3264 Conics in a Second

Paul Breiding, Bernd Sturmfels and Sascha Timme

Abstract

Enumerative algebraic geometry counts the solutions to certain geometric constraints. Numerical algebraic geometry determines these solutions for any given instance. This article illustrates how these two fields complement each other. Our focus lies on the 3264 conics that are tangent to five given conics in the plane. We present a web interface for computing them. It uses the software HomotopyContinuation.jl, which makes this process fast and reliable. We discuss an instance where all 3264 solutions are real.

This article and its accompanying web interface presents Steiner’s conic problem. The intended audience is teachers and their students. Our readers can see current numerical tools in action, on a familiar geometry problem that has inspired scholars for two centuries. The take-home message is that numerical methods in algebraic geometry are fast and reliable.

Let us first recall Steiner’s conic problem: a conic in the plane \( \mathbb{R}^2 \) is the set of solutions to a quadratic equation

\[
A(x, y) = a_1 x^2 + a_2 xy + a_3 y^2 + a_4 x + a_5 y + a_6.
\]

(1)

In algebraic geometry, one replaces the real numbers \( \mathbb{R} \) with the complex numbers \( \mathbb{C} \), and one replaces the affine plane with the projective plane \( \mathbb{P}^2 \) over \( \mathbb{C} \). If there is a second conic

\[
U(x, y) = u_1 x^2 + u_2 xy + u_3 y^2 + u_4 x + u_5 y + u_6,
\]

(2)

then the two conics intersect in four points in \( \mathbb{P}^2 \), counting multiplicities, provided \( A \) and \( U \) are irreducible and not multiples of each other. This is the content of Bézout’s Theorem.

An intersection point \((x, y)\) has multiplicity \( \geq 2 \) if it is a zero of the Jacobian determinant

\[
\frac{\partial A}{\partial x} \cdot \frac{\partial U}{\partial y} - \frac{\partial A}{\partial y} \cdot \frac{\partial U}{\partial x} = 2(a_1 u_2 - a_2 u_1)x^2 + 4(a_1 u_3 - a_3 u_1)xy + \cdots + (a_4 u_5 - a_5 u_4).
\]

(3)

The conic \( U \) is tangent to the conic \( A \) if there exists \((x, y)\) such that (1), (2) and (3) are zero.

By eliminating the two unknowns \( x \) and \( y \) from these three equations we can write this condition directly in terms of the 12 = 6 + 6 coefficients \( a_1, \ldots, a_6, u_1, \ldots, u_6 \) of \( A \) and \( U \):

\[
\mathcal{T}(A, U) = 256a_4^4a_2^2u_5^2u_6^2 - 128a_4^4a_2^2u_3u_5^2u_6^2 + 16a_4^4a_3^2u_4^2u_6^2 - 256a_4^4a_3a_5u_5^2u_6^2 + 128a_4^4a_3a_5u_3u_5^2u_6^2 - 16a_4^4a_3a_5u_3u_5u_6 + 512a_4^4a_3a_6u_3u_5u_6^2 + \cdots + a_4^4a_2^2u_1^2u_2^4.
\]

(4)

This is a sum of 3210 terms of degree 12 = 6 + 6 in the \( a_i \) and \( u_j \). The polynomial \( \mathcal{T} \) is known classically as the tact invariant. It vanishes precisely when the two conics are tangent.
Figure 1: The red ellipse is tangent to four blue ellipses and one blue hyperbola.

The present article concerns the following two subject areas and the questions they ask:

**Enumerative algebraic geometry:** How many conics are tangent to five conics?

**Numerical algebraic geometry:** How do we find all conics tangent to five conics?

The first question was asked in 1848, by Steiner, who suggested the answer 7776. This number turned out to be incorrect. In 1864 Chasles gave the correct answer of 3264. This was further developed by Schubert, whose 1879 book led to Hilbert’s 15th problem, and thus to the 20th century development of enumerative algebraic geometry. The number 3264 appears prominently in the title of the textbook by Eisenbud and Harris [9]. A delightful introduction to Steiner’s problem was presented by Bashelor, Ksir and Traves in [1].

Numerical algebraic geometry is a much younger subject. It started about 20 years ago. The textbook by Sommese and Wampler [15] is a standard reference. It focuses on numerical solutions to polynomial equations. The field is now often seen as a branch of applied mathematics. But, as we demonstrate in this article, it can be used in pure mathematics too.

