1 Guiding problems

Let k denote a field and $k[x_1, x_2, \ldots, x_n]$ the polynomials in $x_1, x_2, \ldots, x_n$ with coefficients in k. We often refer to k as the *base field*. A nonzero polynomial

$$f = \sum_{\alpha_1,\ldots,\alpha_n} c_{\alpha_1\ldots\alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \quad c_{\alpha_1\ldots\alpha_n} \in k,$$

has degree d if $c_{\alpha_1\ldots\alpha_n} = 0$ when $\alpha_1 + \cdots + \alpha_n > d$ and $c_{\alpha_1\ldots\alpha_n} \neq 0$ for some index with $\alpha_1 + \cdots + \alpha_n = d$. It is *homogeneous* if $c_{\alpha_1\ldots\alpha_n} = 0$ whenever $\alpha_1 + \cdots + \alpha_n < d$. We will sometimes use multiindex notation

$$f = \sum_{\alpha} c_\alpha x^\alpha$$

where $\alpha = (\alpha_1, \ldots, \alpha_n)$, $c_\alpha = c_{\alpha_1\ldots\alpha_n}$, $x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, and $|\alpha| = \alpha_1 + \cdots + \alpha_n$,

1.1 Implicitization

Definition 1.1 *Affine space* of dimension n over k is defined

$$\mathbb{A}^n(k) = \{(a_1, a_2, \ldots, a_n) : a_i \in k\}.$$

For $k = \mathbb{R}$ this is just the ubiquitous $\mathbb{R}^n$. Why don't we use the notation k^n for affine space? We write $\mathbb{A}^n(k)$ when we want to emphasize the geometric nature of k^n rather than its algebraic properties (e.g., as a vector space). Indeed, when our discussion does not involve the base field in an essential way we drop it from the notation, writing $\mathbb{A}^n$.

We shall study maps between affine spaces, but not just any maps are allowed in algebraic geometry. We consider only maps given by polynomials:

Definition 1.2 A *morphism* of affine spaces

$$\phi : \mathbb{A}^n(k) \to \mathbb{A}^m(k)$$

is a map given by a polynomial rule

$$(x_1, x_2, \ldots, x_n) \mapsto (\phi_1(x_1, \ldots, x_n), \ldots, \phi_m(x_1, \ldots, x_n)),$$

with the $\phi_i \in k[x_1, \ldots, x_n]$.

Remark 1.3 This makes a tacit reference to the base field k, in that the polynomials ϕ_i have coefficients in k. If we want to make this explicit, we say that the morphism is *defined over* k.

Example 1.4 An affine-linear transformation is a morphism: given an $m \times n$ matrix $A = (a_{ij})$ and an $m \times 1$ matrix $b = (b_i)$ with entries in k, we define

$$\begin{aligned} \phi_{A,b} : \mathbb{A}^n(k) &\rightarrow \mathbb{A}^m(k) \\ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} &\mapsto \begin{pmatrix} a_{11}x_1 + \cdots + a_{1n}x_n + b_1 \\ \vdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n + b_m \end{pmatrix}. \end{aligned}$$

Example 1.5 Consider

$$\mathbb{A}^1(\mathbb{R}) \rightarrow \mathbb{A}^2(\mathbb{R})$$

given by the rule

$$t \mapsto (t, t^2).$$

If y_1 and y_2 are the corresponding coordinates on $\mathbb{R}^2$ then the image is the parabola $\{(y_1, y_2) : y_2 = y_1^2\}$. More generally, consider the morphism

$$\begin{aligned} \phi : \mathbb{A}^1(k) &\rightarrow \mathbb{A}^m(k) \\ t &\mapsto (t, t^2, t^3, \ldots, t^m). \end{aligned}$$

Can we visualize the image of ϕ in $\mathbb{A}^m(k)$? Just as for the parabola, we write down polynomial equations for this locus. Fix coordinates $y_1, \ldots, y_m$ on $\mathbb{A}^m(k)$ so that ϕ is given by $y_i \mapsto t^i$. We find the equations

$$\begin{aligned} y_i y_j &= y_{i+j} \quad 1 \leq i < j \leq m \\ y_i y_j &= y_k y_l \quad i + j = k + l \end{aligned}$$

corresponding to the relations $t^i t^j = t^{i+j}$ and $t^i t^j = t^k t^l$ respectively.

