The many lives of the twisted cubic

Abstract. We trace some of the history of the twisted cubic curves in three-dimensional affine and projective spaces. These curves have reappeared many times in many different guises and at different times they have served as primary objects of study, as motivating examples, and as hidden underlying structures for objects considered in mathematics and its applications.

1. INTRODUCTION Because of its simple coordinate functions, the humble (affine) *twisted cubic curve* in $\mathbb{R}^3$, given in the parametric form

$$\vec{x}(t) = (t, t^2, t^3) \tag{1.1}$$

is staple of computational problems in many multivariable calculus courses. (See Figure 1.) We and our students compute its intersections with planes, find its tangent vectors and lines, approximate the arclength of segments of the curve, derive its curvature and torsion functions, and so forth. But in many calculus books, the curve is not even identified by name and no indication of its protean nature and rich history is given.

This essay is (semi-humorously) in part an attempt to remedy that situation, and (more seriously) in part a meditation on the ways that the things mathematicians study often seem to have existences of their own. Basic structures can reappear at many times in many different contexts and under different names. According to the current consensus view of mathematical historiography, historians of mathematics do well to keep these different avatars of the underlying structure separate because it is almost never correct to attribute our understanding of the sorts of connections we will be considering to the thinkers of the past. For mathematicians, however, it can be revelatory to see the same conceptual building blocks in many different guises.

In this article we will present a number of occurrences of the basic structure of the twisted cubic from a virtual cross-section of the subject of geometry, with a survey of the different tools that have been applied to study geometry, and a discussion of some important applications that lead back to this same geometry. We will start with a sort of "pre-history" of our main character in one of the ancient Greek attempts to *duplicate the cube* – to construct the edge of a cube with twice the volume of a given cube. Here we will be applying our current understanding to what the Greeks did; we are definitely *not* saying that Greek mathematicians would have thought about what they did in anything like the way we will describe it. We will then turn to the initial study of the twisted cubic in 19th century differential and algebraic geometry. The twisted cubic was much studied in the early 19th century as a first example of a nonplanar curve and many of its interesting properties were obtained in that period. In the context of differential geometry we will see how the Frenet-Serret frames introduced by Jean Fréderic Frenet and Joseph Alfred Serret in the 1850's lead to the twisted cubic as a sort of universal local model for the geometry of a space curve. We will then see how this curve served as a key example and test case for the influential and far-reaching work of David Hilbert on free resolutions of modules over polynomial rings. The particular case of the twisted cubic gives an instance of the so-called *Hilbert-Burch theorem*, a key result of modern commutative algebra. Finally we will see how several applications of mathematical ideas such as Bézier curves and binomial probability models

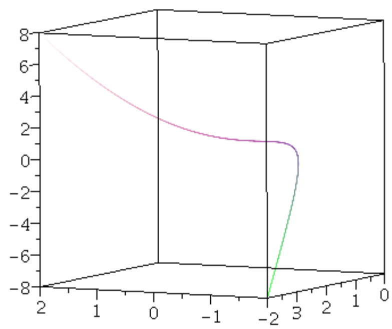


Figure 1. The twisted cubic in $\mathbb{R}^3$, $t \in [-2, 2]$

lead back to the twisted cubic and/or its higher dimensional generalizations. Realizing the connections here have led to some exciting contemporary applications of algebraic geometry in geometric design and statistics.

2. THE "PREHISTORY" OF THE TWISTED CUBIC Three famous construction problems, the *duplication of the cube*, together with the problems of *squaring the circle* and *trisecting a general angle* seem to have played a key role in fueling the development of Greek geometry throughout the Classical and Hellenistic periods. For a fascinating work of historical scholarship on this tradition, see [**8**]. A number of (almost certainly fanciful) traditions deal with the genesis of the duplication problem. For instance, one says that, seeking to halt a plague on their island, the people of Delos consulted the oracle at Delphi for help. The priestess who conveyed the oracle's pronouncements replied that they must double the size of the god Apollo's cubical altar to propitiate him. Unable to find a solution, the Delians supposedly consulted the geometers at Plato's Academy in Athens for the required geometric construction. As a result, the "Delian problem" is often used as a synonym for the duplication problem.

According to fragments of a history of pre-Euclidean mathematics by Eudemus of Rhodes (ca. 370 – ca. 300 BCE) preserved in other sources, this problem was being studied considerably before Plato's time and an important piece of progress had been made before or near the start of Plato's lifetime (ca. 428 - ca. 348 BCE) by Hippocrates of Chios (ca. 470–ca. 410 BCE). None of Hippocrates' own writings have survived, but he is recorded to have observed the following relationships.

Given two line segments AB and GH, following Hippocrates the Greeks said line segments CD and EF were *two mean proportionals in continued proportion between* AB *and* GH if their lengths are proportional as follows:

$$AB : CD = CD : EF = EF : GH. \tag{2.1}$$

Hippocrates' contribution was the realization that if we start with

$$GH = 2AB,$$

then any construction of two mean proportionals as in (2.1) would *solve the problem* *of the duplication of the cube.* The idea is straightforward: If

$$AB : CD = CD : EF = EF : 2AB,$$

then some simple manipulation of proportions (we can do this easily with properties of algebraic ratios) shows

$$CD^3 = 2AB^3.$$

In other words, if AB is the side of the original cube, then CD is the side of the cube with twice the volume.

