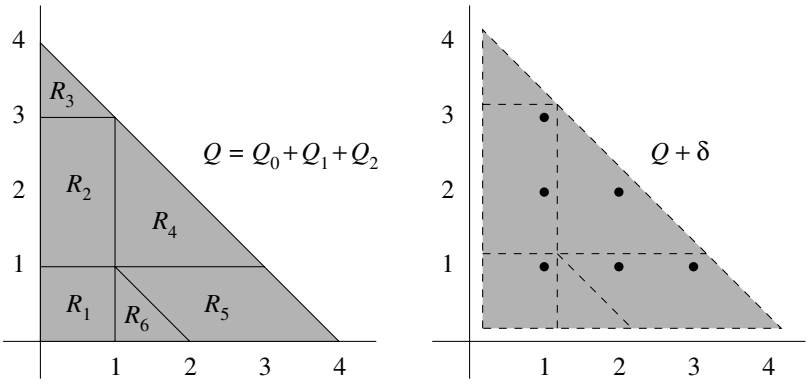

FIGURE 7.9. A coherent mixed subdivision and its shift

lower facet $\mathcal{F} \subset \widehat{Q}$, and one can show that $\mathcal{F}$ can be *uniquely* written as a Minkowski sum

$$\mathcal{F} = \widehat{F}_0 + \cdots + \widehat{F}_n,$$

where $\widehat{F}_i$ is a face of $\widehat{Q}_i$. If $F_i \subset Q_i$ is the projection of $\widehat{F}_i$, then the induced Minkowski sum $R = F_0 + \cdots + F_n$ is called *coherent*. Now, for each i between 0 and n, we define the subset $S_i \subset \mathcal{E}$ as follows:

$$\begin{aligned} S_i = \{\alpha \in \mathcal{E} : &\text{ if } \alpha \in R + \delta \text{ and } R = F_0 + \cdots + F_n \text{ is coherent,} \\ &\text{then } i \text{ is the } \textit{smallest} \text{ index such that } F_i \text{ is a vertex}\}. \end{aligned} \tag{6.8}$$

This gives a disjoint union $\mathcal{E} = S_0 \cup \cdots \cup S_n$. Furthermore, if $\alpha \in S_i$, we let $v(\alpha)$ denote the vertex F_i in (6.8), i.e., $F_i = \{v(\alpha)\}$. Since $Q_i = \mathrm{Conv}(\mathcal{A}_i)$, it follows that $v(\alpha) \in \mathcal{A}_i$.

Exercise 7. For the coherent subdivision of Exercise 6, show that

$$S_0 = \{x^3y, x^2y^2, x^2y\}, \quad S_1 = \{xy^3, xy^2\}, \quad S_2 = \{xy\},$$

and that

$$x^{v(\alpha)} = \begin{cases} x & \text{for } x^\alpha \in S_0 \\ y & \text{for } x^\alpha \in S_1 \\ 1 & \text{for } x^\alpha \in S_2. \end{cases}$$

(Here, we regard $\mathcal{E}$ and the S_i as consisting of monomials rather than exponent vectors.) Hint: The exponent vector $\alpha = (1, 3)$ of xy^3 lies in $R_2 + \delta$, where we are using the labelling of Fig. 7.9. If $\mathcal{F}$ is the lower facet lying over R_2, one computes (using a program such as `qhull`) that

$$\mathcal{F} = \text{edge of } \widehat{Q}_0 + (0, 1, 1) + \text{edge of } \widehat{Q}_2$$

which implies that $R_2 = \text{edge of } Q_0 + (0, 1) + \text{edge of } Q_2$ is coherent. Thus $xy^3 \in S_1$ and $x^{v(\alpha)} = y$, and the other monomials are handled similarly.

The following lemma will allow us to create the determinants used in computing the sparse resultant.