The polynomial equations describing the image of our morphism are an *implicit* description of this locus. Here the sense of 'implicit' is the same as the 'implicit function theorem' from calculus. We can consider the general question:

Problem 1.6 (Implicitization) Write down the polynomial equations satisfied by the image of a morphism.

1.1.1 A special case: linear transformations

Elementary row operations from linear algebra solve Problem 1.6 in the case where ϕ is a linear transformation.

Suppose ϕ is given by the rule

$$\begin{aligned} \mathbb{A}^2(\mathbb{Q}) &\to \mathbb{A}^3(\mathbb{Q}) \\ (x_1, x_2) &\mapsto (x_1 + x_2, x_1 - x_2, x_1 + 2x_2) \end{aligned}$$

and assign coordinates y_1, y_2, y_3 to affine three-space. From this, we extract the system

$$\begin{aligned} y_1 &= x_1 + x_2 \\ y_2 &= x_1 - x_2 \\ y_3 &= x_1 + 2x_2, \end{aligned}$$

or equivalently,

$$\begin{array}{lllllll} x_1 & +x_2 & -y_1 & & & = 0 \\ x_1 & -x_2 & & -y_2 & & = 0 \\ x_1 & +2x_2 & & & -y_3 & = 0, \end{array}$$

which in turn are equivalent to

$$\begin{array}{lllllll} x_1 & +x_2 & -y_1 & & & = 0 \\ & -2x_2 & +y_1 & -y_2 & & = 0 \\ & x_2 & +y_1 & & -y_3 & = 0, \end{array}$$

and

$$\begin{array}{lllllll} x_1 & +x_2 & -y_1 & & & = 0 \\ & -2x_2 & +y_1 & -y_2 & & = 0 \\ & & +\frac{3}{2}y_1 & -\frac{1}{2}y_2 & -y_3 & = 0. \end{array}$$

Thus the image of our morphism is given by

$$3y_1 - y_2 - 2y_3 = 0.$$

Our key tool for solving Problem 1.6 in general – Buchberger's Algorithm – will contain elementary row operations as a special case.

Moral 1: To solve Problem 1.6, choosing an order on the variables is very useful.

1.1.2 A converse to implicitization?

The implicitization problem seeks equations for the image of a morphism

$$\phi : \mathbb{A}^n(k) \to \mathbb{A}^m(k).$$

We will eventually show that this admits an algorithmic solution, at least when the base field is algebraically closed. However, there is a natural converse to this question which is much deeper.

Cambridge University Press
978-0-521-69141-3 - Introduction to Algebraic Geometry
Brendan Hassett
Excerpt
More information

Definition 1.7 A *hypersurface* of degree d is the locus

$$V(f) := \{(a_1, \dots, a_m) \in \mathbb{A}^m(k) : f(a_1, \dots, a_m) = 0\} \subset \mathbb{A}^m(k),$$

where f is a polynomial of degree d.

A *regular parametrization* of a hypersurface $V(f) \subset \mathbb{A}^m(\mathbb{C})$ is a morphism

$$\phi : \mathbb{A}^n(\mathbb{C}) \to \mathbb{A}^m(\mathbb{C})$$

such that

1. the image of ϕ is contained in the hypersurface, i.e., $f \circ \phi = 0$;
2. the image of ϕ is not contained in any other hypersurface, i.e., for any $h \in \mathbb{C}[y_1, \dots, y_m]$ with $h \circ \phi = 0$ we have $f | h$.

Problem 1.8 Which hypersurfaces admit regular parametrizations?