An instance of our problem is a list of $30 = 5 \times 6$ coefficients in $\mathbb{R}$ or $\mathbb{C}$:

\[
\begin{align*}
    A(x, y) &= a_1 x^2 + a_2 xy + a_3 y^2 + a_4 x + a_5 y + a_6, \\
    B(x, y) &= b_1 x^2 + b_2 xy + b_3 y^2 + b_4 x + b_5 y + b_6, \\
    C(x, y) &= c_1 x^2 + c_2 xy + c_3 y^2 + c_4 x + c_5 y + c_6, \\
    D(x, y) &= d_1 x^2 + d_2 xy + d_3 y^2 + d_4 x + d_5 y + d_6, \\
    E(x, y) &= e_1 x^2 + e_2 xy + e_3 y^2 + e_4 x + e_5 y + e_6.
\end{align*}
\]

(5)

If the coefficients are general enough, then we can assume that each conic $U$ that is tangent
to A, B, C, D and E has nonzero constant term $u_6$. Up to scaling we can then set $u_6 = 1$. Steiner’s problem now translates into a system of five polynomial equations in five unknowns $u_1, u_2, u_3, u_4, u_5$. Each of the five tangency constraints is an equation of degree six:

$$\mathcal{T}(A, U) = \mathcal{T}(B, U) = \mathcal{T}(C, U) = \mathcal{T}(D, U) = \mathcal{T}(E, U) = 0.$$  \hspace{1cm} (6)

Steiner used Bézout’s Theorem to argue that these equations have $6^5 = 7776$ solutions. However, this number overcounts because there is a Veronese surface of extraneous solutions, namely the conics $U$ that are squares of linear forms. These extraneous solutions satisfy

$$\text{rank} \begin{pmatrix} 2u_1 & u_2 & u_4 \\ u_2 & 2u_3 & u_5 \\ u_4 & u_5 & 2u_6 \end{pmatrix} \leq 1.$$  \hspace{1cm} (7)

We have derived the following algebraic reformulation of Steiner’s problem:

**Find all solutions of the equations (6) such that the matrix in (7) has rank $\geq 2$.**  \hspace{1cm} (8)

Ronga, Tognoli and Vust \[11\] and Sottile \[13, 14\] proved the existence of five real conics whose $3264$ conics all have real coefficients. In their argument they do not give an explicit instance, but rather show that in the neighborhood of some particular conic arrangement there must be an instance that has all of the $3264$ conics real. Hence, this raises the problem:

**Find an explicit instance $A, B, C, D, E$ such that the $3264$ solutions to the equations (6), where the rank of the matrix in (7) has rank $\geq 2$, are all real.**  \hspace{1cm} (9)

Using numerical algebraic geometry we discovered the following solution:

$$\begin{bmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ b_1 & b_2 & b_3 & b_4 & b_5 & b_6 \\ c_1 & c_2 & c_3 & c_4 & c_5 & c_6 \\ d_1 & d_2 & d_3 & d_4 & d_5 & d_6 \\ e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \end{bmatrix} = \begin{pmatrix} 1012457 & 8554609 & 5860508 & -251402893 & -25443962 \\ 662488724 & 755781377 & 2798943247 & 1016797750 & 277983473 \\ 520811 & 2183697 & 9002222 & -12680955 & -2472323 \\ 178018145 & 54240633 & 652429049 & 37962407 & 10576890 \\ 6537193 & -7424602 & 6264373 & 13097677 & -29825861 \\ 211535591 & 36384915 & 1630169777 & 39806827 & 240478196 \\ 13173269 & 4510030 & 2224435 & 33318719 & 92891037 \\ 2284890206 & 483147459 & 588965799 & 219393000 & 755709662 \\ 8275097 & -19174153 & 5184916 & -23713234 & 28246737 \\ 452566634 & 408565940 & 172253855 & 87676001 & 81404569 \end{pmatrix}.$$  \hspace{1cm} (1)

We claim that all the $3264$ conics that are tangent to those five conics are real:

**Proposition 1.** There are $3264$ real conics tangent to those given by the $5 \times 6$ matrix above.

We provide an animation showing all the $3264$ real conics of this instance at this URL:

http://www.juliahomotopycontinuation.org/3264/

The construction of our example originates from an arrangement of double lines, which we call the **pentagon construction**. One can see the pentagon in the middle of Figure 2. There are points, where the red conics seems to intersect a blue line. But they are actually points where the red conic touches one branch of a blue hyperbola. See also \[14\] for a discussion.

In the later sections, we discuss the algebro-geometric meaning of the pentagon construction, and we present a rigorous computer-assisted proof that indeed all of the $3264$ conics tangent to our five conics are real. But, first, let us introduce our web browser interface.
Figure 2: The five blue conics in the central picture are those in Proposition 1. Displayed in red is one of the 3264 real conics that are tangent to the five blue conics. Each blue conic looks like a pair of lines, but it is a thin hyperbola whose branches are close to each other. The two pictures on the sides show close-ups around two of the five points of tangency. We see that the red conic is tangent to one of the two branches of the blue hyperbola.