With this observation, Hippocrates in effect only reduced one (difficult) problem to another (difficult) problem. Finding a geometric construction of the two mean proportionals in continued proportion was still an open question but this approach did provide a definite way to attack the duplication of the cube and essentially all later work took Hippocrates' reduction as a starting point.

We have it from later sources such as the commentary on Book I of Euclid's *Elements* by Proclus (412 - 485 CE) (see [**10**] for a modern translation) that Menaechmus of Alopeconnesus (380–320 BCE) was one of the geometers at the Academy in Athens in Plato's circle. Another ancient source, a catalog of different methods for finding the two mean proportionals in continued proportion in a commentary on Archimedes' *On the Sphere and the Cylinder* by Eutocius of Ascalon (ca. 480 – ca. 540 CE), includes a purported description of Menaechmus' solution, described (in possibly anachronistic terms, using later terminology for conic sections usually attributed to Apollonius of Perga (262–190 BCE)). See [**11**] for a modern translation of Archimedes' work and Eutocius' commentary.

Given line segments of lengths a, z, finding the two mean proportionals in continued proportion means finding x, y to satisfy:

$$a : x = x : y = y : z. \tag{2.2}$$

Hence, transforming these proportions by the operation we would call "cross-multiplying" and interpreting the resulting equations via coordinate geometry, we see the solution to the Delian problem will come from a simultaneous solution of the equations

$$ay = x^2, \qquad xy = az, \qquad xz = y^2. \tag{2.3}$$

If, as we said above, z is a given length, then these equations describe two parabolas and a hyperbola in the x, y plane and the solution comes from determining the point of intersection of any pair of the curves. However, if we think of z as another variable, the first equation describes a cylinder over a parabola, the middle one describes a hyperbolic paraboloid and the final one is a quadric cone with vertex at the origin.

Setting aside the interesting (and still controversial) historical question of exactly when the Greeks would have understood the connection between relations like those in (2.3) (where they would have interpreted a, x, y, z as lengths and the products as areas) and conics or surfaces in three-space, we can see the claimed connection between what we have said so far and the twisted cubic. Think of setting a unit of distance by making $a = 1$ and then parametrizing all instances of the problem in terms of the length x. From (2.2) we see

$$y = x^2, \qquad z = xy = x^3$$

and hence the problem of finding the two mean proportionals is, essentially, the problem of finding a point of intersection of the twisted cubic from (1.1) and a given plane $z = c$. With the understanding of the conditions for solvability by straightedge and compass obtained via algebra in the 19th century, we can see that this problem, and hence the duplication of the cube, is not solvable by those methods for a general c. In addition we see the fact that the twisted cubic coincides with the intersection of the three quadric surfaces. This way of determining implicit equations of the curve will reappear in an important role later.

On the basis of this description of Menaechmus' work from Eutocius' commentary and some other traditions preserved in other sources such as Proclus' commentary on Euclid, Menaechmus has often been credited with the invention of the theory of the conic sections (at least in some form). If he did that, from our point of view here, it's somewhat ironic that he did that essentially by a method so closely tied to the twisted cubic – a curve that is not even contained in a plane.

3. THE TWISTED CUBIC GETS A NAME AND MOVES TO PROJECTIVE SPACE Apparently, Ferdinand August Möbius (1790 - 1868) – also the discoverer of the famous eponymous nonorientable surface – was the first to consider the twisted cubic systematically as a space curve in his 1827 book *Der barycentriche Calcul*, [**9**]. His broader subject there was essentially an approach to what we know as *projective geometry* and he applied those methods to study plane and space curves. Michel Chasles (1793-1880) also made important early contributions concerning twisted cubics. According to William Rowan Hamilton in [**6**], the name "twisted cubic" was proposed somewhat later by George Salmon (1819 - 1904), the author of a number of influential early algebraic geometry textbooks. The word "twisted" in this context simply refers to the fact that the curve does not lie in any single plane in three-dimensional space. Mathematics written in English has tended to follow Salmon's suggestion, but French mathematicians mostly call these *cubiques gauches* (hence the title of Hamilton's note [**6**]), while Germans settle for the more prosaic *kubische Raumkurven*.

A modernized presentation of (one aspect of) Möbius' approach looks something like this. The affine three-dimensional space k^3 over any field k can be viewed as an open subset of the *projective* 3-space $\mathbb{P}^3$ where the points are described by *homogeneous coordinate vectors*:

$$[x_0 : x_1 : x_2 : x_3]$$

with $x_i \in k$, *not all equal to zero* and where two homogenous coordinate vectors represent the same point if one differs from the other by a nonzero constant scalar multiple $\lambda \in k^*$:

$$[x_0 : x_1 : x_2 : x_3] = [\lambda x_0 : \lambda x_1 : \lambda x_2 : \lambda x_3].$$

The set of points with $x_0 = 1$ gives a subset of $\mathbb{P}^3$ in one-to-one correspondence with the affine space k^3. We get similar projective spaces of any dimension n by considering the nonzero $n + 1$ tuples modulo the nonzero scalar multiples as above.

