A

ALGEBRAIC GEOMETRY

INTRODUCTION

Algebraic geometry is the mathematical study of geometric objects by means of algebra. Its origins go back to the coordinate geometry introduced by Descartes. A classic example is the circle of radius 1 in the plane, which is the geometric object defined by the algebraic equation $x^2 + y^2 = 1$. This generalizes to the idea of a systems of polynomial equations in many variables. The solution sets of systems of equations are called *varieties* and are the geometric objects to be studied, whereas the equations and their consequences are the algebraic objects of interest.

In the twentieth century, algebraic geometry became much more abstract, with the emergence of *commutative algebra* (rings, ideals, and modules) and *homological algebra* (functors, sheaves, and cohomology) as the foundational language of the subject. This abstract trend culminated in Grothendieck's *scheme theory*, which includes not only varieties but also large parts of algebraic number theory. The result is a subject of great power and scope—Wiles' proof of Fermat's Last Theorem makes essential use of schemes and their properties. At the same time, this abstraction made it difficult for beginners to learn algebraic geometry. Classic introductions include Refs. 1 and 2, both of which require a considerable mathematical background.

As the abstract theory of algebraic geometry was being developed in the middle of the twentieth century, a parallel development was taking place concerning the algorithmic aspects of the subject. Buchberger's theory of *Gröbner bases* showed how to manipulate systems of equations systematically, so (for example) one can determine algorithmically whether two systems of equations have the same solutions over the complex numbers. Applications of Gröbner bases are described in Buchberger's classic paper [3] and now include areas such as computer graphics, computer vision, geometric modeling, geometric theorem proving, optimization, control theory, communications, statistics, biology, robotics, coding theory, and cryptography.

Gröbner basis algorithms, combined with the emergence of powerful computers and the development of *computer algebra* (see **SYMBOLIC COMPUTATION**), have led to different approaches to algebraic geometry. There are now several accessible introductions to the subject, including Refs. 4–6.

In practice, most algebraic geometry is done over a field, and the most commonly used fields are as follows:

- The rational numbers $\mathbf{Q}$ used in symbolic computation.
- The real numbers $\mathbf{R}$ used in geometric applications.
- The complex numbers $\mathbf{C}$ used in many theoretical situations.
- The finite field $\mathbf{F}_q$ with $q = p^m$ elements (p prime) used in cryptography and coding theory.

In what follows, k will denote a field, which for concreteness can be taken to be one of the above. We now explore the two main flavors of algebraic geometry: *affine* and *projective*.

AFFINE ALGEBRAIC GEOMETRY

Given a field k, we have *n-dimensional affine space* k^n, which consists of all n-tuples of elements of k. In some books, k^n is denoted $\mathrm{A}^n(k)$. The corresponding algebraic object is the *polynomial ring* $k[\mathrm{x}_1, \ldots, x_n]$ consisting of all polynomials in variables $x_1, \ldots, x_n$ with coefficients in k. By *polynomial*, we mean a finite sum of terms, each of which is an element of k multiplied by a *monomial*

$$x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

where $a_1, \ldots, a_n$ are non-negative integers. Polynomials can be added and multiplied, and these operations are commutative, associative, and distibutive. This is why $k[x_1, \ldots, x_n]$ is called a *commutative ring*.

Given polynomials $f_1, \ldots, f_s$ in $k[x_1, \ldots, x_n]$, the *affine variety* $\mathbf{V}(f_1, \ldots, f_s)$ consists of all points $(u_1, \ldots, u_n)$ in k^n that satisfy the system of equations

$$f_1(u_1, \ldots, u_n) = \cdots = f_s(u_1, \ldots, u_n) = 0.$$

Some books (such as Ref. 1) call $\mathbf{V}(f_1, \ldots, f_s)$ an *affine algebraic set*.

The algebraic object corresponding to an affine variety is called an *ideal*. These arise naturally from a system of equations $f_1 = \cdots = f_s = 0$ as follows. Multiply the first equation by a polynomial h_1, the second by h_2, and so on. This gives the equation

$$h = h_1 f_1 + \cdots + h_s f_s = 0,$$

which is called a *polynomial consequence* of the original system. Note that $h(u_1, \ldots, u_n) = 0$ for every $(u_1, \ldots, u_n)$ in $\mathbf{V}(f_1, \ldots, f_s)$. The *ideal* $\langle f_1, \ldots, f_s \rangle$ consists of all polynomial consequences of the system $f_1 = \cdots = f_s = 0$. Thus, elements of $\langle f_1, \ldots, f_s \rangle$ are linear combinations of $f_1, \ldots, f_s$, where the coefficients are allowed to be arbitrary polynomials.

A general definition of ideal applies to any commutative ring. The *Hilbert Basis Theorem* states that all ideals in a polynomial ring are of the form $\langle f_1, \ldots, f_s \rangle$. We say that $f_1, \ldots, f_s$ is a *basis* of $\langle f_1, \ldots, f_s \rangle$ and that $\langle f_1, \ldots, f_s \rangle$ is *generated* by $f_1, \ldots, f_s$. This notion of "basis" differs from how the term is used in linear algebra because linear independence fails. For example, x, y is a basis of the ideal $\langle x, y \rangle$ in $k[x, y]$, even though $y \cdot x + [-x] \cdot y = 0$.

A key result is that if $\mathbf{V}(f_1, \ldots, f_s) = \mathbf{V}\{g_1, \ldots, g_t)$ whenever $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_t \rangle$. This is useful in practice because switching to a different basis may make it easier to understand the solutions of the equations. From the

theoretical point of view, this shows that an affine variety depends on the ideal I generated by the defining equations, so that the affine variety can be denoted $\mathbf{V}(I)$. Thus, every ideal gives an affine variety.

We can also reverse this process. Given an affine variety V, let $\mathbf{I}(V)$ consist of all polynomials that vanish on all points of V. This satisfies the abstract definition of ideal. Thus, every affine variety gives an ideal, and one can show that we always have

$$V = \mathbf{V}(\mathbf{I}(V)).$$

However, the reverse equality may fail. In other words, there are ideals I such that

$$I \neq \mathbf{I}(\mathbf{V}(I)).$$

An easy example is provided by $I = \langle x^2 \rangle$ in $k[x]$, because $\mathbf{I}(\mathbf{V}(I)) = \langle x \rangle \neq I$. Hence, the correspondence between ideals and affine varieties is not a perfect match. Over the complex numbers, we will see below that there is nevertheless a nice relation between I and $\mathbf{I}(\mathbf{V}(I))$.

One can prove that the *union* and *intersection* of affine varieties are again affine varieties. In fact, given ideals I and J, one has

$$\begin{aligned} V(I) \cup V(J) &= V(I \cap J) \\ V(I) \cap V(J) &= V(I + J), \end{aligned}$$

where

$$\begin{aligned} I \cap J &= \{g \mid g \text{ is in both } I \text{ and } J\} \\ I + J &= \{g + h \mid g \text{ is in } I \text{ and } h \text{ is in } J\} \end{aligned}$$

are the *intersection* and *sum* of I and J (note that $I \cap J$ and $I + J$ are analgous to the intersection and sum of subspaces of a vector space). In this way, algebraic operations on ideals correspond to geometric operations on varieties. This is part of the *ideal-variety correspondence* explained in Chapter 4 of Ref. 4.

Sometimes an affine variety can be written as a union of strictly smaller affine varieties. For example,

$$\mathbf{V}((x-y)(x^2+y^2-1)) = \mathbf{V}(x-y) \cup \mathbf{V}(x^2+y^2-1)$$

expresses the affine variety $\mathbf{V}((x-y)(x^2+y^2-1))$ as the union of the line $y = x$ and the unit circle (Fig. 1).

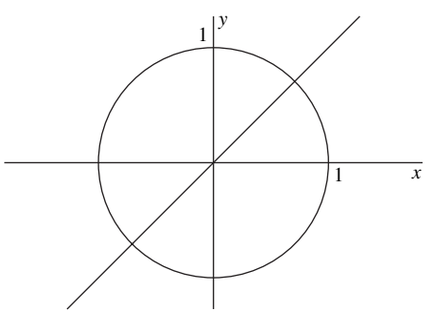

Figure 1.

In general, an affine variety is *irreducible* if it has no such decomposition. In books such as Ref. 1, varieties are always assumed to be irreducible.