Example 1.9 Here are some cases where parametrizations exist:

1. hypersurfaces of degree one (see Exercise 1.5);
2. the curve $V(f) \subset \mathbb{A}^2$, $f = y_1^2 - y_2^3$, has parametrization (cf. Exercise 1.8)
$$\begin{aligned} \phi : \mathbb{A}^1(\mathbb{C}) &\to \mathbb{A}^2(\mathbb{C}) \\ t &\mapsto (t^3, t^2) \end{aligned}$$
3. if $f = y_0^2 + y_1^2 - y_2^2$ then $V(f)$ has a parametrization
$$\phi(s, t) = (2st, s^2 - t^2, s^2 + t^2);$$
4. if $f = y_0^3 + y_1^3 + y_2^3 + y_3^3$ then $V(f)$ has parametrization
$$\begin{aligned} y_0 &= (u_2 + u_1)u_3^2 + \left(u_2^2 + 2u_1^2\right)u_3 - u_2^3 + u_1u_2^2 - 2u_1^2u_2 - u_1^3 \\ y_1 &= u_3^3 - (u_2 + u_1)u_3^2 + \left(u_2^2 + 2u_1^2\right)u_3 + u_1u_2^2 - 2u_1^2u_2 + u_1^3 \\ y_2 &= -u_3^3 + (u_2 + u_1)u_3^2 - \left(u_2^2 + 2u_1^2\right)u_3 + 2u_1u_2^2 - u_1^2u_2 + 2u_1^3 \\ y_3 &= (u_2 - 2u_1)u_3^2 + \left(u_1^2 - u_2^2\right)u_3 + u_2^3 - u_1u_2^2 + 2u_1^2u_2 - 2u_1^3. \end{aligned}$$
The form here is due to Noam Elkies.

We will come back to these questions when we discuss unirationality and rational maps in Chapter 3.

1.2 Ideal membership

Our second guiding problem is algebraic in nature.

Problem 1.10 (Ideal Membership Problem) Given $f_1, \dots, f_r \in k[x_1, \dots, x_n]$, determine whether $g \in k[x_1, \dots, x_n]$ belongs to the ideal $\langle f_1, \dots, f_r \rangle$.

Example 1.11 Consider the ideal

$$I = \langle y_2 - y_1^2, y_3 - y_1 y_2 \rangle \subset k[y_1, y_2, y_3]$$

and the polynomial $g = y_1 y_3 - y_2^2$ (cf. Example 1.5 and the following discussion). Then $g \in I$ because

$$y_1 y_3 - y_2^2 = y_1(y_3 - y_1 y_2) + y_2(y_1^2 - y_2).$$

Again, whenever the f_i and g are all linear, elementary row reductions give a solution to Problem 1.10. However, there is one further case where we already know how to solve the problem. The Euclidean Algorithm yields a procedure to decide whether a polynomial $g \in k[t]$ is contained in a given ideal $I \subset k[t]$. By Theorem A.9, each ideal $I \subset k[t]$ can be expressed $I = \langle f \rangle$ for some $f \in k[t]$. Therefore $g \in I$ if and only if f divides g.

Example 1.12 Check whether $t^5 + t^3 + 1 \in \langle t^3 + 1 \rangle$:

$$\begin{array}{r|rrrr}
 & t^2 & +1 & & \\
\hline
t^3 + 1 & t^5 & +t^3 & & +1 \\
 & t^5 & & +t^2 & \\
\cline{2-4}
 & & +t^3 & -t^2 & +1 \\
 & & +t^3 & & +1 \\
\cline{3-5}
 & & & -t^2 &
\end{array}$$

thus $q = t^2 + 1$ and $r = -t^2$. We conclude $t^5 + t^3 + 1 \notin \langle t^3 + 1 \rangle$:

Moral 2: In solving Problem 1.10, keeping track of *degrees* of polynomials is crucial.

1.3 Interpolation

Let $P_{n,d} \subset k[x_1, \ldots, x_n]$ denote the vector subspace of polynomials of degree $\leq d$. The monomials

$$x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}, \quad \alpha_1 + \cdots + \alpha_n \leq d$$

form a basis for $P_{n,d}$, so we have (see Exercise 1.4)

$$\dim P_{n,d} = \binom{n+d}{n}.$$

Problem 1.13 (Simple Interpolation Problem) Given distinct points

$$p_1, \ldots, p_N \in \mathbb{A}^n(k)$$

what is the dimension of the vector space $I_d(p_1, \ldots, p_N)$ of polynomials of degree $\leq d$ vanishing at each of the points?