Do It Yourself

In this section we invite you, the reader, to chose your own instance of five conics. We offer a convenient way for you to compute the 3264 complex conics that are tangents to your chosen conics. Please find a web interface for solving instances of Steiner’s problem at

\[ \text{www.juliahomotopycontinuation.org/do-it-yourself/} \]  

At this interface, a user can type in their own \(30 = 5 \times 6\) coefficients for the five conics (5). After specifying their five conics, one presses a button and this calls the numerical algebraic software \text{HomotopyContinuation.jl}. This is the Julia package described in [6, 16]. It is freely available to anyone interested in pursuing numerical algebraic geometry in earnest. Those playing with the web interface, however, need not worry about what is under the hood. But, if you are curious, please read our section titled \text{How Does This Work}?

Shortly after the user submits their instance, by entering real floating point coefficients. The web interface reports whether the instance was generic enough to yield 3264 distinct complex solutions. These solutions are computed numerically. The browser displays the number of real solutions, along with a picture of the instance and a rotating sample of real solutions. As promised in our title, the computation of all solutions takes only a second.

\textbf{Remark 2.} In our computation we always assume that the five given conics are real and generic. This ensures that there are 3264 complex solutions, and these conics are tangent to the given conics at \(5 \times 3264\) distinct points. The number of real solutions is even, and our web interface displays them all sequentially. \textit{For every real solution, the points of tangency at the given conics are also real}. This fact uses the genericity assumption, since two special
real conics can be tangent at two complex conjugate points. For instance, the conics defined by $x^2 - y^2 + 1$ and $x^2 - 4y^2 + 1$ are tangent at the points $(i : 0)$ and $(-i : 0)$ where $i = \sqrt{-1}$.

Figure 3 shows what the input and the visual output of our web interface look like. The user inputs five conics and the system shows these in blue. After clicking the “compute” button, the system responds quickly with the number of complex and real conics that were found. The 3264 conics, along with all points of tangency, are available to the user upon request. All the real solutions are shown in red, as seen on the right in Figure 3.

When seeing this output, the user might ask a number of questions. For instance, among the real conics that were computed, how many are ellipses and how many are hyperbolas? Our web interface answers this question. The distinction between ellipses and hyperbolas is characterized by the eigenvalues of the real symmetric matrix
\[
\begin{pmatrix}
2u_1 & u_2 \\
u_2 & 2u_3
\end{pmatrix}.
\]

If the two eigenvalues of this matrix have opposite signs, then the conic is a hyperbola. If they have the same sign, then the conic is an ellipse. Among the ellipses, we might ask for the solution which looks most like a circle. Our program does this by minimizing the expression $(u_1 - u_3)^2 + u_2^2$. Users with a numerical analysis background might like to see the conic which maximizes the distance to the variety of degenerate conics. Equivalently, we ask that, among all 3264 solutions, the $3 \times 3$ matrix in (7) has the smallest condition number.

Most importantly, you can adapt this for your favorite geometry problems. As pointed out above, the Julia package HomotopyContinuation.jl is available to everyone – follow the link at [6]. This may enable you to solve your own polynomial systems in record time.

**Chow Rings, Pentagons, and Real Conics**

In what follows we first present the approach to deriving the number 3264 that would be taught in an algebraic geometry class, along the lines of the article [1]. We then discuss the geometric degeneration that was used to construct the fully real instance in Proposition 1.
Steiner phrased his problem as that of solving five equations of degree six on the five-dimensional space $\mathbb{P}_C^5$. The incorrect count occurred because of the locus of double conics in $\mathbb{P}_C^5$. This locus is a surface of extraneous solutions. One fixes the problem by replacing $\mathbb{P}_C^5$ with another five-dimensional manifold, namely the space of complete conics. This space is the blow-up of $\mathbb{P}_C^5$ at the locus of double conics. It is a compactification of the space of nonsingular conics that has desirable geometric properties. A detailed description of this construction, suitable for a first course in algebraic geometry, can be found in [1, §5.1].

In order to answer enumerative geometry questions about the space of complete conics, one considers its Chow ring, as explained in [1, §5.2]. This ring contains two special classes $P$ and $L$. The class $P$ encodes the conics passing through a fixed point, while the class $L$ encodes the conics tangent to a fixed line. The following relations hold in the Chow ring:

$$P^5 = L^5 = 1, \quad P^4L = PL^4 = 2 \quad \text{and} \quad P^3L^2 = P^2L^3 = 4.$$  

These relations are derived in [1, §4.4–5.3]. See [1, Table 3] for the geometric meaning. Readers wishing to study Chow rings in general are referred to the book by Eisenbud and Harris [9]. The Chow ring for the space of complete conics is worked out in [9, §8.2.4].