(6.9) Lemma. *If $\alpha \in S_i$, then $(x^\alpha / x^{v(\alpha)}) f_i \in L(\mathcal{E})$.*

Proof. If $\alpha \in R + \delta = F_0 + \cdots + F_n + \delta$, then $\alpha = \beta_0 + \cdots + \beta_n + \delta$, where $\beta_j \in F_j \subset Q_j$ for $0 \le j \le n$. Since $\alpha \in S_i$, we know that F_i is the vertex $v(\alpha)$, which implies $\beta_i = v(\alpha)$. Thus

$$\alpha = \beta_0 + \cdots + \beta_{i-1} + v(\alpha) + \beta_{i+1} + \cdots + \beta_n + \delta.$$

It follows that if $\beta \in \mathcal{A}_i$, then the exponent vector of $(x^\alpha / x^{v(\alpha)}) x^\beta$ is

$$\alpha - v(\alpha) + \beta = \beta_0 + \cdots + \beta_{i-1} + \beta + \beta_{i+1} + \cdots + \beta_n + \delta \subset Q + \delta.$$

This vector is integral and hence lies in $\mathcal{E} = \mathbb{Z}^n \cap (Q + \delta)$. Since f_i is a linear combination of the x^β for $\beta \in \mathcal{A}_i$, the lemma follows. □

Now consider the equations

$$(x^\alpha/x^{v(\alpha)})f_i = 0, \quad \alpha \in S_i. \tag{6.10}$$

We get one equation for each α, which means that we have $|\mathcal{E}|$ equations, where $|\mathcal{E}|$ denotes the number of elements in $\mathcal{E}$. By Lemma (6.9), each $(x^\alpha/x^{v(\alpha)})f_i$ can be written as a linear combination of the monomials x^β for $\beta \in \mathcal{E}$. If we regard these monomials as "unknowns", then (6.10) is a system of $|\mathcal{E}|$ equations in $|\mathcal{E}|$ unknowns.

(6.11) Definition. D_n is the determinant of the coefficient matrix of the $|\mathcal{E}| \times |\mathcal{E}|$ system of linear equations given by (6.10).

Notice the similarity with Definition (4.2) of Chapter 3. Here is a specific example of what this determinant looks like.

Exercise 8. Consider the polynomials f_0, f_1, f_2 from Exercise 6 and the decomposition $\mathcal{E} = S_0 \cup S_1 \cup S_2$ from Exercise 7.

a. Show that the equations (6.10) are *precisely* the equations obtained from (2.11) in Chapter 3 by setting $z = 1$ and multiplying each equation by xy. This explains why we wrote the elements of $\mathcal{E}$ in the order $x^3y, x^2y^2, x^2y, xy^3, xy^2, xy$.

b. Use Proposition (2.10) of Chapter 3 to conclude that the determinant D_2 satisfies

$$D_2 = \pm a_1 \mathrm{Res}_{1,1,2}(f_0, f_1, f_2).$$

This exercise suggests a close relation between D_n and $\mathrm{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}$. In general, we have the following result.

(6.12) Theorem. *The determinant D_n is a nonzero multiple of the mixed sparse resultant $\mathrm{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}$. Furthermore, the degree of D_n as a polynomial in the coefficients of f_n is the mixed volume $MV_n(Q_0, \dots, Q_{n-1})$.*

PROOF. If the equations $f_0 = \cdots = f_n = 0$ have a solution in $(\mathbb{C}^*)^n$, then the equations (6.10) have a nontrivial solution, and hence the coefficient matrix has zero determinant. It follows that D_n vanishes on the set $Z(\mathcal{A}_0, \dots, \mathcal{A}_n)$ from Theorem (6.2). Since the resultant is the irreducible defining equation of this set, it must divide D_n. (This argument is similar to one used frequently in Chapter 3.)

To show that D_n is nonzero, we must find $f_0, \dots, f_n$ for which $D_n \neq 0$. For this purpose, introduce a new variable t and let

$$f_i = \sum_{\alpha \in \mathcal{A}_i} t^{l_i \cdot \alpha} x^\alpha, \tag{6.13}$$

where the $l_i \in \mathbb{Z}^n$ are the vectors used in the construction of the coherent mixed subdivision of $Q = Q_0 + \cdots + Q_n$. Section 4 of [CE1] shows that

$D_n \neq 0$ for this choice of the f_i. We should also mention that without coherence, it can happen that D_n is identically zero. See Exercise 10 at the end of the section for an example.