Here is some common terminology used in these questions:

Definition 1.14 Given $S \subset \mathbb{A}^n(k)$, the number of conditions imposed by S on polynomials of degree $\leq d$ is defined

$$C_d(S) := \dim P_{n,d} - \dim I_d(S).$$

S is said to *impose independent conditions on* $P_{n,d}$ if

$$C_d(S) = |S|.$$

It *fails to impose independent conditions* otherwise.

Another formulation of the Simple Interpolation Problem is:

When do N points in $\mathbb{A}^n(k)$ fail to impose independent conditions on polynomials of degree $\leq d$?

In analyzing examples, it is useful to keep in mind that affine linear transformations do not affect the number conditions imposed on $P_{n,d}$:

Proposition 1.15 *Let $S \subset \mathbb{A}^n(k)$ and consider an invertible affine-linear transformation $\phi : \mathbb{A}^n(k) \to \mathbb{A}^n(k)$. Then $C_d(S) = C_d(\phi(S))$ for each d.*

Proof By Exercise 1.11, ϕ induces an invertible linear transformation $\phi^* : P_{n,d} \to P_{n,d}$ with $\phi^*(f(x_1, \dots, x_n)) = (f \circ \phi)(x_1, \dots, x_n)$. Thus $(\phi^* f)(p) = 0$ for each $p \in S$ if and only if $f(q) = 0$ for each $q \in \phi(S)$. In particular, $\phi^*(I_d(\phi(S))) = I_d(S)$ so these spaces have the same dimension. □

1.3.1 Some examples

Let $S = \{p_1, p_2, p_3\} \subset \mathbb{A}^n(k)$ be collinear with $n > 1$ or $S = \{p_1, p_2, p_3, p_4\} \subset \mathbb{A}^n(k)$ coplanar with $n > 2$. Then S fails to impose independent conditions on polynomials of degree ≤ 1.

Let $S = \{p_1, p_2, p_3, p_4, p_5, p_6\} \subset \mathbb{A}^2(\mathbb{R})$ lie on the unit circle

$$x_1^2 + x_2^2 = 1.$$

Then S fails to impose independent conditions on polynomials of degree ≤ 2; indeed, $C_2(S) = 5 < 6$.

When does a set of four points $\{p_1, p_2, p_3, p_4\} \subset \mathbb{A}^2(k)$ fail to impose independent conditions on quadrics ($d = 2$)? Assume that three of the points are non-collinear, e.g., p_1, p_2, p_3. After translating suitably we may assume $p_1 = (0, 0)$, and after a further linear change of coordinates we may assume $p_2 = (1, 0)$ and $p_3 = (0, 1)$. (Proposition 1.15 allows us to change coordinates without affecting the number of conditions imposed.) If $p_4 = (a_1, a_2)$ then the conditions on

$$c_{00} + c_{10}x_1 + c_{01}x_2 + c_{20}x_1^2 + c_{11}x_1x_2 + c_{02}x_2^2 \in P_{2,2}$$

take the form

$$\begin{aligned} c_{00} &= 0 \qquad (p_1)\\ c_{00} + c_{10} + c_{20} &= 0 \qquad (p_2)\\ c_{00} + c_{01} + c_{02} &= 0 \qquad (p_3)\\ c_{00} + c_{10}a_1 + c_{01}a_2 + c_{20}a_1^2 + c_{11}a_1a_2 + c_{02}a_2^2 &= 0. \qquad (p_4) \end{aligned}$$

If these are not independent, the matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & a_1^2 - a_1 & a_1a_2 & a_2^2 - a_2 \end{pmatrix}$$

has rank 3. This can only happen if

$$a_1^2 - a_1 = a_1a_2 = a_2^2 - a_2 = 0,$$

which means $p_4 \in \{(0, 0), (1, 0), (0, 1)\} = \{p_1, p_2, p_3\}$, a contradiction. Thus we have shown:

Proposition 1.16 *Four distinct points in the plane fail to impose independent conditions on quadrics only if they are all collinear.*

Here are some sample results:

Proposition 1.17 *Any N points in the affine line $\mathbb{A}^1(k)$ impose independent conditions on $P_{1,d}$ for $d \geq N - 1$.*

Assume k is infinite. For each $N \leq \binom{n+d}{d}$, there exist N points in $\mathbb{A}^n(k)$ imposing independent conditions on $P_{n,d}$.