We write $C$ for the class of conics tangent to a given conic. In the Chow ring, we have

$$C = 2P + 2L.$$  

This identity is derived by a Chow ring calculation in [1, equation (8)]. Our preferred proof of this equation is to inspect the first three terms in the expression (4) for the tact invariant:

$$T(A,U) = 16 \cdot u_6^2(4u_3u_6 - u_5^2)^2 \cdot a_1^4a_2^3 \mod \langle a_2, a_3, a_4, a_5, a_6 \rangle.$$  

This has the following interpretation: We assume that the given fixed quadric $A$ satisfies

$$|a_1| \gg |a_3| \gg \{|a_2|, |a_4|, |a_5|, |a_6|\}.$$  

Thus the quadric $A$ is very close to $x^2 - \epsilon y^2$, where $\epsilon$ is a small quantity. The process of letting $\epsilon$ tend to zero is understood as a degeneration in the sense of algebraic geometry. With this, the condition for $U$ to be tangent to $A$ degenerates to $u_6^2 \cdot (4u_3u_6 - u_5^2)^2 = 0$.

The first factor $u_6$ represents all conics that pass through the point $(0,0)$, while the second factor $4u_3u_6 - u_5^2$ represents all conics that are tangent to the line $\{x = 0\}$. The Chow ring classes of these factors are $P$ and $L$. Each of these arises with multiplicity 2, as seen from the exponents. The desired intersection number is now obtained from the Binomial Theorem:

$$C^5 = 32(L + P)^5 = 32 \cdot (L^5 + 5L^4P + 10L^3P^2 + 10L^2P^3 + 5LP^4 + P^5) = 32 \cdot (1 + 5 \cdot 2 + 10 \cdot 4 + 10 \cdot 4 + 5 \cdot 2 + 1) = 32 \cdot 102 = 3264.$$  

The final step in turning this into a rigorous proof of Chasles’s result is carried out in [1, §7].

The degeneration idea in [11] can be used to construct real instances of Steiner’s problem whose 3264 solutions are all real. This was first observed by Fulton, and worked out in detail by Ronga, Tognoli and Vust [11] and Sottile [13, 14]. One fixes a convex pentagon in $\mathbb{R}^2$ and one special point somewhere in the relative interior of each edge. Consider all conics $C$
such that, for each edge of the pentagon, $C$ either passes through the special point or is tangent to the line spanned by the edge. By the count above, there are $(L + P)^5 = 102$ such conics $C$ and they are all real. We now replace each pointed edge by a nearby hyperbola, satisfying \((11)\). For instance, if the edge has equation $x = 0$ and $(0,0)$ is its special point then we take the hyperbola $x^2 - \epsilon y^2 + \delta z^2$, where $\epsilon > \delta > 0$ are very small. After making appropriate choices of these parameters along all edges of the pentagon, each of the 102 conics splits into 32 conics, each tangent to the five hyperbolas. All 3264 conics are real.

The argument shows that there exists an instance in the neighborhood of the pentagon construction $(L+P)^5$, whose 3264 conics are all real, but it does not say how close they should be. Serious hands-on experimentation was necessary for finding the instance in Proposition 1.

The space of complete conics is a compactification of the space of smooth conics. In the boundary of that compactification we find pairs of lines as well as double lines with a marked point. That point remembers the intersection point of two lines that were degenerated into a double line. Remembering such marked points is very important in algebraic geometry.

The idea of marked points leads to an alternative algebraic formulation of our problem, where we remember the five points of tangency on each solution conic. The five sextics in \((6)\) did not involve these points. They were obtained directly from the tact invariant.

The following alternative formulation of Steiner’s conic problem as a system of polynomial equations avoids the use of the tact invariant. It uses five copies of the triple \((1)–(3)\), each with a different point of tangency $(x_i, y_i)$, for $i = 1, 2, 3, 4, 5$. The ten equations from \((1)\) and \((2)\) are quadrics. The five equations from \((3)\) are cubics. Altogether, we get the following system of 15 equations that we display as a $5 \times 3$ matrix:

$$F_{(A,B,C,D,E)}(x) = \begin{bmatrix} A(x_1, y_1) & U(x_1, y_1) & (\frac{\partial A}{\partial x} \cdot \frac{\partial U}{\partial y} - \frac{\partial A}{\partial y} \cdot \frac{\partial U}{\partial x})(x_1, y_1) \\ B(x_2, y_2) & U(x_2, y_2) & (\frac{\partial B}{\partial x} \cdot \frac{\partial U}{\partial y} - \frac{\partial B}{\partial y} \cdot \frac{\partial U}{\partial x})(x_2, y_2) \\ C(x_3, y_3) & U(x_3, y_3) & (\frac{\partial C}{\partial x} \cdot \frac{\partial U}{\partial y} - \frac{\partial C}{\partial y} \cdot \frac{\partial U}{\partial x})(x_3, y_3) \\ D(x_4, y_4) & U(x_4, y_4) & (\frac{\partial D}{\partial x} \cdot \frac{\partial U}{\partial y} - \frac{\partial D}{\partial y} \cdot \frac{\partial U}{\partial x})(x_4, y_4) \\ E(x_5, y_5) & U(x_5, y_5) & (\frac{\partial E}{\partial x} \cdot \frac{\partial U}{\partial y} - \frac{\partial E}{\partial y} \cdot \frac{\partial U}{\partial x})(x_5, y_5) \end{bmatrix}.$$  

(12)

Each matrix entry is a polynomial in the 15 entries of

$$x = (u_1, u_2, u_3, u_4, u_5, x_1, y_1, x_2, y_2, x_3, y_3, x_4, y_4, x_5, y_5).$$  

(13)

The parameters of this system are the coefficients of the five given conics $A, B, C, D, E$. The system of five equations in five variables $U = (u_1, u_2, u_3, u_4, u_5)$ seen in \((6)\) is obtained by eliminating the 10 variables $x_1, y_1, x_2, y_2, x_3, y_3, x_4, y_4, x_5, y_5$ from the system $F_{(A,B,C,D,E)}(x)$.