Finally, we compute the degree of D_n as a polynomial in the coefficients of f_n. In (6.10), the coefficients of f_n appear in the equations coming from S_n, so that D_n has degree $|S_n|$ in these coefficients. So we need only prove

$$|S_n| = MV_n(Q_0, \dots, Q_{n-1}). \tag{6.14}$$

If $\alpha \in S_n$, the word *smallest* in (6.8) means that $\alpha \in R + \delta$, where $R = F_0 + \cdots + F_n$ and $\dim(F_i) > 0$ for $i = 0, \dots, n-1$. Since the dimensions of the F_i sum to n, we must have $\dim(F_0) = \cdots = \dim(F_{n-1}) = 1$. Thus R is a mixed cell with F_n as the unique vertex in the sum. Conversely, any mixed cell of the subdivision must have exactly one F_i which is a vertex (since the $\dim(F_i) \leq 1$ add up to n). Thus, if R is a mixed cell where F_n is a vertex, then $\mathbb{Z}^n \cap (R + \delta) \subset S_n$ follows from (6.8). This gives the formula

$$|S_n| = \sum_{F_n \text{ is a vertex}} |\mathbb{Z}^n \cap (R + \delta)|,$$

where the sum is over all mixed cells $R = F_0 + \cdots + F_n$ of the subdivision of Q for which F_n is a vertex.

We now use two nice facts. First, the mixed cells R where F_n is a vertex are translates of the mixed cells in a mixed subdivision of $Q_0 + \cdots + Q_{n-1}$. Furthermore, Lemma 5.3 of [Emi1] implies that *all* mixed cells in this subdivision of $Q_0 + \cdots + Q_{n-1}$ appear in this way. Since translation doesn't affect volume, Theorem (6.7) then implies

$$MV_n(Q_0, \dots, Q_{n-1}) = \sum_{F_n \text{ is a vertex}} \mathrm{Vol}_n(R),$$

where we sum over the same mixed cells as before. The second nice fact is that each of these cells R is a Minkowski sum of edges (up to translation by the vertex F_n), so that by Section 5 of [CE1], the volume of R is the number of lattice points in a generic small translation. This means

$$\mathrm{Vol}_n(R) = |\mathbb{Z}^n \cap (R + \delta)|,$$

and (6.14) now follows immediately. □

This shows that D_n has the desired properties. Furthermore, we get other determinants $D_0, \dots, D_{n-1}$ by changing how we choose the subsets $S_i \subset \mathcal{E}$. For instance, if we replace *smallest* by *largest* in (6.8), then we get a determinant D_0 whose degree in the coefficients of f_0 is $MV_n(Q_1, \dots, Q_n)$. More generally, for each j between 0 and n, we can find a determinant D_j which is a nonzero multiple of the resultant and whose degree in the coefficients of f_j is the mixed volume

$$MV_n(Q_1, \dots, Q_{j-1}, Q_{j+1}, \dots, Q_n)$$

(see Exercise 11 below). Using Theorem (6.3) of this section and the argument of Proposition (4.7) of Chapter 3, we conclude that

$$\mathrm{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0,\dots,f_n) = \pm\mathrm{GCD}(D_0,\dots,D_n).$$

As in Chapter 3, the GCD computation needs to be done for $f_0,\dots,f_n$ with symbolic coefficients.

Recently, D'Andrea showed that there is also a direct formula for the resultant which doesn't involve a GCD computation. Theorem (6.12) tells us that D_n is the product of the resultant times an extraneous factor. The main result of [D'An] states that the extraneous factor is the determinant D_n' of a recursively computable submatrix of the matrix used to compute D_n. This gives the formula

$$\mathrm{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n} = \frac{D_n}{D_n'},$$

which generalizes Macaulay's formula for the dense resultant (Theorem (4.9) of Chapter 3).

In practice, this method for computing the sparse resultant is not very useful, mainly because the D_j tend to be enormous polynomials when the f_i have symbolic coefficients. But if we use numerical coefficients for the f_i, the GCD computation doesn't make sense. Two methods for avoiding this difficulty are explained in Section 5 of [CE1]. Fortunately, for many purposes, it suffices to work with just one of the D_j (we will give an example below), and D_j can be computed by the methods discussed at the end of §4 of Chapter 3.

The matrices D_j are sometimes called *Sylvester matrices* since each entry is either 0 or a coefficient, just like Sylvester's formula for the resultant of two univariate polynomials (see (1.2) of Chapter 3). Methods for computing these matrices and their variants are described in [EC], [CE1], and [CE2], and software implementing the resulting algorithms for computing resultants is available from:

- `http://www.cs.unc.edu/~geom/MARS`, described in [WEM];
- `http://www-sop.inria.fr/galaad/logiciels/emiris/soft_alg.html`, described in [Emi3]; and
- `http://www-sop.inria.fr/galaad/logiciels/multires.html`, described in [Mou2].