With homogeneous coordinates, in modern presentations of algebraic geometry, the twisted cubic is often described as the 3-tuple Veronese embedding of the projective line $\mathbb{P}^1$. This means that we consider the projective parametrization mapping

$$\begin{aligned} \nu : \mathbb{P}^1 &\longrightarrow \mathbb{P}^3 \\ [t_0 : t_1] &\longrightarrow [t_0^3 : t_0^2 t_1 : t_0 t_1^2 : t_1^3], \end{aligned} \tag{3.1}$$

and the image of ν is the projective twisted cubic. We recover the affine curve from (1.1) by taking the image of the subset of $\mathbb{P}^1$ with $t_0 = 1$ and omitting the first component $x_0 = t_0^3 = 1$ in the projective parametrization (3.1). Note that the coordinate functions here are a vector space basis for the homogeneous polynomials of degree 3 in t_0, t_1. Moreover, the following homogeneous implicit equations are satisfied on the image $\nu(\mathbb{P}^1)$. If $[x_0 : x_1 : x_2 : x_3] = [t_0^3 : t_0^2 t_1 : t_0 t_1^2 : t_1^3]$, then

$$x_0x_2 - x_1^2 = 0, \qquad x_0x_3 - x_1x_2 = 0, \qquad x_1x_3 - x_2^2 = 0. \tag{3.2}$$

After renaming the variables, we have exactly the same three homogeneous equations seen in (2.3) above in the discussion of Menaechmus' work on the duplication of the cube.

These projective curves have some beautiful geometric properties that become surprisingly regular when we take the field to be $\mathbb{C}$ or any other algebraically closed field. It was properties such as these that were the focus of the 19th century geometers such as Salmon, Chasles, Jakob Steiner (1796 - 1863), Luigi Cremona (1830 - 1903), and others.

We say a curve $C \subset \mathbb{P}^3$ has degree n if (counting with multiplicity) a plane L meets C in n points. For instance, every plane

$$a_0x_0 + a_1x_1 + a_2x_2 + a_3x_3 = 0$$

in $\mathbb{P}^3$ intersects the twisted cubic $C = \nu(\mathbb{P}^1)$ from (3.1) at the points satisfying

$$a_0t_0^3 + a_1t_0^2t_1 + a_2t_0t_1^2 + a_3t_1^3 = 0$$

By the "Fundamental Theorem of Algebra" any homogenous polynomial in two variables factors completely into linear factors over $\mathbb{C}$. Hence taking the multiplicity from the factorization, we see that L meets C three times and hence C has degree 3. Following this train of thought,

- Every collection of 4 points on C spans $\mathbb{P}^3$. (Vandermonde determinants give the fastest proof.)
- The twisted cubics are the curves of *minimal degree* in $\mathbb{P}^3$ that do not lie in any plane. (Curves of degree 1 are lines that are contained in infinitely many planes in $\mathbb{P}^3$. On the other hand, if C has degree 2 and we take any three noncollinear points on C, they determine a plane L, but then $L \cap C$ contains at least three points, so C must lie entirely in L.)
- Linear changes of coordinates in $\mathbb{P}^1$ (given by invertible 2×2 matrices modulo scalar matrices) and $\mathbb{P}^3$ (given by 4×4 invertible matrices modulo scalar matrices) yield curves that are projectively equivalent to the curve in (3.1). It follows that there is a $15 - 3 = 12$-dimensional family of twisted cubic curves in $\mathbb{P}^3$, all projectively equivalent.
- Any irreducible curve of degree 3 in $\mathbb{P}^3$ that does not lie in a plane is one of these curves.
- There is a twisted cubic curve passing through any 6 points in $\mathbb{P}^3$ in general position (no 4 coplanar).
- Every secant line to a twisted cubic C meets C in exactly two points; the collection of all secant lines containing any one point on C sweeps out a quadric cone containing C. The surfaces defined by the first and the third equations in (3.2) have this form.

- (The "Steiner construction.") Let L_1, L_2, L_3 be three general lines in $\mathbb{P}^3$. Each line L_i is contained in a 1-parameter family of planes $\Pi_i(t_0, t_1)$, parametrized by $\mathbb{P}^1$. Fix three such parametrizations and look at the curve swept out by the intersections

$$\Pi_1(t_0, t_1) \cap \Pi_2(t_0, t_1) \cap \Pi_3(t_0, t_1)$$

as $[t_0 : t_1]$ runs through the points of $\mathbb{P}^1$. Then the resulting curve is a twisted cubic. For instance if the three lines are

$$\begin{aligned} L_1 &: x_0 = x_1 = 0 \\ L_2 &: x_1 = x_2 = 0 \\ L_3 &: x_2 = x_3 = 0, \end{aligned}$$

then the planes Π_i can be written as

$$\begin{aligned} \Pi_1 &: t_0x_0 + t_1x_1 = 0 \\ \Pi_2 &: t_0x_1 + t_1x_2 = 0 \\ \Pi_3 &: t_0x_2 + t_1x_3 = 0. \end{aligned}$$

A point $[x_0 : x_1 : x_2 : x_3] \in \mathbb{P}^3$ gives a system of equations with a solution corresponding to a single point $[t_0 : t_1] \in \mathbb{P}^1$ if and only if t_0 and t_1 are not both equal to zero, which means the rank of the matrix satisfies

$$\operatorname{rank} \begin{pmatrix} x_0 & x_1 \\ x_1 & x_2 \\ x_2 & x_3 \end{pmatrix} \leq 1. \tag{3.3}$$

Setting the determinants of three 2×2 principal minors equal to zero gives the conditions

$$x_0x_2 - x_1^2 = 0, \qquad x_0x_3 - x_1x_2 = 0, \qquad x_1x_3 - x_2^2 = 0.$$

These are exactly the equations given in (3.2) above. For a vast generalization, see the discussion of Steiner constructions in [**5**].