At first glance, it looks like the new formulation \((12)\) is worse than the one in \((6)\). Indeed, the number of variables has increased from 6 to 15, and the Bézout number has increased from $6^5 = 7776$ to $2^{10}3^5 = 248832$. However, the new formulation is better suited for the numerical solver that powers our website. We explain this in the last section.
Approximate Solutions and Certification

Steiner’s conic problem amounts to solving a system of polynomial equations. Two formulations were given in ([6] and [12]). But what does “solving” actually mean? One answer is suggested in the textbook by Cox, Little and O’Shea [7]: Solving means computing a Gröbner basis \( G \). Indeed, crucial invariants, like the dimension and degree of the solution variety, are encoded in \( G \). The number of real solutions is found by applying techniques like Sturm sequences to the polynomials in \( G \). Yet, while Gröbner bases are nice in theory, they can take a very long time to compute. We found them impractical for Steiner’s problem.

Computing 3264 conics in a second requires numerical methods. Our encoding of the solutions are not Gröbner bases but numerical approximations. How does one make this rigorous? This question can be phrased as follows. Suppose \( u_1, \ldots, u_6 \) are the true coordinates of a solution and \( u_1 + \Delta u_1, \ldots, u_6 + \Delta u_6 \) are approximations of those complex numbers. How small must the norms of \( \Delta u_1, \ldots, \Delta u_6 \) be before it is justified to call them approximations?

Is there a global definition of “small”? Those questions are elegantly circumvented by using Smale’s definition of approximate zero; see [5, Definition 1 in §8]:

**Definition 3** (Approximate zero). Let \( F(x) = (f_1(x), \ldots, f_n(x)) \) be a system of \( n \) polynomials in \( n \) variables and \( JF(x) \) its \( n \times n \) Jacobian matrix. A point \( z \in \mathbb{C}^n \) is an approximate zero of \( F \) if there exists a zero \( \zeta \in \mathbb{C}^n \) of \( F \) such that the sequence of Newton iterates

\[
z_{k+1} = N_F(z_k), \quad \text{where} \quad N_F(x) = \begin{cases} x - JF(x)^{-1}F(x), & \text{if } JF(x) \text{ is invertible} \\ x, & \text{else} \end{cases}
\]

starting at \( z_0 = z \) satisfies

\[ \|z_{k+1} - \zeta\| \leq \frac{1}{2} \|z_k - \zeta\|^2 \quad \text{for all } k = 1, 2, 3, \ldots \]

If this holds, then we call \( \zeta \) the associated zero of \( z \). Here \( \|x\| := (\sum_{i=1}^{n} x_i \bar{x}_i)^{1/2} \) is the standard norm in \( \mathbb{C}^n \), and the zero \( \zeta \) is assumed to be nonsingular, i.e. \( \det(JF(\zeta)) \neq 0 \).

The reader should think of approximate zeros as a data structure representing solutions to polynomial systems, just like a Gröbner basis is a data structure, too. Different types of representations of data provide different levels of accessibility to the desired information. For instance, approximate zeros are not well suited for computing algebraic features of an ideal. But they are a powerful tool for answering geometric questions in a fast and reliable manner.

Suppose that \( z \) is a point in \( \mathbb{C}^n \) whose real and imaginary part are rational numbers. How can we tell whether \( z \) is an approximate zero of \( F \)? This is not clear from the definition.

It is possible to certify that \( z \) is an approximate zero without dealing with the infinitely many steps of the algorithm. We next explain how this works. This involves the two numbers

\[
\beta(F, z) = \|JF(z)^{-1}F(z)\| \quad \text{and} \quad \gamma(F, z) = \max_{k \geq 2} \frac{1}{k!} \|JF(z)^{-1}D^k F(z)\|^\frac{1}{k-1},
\]

where \( D^k F(z) \) is the tensor of order-\( k \) derivatives at \( z \), the tensor \( JF(z)^{-1}D^k F(z) \) is understood as a multilinear map \( (\mathbb{C}^n)^k \to \mathbb{C}^n \), and the norm is \( \|A\| := \max_{\|v\|=1} \|A(v, \ldots, v)\| \).
Smale’s α-number is defined as the product of the β-number and the γ-number:

$$\alpha(F, z) = \beta(F, z) \cdot \gamma(F, z).$$

Shub and Smale \[12\] derived an upper bound for \(\gamma(F, z)\) which can be computed exactly. Based on the next theorem, one can thus decide algorithmically if \(z\) is an approximate zero, using only data of the point \(z\) itself. The following result is \[5\, Theorem 4 in Chapter 8\].