One can show that every affine variety V can be written as

$$V = V_1 \cup \cdots \cup V_m$$

where each V_i is irreducible and no V_i is contained in V_j for $j \neq i$. We say that the V_i are the *irreducible components* of V. Thus, irreducible varieties are the "building blocks" out of which all varieties are built. Algebraically, the above decomposition means that the ideal of V can be written as

$$\mathbf{I}(V) = P_1 \cap \cdots \cap P_m$$

where each P_i is *prime* (meaning that if a product ab lies in P_i, then so does a or b) and no P_i contains P_j for $j \neq i$. This again illustrates the close connection between the algebra and geometry. (For arbitrary ideals, things are a bit more complicated: The above intersection of prime ideals has to be replaced with what is called a *primary decomposition*—see Chapter 4 of Ref. 4).

Every variety has a *dimension*. Over the real numbers $\mathbf{R}$, this corresponds to our geometric intuition. But over the complex numbers $\mathbf{C}$, one needs to be careful. The affine space $\mathbf{C}^2$ has dimension 2, even though it looks four-dimensional from the real point of view. The dimension of a variety is the maximum of the dimensions of its irreducible components, and irreducible affine varieties of dimensions 1, 2, and 3 are called curves, surfaces, and 3-folds, respectively. An affine variety in k^n is called a *hypersurface* if every irreducible component has dimension $n-1$.

PROJECTIVE ALGEBRAIC GEOMETRY

One problem with affine varieties is that intersections sometimes occur "at infinity." An example is given by the intersection of a hyperbola with one of its asymptotes in Fig. 2.

(Note that a line has a single point at infinity.) Points at infinity occur naturally in computer graphics, where the horizon in a perspective drawing is the "line at infinity" where parallel lines meet. Adding points at infinity to affine space leads to the concept of projective space.

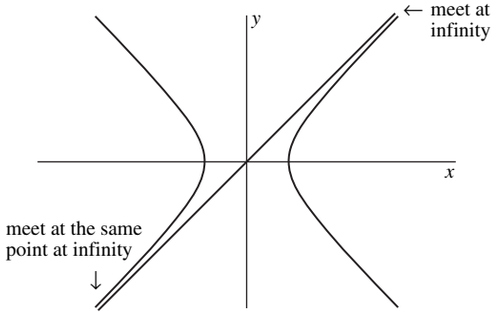

Figure 2.

The most common way to define *n-dimensional projective space* $\mathbf{P}^n(k)$ is via *homogeneous coordinates*. Every point in $\mathbf{P}^n(k)$ has homogeneous coordinates $[u_0, \ldots, u_n]$, where $(u_0, \ldots, u_n)$ is an element of k^{n+1} different from the zero element $(0, \ldots, 0)$. The square brackets in $[u_0, \ldots, u_n]$ indicate that homogeneous coordinates are *not* unique; rather,

$$[u_0, \ldots, u_n] = [v_0, \ldots, v_n]$$

if and only if there is a nonzero λ in k such that $\lambda u_i = v_i$ for $i = 0, \ldots, n$, i.e., $\lambda(u_0, \ldots, u_n) = (v_0, \ldots, v_n)$. This means that two nonzero points in k^{n+1} give the same point in $\mathbf{P}^n(k)$ if and only if they lie on the same line through the origin.

Consider those points in $P^n(k)$ where $u_0 \neq 0$. As $(1/u_0)$ $(u_0, u_1, \ldots, u_n) = (1, u_1/u_0, \ldots, u_n/u_n)$, one sees easily that

$$\mathbf{P}^n(k) = k^n \cup \mathbf{P}^{n-1}(k).$$

We call $\mathbf{P}^{n-1}(k)$ the *hyperplane at infinity* in this situation. One virtue of homogeneous coordinates is that they have a rich supply of coordinate changes. For example, an invertible 4×4 matrix with real entries gives an invertible transformation from $\mathbf{P}^3(\mathbf{R})$ to itself. The reason you see 4×4 matrices in computer graphics is that you are really working in three-dimensional projective space $\mathbf{P}^3(\mathbf{R})$, although this is rarely mentioned explicitly. See THREE-DIMENSIONAL GRAPHICS.

Now that we have $\mathbf{P}^n(k)$, we can define projective varieties as follows. A polynomial F in $k[x_0, \ldots, x_n]$ is *homogeneous of degree d* if every monomial $x_0^{a_0} \ldots x_n^{a_n}$ appearing in F has degree d, i.e., $a_0 + \cdots + a_n = d$. Such a polynomial has the property that

$$F(\lambda x_0, \ldots, \lambda x_n) = \lambda^d F(x_0, \ldots, x_n).$$

For a point $[u_0, \ldots, u_n]$ of $\mathbf{P}^n(k)$, the quantity $F(u_0, \ldots, u_n)$ is not well defined because of the ambiguity of homogeneous coordinates. But when F is homogeneous, the equation $F(u_0, \ldots, u_n) = 0$ is well defined. Then, given homogeneous polynomials $F_1, \ldots, F_s$, the *projective variety* $\mathbf{V}(F_1, \ldots, F_s)$ consists of all points $[u_0, \ldots, u_n]$ in $\mathbf{P}^n(k)$ that satisfy the system of equations

$$F_1(u_1, \ldots, u_n) = \cdots = F_s(u_1, \ldots, u_n) = 0.$$

Some books (such as Ref. 1) call $\mathbf{V}(F_1, \ldots, F_s)$ a *projective algebraic set*.

The algebraic object corresponding to $\mathbf{P}^n(k)$ is the polynomial ring $k[x_0, \ldots, x_n]$, which we now regard as a *graded ring*. This means that by grouping together terms of the same degree, every polynomial f of degree d can be uniquely written as

$$f = f_0 + f_1 + \cdots + f_d,$$

where f_i is homogeneous of degree i (note that f_i may be zero). We call the f_i the *homogeneous components* of f. An ideal I is *homogeneous* if it is generated by homogeneous polynomials. If I is homogeneous, then a polynomial lies in I if and only if its homogeneous components lie in I.

Most concepts introduced in the affine context carry over to the projective setting. Thus, we can ask whether a projective variety is irreducible and what is its dimension. We also have a projective version of the ideal-variety correspondence, where homogeneous ideals correspond to projective varieties. This is a bit more sophisticated than the affine case, in part because the ideal $\langle x_0, \ldots, x_n \rangle$ defines the empty variety because homogeneous coordinates are not allowed to all be zero.

Given a projective variety V in $\mathbf{P}^n(k)$, we get a homogeneous ideal $I = \mathbf{I}(V)$ in $k[x_0, \ldots, x_n]$. Let I_d consist of all homogeneous polynomials of degree d that lie in I. Then I_d is a finite-dimensional vector space over k, and by a theorem of Hilbert, there is a polynomial $P(x)$, called the *Hilbert polynomial*, such that for all sufficiently large integers d sufficiently large, we have

$$\binom{n+d}{n} - \dim_k I_d = P(d),$$

where the binomial coefficient $\binom{n+d}{n}$ is the dimension of the space of all homogeneous polynomials of degree n. Then one can prove that the dimension m of V equals the degree of $P(x)$. Furthermore, if we write the Hilbert polynomial $P(x)$ in the form

$$P(x) = \frac{D}{m!}x^m + \text{terms of lower degree},$$

then D is a positive integer called the *degree* of V. For example, when V is defined by $F = 0$ over the complex numbers, where F is irreducible and homogeneous of degree d, then V has degree d according to the above definition. This shows just how much information is packed into the ideal I. Later we will discuss the algorithmic methods for computing Hilbert polynomials.

THE COMPLEX NUMBERS

Although many applications of algebraic geometry work over the real numbers $\mathbf{R}$, the theory works best over the complex numbers $\mathbf{C}$. For instance, suppose that $V = \mathbf{V}(f_1, \ldots, f_s)$ is a variety in $\mathbf{R}^n$ of dimension d. Then we expect V to be defined by at least $n - d$ equations because (roughly speaking) each equation should lower the dimension by one. But if we set $f = f_1^2 + \cdots + f_s^2$, then $f = 0$ is equivalent to $f_1 = \cdots = f_s = 0$ because we are overworking $\mathbf{R}$. Thus, $V = \mathbf{V}(f_1, \ldots, f_s)$ can be defined by one equation, namely $f = 0$. In general, the relation between ideals and varieties is complicated when working over $\mathbf{R}$.