4. A SIDE TRIP INTO DIFFERENTIAL GEOMETRY AND AN UNEXPECTED APPEARANCE OF THE TWISTED CUBIC

Something close to the modern form of differential geometry of space curves was developed independently by Jean Fréderic Frenet (1816-1900) and Joseph Alfred Serret (1819 -1885). Frenet's work came as part of his 1847 Ph.D. thesis *Sur les fonctions qui servent à déterminer l'attraction des sphéroides quelconques. Programme d'une thèse sur quelque propriétés des courbes à double courbure*. Serret's work followed closely in his 1851 paper *Sur quelques formules relatives à la théorie des courbes à double courbure*. The "double curvature" appearing in both titles is a reflection of the realization that, unlike the case of plane curves where a single curvature function suffices to describe the geometry of a curve in its ambient space, curves in $\mathbb{R}^3$ require two such functions, now usually called the *curvature* and the *torsion*. Classic texts such as [**4**] follow Frenet and Serret's presentation quite closely. It is instructive to compare the derivation leading to equations in (50) on page 17 in Chapter I of [**4**] with modern derivations. Eisenhart's version of the Frenet-Serret formulas gives component-wise expressions for the derivatives with respect to arc length of the unit tangent vector $\mathbf{T} = (\alpha, \beta, \gamma)$, the principal normal vector $\mathbf{N} = (l, m, n)$ and the principal binormal vector $\mathbf{B} = (\lambda, \mu, \nu)$ in the form

$$\begin{gathered} \alpha' = \frac{l}{\rho}, \quad \beta' = \frac{m}{\rho}, \quad \gamma' = \frac{n}{\rho} \\ l' = -\left(\frac{\alpha}{\rho} + \frac{\lambda}{\tau}\right) \quad m' = -\left(\frac{\beta}{\rho} + \frac{\mu}{\tau}\right) \quad n' = -\left(\frac{\gamma}{\rho} + \frac{\nu}{\tau}\right) \\ \lambda' = \frac{l}{\tau}, \quad \mu' = \frac{m}{\tau} \quad \nu' = \frac{n}{\tau}, \end{gathered}$$

where ρ is the *radius of curvature* and τ is the negative of the reciprocal of the usual torsion. Using these, in equations (53) on page 18 of [**4**], Eisenhart derives Taylor series expansions of the arclength-parameter coordinate functions of a general curve in $\mathbb{R}^3$ locally near a point (taken to be $(0, 0, 0)$) if the unit tangent is taken to point along the positive x-axis and the principal normal points along the positive y-axis:

$$\begin{aligned} x(s) &= s - \frac{1}{6\rho}s^3 + \cdots \\ y(s) &= \frac{s^2}{2\rho} - \frac{1}{6}\frac{\rho'}{\rho}s^3 + \cdots \\ z(s) &= -\frac{1}{6\rho\tau}s^3 + \cdots . \end{aligned} \tag{4.1}$$

Here, for simplicity, we write ρ and τ for the values of those functions at $s = 0$, and ρ' is the derivative of the ρ function at $s = 0$. All terms in the portions of the series represented by the ellipses contain s^4 and higher powers of s. If we ignore those terms of higher order in s, this parametrization *describes a twisted cubic*, essentially the image of a parametrization like the one in (1.1) (but rewritten in terms of the arc-length parameter s) under a certain invertible linear change of coordinates in $\mathbb{R}^3$. Hence the twisted cubic has made a surprise appearance here as a sort of *universal approximate local model* for general points on (non-planar) space curves. "General" here means, of course, that neither the radius of curvature nor the radius of torsion can vanish. Eisenhart goes on to exploit this observation to derive, among other things, properties of the tangent developable surface of a general curve.

5. THE TWISTED CUBIC IN HILBERT'S "ÜBER DIE THEORIE DER ALGEBRAISCHEN FORMEN" By the time David Hilbert (1862-1943) wrote his epochal article "Über die Theorie der Algebraischen Formen" ([**7**]) in 1890, algebraic geometry had progressed far beyond study of individual curves such as the twisted cubic. The theory of curves of arbitrary genus was well advanced through the synthesis of Riemann's results on complex functions on compact Riemann surfaces and Dedekind and Weber's algebraic reformulation in terms of function fields. Kronecker had begun the general study of the correspondence between homogeneous ideals in polynomial rings and varieties in $\mathbb{P}^n$. A vibrant school of Italian algebraic geometers centered around Castelnuovo, Enriques, and (later) Severi was closing in on a classification of algebraic surfaces over $\mathbb{C}$ up to birational equivalence and looking to extend those results to higher-dimensional varieties. At the same time, invariant theory had exploded into a central mathematical subject with strong connections to algebraic geometry.