Proof For the first statement, suppose that $f \in k[x_1]$ is a polynomial vanishing at

$$p_1, \ldots, p_N \in \mathbb{A}^1(k).$$

The Euclidean Algorithm implies that f is divisible by $x - p_j$ for each $j = 1, \ldots, N$. Consequently, it is also divisible by the product $(x_1 - p_1) \ldots (x_1 - p_N)$ (see Exercise A.13). Moreover, if $f \neq 0$ we have a unique expression

$$f = q(x_1 - p_1) \ldots (x_1 - p_N), \quad q \in P_{1,d-N}.$$

The polynomials of this form (along with 0) form a vector space of dimension $d - N + 1$, so

$$C_d(p_1, \ldots, p_N) = \min(N, d + 1).$$

The second statement is established by producing a sequence of points $p_1, \ldots, p_{\binom{n+d}{d}}$ such that

$$I_d(p_1, \ldots, p_j) \supsetneq I_d(p_1, \ldots, p_{j+1})$$

for each $j < \binom{n+d}{d}$. The argument proceeds by induction. Given $p_1, \ldots, p_j$, linear algebra gives a nonzero $f \in P_{n,d}$ with $f(p_1) = \ldots = f(p_j) = 0$. It suffices to find some $p_{j+1} \in \mathbb{A}^n(k)$ such that $f(p_{j+1}) \neq 0$, which follows from the fact (Exercise 1.9) that every nonzero polynomial over an infinite field takes a nonzero value somewhere in $\mathbb{A}^n(k)$. □

1.4 Exercises

1.1 Consider the linear morphism

$$\begin{aligned} \phi : \mathbb{A}^3(\mathbb{R}) &\to \mathbb{A}^4(\mathbb{R}) \\ (t_1, t_2, t_3) &\mapsto (3t_1 + t_3, t_2 + 4t_3, t_1 + t_2 + t_3, t_1 - t_2 - t_3). \end{aligned}$$

Describe image(ϕ) as the locus where a linear polynomial vanishes.

1.2 Decide whether $g = t^3 + t^2 - 2$ is contained in the ideal

$$\langle t^3 - 1, t^5 - 1 \rangle \subset \mathbb{Q}[t].$$

If so, produce $h_1, h_2 \in \mathbb{Q}[t]$ such that

$$g = h_1(t^3 - 1) + h_2(t^5 - 1).$$

1.3 Consider the ideal

$$I = \left\langle y_2 - y_1^2, y_3 - y_1 y_2, \ldots, y_m - y_1 y_{m-1} \right\rangle \subset k[y_1, \ldots, y_m].$$

Show this contains all the polynomials $y_{i+j} - y_i y_j$ and $y_i y_j - y_k y_l$ where $i + j = k + l$ (cf. Example 1.5.)

1.4 Show that the dimension of the vector space of polynomials of degree $\leq d$ in n variables is equal to the binomial coefficient

$$\binom{n+d}{d} = \frac{(n+d)!}{d!\,n!}.$$

Compute the dimension of the vector space of homogeneous polyonomials of degreee d in $n + 1$ variables.

1.5 Given

$$f = c_1 x_1 + c_2 x_2 + \cdots + c_n x_n + c_0$$

with $c_i \neq 0$ for some $i > 0$, exhibit a morphism

$$\phi : \mathbb{A}^{n-1} \to \mathbb{A}^n$$

such that image(ϕ) $= V(f)$ and ϕ is one-to-one.