**Theorem 4** (Smale’s α-theorem). If \(\alpha(F, z) < 0.03\), then the point \(z\) is an approximate zero of the system \(F\). Furthermore, if \(y \in \mathbb{C}^n\) is any point with \(\|y - z\| < (20\gamma(F, z))^{-1}\), then \(y\) is also an approximate zero of \(F\) with the same associated zero \(\zeta\) as \(z\).

Actually, Smale’s α-theorem is more general in the sense that \(\alpha_0 = 0.03\) and \(t_0 = 20\) can be replaced by any two positive numbers \(\alpha_0\) and \(t_0\) that satisfy a certain list of inequalities. In order to simplify our exposition, we decided to incorporate \[5\, Remark 6 in Chapter 8\] into the theorem, which says that \(\alpha_0 = 0.03\) and \(t_0 = 20\) do the job.

Hauenstein and Sottile \[10\] use this theorem in an algorithm, called \texttt{alphaCertified}, that decides if a point \(z \in \mathbb{C}^n\) is an approximate zero and if two approximate zeros have distinct associated solutions. An implementation is publicly available for download. Furthermore, if the polynomial system \(F\) has only real coefficients, \texttt{alphaCertified} can decide if an associated zero is real. The idea behind this is as follows: let \(z \in \mathbb{C}^n\) be an approximate zero of the system \(F\) with associated zero \(\zeta\). If the coefficients of \(F\) are all real, then the Newton operator \(N_F(x)\) from Definition 3 satisfies \(N_F(\overline{x}) = \overline{N_F(x)}\). This implies that \(\overline{\zeta}\) is also an approximate zero of \(F\) with associated zero \(\overline{\zeta}\). Consequently, if \(\|z - \overline{\zeta}\| < (20\gamma(F, z))^{-1}\), then, by Theorem 4, the associated zeros of \(z\) and \(\overline{\zeta}\) are equal. This means that \(\zeta = \overline{\zeta}\).

A fundamental insight is that Theorem 3 allows us to certify candidates for approximate zeros regardless of how they were obtained. Typically, candidates are found by inexact computations, using floating point arithmetic. But never mind what happens in that computation. We do not need to know, because we can certify the result \textit{a posteriori}. Certification constitutes a rigorous proof of a mathematical result. Let us see this in action.

**Proof of Proposition 1**. Fix the five conics with rational coefficients listed after equation (9). We apply the software \texttt{HomotopyContinuation.jl} \[6\] to compute 3264 solutions in 64-bit floating point arithmetic. The output is inexact. Each coefficient \(u_i\) of each true solution \(U\) is a complex number that is algebraic of degree 3264 over \(\mathbb{Q}\). The floating point numbers that represent these coefficients are rational numbers. And, we treat them as elements of \(\mathbb{Q}\).
Our proof starts with the resulting list of 3264 vectors \( x \in \mathbb{Q}_{15} \) as in (13). The computation was mentioned to make the exposition more friendly. This is not part of the proof.

We are now given 3264 candidates for approximate zeros of the square polynomial system in (12). These candidates have rational coordinates. We use them as input to the software \texttt{alphaCertified} from [10]. That software performs exact computations in rational arithmetic. Its output shows that the 3264 vectors \( x \) are approximate zeros, that their associated zeros \( \zeta \) are distinct, and that they all have real coordinates; see Figure (4). The output data of \texttt{alphaCertified} is available for download on our webpage.

This was a rigorous proof of Proposition [1] just as trustworthy as a human-assisted proof by symbolic computation (e.g. Gröbner bases and Sturm sequences) might have been. Readers who are experts in algebra should not get distracted by the appearance of floating point arithmetic: it is not part of the proof! Floating point numbers are only a tool for obtaining the 3264 candidates. The actual proof is carried out by exact symbolic computations.

How Does This Work?

In this section we discuss the methodology and software that powers the web interface.

We use the software \texttt{HomotopyContinuation.jl} that was developed by two of us [6]. This is a Julia [4] implementation of a computational paradigm called homotopy continuation. The reasons why we choose Julia as the programming language are threefold: the first is that Julia is open source and free for anyone to download. The second is that Julia is fast. For instance, we use Julia’s JIT compiler for fast evaluation of polynomials. Finally, the third reason is that, despite its high performance, Julia still provides an easy high-level syntax. This makes our software accessible for users from many backgrounds. Please try it!