In all of these methods, problems arise when the extraneous factor (i.e., the denominator in the resultant formula) vanishes. Methods for avoiding these problems are discussed in [CE2], [D'AE], [Mou1], [Roj2], and [Roj4].

Sparse resultants can be also formulated using *Bézout* or *Dixon* matrices. Here, the entries are more complicated combinations of the coefficients, though the resulting matrices may be smaller. A survey of such matrices appears in [EmM], which includes many references. The paper [BU] has more on Bézout matrices and the `multires` package mentioned above computes

Bézout matrices (this package also computes the matrix $\widetilde{M}$ of Theorem (6.21)—see [Mou2] for examples). The Dixon formulation has been studied extensively, starting with [KSY], [KS1], and [KS2] and more recently in [CK1] and [CK2]. Software packages related to the Dixon resultant formulation are available at:

- `http://www.cs.albany.edu/~artas/dixon/`, related to [CK1] and [CK2]; and
- `http://www.bway.net/~lewis/home.html`, based on the Fermat computer algebra system.

It is also possible to mix Sylvester and Bézout matrices. See [CDS] for some interesting resultant formulas of this type.

We will end this section with a brief discussion (omitting most proofs) of how sparse resultants can be used to solve equations. The basic idea is that given Laurent polynomials $f_i \in L(\mathcal{A}_i)$, we want to solve the equations

$$f_1(x_1, \dots, x_n) = \cdots = f_n(x_1, \dots, x_n) = 0. \tag{6.15}$$

If we assume that the f_i are generic, then by Bernstein's Theorem from §5, the number of solutions in $(\mathbb{C}^*)^n$ is the mixed volume $MV_n(Q_1, \dots, Q_n)$, where $Q_i = \operatorname{Conv}(\mathcal{A}_i)$.

To solve (6.15), we can use sparse resultants in a variety of ways, similar to what we did in the multipolynomial case studied in Chapter 3. We begin with a sparse version of the u-resultant from §5 of Chapter 3. Let

$$f_0 = u_0 + u_1 x_1 + \cdots + u_n x_n,$$

where $u_0, \dots, u_n$ are variables. The Newton polytope of f_0 is $Q_0 = \operatorname{Conv}(\mathcal{A}_0)$, where $\mathcal{A}_0 = \{0, \vec{e}_1, \dots, \vec{e}_n\}$ and $\vec{e}_1, \dots, \vec{e}_n$ are the usual standard basis vectors. Then the *u-resultant* of $f_1, \dots, f_n$ is the resultant $\operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0, \dots, f_n)$, which written out more fully is

$$\operatorname{Res}_{\mathcal{A}_0,\mathcal{A}_1,\dots,\mathcal{A}_n}(u_0 + u_1 x_1 + \cdots + u_n x_n, f_1, \dots, f_n).$$

For $f_1, \dots, f_n$ generic, one can show that there is a nonzero constant C such that

$$\operatorname{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0, \dots, f_n) = C \prod_{p \in \mathbf{V}(f_1,\dots,f_n) \cap (\mathbb{C}^*)^n} f_0(p). \tag{6.16}$$

This generalizes Theorem (5.8) of Chapter 3 and is proved using a sparse analog (due to Pedersen and Sturmfels [PS2]) of Theorem (3.4) from Chapter 3. If $p = (a_1, \dots, a_n)$ is a solution of (6.15) in $(\mathbb{C}^*)^n$, then

$$f_0(p) = u_0 + u_1 a_1 + \cdots + u_n a_n,$$

so that factoring the u-resultant gives the solutions of (6.15) in $(\mathbb{C}^*)^n$.

In (6.16), generic means that the solutions all have multiplicity 1. If some of the multiplicities are > 1, the methods of Chapter 4 can be adapted to show that

$$\mathrm{Res}_{\mathcal{A}_0,\dots,\mathcal{A}_n}(f_0,\dots,f_n) = C \prod_{p\in \mathbf{V}(f_1,\dots,f_n)\cap(\mathbb{C}^*)^n} f_0(p)^{m(p)},$$

where $m(p)$ is the multiplicity of p as defined in §2 of Chapter 4.