Hilbert's article is devoted to the study of what we now call *homogeneous ideals* in polynomial rings, although in intuitive terms, what he is really doing is *linear algebra* over polynomial rings. His Theorem I is the celebrated "Hilbert Basis Theorem" that asserts the existence of a finite generating set for any such ideal. After proving it in general by an inductive argument on the number of indeterminates, Hilbert proposes to illustrate the general statement by means of an *"anschauliches Beispiel"* – a clear example. For this he turns to the question of determining the complete system of homogeneous polynomials $F(x_0, x_1, x_2, x_3)$ vanishing on a given space curve. Specializing again, he turns to our main character, the trusty projective twisted cubic curve. He gives the three quadrics from (3.2) and then shows that any F vanishing on the twisted cubic must satisfy

$$F = A_1 \cdot (x_0x_2 - x_1^2) + A_2 \cdot (x_0x_3 - x_1x_2) + A_3 \cdot (x_1x_3 - x_2^2)$$

for some homogeneous polynomials A_1, A_2, A_3, or in other words, that the quadrics generate the ideal of all such polynomials F. The ingenious, seemingly *ad hoc*, argument is as follows. By using the three quadrics to eliminate terms containing x_0 and x_2 together, x_0 and x_3 together, or x_1 and x_3 together, any such F can be rewritten as an element of the ideal generated by the quadrics plus a "remainder"

$$\overline{F} = \sum_{\kappa_0,\kappa_1} C_{\kappa_0\kappa_1} x_0^{\kappa_0} x_1^{\kappa_1} + \sum_{\lambda_1,\lambda_2} C_{\lambda_1\lambda_2} x_1^{\lambda_1} x_2^{\lambda_2} + \sum_{\mu_2,\mu_3} C_{\mu_2\mu_3} x_2^{\mu_2} x_3^{\mu_3},$$

where the coefficients $C_{\kappa_0,\kappa_1}, C_{\lambda_1,\lambda_2}, C_{\mu_2,\mu_3}$ are constants. Since F and the quadrics are homogeneous, the same is true of $\overline{F}$, and hence $\kappa_0 + \kappa_1 = \lambda_1 + \lambda_2 = \mu_2 + \mu_3$ in every term. But now we can substitute the component functions for the homogeneous parametrization of the twisted cubic from (3.1). When we do this substitution,

$$\begin{aligned} x_0^{\kappa_0} x_1^{\kappa_1} &\mapsto t_0^{3\kappa_0+2\kappa_1} t_1^{\kappa_1} \\ x_1^{\lambda_1} x_2^{\lambda_2} &\mapsto t_0^{2\lambda_1+\lambda_2} t_1^{\lambda_1+2\lambda_2} \\ x_2^{\mu_2} x_3^{\mu_3} &\mapsto t_0^{\mu_2} t_1^{2\mu_2+3\mu_3}. \end{aligned}$$

Since $\kappa_0 + \kappa_1 = \lambda_1 + \lambda_2 = \mu_2 + \mu_3$, the exponents of t_0 in each of these terms must be distinct. Hence the only way this remainder $\overline{F}$ can vanish at all points of the twisted cubic is if all the coefficients $C_{\kappa_0,\kappa_1}, C_{\lambda_1,\lambda_2}, C_{\mu_2,\mu_3}$ equal *zero*. (Hilbert is making the implicit assumption that the coefficient field of the polynomials is infinite in this argument.) The process of finding the "remainder" $\overline{F}$ can be done algorithmically by a multivariable version of polynomial division using a monomial order, as explained, for instance in [**2**], though Hilbert apparently just understands that such a representation is possible by looking at the polynomials involved.

Theorem III in Hilbert's paper is another landmark result, the "Hilbert Syzygy Theorem," which in modern language states that any finitely generated module M over the polynomial ring $S = k[x_0, \ldots, x_n]$ has a finite *free resolution* of length at most $n + 1$. That is, there is an exact sequence

$$0 \longrightarrow F_{n+1} \longrightarrow F_n \longrightarrow \cdots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0$$

where the F_i are free modules over S and the mappings can be described by matrices with polynomial entries. For example, when $M = \langle f_1, \ldots, f_t \rangle$ is an ideal in S, we would take $F_0 = S^t$ and the mapping $F_0 \longrightarrow M$ defined by multiplication of a column vector in S^t by the 1-row matrix

$$(f_1 \quad f_2 \quad \cdots \quad f_t).$$

Hilbert was concerned as always with homogeneous ideals and his key insight was that free resolutions encode a tremendous amount information about them. When M is an ideal in S, in particular, using a free resolution, one can compute the *Hilbert function* – the function of an integer variable $s \geq 0$ giving the dimension of the vector subspaces of the homogeneous ideal in each degree s.

Once again he turns to the twisted cubic, this time to compute an explicit example of a free resolution. The first observation is that using the generators (3.2) for the ideal I of polynomials vanishing on the twisted cubic, then there are obvious elements of the kernel of $S^3 \longrightarrow I$ coming from the fact that the three quadrics are the determinants of the 2×2 minors of the matrix from (3.3). Adjoining another copy of either column at the left yields 3×3 matrices

$$\begin{pmatrix} x_0 & x_0 & x_1 \\ x_1 & x_1 & x_2 \\ x_2 & x_2 & x_3 \end{pmatrix} \qquad \text{and} \qquad \begin{pmatrix} x_1 & x_0 & x_1 \\ x_2 & x_1 & x_2 \\ x_3 & x_2 & x_3 \end{pmatrix}$$

that automatically have determinant zero because of the repeated columns. Expanding along the first column gives, as Hilbert says, two different solutions of the linear equations in new variables X_1, X_2, X_3:

$$(x_0x_2 - x_1^2)X_1 + (x_0x_3 - x_1x_2)X_2 + (x_1x_3 - x_2^2)X_3 = 0, \tag{5.1}$$

namely

$$(X_1, X_2, X_3) = (x_2, -x_1, x_0) \qquad \text{and} \qquad (X_1, X_2, X_3) = (x_3, -x_2, x_1). \tag{5.2}$$

For typographical reasons, we are writing these as row vectors, but they should really be thought of as the columns of a 3×2 matrix

$$A = \begin{pmatrix} x_2 & x_3 \\ -x_1 & -x_2 \\ x_0 & x_1 \end{pmatrix}.$$

That matrix fits together with the 1-row matrix B consisting of the three quadrics in a sequence of mappings

$$S^2 \xrightarrow{A} S^3 \xrightarrow{B} I \longrightarrow 0.$$

where $BA = 0$ (that is, the image of A is contained in the kernel of B).