Homotopy continuation works as follows: We wish to find a zero in \( \mathbb{C}^n \) of a system \( F(x) = (f_1(x), \ldots, f_n(x)) \) of \( n \) polynomials in \( n \) variables. Suppose \( G(x) = (g_1(x), \ldots, g_n(x)) \) is another system with a known zero: \( G(\zeta) = 0 \). We connect \( F \) and \( G \) in the space of polynomial systems by a path \( t \mapsto H(x, t) \) with \( H(x, 0) = F(x) \) and \( H(x, 1) = G(x) \).

The aim is to approximately follow the solution path \( x(t) \) defined by \( H(x(t), t) = 0 \). For this, the path is discretized into time steps \( t_0 = 0 < t_1 < \cdots < t_k = 1 \). If the discretization is fine enough then \( \zeta \) is also an approximate zero of \( H(x, t_1) \). Hence, by Definition [3] applying the Newton operator \( N_{H(x, t)}(x) \) to \( \zeta \), we get a sequence \( \zeta_0, \zeta_1, \zeta_2, \ldots \) of points that converges towards a zero \( \xi \) of \( H(x, t_1) \). Then, if \( t_2 - t_1 \) is small enough and if \( \| \zeta_i - \xi \| \) is small enough for some \( i \geq 0 \), the iterate \( \zeta_i \) is an approximate zero of \( H(x, t_2) \). We may repeat the procedure for \( H(x, t_2) \) and starting with \( \zeta_i \). Inductively, we find an approximate zero of \( H(x, t_j) \) for all \( j \). In the end, we will find an approximate zero for the system \( F(x) = H(x, t_k) \).

Beltrán and Leykin [3] use Smale’s \( \alpha \)-theorem to quantify the “fine enough” and “small enough” above. They give an algorithm whose output is a certified approximate zero. However, most implementations of homotopy continuation, including \texttt{Bertini} [2] and \texttt{HomotopyContinuation.jl} [6], use heuristics for setting the step-sizes \( t_{j+1} - t_j \) and number of Newton iterations. Heuristics work significantly faster than the certified path tracking [3]. And, most importantly, we can certify our computational results \textit{a posteriori}, via Theorem [4].
Our homotopy for Steiner's conic problem computes zeros of the system \( F_{(A,B,C,D,E)}(x) \). We prefer (12) over (6) because the former equations have lower degree, and high degrees introduce numerical instability in the evaluation of polynomials. We use the homotopy

\[
H(x,t) = F_{((1-t)A'+A,tB+(1-t)B',tC+(1-t)C',tD+(1-t)D',tE+(1-t)E')}(x).
\] (14)

The conic \( tA+(1-t)A' \) has coefficients \( ta_i + (1-t)a'_i \), where \( a'_i \) are the coefficients of \( A \) and \( a_i \) the coefficients of \( A' \). This is called a parameter homotopy in the literature. Geometrically, (14) is a straight line in the space of quintuples of conics. An alternative would have been

\[
\tilde{H}(x,t) = tF_{(A,B,C,D,E)} + (1-t)F_{(A',B',C',D',E')}.
\] (15)

The advantage of (14) over (15) is that the path stays within the space of structured systems \( \{ F_{(A,B,C,D,E)}(x) \mid (A, B, C, D, E) \text{ are conics} \} \). The structure of the equations is preserved: They have 3264 solutions for almost all \( t \), whereas (15) has 7776 solutions for random \( t \). In the language of algebraic geometry, we prefer the flat family (14) over (15), which is not flat.

The last missing piece in our Steiner homotopy is a start system. That is, we need explicit conics \( A, B, C, D, E \) together with all 3264 solutions. Here is how we obtain this data: first we sample six random complex numbers \( u_1, \ldots, u_5 \). Then, we randomly choose five points \( (x_1, y_1), \ldots, (x_5, y_5) \in \mathbb{C}^2 \) on the conic \( U(x,y) = u_1 x^2 + u_2 xy + u_3 y^2 + u_4 x + u_5 y + 1 = 0 \).

This can be done for instance, by computing a parametrization of the conic. Now, for the point \( (x_1, y_1) \) we compute another conic \( A(x,y) = a_1 x^2 + a_2 xy + a_3 y^2 + a_4 x + a_5 y + a_6 \) that is tangent to \( U(x,y) \) at \( (x_1, y_1) \) i.e. a conic that satisfies the linear system \( A(x_1,y_1) = 0 \) and \( \left( \frac{\partial A}{\partial x} \cdot \frac{\partial U}{\partial y} - \frac{\partial A}{\partial y} \cdot \frac{\partial U}{\partial x} \right)(x_1, x_2) = 0 \). Similarly, we obtain conics \( B, C, D, E \) for the other four points. We thus obtain a 5-tuple of conics \( (A, B, C, D, E) \) and a solution of our system (12):

\[
F_{(A,B,C,D,E)}(u_1, u_2, u_3, u_4, u_5, x_1, y_1, x_2, y_2, x_3, y_3, x_4, y_4, x_5, y_5) = 0.
\]