1.6 Let $A = (a_{ij})$ be an $m \times n$ matrix with entries in k and $b = (b_1, \dots, b_n) \in k^n$. For each $i = 1, \dots, m$, set

$$f_i = a_{i1}x_1 + \cdots + a_{in}x_n \in k[x_1, \dots, x_n]$$

and $g = b_1x_1 + \cdots + b_nx_n$. Show that $g \in \langle f_1, \dots, f_m \rangle$ if and only if b is contained in the span of the rows of A.

1.7 Consider the morphism

$$\begin{aligned} j : \mathbb{A}^3(k) &\to \mathbb{A}^6(k) \\ (u, v, w) &\mapsto (u^2, uv, v^2, vw, w^2, uw). \end{aligned}$$

Let $a_{11}, a_{12}, a_{22}, a_{23}, a_{33}$, and a_{13} be the corresponding coordinates on $\mathbb{A}^6(k)$ and

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix}$$

the symmetric matrix with these entries.

(a) Show that the image of j satisfies the equations given by the two-by-two minors of A.

(b) Compute the dimension of the vector space V in

$$R = k[a_{11}, a_{12}, a_{22}, a_{23}, a_{33}, a_{13}]$$

spanned by these two-by-two minors.

(c) Show that every homogeneous polynomial of degree 2 in R vanishing on the image of j is contained in V. *Hint:* Degree-2 polynomials in R yield degree-4 polynomials in $k[u, v, w]$. Count dimensions!

1.8 Show that the parametrization given for the curve $V(f) \subset \mathbb{A}^2(\mathbb{C})$, $f = x_1^2 - x_2^3$ satisfies the required properties.

1.9 Let k be an infinite field. Suppose that $f \in k[x_1, \dots, x_n]$ is nonzero. Show there exists $a = (a_1, \dots, a_n) \in \mathbb{A}^n(k)$ with $f(a_1, \dots, a_n) \neq 0$.

1.10 Let $S \subset \mathbb{A}^n(k)$ be a finite nonempty subset and let $k[S]$ denote the ring of k-valued functions on S. Show that the linear transformation

$$\begin{aligned} P_{n,d} &\to k[S] \\ f &\mapsto f|S \end{aligned}$$

is surjective if and only if S imposes independent conditions on polynomials of degree d.

1.11 Let $\phi : \mathbb{A}^n(k) \to \mathbb{A}^m(k)$ be an affine linear transformation given by the matrix formula $\phi(x) = Ax + b$ (see Example 1.4). Consider the map induced by composition of polynomials

$$\begin{aligned} \phi^* : k[y_1, \dots, y_m] &\to k[x_1, \dots, x_n] \\ P(y) &\mapsto P(Ax + b). \end{aligned}$$

Show that
(a) ϕ^* takes polynomials of degree $\leq d$ to polynomials of degree $\leq d$;
(b) ϕ is a k-algebra homomorphism;
(c) if the matrix A is invertible then so is ϕ^*.
Moreover, in case (c) the induced linear transformation $\phi^* : P_{n,d} \to P_{n,d}$ is also invertible.

1.12 Consider five distinct points in $\mathbb{A}^2(\mathbb{R})$ that fail to impose independent conditions on $P_{2,3}$. Show that these points are collinear, preferably by concrete linear algebra.

1.13 Show that $d+1$ distinct points

$$p_1, \ldots, p_{d+1} \in \mathbb{A}^n(\mathbb{Q})$$

always impose independent conditions on polynomials in $P_{n,d}$.

1.14 Let ℓ_1, ℓ_2, ℓ_3 be arbitrary lines in $\mathbb{A}^3(\mathbb{Q})$. (By definition, a line $\ell \subset \mathbb{A}^3$ is the locus where two consistent independent linear equations are simultaneously satisfied, e.g., $x_1 + x_2 + x_3 - 1 = x_1 - x_2 + 2x_3 - 4 = 0$.) Show there exists a nonzero polynomial $f \in P_{3,2}$ such that f vanishes on ℓ_1, ℓ_2, and ℓ_3.

Optional Challenge: Assume that ℓ_1, ℓ_2, and ℓ_3 are pairwise skew. Show that f is unique up to scalar.