Many of the comments about the u-resultant from §5 of Chapter 3 carry over without change to the sparse case. In particular, we saw in Chapter 3 that for many purposes, we can replace the sparse resultant with the determinant D_0. This is true in the sparse case, provided we use D_0 as defined in this section. Thus, (6.16) holds using D_0 in place of the sparse resultant, i.e., there is a constant C' such that

$$D_0 = C' \prod_{p\in \mathbf{V}(f_1,\dots,f_n)\cap(\mathbb{C}^*)^n} f_0(p).$$

This formula is reasonable since D_0, when regarded as a polynomial in the coefficients $u_0,\dots,u_n$ of f_0, has degree $MV_n(Q_1,\dots,Q_n)$, which is the number of solutions of (6.15) in $(\mathbb{C}^*)^n$. There is a similar formula when some of the solutions have multiplicities > 1.

We can also find solutions of (6.15) using the eigenvalue and eigenvector techniques discussed in §6 of Chapter 3. To see how this works, we start with the ring $\mathbb{C}[x_1^{\pm1},\dots,x_n^{\pm1}]$ of all Laurent polynomials. The Laurent polynomials in our equations (6.15) give the ideal

$$\langle f_1,\dots,f_n\rangle \subset \mathbb{C}[x_1^{\pm1},\dots,x_n^{\pm1}].$$

We want to find a basis for the quotient ring $\mathbb{C}[x_1^{\pm1},\dots,x_n^{\pm1}]/\langle f_1,\dots,f_n\rangle$.

For this purpose, consider a coherent mixed subdivision of the Minkowski sum $Q_1+\cdots+Q_n$. If we combine Theorem (6.7) and the proof of Theorem (6.12), we see that if δ is generic, then

$$MV_n(Q_1,\dots,Q_n) = \sum_R |\mathbb{Z}^n \cap (R+\delta)|,$$

where the sum is over all mixed cells in the mixed subdivision. Thus the set of exponents

$$\widehat{\mathcal{E}} = \{\beta\in\mathbb{Z}^n : \beta\in R+\delta \text{ for some mixed cell } R\}$$

has $MV_n(Q_1,\dots,Q_n)$ elements. This set gives the desired basis of our quotient ring.

(6.17) Theorem. *For the set $\widehat{\mathcal{E}}$ described above, the cosets $[x^\beta]$ for $\beta\in\widehat{\mathcal{E}}$ form a basis of the quotient ring $\mathbb{C}[x_1^{\pm1},\dots,x_n^{\pm1}]/\langle f_1,\dots,f_n\rangle$.*

Proof. This was proved independently in [ER] and [PS1]. In the terminology of [PS1], the cosets $[x^\beta]$ for $\beta\in\widehat{\mathcal{E}}$ form a *mixed monomial basis* since they come from the mixed cells of a mixed subdivision.

We will prove this in the following special case. Consider $f_0 = u_0 + u_1x_1 + \cdots + u_nx_n$, and let $\mathcal{A}_0$ and Q_0 be as above. Then pick a coherent mixed subdivision of $Q = Q_0 + Q_1 + \cdots + Q_n$ and let $\mathcal{E} = \mathbb{Z}^n \cap (Q + \delta)$. Also define $S_i \subset \mathcal{E}$ using (6.8) with *smallest* replaced by *largest*. Using the first "nice fact" used in the proof of Theorem (6.12), one can show that the coherent mixed subdivision of Q induces a coherent mixed subdivision of $Q_1 + \cdots + Q_n$. We will show that the theorem holds for the set $\widehat{\mathcal{E}}$ coming from this subdivision.

The first step in the proof is to show that

$$\alpha \in S_0 \iff \alpha = v(\alpha) + \beta \text{ for some } v(\alpha) \in \mathcal{A}_0 \text{ and } \beta \in \widehat{\mathcal{E}}. \tag{6.18}$$

This follows from the arguments used in the proof of Theorem (6.12). Now let M_0 be the coefficient matrix of the equations (6.10). These equations begin with

$$(x^\alpha / x^{v(\alpha)}) f_0 = 0, \quad \alpha \in S_0,$$

which, using (6.18), can be rewritten as

$$x^\beta f_0 = 0, \quad \beta \in \widehat{\mathcal{E}}. \tag{6.19}$$

From here, we will follow the proof of Theorem (6.2) of Chapter 3. We partition M_0 so that the rows and columns of M_0 corresponding to elements of S_0 lie in the upper left hand corner, so that

$$M_0 = \begin{pmatrix} M_{00} & M_{01} \\ M_{10} & M_{11} \end{pmatrix}.$$

By Lemma 4.4 of [Emi1], M_{11} is invertible for generic $f_1, \ldots, f_n$ since we are working with a coherent mixed subdivision—the argument is similar to showing $D_0 \neq 0$ in the proof of Theorem (6.12).