As an example of why things are nicer over $\mathbf{C}$, consider an ideal I in $\mathbf{C}[x_1, \ldots, x_n]$ and let $V = \mathbf{V}(I)$ be the corresponding affine variety in $\mathbf{C}^n$. The polynomials in I clearly vanish on V, but there may be others. For example, suppose that f is not in I but some power of f, say f^ℓ, is in I. Then f^ℓ and hence f vanish on V. The *Hilbert Nullstellensatz* states that these are the only polynomials that vanish on V, i.e.,

$$\begin{aligned}\mathbf{I}(V) &= \mathbf{I}(\mathbf{V}(I)) \\ &= \{ f \text{ in } \mathbf{C}[x_1, \ldots, x_n] \mid f^\ell \text{ is in } I \text{ for some integer } \ell \geq 0 \}.\end{aligned}$$

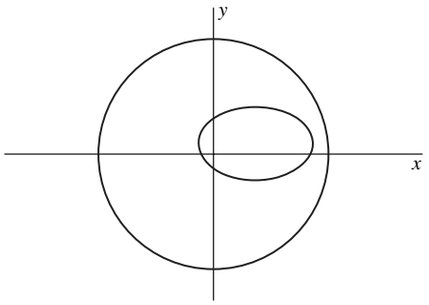

Figure 3.

The ideal on the right is called the *radical* of I and is denoted $\mathrm{rad}(I)$. Thus, the Nullstellensatz asserts that over $\mathbf{C}$, we have $\mathbf{I}(\mathbf{V}(I)) = \mathrm{rad}(I)$. It is easy to find examples where this fails over $\mathbf{R}$.

Another example of why $\mathbf{C}$ is nice comes from *Bézout's Theorem* in Fig. 3. In its simplest form, this asserts that distinct irreducible plane curves of degrees m and n intersect in mn points, counted with multiplicity. For example, consider the intersection of a circle and an ellipse. These are curves of degree 2, so we should have four points of intersection. But if the ellipse is really small, it can fit entirely inside the circle, which makes it seem that there are no points of intersection:

This is because we are working over $\mathbf{R}$; over $\mathbf{C}$, there really are four points of intersection.

Bézout's Theorem also illustrates the necessity of working over the projective plane. Consider, for example, the intersection of a hyperbola and one of its asymptotes in Fig. 4.

These are curves of degree 2 and 1, respectively, so there should be 2 points of intersection. Yet there are none in $\mathbf{R}^2$ or $\mathbf{C}^2$. But once we go to $\mathbf{P}^2(\mathbf{R})$ or $\mathbf{P}^2(\mathbf{C})$, we get one point of intersection at infinity, which has multiplicity 2 because the asymptote and the hyperbola are tangent at infinity. We will say more about multiplicity later in the article.

In both the Nullstellensatz and the Bézout's theorems, we can replace $\mathbf{C}$ with any *algebraically closed field*, meaning a field where every nonconstant polynomial has a root. A large part of algebraic geometry involves the study of irreducible projective varieties over algebraically closed fields.

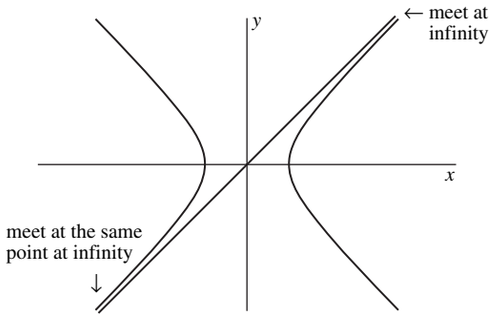

Figure 4.

FUNCTIONS ON AFFINE AND PROJECTIVE VARIETIES

In mathematics, one often studies objects by considering the functions defined on them. For an affine variety V in k^n, we let $k[V]$ denote the set of functions from V to k given by polynomials in $k[x_1, \ldots, x_n]$. One sees easily that $k[V]$ is a ring, called the *coordinate ring* of V.

An important observation is that two distinct polynomials f and g in $k[x_1, \ldots, x_n]$ can give the same function on V. This happens precisely when $f - g$ vanishes on V, i.e., when $f - g$ is in the ideal $\mathbf{I}(V)$. We express this by writing

$$f \equiv g \bmod \mathbf{I}(V),$$

similar to the congruence notation introduced by Gauss. It follows that computations in $k[x_1, \ldots, x_n]$ modulo $\mathbf{I}(V)$ are equivalent to computations in $k[V]$. In the language of abstract algebra, this is expressed by the ring isomorphism

$$k[x_1, \ldots, x_n]/\mathbf{I}(V) \simeq k[V],$$

where $k[x_1, \ldots, x_n]/\mathbf{I}(V)$ is the set of equivalence classes of the equivalence relation $f = g \bmod \mathbf{I}(V)$. More generally, given any ideal I in $k[x_1, \ldots, x_n]$, one gets the *quotient ring* $k[x_1, \ldots, x_n]/I$ coming from the equivalence relation $f = g \bmod I$. We will see later that Gröbner bases enable us to compute effectively in quotient rings.

We can use quotients to construct finite fields as follows. For a prime p, we get $\mathbf{F}_p$ by considering the integers modulo p. To get $\mathbf{F}_{p^m}$ when $m > 1$, take an irreducible polynomial f in $\mathbf{F}_p[x]$ of degree m. Then the quotient ring $\mathbf{F}_p[x]/\langle f \rangle$ is a model of F_{p^m}. Thus, for example, computations in $\mathrm{F}_2[x]$ modulo $x^2 + x + 1$ represent the finite field $\mathbf{F}_4$. See ALGEBRAIC CODING THEORY for more on finite fields.

The coordinate ring $\mathbf{C}[V]$ of an affine variety V in $\mathbf{C}^n$ has an especially strong connection to V. Given a point $(u_1, \ldots, u_n)$ of V, the functions in $\mathbf{C}[V]$ vanishing at $(u_1, \ldots, u_n)$ generate a *maximal ideal*, meaning an ideal of $\mathbf{C}[V]$ not equal to the whole ring but otherwise as big as possible with respect to inclusion. Using the Nullstellensatz, one can show that *all* maximal ideals of $\mathbf{C}[V]$ arise this way. In other words, there is a one-to-one correspondence

$$\text{points of } V \longleftrightarrow \text{maximal ideals of } \mathbf{C}[V].$$

Later we will use this correspondence to motivate the definition of *affine scheme*.

Functions on projective varieties have a different flavor, since a polynomial function defined everywhere on a connected projective variety must be constant. Instead, two approaches are used, which we will illustrate in the case of $\mathbf{P}^n(k)$. In the first approach, one considers *rational functions*, which are quotients

$$\frac{F(x_0, \ldots, x_n)}{G(x_0, \ldots, x_n)}$$

of homogeneous polynomials of the same degree, say d. This function is well defined despite the ambiguity of homogeneous coordinates, because

$$\frac{F(\lambda x_0,\ldots,\lambda x_n)}{G(\lambda x_0,\ldots,\lambda x_n)}=\frac{\lambda^d F(x_0,\ldots,x_n)}{\lambda^d G(x_0,\ldots,x_n)}=\frac{F(x_0,\ldots,x_n)}{G(x_0,\ldots,x_n)}.$$

However, this function is *not* defined when the denominator vanishes. In other words, the above quotient is only defined where $G\neq 0$. The set of all rational functions on $\mathbf{P}^n(k)$ forms a field called the *field of rational functions on* $\mathbf{P}^n(k)$. More generally, any irreducible projective variety V has a field of rational functions, denoted $k(V)$.

The second approach to studying functions on $\mathbf{P}^n(k)$ is to consider the polynomial functions defined on certain large subsets of $\mathbf{P}^n(k)$. Given projective variety V in $\mathbf{P}^n(k)$, its *complement* U consists of all points of $\mathbf{P}^n(k)$ not in V. We call U a *Zariski open subset* of $\mathbf{P}^n(k)$. Then let $\Gamma(U)$ be the ring of all rational functions on $\mathbf{P}^n(k)$ defined at all points of U. For example, the complement U_0 of $\mathbf{V}(x_0)$ consists of points where $x_0\neq 0$, which is a copy of $\mathbf{k}^n$. So here $\Gamma(U_0)$ is the polynomial ring $k[x_1/x_0,\ldots,x_n/x_0]$. When we consider the rings $\Gamma(U)$ for all Zariki open subsets U, we get a mathematical object called the *structure sheaf of* $\mathbf{P}^n(k)$. More generally, any projective variety V has a structure sheaf, denoted O_v. We will see below that sheaves play an important role in abstract algebraic geometry.