To get the remaining 3263 solutions of the start system, we use the monodromy method due to Duff et al. [8]. For a conic \( U \), consider \( \mathcal{I}(U) = \{(A,x,y) \mid U \text{ is tangent to } A \text{ at } (x,y) \in \mathbb{C}^2 \} \). The incidence variety for our problem is the following union over all conics \( U \):

\[
\mathcal{I} := \bigcup_U \{U\} \times \mathcal{I}(U) \times \mathcal{I}(U) \times \mathcal{I}(U) \times \mathcal{I}(U) \times \mathcal{I}(U).
\]

Computing 3264 solutions translates to computing fibers of the projection \( \pi: \mathcal{I} \to (\mathbb{C}^6)^5 \) from the incidence variety onto the coefficients of the five conics \( A, B, C, D, E \). The projection \( \pi \) gives a branched covering of \( (\mathbb{C}^6)^5 \). A loop in the complement of the branch locus of \( \pi \), which starts and ends at \( (A, B, C, D, E) \), induces a permutations of the fiber \( \pi^{-1}(A, B, C, D, E) \). We exploit this fact and track the one solution \( (U, x_1, y_1, \ldots, x_5, y_5) \) along random loops using our homotopy (14). This procedure gives new solutions in \( \pi^{-1}(A, B, C, D, E) \). We track along random loops until 3264 distinct solutions are found.

In closing, we emphasize the important role played by enumerative geometry. It furnishes a termination criterion for the monodromy method. Of course, we can always run that method. But knowing the number of solutions a priori means knowing when to stop looking for new solutions. This is why numbers like 3264 are so important, and why a numerical analyst might care about Chow rings and the pentagon construction. This underscores how enumerative algebraic geometry and numerical algebraic geometry complement each other.
References

[1] A. Bashelor, A. Ksir and W. Traves: *Enumerative algebraic geometry of conics*, Amer. Math. Monthly 115 (2008) 701–728.

[2] D. Bates, J. Hauenstein, A. Sommese and C. Wampler: *Bertini: Software for Numerical Algebraic Geometry*. Available at www.bertini.nd.edu, dx.doi.org/10.7274/R0H41PB5.

[3] C. Beltrán and A. Leykin: *Certified numerical homotopy tracking*, Experiment. Math. 21 (2012) 69–83.

[4] J. Bezanson, A. Edelman, S. Karpinski and V. Shah: *Julia: A fresh approach to numerical computing*, SIAM Review 59 (2017) 65–98.

[5] L. Blum, F. Cucker, M. Shub and S. Smale: *Complexity and Real Computation*, Springer, 1998.

[6] P. Breiding and S. Timme: *HomotopyContinuation.jl - a package for solving systems of polynomial equations in Julia*, Mathematical Software – ICMS 2018. Lecture Notes in Computer Science. Software available at www.juliahomotopycontinuation.org.

[7] D. Cox, J. Little and D. O'Shea: *Ideals, Varieties, and Algorithms*: An Introduction to Computational Algebraic Geometry and Commutative Algebra, 4th ed., Undergrad. Texts in Math., Springer, 2015.

[8] T. Duff, C. Hill, A. Jensen, K. Lee, A. Leykin and J. Sommars: *Solving polynomial systems via homotopy continuation and monodromy*, IMA Journal of Numerical Analysis (2018).

[9] D. Eisenbud and J. Harris: *3264 And All That – a Second Course in Algebraic Geometry*, Cambridge University Press, 2016.

[10] J. Hauenstein and F. Sottile: *alphaCertified: Certifying Solutions to Polynomial Systems*, ACM Transactions on Mathematical Software (TOMS) 38 (2012), download at www.math.tamu.edu/~sottile/research/stories/alphaCertified/.

[11] F. Ronga, A. Tognoli and T. Vust: *The number of conics tangent to five given conics: the real case*, Rev. Mat. Univ. Complut. Madrid 10 (1997) 391–421.

[12] M. Shub and S. Smale: *Complexity of Bézouts theorem I. Geometric aspects*, J. Amer. Math. Soc. 6 (1993) 459–501.

[13] F. Sottile: *Enumerative geometry for real varieties*, Algebraic geometry – Santa Cruz 1995, 435–447, Proc. Sympos. Pure Math., 62, Part 1, Amer. Math. Soc., Providence, RI, 1997.

[14] F. Sottile: *3264 real conics*, www.math.tamu.edu/~sottile/research/stories/3264/.

[15] A. Sommese and C. Wampler: *The Numerical Solution of Systems of Polynomials Arising in Engineering and Science*, World Scientific, 2005.

[16] S. Timme: *Adaptive step size control for polynomial homotopy continuation methods*, arXiv:1902.02968.

Authors’ addresses:
Paul Breiding, MPI-MiS Leipzig breiding@mis.mpg.de
Bernd Sturmfels, MPI-MiS Leipzig and UC Berkeley bernd@mis.mpg.de
Sascha Timme, TU Berlin timme@math.tu-berlin.de