Hilbert next shows that the image of A is all of the kernel of B. If (X_1, X_2, X_3) is any solution of (5.1), then any terms in X_3 containing x_2 can be cancelled by subtracting a multiple of the first solution in (5.2), and then any remaining terms involving x_3 can be cancelled by subtracting a multiple of the second. This yields another solution (X_1', X_2', X_3') of (5.1) where X_1' depends only on x_0 and x_1. The equation (5.1) is an identity of polynomials so we can now set $x_2 = x_3 = 0$ in the equation

$$(x_0x_2 - x_1^2)X_1' + (x_0x_3 - x_1x_2)X_2' + (x_1x_3 - x_2^2)X_3' = 0$$

yielding an equation that shows $X_1' = 0$. It then follows that $X_2' = -Q(x_1x_3 - x_2^2)$ and $X_3' = Q(x_0x_3 - x_1x_2)$ for some polynomial Q, possibly containing all four of the variables. Hence

$$\begin{aligned}(X_1', X_2', X_3') &= (0, Q(x_1x_3 - x_2^2), -Q(x_0x_3 - x_1x_2)) \\ &= (-Qx_3)(x_2, -x_1, x_0) + (Qx_2)(x_3, -x_2, x_1),\end{aligned}$$

which shows that (X_1', X_2', X_3'), and therefore (X_1, X_2, X_3) also, are in the S-module generated by the two solutions (5.2).

It remains to consider the kernel of the mapping defined by the matrix A. Any column vector $(Y_1, Y_2)^t$ in the kernel of A would satisfy

$$\begin{aligned}0 &= x_2Y_1 + x_3Y_2 \\ 0 &= x_1Y_1 + x_2Y_2 \\ 0 &= x_0Y_1 + x_1Y_2.\end{aligned}$$

The only polynomials that satisfy these three equations simultaneously are $Y_1 = Y_2 = 0$. Hence we have a free resolution of the ideal of the twisted cubic

$$0 \longrightarrow S^2 \xrightarrow{A} S^3 \xrightarrow{B} I \longrightarrow 0.$$

Note that in this case, the free resolution is *shorter than the upper bound* on the length from the Syzygy Theorem. From the general proof of that theorem, it seems clear that Hilbert understood that a similar early termination of the process of computing the resolution would happen whenever the generators of an ideal are the determinants of the $m \times m$ minors of an $(m+1) \times m$ matrix, though he (interestingly) never explicitly says that. When $k = \mathbb{C}$ (or another algebraically closed field) and the ideal I defines a subvariety of $\mathbb{P}^n$ of codimension 2 (as is true for the twisted cubic), and I has a free resolution of the form

$$0 \longrightarrow S^m \xrightarrow{A} S^{m+1} \xrightarrow{B} I \longrightarrow 0,$$

then it is not difficult to see that the ideal I is generated by the determinants of the $m \times m$ minors of the $(m+1) \times m$ matrix A. The condition that guarantees the existence of such a resolution was proved later by L. Burch in [**1**]. This happens exactly when the quotient ring S/I is *Cohen-Macaulay* of codimension 2.

The final section of Hilbert's paper is devoted to the application of these methods to the proof of the finite generation of the ring of invariants of binary forms of a fixed degree. Paul Gordan (1837 - 1912), who devoted much of his career to explicit and arduous computations of those invariants, was supposedly not impressed by Hilbert's non-constructive proof, reportedly (and famously) remarking "this is not mathematics, this is theology." The evidence for saying this anecdote reflects something that actually occurred is rather skimpy, though. In any case Hilbert's paper is a milestone in modern, "abstract," algebra, and the twisted cubic played a conspicuous role in making these ideas accessible to Hilbert's readers.

6. THE TWISTED CUBIC IN APPLICATIONS In recent years, the twisted cubic has continued to show up, Zelig-like, in many important areas of mathematics. As is also true for the subject as a whole, applications of various sorts have assumed greater prominence during this time.

The first example we will consider deals with the so-called *Bézier cubic curves* in $\mathbb{R}^2$. These are named after Pierre Bézier (1910 - 1999), who was a design engineer at the Renault auto works in France. He invented these curves (and surfaces derived from them) as a way to describe and manipulate shapes of portions of automobile bodies, especially via computer-based design and manufacturing. Given four *control points*,

$$p_i = (x_i, y_i)$$

$i = 0, 1, 2, 3$, in the plane, the corresponding Bézier cubic curve has the parametrization:

$$\varphi(t) = \sum_{i=0}^{3} p_i B_i(t) \tag{6.1}$$

for $t \in [0, 1]$. Here $B_0(t) = (1-t)^3$, $B_1(t) = 3(1-t)^2 t$, $B_2 = 3(1-t)t^2$, and $B_3(t) = t^3$ are the three one-variable so-called *Bernstein basis* polynomials. (In geometric design, the products $B_i(t)$ are known as the "blending functions" that take the given control points and define the Bézier curve.)