GRÖBNER BASES

Buchberger introduced Gröbner bases in 1965 in order to do algorithmic computations on ideals in polynomial rings. For example, suppose we are given polynomials f, $f_1,\ldots,f_s\in k[x_1,\ldots,x_n]$, where k is a field whose elements can be represented exactly on a computer (e.g., k is a finite field or the field of rational numbers). From the point of view of pure mathematics, either f lies in the ideal $\langle f_1,\ldots,f_s\rangle$ or it does not. But from a practical point of view, one wants an algorithm for deciding which of these two possibilities actually occurs. This is the *ideal membership question*.

In the special case of two univariate polynomials f, g in $k[x]$, f lies in $\langle g\rangle$ if and only if f is a multiple of g, which we can decide by the division algorithm from high-school algebra. Namely, dividing g into f gives $f=qg+r$, where the remainder r has degree strictly smaller than the degree of g. Then f is a multiple of g if and only if the remainder is zero. This solves the ideal membership question in our special case.

To adapt this strategy to $k[x_1,\ldots,x_n]$, we first need to order the monomials. In $k[x]$, this is obvious: The monomials are 1, x, x^2, etc. But there are many ways to do this when there are two or more variables. A *monomial order* $>$ is an order relation on monomials $U, V, W,\ldots$ in $k[x_1,\ldots,x_n]$ with the following properties:

1. Given monomials U and V, exactly one of $U>V$, $U=V$, or $U<V$ is true.
2. If $U>V$, then $UW>VW$ for all monomials W.
3. If $U\neq 1$, then $U>1$; i.e., 1 is the least monomial with respect to $>$.

These properties imply that $>$ is a *well ordering*, meaning that any strictly decreasing sequence with respect to $>$ is finite. This is used to prove termination of various algorithms. An example of a monomial order is *lexicographic order*, where

$$x_1^{a_1}x_2^{a_2}\ldots x_n^{a_n}>x_1^{b_1}x_2^{b_2}\ldots x_n^{b_n}$$

provided

$$a_1>b_1;\ \text{or}\ a_1=b_1\ \text{and}\ a_2>b_2;\ \text{or}\ a_1=b_1,\ a_2=b_2\ \text{and}\ a_3>b_3;\ \text{etc.}$$

Other important monomial orders are *graded lexicographic order* and *graded reverse lexicographic order*. These are described in Chapter 2 of Ref. 4.

Now fix a monomial order $>$. Given a nonzero polynomial f, we let $\mathrm{lt}(f)$ denote the *leading term* of f, namely the nonzero term of f whose monomial is maximal with respect to $>$ (in the literature, $\mathrm{lt}(f)$ is sometimes called the *initial term* of f, denoted $\mathrm{in}(f)$). Given $f_1,\ldots,f_s$, the *division algorithm* produces polynomials $q_1,\ldots,q_s$ and r such that

$$f=q_1f_1+\cdots+q_sf_s+r$$

where every nonzero term of r is divisible by none of $\mathrm{lt}(f_1),\ldots,\mathrm{lt}(f_s)$. The remainder r is sometimes called the *normal form* of f with respect to $f_1,\ldots,f_s$. When $s=1$ and f and f_1 are univariate, this reduces to the high-school division algorithm mentioned earlier.

In general, multivariate division behaves poorly. To correct this, Buchberger introduced a special kind of basis of an ideal. Given an ideal I and a monomial order, its *ideal of leading terms* $\mathrm{lt}(I)$ (or *initial ideal* $\mathrm{in}(I)$is the ideal generated by $\mathrm{lt}(f)$ for all f in I. Then elements $g_1,\ldots,g_t$ of I form a *Gröbner basis* of I provided that $\mathrm{lt}(g_1),\ldots,\mathrm{lt}(g_t)$ form a basis of $\mathrm{lt}(I)$. Buchberger showed that a Gröbner basis is in fact a basis of I and that, given generators $f_1,\ldots,f_s$ of I, there is an algorithm (the *Buchberger algorithm*) for producing the corresponding Gröbner basis. A description of this algorithm can be found in Chapter 2 of Ref. 4.

The complexity of the Bucherger algorithm has been studied extensively. Examples are known where the input polynomials have degree $\leq d$, yet the corresponding Gröbner basis contains polynomials of degree 2^{2^d}. Theoretical results show that this doubly exponential behavior is the worst that can occur (for precise references, see Chapter 2 of Ref. 4). However, there are many geometric situations where the complexity is less. For example, if the equations have only finitely many solutions over $\mathbf{C}$, then the complexity drops to a single exponential. Furthermore, obtaining geometric information about an ideal, such as the dimension of its associated variety, often has single exponential complexity. When using graded

reverse lexicographic order, complexity is related to the *regularity* of the ideal. This is discussed in Ref. 7. Below we will say more about the practical aspects of Gröbner basis computations.

Using the properties of Gröbner bases, one gets the following *ideal membership algorithm*: Given $f, f_1, \ldots, f_s$, use the Buchberger algorithm to compute a Gröbner basis $g_1, \ldots, g_t$ of $\langle f_1, \ldots, f_s \rangle$ and use the division algorithm to compute the remainder of f on division by $g_1, \ldots, g_t$. Then f is in the ideal $\langle f_1, \ldots, f_s \rangle$ if and only if the remainder is zero.

Another important use of Gröbner bases occurs in *elimination theory*. For example, in geometric modeling, one encounters surfaces in $\mathbf{R}^3$ parametrized by polynomials, say

$$x = f(s, t), \quad y = g(s, t), \quad z = h(s, t).$$

To obtain the equation of the surface, we need to eliminate s, t from the above equations. We do this by considering the ideal

$$\langle x - f(s, t), y - g(s, t), z - h(s, t) \rangle$$

in the polynomial ring $\mathbf{R}[s, f, x, y, z]$ and computing a Gröbner basis for this ideal using lexicographic order, where the variables to be eliminated are listed first. The *Elimination Theorem* (see Chapter 3 of Ref. 4) implies that the equation of the surface is the only polynomial in the Gröbner basis not involving s, t. In practice, elimination is often done by other methods (such as *resultants*) because of complexity issues. See also the entry on **SURFACE MODELING**.

Our final application concerns a system of equations $f_1 = \cdots = f_s = 0$ in n variables over $\mathbf{C}$. Let $I = \langle f_1, \ldots, f_s \rangle$, and compute a Gröbner basis of I with respect to any monomial order. The *Finiteness Theorem* asserts that the following are equivalent:

1. The equations have finitely many solutions in $\mathbf{C}^n$.
2. The Gröbner basis contains elements whose leading terms are pure powers of the variables (i.e., x_1 to a power, x_2 to a power, etc.) up to constants.
3. The quotient ring $\mathbf{C}[x_1, \ldots, x_n]/I$ is a finite-dimensional vector space over $\mathbf{C}$.

The equivalence of the first two items gives an algorithm for determining whether there are finitely many solutions over $\mathbf{C}$. From here, one can find the solutions by several methods, including *eigenvalue methods* and *homotopy continuation*. These and other methods are discussed in Ref. 8. The software PHCpack (9) is a freely available implementation of homotopy continuation. Using homotopy techniques, systems with 10^5 solutions have been solved. Without homotopy methods but using a robust implementation of the Buchberger algorithm, systems with 1000 solutions have been solved, and in the context of computational biology, some highly structured systems with over 1000 equations have been solved.

However, although solving systems is an important practical application of Gröbner basis methods, we want to emphasize that many theoretical objects in algebraic geometry, such as Hilbert polynomials, free resolutions (see below), and sheaf cohomology (also discussed below), can also be computed by these methods. As more and more of these theoretical objects are finding applications, the ability to compute them is becoming increasingly important.