Now let $\widehat{\mathcal{E}} = \{\beta_1, \ldots, \beta_\mu\}$, where $\mu = MV_n(Q_1, \ldots, Q_n)$. Then, for generic $f_1, \ldots, f_n$, we define the $\mu \times \mu$ matrix

$$\widetilde{M} = M_{00} - M_{01}M_{11}^{-1}M_{10}. \tag{6.20}$$

Also, for $p \in \mathbf{V}(f_1, \ldots, f_n) \cap (\mathbb{C}^*)^n$, let $\mathbf{p}^\beta$ denote the column vector

$$\mathbf{p}^\beta = \begin{pmatrix} p^{\beta_1} \\ \vdots \\ p^{\beta_\mu} \end{pmatrix}.$$

Similar to (6.6) in Chapter 3, one can prove

$$\widetilde{M}\,\mathbf{p}^\beta = f_0(p)\,\mathbf{p}^\beta$$

because (6.19) gives the rows of M_0 coming from S_0.

The final step is to show that the cosets $[x^{\beta_1}], \dots, [x^{\beta_\mu}]$ are linearly independent. The argument is identical to what we did in Theorem (6.2) of Chapter 2. □

Using the mixed monomial basis, the next step is to find the matrix of the multiplication map $m_{f_0} : A \to A$, where

$$A = \mathbb{C}[x_1^{\pm 1}, \dots, x_n^{\pm 1}]/\langle f_1, \dots, f_n \rangle$$

and $m_{f_0}([g]) = [f_0 g]$ for $[g] \in A$. As in Chapter 3, this follows immediately from the previous result.

(6.21) Theorem. *Let $f_i \in L(\mathcal{A}_i)$ be generic Laurent polynomials, and let $f_0 = u_0 + u_1 x_1 + \cdots + u_n x_n$. Using the basis from Theorem (6.17), the matrix of the multiplication map $m_{f_0} : A \to A$ defined above is the* **transpose** *of the matrix*

$$\widetilde{M} = M_{00} - M_{01} M_{11}^{-1} M_{10}$$

from (6.20).

If we write $\widetilde{M}$ in the form

$$\widetilde{M} = u_0\, I + u_1\, \widetilde{M}_1 + \cdots + u_n\, \widetilde{M}_n,$$

where each $\widetilde{M}_i$ has constant entries, then Theorem (6.21) implies that for all i, $(\widetilde{M}_i)^T$ is the matrix of multiplication by x_i. Thus, as in Chapter 3, $\widetilde{M}$ *simultaneously* computes the matrices of the multiplication maps by *all* of the variables $x_1, \dots, x_n$.

Now that we have these multiplication maps, the methods mentioned in Chapters 2 and 3 apply with little change. More detailed discussions of how to solve equations using matrix methods and resultants, including examples, can be found in [Emi1], [Emi2], [Emi3], [EmM], [ER], [Man1], [Mou1], [Mou2], and [Roj4]. It is also possible to apply these methods to study varieties of positive dimension. Here, a typical goal would be to find a point in every irreducible component of the variety. Some references (which employ a variety of approaches) are [ElM3], [KM], [Roj2], and [SVW].

We should mention that other techniques introduced in Chapter 3 can be adapted to the sparse case. For example, the generalized characteristic polynomial (GCP) from §6 of Chapter 3 can be generalized to the *toric GCP* defined in [Roj4]. This is useful for dealing with the types of degeneracies discussed in Chapter 3.

Additional Exercises for §6

Exercise 9. Consider the following system of equations taken from [Stu3]:

$$0 = f_0 = ax + by$$
$$0 = f_1 = cx + dy$$
$$0 = f_2 = ex + fy + g.$$

a. Explain why the hypothesis of Theorem (6.2) is not satisfied. Hint: Look at the Newton polytopes.
b. Show that the sparse resultant exists and is given by $\mathrm{Res}(f_0, f_1, f_2) = ad - bc$.