As seen in the Figure 2, the position of the control points affects the shape of the resulting curve in interesting, but entirely predictable, ways once the patterns are understood. In these plots, $p_0 = (1, 0)$ and $p_3 = (0, 1)$ in all cases. The locations of the other control points are shown in the plots and the coordinates are given in the captions. Note that some of these curves will be smooth, while others such as the curve in (b) will have *ordinary double points, or nodes*, and still others such as the curve in (c) will have *cuspidal double points*. It is not difficult to see from (6.1) that:

- As t increases from 0 to 1, the curve $\varphi(t)$ starts from $\varphi(0) = p_0$ and ends at $\varphi(1) = p_3$.
- The vectors $\overrightarrow{p_0 p_1}$ and $\overrightarrow{p_2 p_3}$ determine the tangents $\varphi'(0)$ and $\varphi'(1)$ respectively.
- The curve $\varphi(t)$ lies entirely within the *convex hull* of the set of control points $\{p_0, p_1, p_2, p_3\}$.

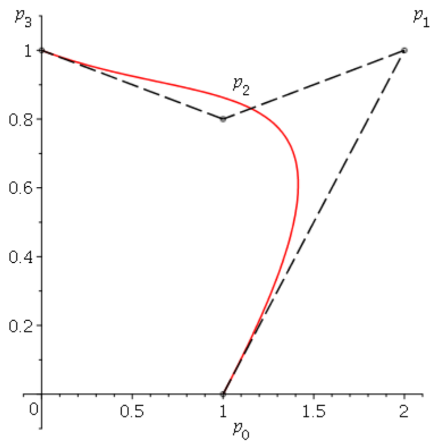
All this makes Bézier curves very suitable for designing shapes, but where is the twisted cubic? Well, notice that the four functions $B_0(t), B_1(t), B_2(t), B_3(t)$ are also a basis of the vector space of polynomials of degree 3 or less in t. Hence if we considered

$$\Phi(t) = (B_0(t), B_1(t), B_2(t), B_3(t)) \tag{6.2}$$

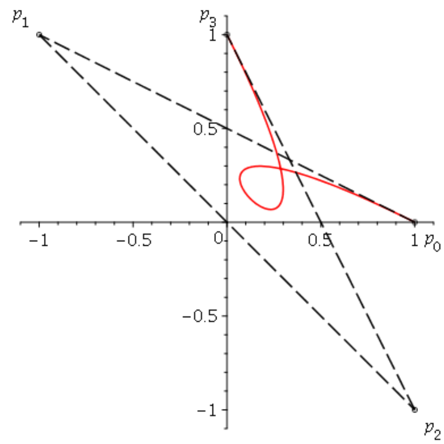
the resulting parametric curve would be a twisted cubic. in the hyperplane $x_0 + x_1 + x_2 + x_3 = 1$ in $\mathbb{R}^4$. Taking $t \in [0, 1]$ gives a segment of that curve. Now the different Bézier curves we saw in Figure 2 are, in fact, just *linear projections* (not necessarily orthogonal projections) of that twisted cubic into $\mathbb{R}^2$ where the control $p_i = (x_i, y_i)$ points define the projection matrix:

$$P = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \end{pmatrix}.$$

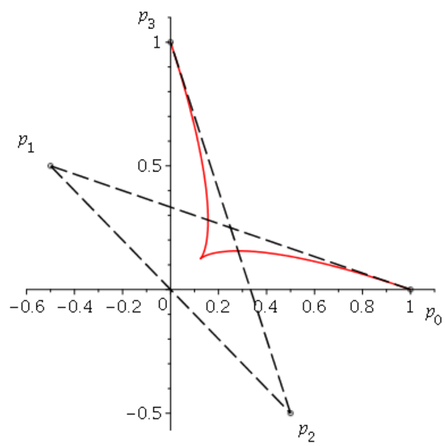
It is easy to check that the matrix product $P\Phi(t)^T$ (multiplying by the transpose of $\Phi(t)$ from (6.2)) gives the planar parametric curve from (6.1), written as a column vector. The nodal and cuspidal singularities are exactly the sorts of singular points



(a) $p_1 = (2, 1), p_2 = (1, 4/5)$



(b) $p_1 = (-1, 1), p_2 = (1, -1)$



(c) $p_1 = (-1/2, 1/2), p_2 = (1/2, -1/2)$

Figure 2. Bézier cubics with control points and polygons

we get on the planar projections of the twisted cubic in $\mathbb{R}^3$. Hence Bézier cubics are nothing but the different *"shadows"* of a twisted cubic in a plane.

Finally, one of the key ideas in the emerging field of *algebraic statistics* (the forthcoming book [**12**] by Seth Sullivant is an excellent snapshot of the current state of this subject) is that when probabilities for discrete random variables depend *polynomially* on some parameters, we can think of those parametrized families of probability distributions *as algebraic varieties*. If a (collection of) random variable(s) X with values $s \in \mathcal{S}$ has $P(X = s) = g_s(\theta_1, \dots, \theta_n)$ for some parameters θ_j, then we can consider the mapping

$$\varphi : \mathbb{R}^n \to \mathbb{R}^{\mathcal{S}}$$
$$\theta = (\theta_1, \dots, \theta_n) \mapsto (g_s(\theta) : s \in \mathcal{S})$$

We will also assume that the g_i are *polynomial*, or at worst *rational* functions of θ. By standard results, this implies that $\varphi(\mathbb{R}^n)$ is a subset of some algebraic variety in $\mathbb{R}^{\mathcal{S}}$.