Gröbner basis algorithms have been implemented in computer algebra systems such as Maple (10) and Mathematica (11). For example, the solve command in Maple and Solve command in Mathematica make use of Gröbner basis computations. We should also mention CoCoA (12), Macaulay 2 (13), and Singular (14), which are freely available on the Internet. These powerful programs are used by researchers in algebraic geometry and commutative algebra for a wide variety of experimental and theoretical computations. With the help of books such as Ref. 5 for Macaulay 2, Ref. 15 for CoCoA, and Ref. 16 for Singular, these programs can be used by beginners. The program Magma [17] is not free but has a powerful implementation of the Buchberger algorithm.

MODULES

Besides rings, ideals, and quotient rings, another important algebraic structure to consider is the concept of *module over a ring*. Let R denote the polynomial ring $k[x_0, \ldots, x_n]$. Then saying that M is an R-module means that M has addition and scalar multiplication with the usual properties, except that the "scalars" are now elements of R. For example, the *free R-module* R^m consists of m-tuples of elements of R. We can clearly add two such m-tuples and multiply an m-tuple by an element of R.

A more interesting example of an R-module is given by an ideal $I = \langle f_1, \ldots, f_s \rangle$ in R. If we choose the generating set $f_1, \ldots, f_s$ to be as small as possible, we get a minimal basis of I. But when $s \geq 2$, $f_1, \ldots, f_s$ cannot be linearly independent over R, because $f_j \cdot f_i + (-f_i) \cdot f_j = 0$ when $i \neq j$. To see how badly the f_i fail to be independent, consider

$$R^s \to I \to 0,$$

where the first arrow is given by a dot product with $(f_1, \ldots, f_s)$ and the second arrow is a standard way of saying the first arrow is onto, which is true because $I = \langle f_1, \ldots, f_s \rangle$. The kernel or nullspace of the first arrow measures the failure of the f_i to be independent. This kernel is an R-module and is called the *syzygy module* of $f_1, \ldots, f_s$, denoted $\mathrm{Syz}(f_1, \ldots, f_s)$.

The *Hilbert Basis Theorem* applies in this situation, so that there are finitely many syzygies $\mathbf{h}_1, \ldots, \mathbf{h}_\ell$ in $\mathrm{Syz}(f_1, \ldots, f_s)$ such that every syzygy is a linear combination, with coefficients in R, of $\mathbf{h}_1, \ldots, \mathbf{h}_\ell$. Each h_i is a vector of polynomials; if we assemble these into a matrix, then matrix multiplication gives a map

$$R^\ell \to R^s$$

whose image is $\mathrm{Syz}(f_1, \ldots, f_s)$. This looks like linear algebra, except that we are working over a ring instead of a field. If we think of the variables in $R = k[x_1, \ldots, x_n]$ as parameters, then we are doing *linear algebra with parameters*.

The generating syzgyies $\mathbf{h}_i$ may fail to be independent, so that the above map may have a nonzero kernel. Hence we can iterate this process, although the *Hilbert Syzygy Theorem* implies that kernel is eventually zero. The result is a collection of maps

$$0 \to R^t \to \cdots \to R^\ell \to R^s \to I \to 0,$$

where at each stage, the image of one map equals the kernel of the next. We say that this is a *free resolution* of I. By adapting Gröbner basis methods to modules, one obtains algorithms for computing free resolutions.

Furthermore, when I is a homogeneous ideal, the whole resolution inherits a graded structure that makes it straightforward to compute the Hilbert polynomial of I. Given what we know about Hilbert polynomials, this gives an algorithm for determining the dimension and degree of a projective variety. A discussion of modules and free resolutions can be found in Ref. 18.

Although syzygies may seem abstract, there are situations in geometric modeling where syzygies arise naturally as *moving curves* and *moving surfaces* (see Ref. 19). This and other applications show that algebra needs to be added to the list of topics that fall under the rubric of applied mathematics.

LOCAL PROPERTIES

In projective space $\mathbf{P}^n(k)$, let U_i denote the Zariski open subset where $x_i \neq 0$. Earlier we noted that U_0 looks theaffine space k^n; the same is true for the other U_i. This means that $\mathbf{P}^n(k)$ locally looks like affine space. Furthermore, if V is a projective variety in $\mathbf{P}^n(k)$, then one can show that $V_i = V \cap U_i$ is a affine variety for all i. Thus, every projective variety locally looks like an affine variety.

In algebraic geometry, one can get even more local. For example, let $\mathbf{p} = [u_0, \ldots, u_n]$ be a point of $\mathbf{P}^n(k)$. Then let O_p consist of all rational functions on $\mathbf{P}^n(k)$ defined at $\mathbf{p}$. Then O_p is clearly a ring, and the subset consisting of those functions that vanish at $\mathbf{p}$ is a maximal ideal. More surprising is the fact that this is the unique maximal ideal of O_p. We call O_p the *local ring* of $\mathbf{P}^n(k)$ at $\mathbf{p}$, and in general, a commutative ring with a unique maximal ideal is called a *local ring*. In a similar way, a point $\mathbf{p}$ of an affine or projective variety V has a local ring $O_{V,\mathbf{P}}$.

Many important properties of a variety at a point are reflected in its local ring. As an example, we give the definition of *multiplicity* that occurs in Bézout's Theorem. Recall the statement: Distinct irreducible curves in $\mathbf{P}^2(\mathbf{C})$ of degrees m and n intersect at mn points, counted with multiplicity. By picking suitable coordinates, we can assume that the points of intersection lie in $\mathbf{C}^2$ and that the curves are defined by equations $f = 0$ and $g = 0$ of degrees m and n, respectively. If $\mathbf{p}$ is a point of intersection, then its *multiplicity* is given by

$$\mathrm{mult}(\mathbf{p}) = \dim_{\mathbf{C}} O_\mathbf{p}/\langle f, g\rangle, \quad O_\mathbf{p} = \text{local ring of } \mathbf{P}^2(\mathbf{C}) \text{ at } \mathbf{p},$$

and the precise version of Bézout's Theorem states that

$$m\,n = \sum_{f(\mathbf{p})=g(\mathbf{p})=0} \mathrm{mult}(\mathbf{p}).$$

A related notion of multiplicity is the *Hilbert–Samuel multiplicity* of an ideal in O_p, which arises in geometric modeling when considering the influence of a basepoint on the degree of the defining equation of a parametrized surface.

SMOOTH AND SINGULAR POINTS

In multivariable calculus, the *gradient* $\nabla f = \frac{\partial f}{\partial x}\mathbf{i} + \frac{\partial f}{\partial y}\mathbf{j}$ is perpendicular to the level curve defined by $f(x, y) = 0$. When one analzyes this carefully, one is led to the following concepts for a point on the level curve:

- A *smooth point*, where ∇f is nonzero and can be used to define the tangent line to the level curve.
- A *singular point*, where ∇f is zero and the level curve has no tangent line at the point.

These concepts generalize to arbitrary varieties. For any variety, most points are smooth, whereas others—those in the *singular locus*—are singular. Singularities can be important. For example, when one uses a variety to describe the possible states of a robot arm, the singularities of the variety often correspond to positions where the motion of the arm is less predictable (see Chapter 6 of Ref. 4 and the entry on ROBOTICS).

A variety is *smooth* or *nonsingular* when every point is smooth. When a variety has singular points, one can use *blowing up* to obtain a new variety that is less singular. When working over an algebraically closed field of *characteristic* 0 (meaning fields that contain a copy of $\mathbf{Q}$), Hironaka proved in 1964 that one can always find a sequence of blowing up that results in a smooth variety. This is called *resolution of singularities*. Resolution of singularities over a field of *characteristic* p (fields that contain a copy of $\mathbf{F}_p$) is still an open question. Reference 20 gives a nice introduction to resolution of singularities. More recently, various groups of people have figured out how to do this algorithmically, and work has been done on implementing these algorithms, for example, the software desing described in Ref. 21. We also note that singularities can be detected numerically using condition numbers (see Ref. 22).

SHEAVES AND COHOMOLOGY

For an affine variety, modules over its coordinate ring play an important role. For a projective variety V, the corresponding objects are *sheaves of O_V-modules*, where O_V is the structure sheaf of V. Locally, V looks like an affine variety, and with a suitable hypothesis called *quasicoherence*, a sheaf of O_V-modules locally looks like a module over the coordinate ring of an affine piece of V.