Exercise 10. In Exercise 7, we defined the decomposition $\mathcal{E} = S_0 \cup S_1 \cup S_2$ using coherent Minkowski sums $R = F_0 + F_1 + F_2$. This exercise will explore what can go wrong if we don't use coherent sums.
a. Exercise 7 gave the coherent Minkowski sum $R_2 =$ edge of $Q_0 + (0,1) +$ edge of Q_2. Show that $R_2 = (0,1) +$ edge of $Q_1 +$ edge of Q_2 also holds.
b. If we use coherent Minkowski sums for R_i when $i \neq 2$ and the non-coherent one from part a when $i = 2$, show that (6.8) gives $S_0 = \{x^3y, x^2y^2, x^2y, xy^3, xy^2\}$, $S_1 = \emptyset$ and $S_2 = \{xy\}$.
c. If we compute the determinant D_2 using S_0, S_1, S_2 as in part b, show that D_2 does not involve the coefficients of f_1 and conclude that D_2 is identically zero in this case. Hint: You don't need explicit computations. Argue instead that D_2 is divisible by $\mathrm{Res}_{1,1,2}$.

Exercise 11. This exercise will discuss the determinant D_j for $j < n$. The index j will be fixed throughout the exercise. Given $\mathcal{E}$ as usual, define the subset $S_i \subset \mathcal{E}$ to consist of all $\alpha \in \mathcal{E}$ such that if $\alpha \in R + \delta$, where $R = F_0 + \cdots + F_n$ is coherent, then

$$i = \begin{cases} j & \text{if } \dim(F_k) > 0 \ \forall k \neq j \\ \min(k \neq j : F_k \text{ is a vertex}) & \text{otherwise.} \end{cases}$$

By adapting the proof of Theorem (6.12), explain why this gives a determinant D_j which is a nonzero multiple of the resultant and whose degree as a polynomial in the coefficients of f_j is the mixed volume $MV_n(Q_1, \ldots, Q_{j-1}, Q_{j+1}, \ldots, Q_n)$.

Exercise 12. Prove that as polynomials with integer coefficients, we have

$$\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}(f_0, \ldots, f_n) = \pm \mathrm{GCD}(D_0, \ldots, D_n).$$

Hint: Since D_j and $\mathrm{Res}_{\mathcal{A}_0,\ldots,\mathcal{A}_n}$ have the same degrees when regarded as polynomials in the coefficients of f_j, it is relatively easy to prove this over $\mathbb{Q}$. To prove that it is true over $\mathbb{Z}$, it suffices to show that the coefficients of each D_j are relatively prime. To prove this for $j = n$, consider the polynomials f_i defined in (6.13) and use the argument of Section 4 of [CE1] (or, for a more detailed account, Section 5 of [CE2]) to show that D_n has a leading coefficient 1 as a polynomial in t.

Exercise 13. Compute the mixed sparse resultant of the polynomials

$$f_0 = a_1 + a_2xy + a_3x^2y + a_4x$$
$$f_1 = b_1y + b_2x^2y^2 + b_3x^2y + b_4x$$
$$f_2 = c_1 + c_2y + c_3xy + c_4x.$$

Hint: To obtain a coherent mixed subdivision, let $l_0 = (L, L^2)$, $l_1 = -(L^2, 1)$ and $l_2 = (1, -L)$, where L is a sufficiently large positive integer. Also let $\delta = -(3/8, 1/8)$. The full details of this example, including the explicit matrix giving D_0, can be found in [CE1].

Exercise 14. In Definition (6.5), we require that a mixed subdivision of $Q_1 + \cdots + Q_m$ satisfy the compatibility condition

$$R_i \cap R_j = (F_1 \cap F_1') + \cdots + (F_m \cap F_m'),$$

where $R_i = F_1 + \cdots + F_m$ and $R_j = F_1' + \cdots + F_m'$ are two cells in the subdivision and F_i, F_i' are faces of Q_i. This condition is essential for the scaling used in the proof of Theorem (6.7). To see why, consider the unit square Q in the plane with vertices labeled v_1, v_2, v_3, v_4.

a. Show that $R_i = v_i + Q$, $1 \le i \le 4$, gives a polyhedral subdivision of $Q + Q$ which satisfies Definition (6.5) except for the compatibility condition. Also show that if Theorem (6.7) applied to this subdivision, then the mixed volume $MV_2(Q, Q)$ would be 0.
b. Show that the subdivision of part a does not scale. Hint: Consider $Q + \lambda Q$ and $R_i' = v_i + \lambda Q$.
c. Find a mixed subdivision of $Q + Q$ that satisfies all parts of Definition (6.5) and draw a picture of $Q + \lambda Q$ to illustrate how the subdivision scales.

This example is due to Lyle Ramshaw.