Given such a φ, the corresponding *model* is the set

$$\overline{\varphi(\mathbb{R}^n)} \cap \Delta$$

where Δ is the probability simplex in $\mathbb{R}^{\mathcal{S}}$ (the set of vectors with non-negative entries summing to 1).

For instance, if X is a *binomial random variable* based on n trials, with success probability θ, then X takes values in $\{0, 1, \ldots, n\}$ with probabilities given by:

$$P(X = k) = p_k(\theta) = \binom{n}{k}\theta^k(1-\theta)^{n-k}.$$

This defines a mapping

$$\begin{aligned}\varphi : \mathbb{R} &\to \mathbb{R}^{n+1}\\ \theta &\mapsto (p_0(\theta), p_1(\theta), \ldots, p_n(\theta)).\end{aligned}$$

Since $\sum_i p_i(\theta) = 1$, the image $\varphi(\mathbb{R})$ is a *curve* in the hyperplane $\sum_i p_i = 1$. If $\theta \in [0, 1]$, then $\varphi(\theta) \in \Delta_{n+1}$, the probability simplex defined by $\sum_i p_i = 1$, and $p_i \geq 0$ for $i = 0, \ldots, n$. What curve is this? For general n, we get a *rational normal curve* of degree n in a hyperplane in $\mathbb{R}^{n+1}$, the direct generalization of the twisted cubic to higher-dimensional ambient spaces (but with a slightly nonstandard parametrization because of the binomial coefficient factors). The case $n = 3$ gives nothing other than the (or better, perhaps, a) twisted cubic. People have studied binomial probabilities since Jacob Bernoulli's *Ars Conjectandi* (1713) at least and the twisted cubic and related curves have been there all along.

7. IN CONCLUSION This is hardly the end of the ways the twisted cubic and its generalizations pop up in unexpected places. For instance, I thank Hal Schenck for the suggestion that the reader may also enjoy looking up the n-dimensional *cyclic polytopes* $C(n, d)$, the convex hulls of $n \geq d$ distinct points on the rational normal curve in $\mathbb{R}^d$ parametrized by

$$(t, t^2, t^3, \ldots, t^d).$$

The boundary of $C(n, d)$ has the largest number of faces in each dimension among all simplicial spheres of dimension $d - 1$ with n vertices, a fact established by Peter McMullen for simplicial polytopes and by Richard Stanley for simplicial spheres. See [**13**] for an introductory discussion and further references.

I think it is examples like the case of the twisted cubic that make many mathematicians into "naive Platonists" (see for instance, [**3**]). The ways this basic curve has reappeared in so many different contexts makes it easy to think that mathematical objects have an existence of their own, independent of humans, and that we merely discover those objects and their properties. Of course, it could also be argued that structures like this are simply part of the way humans think so the fact that they get reused and rediscovered is not, after all, that surprising. Without taking sides in that philosophical debate, I would simply leave you with the observation that it's rather amazing how often the twisted cubic and things related to it have occurred in some of the most central developments in geometry and its applications.

REFERENCES

1. LINDSAY BURCH, “On ideals of finite homological dimension in local rings,” Proc. Cambridge Phil. Soc. **64** (1968), 941–948.
2. DAVID A. COX, JOHN B. LITTLE, AND DONAL B. O'SHEA, *Ideals, Varieties, and Algorithms*, 4th ed. New York: Springer, 2015.
3. PHILIP DAVIS, REUBEN HERSH, ELENA A. MARCHISOTTO, *The Mathematical Experience, Study Edition*, Boston: Birhäuser, 1995.
4. LUTHER P. EISENHART, *A Treatise on the Differential Geometry of Curves and Surfaces*, Boston: Ginn and Company, 1909.
5. PHILLIP GRIFFITHS AND JOE HARRIS, *Principles of Algebraic Geometry*, New York: Wiley, 1978.
6. WILLIAM R. HAMILTON, “On ‘gauche’ curves of the third degree,” Proceedings of the Royal Irish Academy, **8** (1864), 331–334.
7. DAVID HILBERT, “Über die Theorie der algebraischen Formen,” Math. Annalen, **36** (1890), 473–534.
8. WILBUR KNORR, *The Ancient Tradition of Geometric Problems*, New York: Dover, 1993; corrected reprint of original ed., Boston: Birkhäuser, 1986.
9. FERDINAND A. MÖBIUS, Der barycentrische Calcul (1827), Gesammelte Werke, Band I, R. Baltzer, ed. Leipzig: S. Hirzel Verlag, 1885.
10. GLENN R. MORROW, *Proclus: A Commentary on the First Book of Euclid's* Elements, Princeton: Princeton University Press, 1970.
11. REVIEL NETZ, *The Works of Archimedes, Volume 1: The Two Books On the Sphere and the Cylinder*, New York: Cambridge University Press, 2004.
12. SETH SULLIVANT, *Algebraic Statistics*, `http://www4.ncsu.edu/ smsulli2/Pubs/asbook.pdf`
13. GUNTER ZIEGLER, *Lectures on Polytopes*, Graduate Texts in Mathematics 152, New York: Springer, 1995.