From sheaves, one is led to the idea of *sheaf cohomology*, which (roughly speaking) measures how the local pieces of the sheaf fit together. Given a sheaf F on V, the sheaf cohomology groups are denoted $H^i(V,F)$. We will see below that the sheaf cohomology groups are used in the classification of projective varieties. For another application of sheaf cohomology, consider a finite collection V of points in $\mathbf{P}^n(k)$. From the sheaf point of view, V is defined by an *ideal sheaf* I_V. In interpolation theory, one wants to model arbitrary functions on V using polynomials of a fixed degree, say m. If m is too small, this may not be possible, but we always succeed if m is large enough. A precise description of which degrees m work is given by sheaf cohomology. The ideal sheaf I_V has a *twist* denoted $I_V(m)$. Then all functions on V come from polynomials of degree m if and only if $H^1(\mathbf{P}^n(k), I_V(m)) = \{0\}$. We also note that vanishing theorems for sheaf cohomology have been used in geometric modeling (see Ref. 23).

References 1, 2, and 24 discuss sheaves and sheaf cohomology. Sheaf cohomology is part of *homological algebra*. An introduction to homological algebra, including sheaves and cohomology, is given in Ref. 5.

SPECIAL VARIETIES

We next discuss some special types of varieties that have been studied extensively.

1. *Elliptic Curves and Abelian Varieties*. Beginning with the middle of the eighteenth century, *elliptic integrals* have attracted a lot of attention. The study of these integrals led to both *elliptic functions* and *elliptic curves*. The latter are often described by an equation of the form

$$y^2 = ax^3 + bx^2 + cx + d,$$

where $ax^3 + bx^2 + cx + d$ is a cubic polynomial with distinct roots. However, to get the best properties, one needs to work in the projective plane, where the above equation is replaced with the homogeneous equation

$$y^2z = ax^3 + bx^2z + cxz^2 + dz^3.$$

The resulting projective curve E has an extra structure: Given two points on E, the line connecting them intersects E at a third point by Bézout's Theorem. This leads to a group structure on E where the point at infinity is the identity element.

Over the field of rational numbers $\mathbf{Q}$, elliptic curves have a remarkably rich theory. The group structure is related to the *Birch–Swinnerton–Dyer Conjecture*, and Wiles's proof of Fermat's Last Theorem was a corollary of his solution of a large part of the *Taniyama–Shimura Conjecture* for elliptic curves over $\mathbf{Q}$. On the other hand, elliptic curves over finite fields are used in cryptography (see Ref. 25). The relation between elliptic integrals and elliptic curves has been generalized to *Hodge theory*, which is described in Ref. 24. Higher dimensional analogs of elliptic curves are called *abelian varieties*.

2. *Grassmannians and Schubert Varieties*. In $\mathbf{P}^n(k)$, we use homogeneous coordinates $[u_0, \ldots, u_n]$, where $[u_0, \ldots, u_n] = [v_0, \ldots, v_n]$ if both lie on the same line through the origin in k^{n+1}. Hence points of $\mathbf{P}^n(k)$ correspond to one-dimensional subspaces of k^{n+1}. More generally, the *Grassmannian G(N, m)(k)* consists of all m-dimensional subspaces of k^n. Thus, $G(n+1, 1)(k) = \mathbf{P}^n(k)$.

Points of *G(N, m)(k)* have natural coordinates, which we describe for $m = 2$. Given a two-dimensional sub-space W of k^N, consider a $2 \times N$ matrix

$$\begin{pmatrix} u_1 & u_2 & \ldots & u_N \\ v_1 & v_2 & \ldots & v_N \end{pmatrix}$$

whose rows give a basis of W. Let p_{ij}, $ilt; j$, be the determinant of the 2×2 matrix formed by the ith and jth columns. The $M = \binom{N}{2}$ numbers p_{ij} are the *Plücker coordinates* of W. These give a point in $\mathbf{P}^{M1}(k)$ that depends only on W and not on the chosen basis. Furthermore, the subspace W can be reconstructed from its Plücker coordinates. The Plücker coordinates satisfy the *Plücker relations*

$$p_{ij}p_{kl} - p_{ik}p_{jl} + p_{il}p_{jk} = 0,$$

and any set of numbers satisfying these relations comes from a subspace W. It follows that the Plücker relations define $G(N, 2)(k)$ as a projective variety in $\mathbf{P}^{M-1}(k)$. In general, $G(N, m)(k)$ is a smooth projective variety of dimension $m(N - m)$.

The Grassmannian $G(N, m)(k)$ contains interesting varieties called *Schubert varieties*. The *Schuberi calculus* describes how these varieties intersect. Using the Schubert calculus, one can answer questions such as how many lines in $\mathbf{P}^3(k)$ intersect four lines in general position? (The answer is two.) An introduction to Grassmannians and Schubert vareties can be found in Ref. 26.

The question about lines in $\mathbf{P}^3(k)$ is part of *enumerative algebraic geometry*, which counts the number of geometrically interesting objects of various types. Bezout's Theorem is another result of enumerative algebraic geometry. Another famous enumerative result states that a smooth cubic surface in $\mathbf{P}^3(\mathbf{C})$ contains exactly 27 lines.

3. *Rational and Unirational Varieties*. An irreducible variety V of dimension n over $\mathbf{C}$ is *rational* if there is a one-to-one rational parametrization $U \to V$, where U is a Zariski open subset of $\mathbf{C}^n$. The simplest example of a rational variety is $\mathbf{P}^n(\mathbf{C})$. Many curves and surfaces that occur in geometric modeling are rational.

More generally, an irreducible variety of dimension n is *unirational* if there is a rational parametrization $U \to V$ whose image fills up most of V, where U is a Zariski open subset of $\mathbf{C}^m$, $m \geq n$. For varieties of dimension 1 and 2, unirational and rational coincide,

but in dimensions 3 and greater, they differ. For example, a smooth cubic hypersurface in $\mathbf{P}^4(\mathbf{C})$ is unirational but not rational.

A special type of rational variety is a *toric variety*. In algebraic geometry, a *torus* is $(\mathbf{C}^*)^n$, which is the Zariski open subset of $\mathbf{C}^n$ where all coordinates are nonzero. A toric variety V is an n-dimensional irreducible variety that contains a copy of $(\mathbf{C}^*)^n$ as a Zariski open subset in a suitably nice manner. Both $\mathbf{C}^n$ and $\mathbf{P}^n(\mathbf{C})$ are toric varieties. There are strong relations between toric varieties and polytopes, and toric varieties also have interesting applications in geometric modeling (see Ref. 27), algebraic statistics, and computational biology (see Ref. 28). The latter includes significant applications of Gröbner bases.

4. *Varieties over Finite Fields*. A set of equations defining a projective variety V over $\mathbf{F}_p$ also defines V as a projective variety over $\mathbf{F}_{p^m}$ for every $m \geq 1$. As $\mathbf{P}^n(\mathbf{F}_{p^m})$ is finite, we let N_m denote the number of points of V when regarded as lying in $\mathbf{P}^n(\mathbf{F}_{p^m})$. To study the asymptotic behavior of N_m as m gets large, it is convenient to assemble the N_m into the *zeta function*

$$Z(V, t) = \exp\left(\sum_{m=1}^{\infty} N_m t^m / m\right).$$

The behavior of $Z(V, t)$ is the subject of some deep theorems in algebraic geometry, including the *Riemann hypothesis* for smooth projective varieties over finite fields, proved by Deligne in 1974.

Suppose for example that V is a smooth curve. The *genus* g of V is defined to be the dimension of the sheaf cohomology group $H^1(V, O_V)$. Then the Riemann hypothesis implies that

$$|N_m - p^{m-} 1| \leq 2g\, p^{m/2}.$$

Zeta functions, the Riemann hypothesis, and other tools of algebraic geometry such as the *Riemann–Roch Theorem* have interesting applications in algebraic coding theory. See Ref. 29 and the entry on ALGEBRAIC CODING THEORY. References 18 and 30 discuss aspects of coding theory that involve Gröbner bases.

CLASSIFICATION QUESTIONS

One of the enduring questions in algebraic geometry concerns the classification of geometric objects of various types. Here is a brief list of some classification questions that have been studied.

1. *Curves*. For simplicity, we work over $\mathbf{C}$. The main invariant of smooth projective curve is its genus g, defined above as the dimension of $H^1(V, O_V)$. When the genus is 0, the curve is $\mathbf{P}^1(\mathbf{C})$, and when the genus is 1, the curve is an elliptic curve E. After a coordinate change, the affine equation can be written as

$$y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0.$$

The *j-invariant* $j(E)$ is defined to be

$$j(E) = \frac{2^8 3^3 a^3}{4a^3 + 27b^2}$$

and two elliptic curves over $\mathbf{C}$ are isomorphic as varieties if and only if they have the same j-invariant. It follows that isomorphism classes of elliptic curves correspond to complex numbers; one says that $\mathbf{C}$ is the *moduli space* for elliptic curves. Topologically, all elliptic curves look like a torus (the surface of a donut), but algebraically, they are the same if and only if they have the same j-invariant.

Now consider curves of genus $g \geq 2$ over $\mathbf{C}$. Topologically, these look like a surface with g holes, but algebraically, there is a moduli space of dimension $3g - 3$ that records the algebraic structure. These moduli spaces and their compactifications have been studied extensively. Curves of genus $g \geq 2$ also have strong connections with non-Euclidean geometry.

2. *Surfaces*. Smooth projective surfaces over $\mathbf{C}$ have a richer structrure and hence a more complicated classification. Such a surface S has its *canonical bundle* ω_S, which is a sheaf of O_S-modules that (roughly speaking) locally looks like multiples of $dxdy$ for local coordinates x, y. Then we get the associated bundle ω_S^m, which locally looks like multiples of $(dxdy)^m$. The dimension of the sheaf cohomology group $H^0(S, \omega_S^m)$ grows like a polynomial in m, and the degree of this polynomial is the *Kodaira dimension* κ of S, where the zero polynomial has degree $-\infty$. Using the Kodaira dimension, we get the following *Enriques-Kodaira classification*:

- $\kappa = -\infty$: Rational surfaces and ruled surfaces over curves of genus > 0.
- $\kappa = 0$: K3 surfaces, abelian surfaces, and Enriques surfaces.
- $\kappa = 1$: Surfaces mapping to a curve of genus ≥ 2 whose generic fiber is an elliptic curve.
- $\kappa = 2$: Surfaces of general type.

One can also define the Kodaira dimension for curves, where the possible values $\kappa = -\infty$, 0, 1 correspond to the classication by genus $g = 0$, 1 or ≥ 2. One difference in the surface case is that blowing up causes problems. One needs to define the *minimal model* of a surface, which exists in most cases, and then the minimal model gets "classified" by describing its moduli space. These moduli spaces are well understood except for surfaces of general type, where many unsolved problems remain.

To say more about how this classification works, we need some terminology. Two irreducible varieties are *birational* if they have Zariski open subsets that are isomorphic. Thus, a variety over $\mathbf{C}$ is rational if and only if it

is birational to $\mathbf{P}^n(\mathbf{C})$, and two smooth projective surfaces are birational if and only if they have the same minimal model. As for moduli, consider the equation

$$a\left(x_0^4 + x_1^4 + x_2^4 + x_3^4\right) = x_0x_1x_2x_3 = 0.$$

This defines a K3 surface in $\mathbf{P}^3(\mathbf{C})$ provided $a \neq 0$. As we vary a, we get different K3 surfaces that can be *deformed* into each other. This (very roughly) is what happens in a moduli space, although a lot of careful work is needed to make this idea precise.

The Enriques–Kodaira classification is described in detail in Ref. 31. This book also discuss the closely related classication of smooth complex surfaces, not necessarily algebraic.

1. *Higher Dimensions*. Recall that a three-fold is a variety of dimension 3. As in the surface case, one uses the Kodaira dimension to break up all three-folds into classes, this time according to $k = -\infty, 0, 1, 2, 3$. One new feature for three-folds is that although minimal models exist, they may have certain mild singularities. Hence, the whole theory is more sophisticated than the surface case. The general strategy of the *minimal model program* is explained in Ref. 32.
2. *Hilbert Schemes*. Another kind of classification question concerns varieties that live in a fixed ambient space. For example, what sorts of surfaces of small degree exist in $\mathbf{P}^4(\mathbf{C})$? There is also the *Hartshorne conjecture*, which asserts that a smooth variety V of dimension n in $\mathbf{P}^N(\mathbf{C})$, where $N < \frac{3}{2}n$, is a *complete intersection*, meaning that V is defined by a system of exactly $N - n$ equations.

   In general, one can classify *all* varieties in $\mathbf{P}^n(\mathbf{C})$ of given degree and dimension. One gets a better classification by looking at all varieties with given Hilbert polynomial. This leads to the concept of a *Hilbert scheme*. There are many unanswered questions about Hilbert schemes.
3. *Vector Bundles*. A *vector bundle of rank r* on a variety V is a sheaf that locally looks like a free module of rank r. For example, the tangent planes to a smooth surface form its *tangent bundle*, which is a vector bundle of rank 2.

   Vector bundles of rank 1 are called *line bundles* or *invertible sheaves*. When V is smooth, line bundles can be described in terms of *divisors*, which are formal sums $a_1D_1 + \cdots + a_mD_m$, where a_i is an integer and D_i is an irreducible hypersurface. Furthermore, line bundles are isomorphic if and only if their corresponding divisors are *rationally equivalent*. The set of isomorphism classes of line bundles on V forms the *Picard group* $\mathrm{Pic}(V)$.

   There has also been a lot of work classifying vector bundles on $\mathbf{P}^n(\mathbf{C})$. For $n = 1$, a complete answer is known. For $n > 2$, one classifies vector bundles E according to their rank r and their *Chern classes* $C_i(E)$. One important problem is understanding how to compactify the corresponding moduli spaces. This involves the concepts of *stable* and *semistable* bundles. Vector bundles also have interesting connections with mathematical physics (see Ref. 33).
4. *Algebraic Cycles*. Given an irreducible variety V of dimension n, a variety W contained in V is called a *subvariety*. Divisors on V are integer combinations of irreducible subvarieties of dimension $n - 1$. More generally, an *m-cycle* on V is an integer combination of irreducible subvarieties of dimension m. Cycles are studied using various equivalence relations, including *rational equivalence, algebraic equivalence, numerical equivalence*, and *homological equivalence*. The *Hodge Conjecture* concerns the behavior of cycles under homological equivalence, whereas the *Chow groups* are constructed using rational equivalence.

   Algebraic cycles are linked to other topics in algebraic geometry, including *motives, intersection theory*, and *variations of Hodge structure*. An introduction to some of these ideas can be found in Ref. 34.

REAL ALGEBRAIC GEOMETRY

In algebraic geometry, the theory usually works best over $\mathbf{C}$ or other algebraically closed fields. Yet many applications of algebraic geometry deal with real solutions of polynomial equations. We will explore several aspects of this question.

When dealing with equations with finitely many solutions, there are powerful methods for estimating the number of solutions, including a multivariable version of Bézout's Theorem and the more general *BKK bound*, both of which deal with complex solutions. But these bounds can differ greatly from the number of real solutions. An example from Ref. 35 is the system

$$\begin{aligned} axyz^m + bx + cy + d &= 0 \\ a'xyz^m + b'x + c'y + d' &= 0 \\ a''xyz^m + b''x + c''y + d'' &= 0 \end{aligned}$$

where m is a positive integer and $a, b, \ldots, c'', d''$ are random real coefficients. The BKK bound tells us that there are m complex solutions, and yet there are at most two real solutions.

Questions about the number of real solutions go back to *Descartes' Rule of Signs* for the maximum number of positive and negative roots of a real univariate polynomial. There is also *Sturm's Theorem*, which gives the number of real roots in an interval. These results now have multivariable generalizations. Precise statements can be found in Refs. 18 and 30.

Real solutions also play an important role in enumerative algebraic geometry. For example, a smooth cubic surface S defined over $\mathbf{R}$ has 27 lines when we regard S as lying in $\mathbf{P}^3(\mathbf{C})$. But how many of these lines are real? In other words, how many lines lie on S when it is regarded as lying in $\mathbf{P}^3(\mathbf{R})$? (The answer is 27, 15, 7, or 3, depending on the equation of the surface.) This and other examples from *real enumerative geometry* are discussed in Ref. 35.

Over the real numbers, one can define geometric objects using inequalities as well as equalities. For example, a solid sphere of radius 1 is defined by $x^2 + y^2 + z^2 \leq 1$. In general, a finite collection of polynomial equations and inequalities define what is known as a *semialgebraic variety*. Inequalities arise naturally when one does *quantifier elimination*. For example, given real numbers a and b, the question

$$\text{Does there exist } x \text{ in } \mathbf{R} \text{ with } x^2 + bx + c = 0?$$

is equivalent to the inequality

$$b^2 - 4c \geq 0$$

by the quadratic formula. The theory of real quantifier elimination is due to Tarksi, although the first practical algorithmic version is Collin's *cylindrical algebraic decomposition*. A brief discussion of these issues appears in Ref. 30. Semialgebraic varieties arise naturally in robotics and motion planning, because obstructions like floors and walls are defined by inequalities (see **ROBOTICS**).

SCHEMES

An affine variety V is the geometric object corresponding to the algebraic object given by its coordinate ring $k[V]$. More generally, given *any* commutative ring R, Grothendieck defined the *affine scheme* Spec (R) to be the geometric object corresponding to R. The points of Spec(R) correspond to prime ideals of R, and Spec(R) also has a structure sheaf $\mathrm{O}_{\mathrm{spec(R)}}$ that generalizes the sheaves O_V mentioned earlier.

As an example, consider the coordinate ring $\mathbf{C}[V]$ of an affine variety V in $\mathbf{C}^n$. We saw earlier that the points of V correspond to maximal ideals of $\mathbf{C}[V]$. As maximal ideals are prime, it follows that Spec$(\mathbf{C}[V])$ contains a copy of V. The remaining points of Spec$(\mathbf{C}[V])$ correspond to the other irreducible varieties lying in V. In fact, knowing Spec$(\mathbf{C}[V])$ is equivalent to knowing V in a sense that can be made precise.

Affine schemes have good properties with regard to maps between rings, and they can be patched together to get more general objects called *schemes*. For example, every projective variety has a natural scheme structure. One way to see the power of schemes is to consider the intersection of the curves in $\mathbf{C}^2$ defined by $f = 0$ and $g = 0$, as in our discussion of Bezout's Theorem. As varieties, this intersection consists of just points, but if we consider the intersection as a scheme, then it has the additional structure consisting of the ring $O_{\mathbf{p}}/\langle f, g\rangle$ at every intersection point $\mathbf{p}$. So the scheme–theoretic intersection knows the multiplicities. See Ref. 36 for an introduction to schemes. Scheme theory is also discussed in Refs. 1 and 2.

BIBLIOGRAPHY

1. R. Hartshorne, *Algebraic Geometry*, New York: Springer, 1977.
2. I. R. Shafarevich, Basic Algebraic Geometry, New York: Springer, 1974.
3. B. Buchberger, Gröbner bases: An algorithmic method in polynomial ideal theory, in N. K. Bose (ed.), *Recent Trends in Multidimensional Systems Theory*, Dordrecht: D. Reidel, 1985.
4. D. Cox, J. Little, and D. O'Shea, *Ideals, Varieties and Algorithms*, 3rd ed., New York: Springer, 2006.
5. H. Schenck, *Computational Algebraic Geometry*, Cambridge: Cambridge University Press, 2003.
6. K. Smith, L. Kahanpää, P. Kekäläinen, and W. Traves, *An Invitation to Algebraic Geometry*, New York: Springer, 2000.
7. D. Bayer and D. Mumford, What can be computed in algebraic geometry? in D. Eisenbud and L. Robbiano (eds.), *Computational Algebraic Geometry and Commutative Algebra*, Cambridge: Cambridge University Press, 1993.
8. A. Dickenstein and I. Emiris, *Solving Polynomial Systems*, New York: Springer, 2005.
9. PHCpack, a general purpose solver for polynomial systems by homotopy continuation. Available: http://www.math.uic.edu/jan/PHCpack/phcpack.html.
10. Maple. Available: http://www.maplesoft.com.
11. Mathematica. Available: http://www.wolfram.com.
12. CoCoA, Computational Commutative Algebra. Available: http://www.dima.unige.it.
13. Macaulay 2, a software for system for research in algebraic geometry. Available: http://www.math.uiuc.edu/Macaulay2.
14. Singular, a computer algebra system for polynomial computations. Available: http://www.singular.uni-kl.de.
15. M. Kreuzer and L. Robbiano, *Computational Commutative Algebra 1*, New York: Springer, 2000.
16. G.-M. Greuel and G. Pfister, *A Singular Introduction of Commutative Algebra*, New York: Springer, 2002.
17. Magma, The Magma Computational Algebra System. Available: http://magma. maths. usyd. edu. au/magma/.
18. D. Cox, J. Little, and D. O'Shea, *Using Algebraic Geometry*, 2nd ed., New York: Springer, 2005.
19. T. W. Sederberg and F. Chen, Implicitization using moving curves and surfaces, in S. G. Mair and R. Cook (eds.), *Proceedings of the 22nd Annual Conference on Computer graphics and interactive techniques (SIGGRAPH1995)*, New York: ACM Press, 1995, pp. 301–308.
20. H. Hauser, The Hironaka theorem on resolution of singularities (or: a proof we always wanted to understand), *Bull. Amer. Math. Soc.*, **40**: 323–403, 2003.
21. G. Bodnár and J. Schicho, Automated resolution of singularities for hypersurfaces, *J. Symbolic Computation.*, **30**: 401–429, 2000. Available: http://www.rise.uni-linz.ac.at/projects/basic/adjoints/blowup.
22. H. Stetter, *Numerical Polynomial Algebra*, Philadelphia: SIAM, 2004.
23. D. Cox, R. Goldman, and M. Zhang, On the validity of implicitization by moving quadrics for rational surfaces with no base points, *J. Symbolic Computat.*, **29**: 419–440, 2000.
24. P. Griffiths and J. Harris, *Principles of Algebraic Geometry*, New York: Wiley, 1978.
25. N. Koblitz, *A Course in Number Theory and Cryptography*, 2nd ed., New York: Springer, 1994.
26. S. L. Kleiman and D. Laksov, Schubert calculus, *Amer. Math. Monthly*, **79**: 1061–1082, 1972.
27. R. Goldman and R. Krasauskas (eds.), *Topics in Algebraic Geometry and Geometric Modeling*, Providence, RI: AMS, 2003.
28. L. Pachter and B. Sturmfels (eds.), *Algebraic Statistics for Computational Biology*, Cambridge: Cambridge University Press, 2005.

29. C. Moreno, *Algebraic Curves over Finite Fields*, Cambridge: Cambridge University Press, 1991.
30. A. M. Cohen, H. Cuypers, and H. Sterk (eds.), *Some Tapas of Computer Algebra*, New York: Springer, 1999.
31. W. P. Barth, C. A. Peters, and A. A. van de Ven, *Compact Complex Surfaces*, New York: Springer, 1984.
32. C. Cadman, I. Coskun, K. Jarbusch, M. Joyce, S. Kovács, M. Lieblich, F. Sato, M. Szczesny, and J. Zhang, A first glimpse at the minimal model program, in R. Vakil (ed.), *Snowbird Lectures in Algebraic Geometry*, Providence, RI: AMS, 2005.
33. V. S. Vardarajan, Vector bundles and connections in physics and mathematics: Some historical remarks, in V. Lakshmibai, V. Balaji, V. B. Mehta, K. R. Nagarajan, K. Paranjape, P. Sankaran, and R. Sridharan (eds), *A Tribute to C. S. Seshadri*, Basel: Birkhäuser-Verlag, 2003, pp. 502–541.
34. W. Fulton, *Introduction to Intersection Theory in Algebraic Geometry*, Providence, RI: AMS, 1984.
35. F. Sottile, Enumerative real algebraic geometry, in S. Basu and L. Gonzalez-Vega (eds.), *Algorithmic and quantitative real algebraic geometry (Piscataway, NJ, 2001)*, Providence, RI: AMS, 2003, pp. 139–179.
36. D. Eisenbud and J. Harris, *The Geometry of Schemes*, New York: Springer, 2000.

DAVID A. COX
Amherst College