# University of Massachusetts - Amherst ScholarWorks@UMass Amherst

Mathematics and Statistics Department Faculty Publication Series

Mathematics and Statistics

2000

# An Excursion from Enumerative Geometry to Solving Systems of Polynomial Equations with Macaulay 2

Frank Sottile University of Massachusetts - Amherst, sottile@math.tamu.edu

Follow this and additional works at: http://scholarworks.umass.edu/math\_faculty\_pubs Part of the <u>Physical Sciences and Mathematics Commons</u>

Sottile, Frank, "An Excursion from Enumerative Geometry to Solving Systems of Polynomial Equations with Macaulay 2" (2000). *Mathematics and Statistics Department Faculty Publication Series*. Paper 121. http://scholarworks.umass.edu/math\_faculty\_pubs/121

This Article is brought to you for free and open access by the Mathematics and Statistics at ScholarWorks@UMass Amherst. It has been accepted for inclusion in Mathematics and Statistics Department Faculty Publication Series by an authorized administrator of ScholarWorks@UMass Amherst. For more information, please contact scholarworks@library.umass.edu.

# AN EXCURSION FROM ENUMERATIVE GEOMETRY TO SOLVING SYSTEMS OF POLYNOMIAL EQUATIONS WITH MACAULAY 2

### FRANK SOTTILE

ABSTRACT. Solving a system of polynomial equations is a ubiquitous problem in the applications of mathematics. Until recently, it has been hopeless to find explicit solutions to such systems, and mathematics has instead developed deep and powerful theories about the solutions to polynomial equations. Enumerative Geometry is concerned with counting the number of solutions when the polynomials come from a geometric situation and Intersection Theory gives methods to accomplish the enumeration.

We use *Macaulay 2* to investigate some problems from enumerative geometry, illustrating some applications of symbolic computation to this important problem of solving systems of polynomial equations. Besides enumerating solutions to the resulting polynomial systems, which include overdetermined, deficient, and improper systems, we address the important question of real solutions to these geometric problems.

The text contains evaluated *Macaulay 2* code to illuminate the discussion. This is intended as a chapter in a book on applications of Macaulay 2 to problems in mathematics. While this chapter is largely expository, the results in the last section concerning lines tangent to quadrics are new.

#### 1. INTRODUCTION

A basic question to ask about a system of polynomial equations is its number of solutions. For this, the fundamental result is the following Bézout Theorem.

**Theorem 1.1.1.** The number of isolated solutions to a system of polynomial equations

$$f_1(x_1, \dots, x_n) = f_2(x_1, \dots, x_n) = \dots = f_n(x_1, \dots, x_n) = 0$$

is bounded by  $d_1d_2\cdots d_n$ , where  $d_i := \deg f_i$ . If the polynomials are generic, then this bound is attained for solutions in an algebraically closed field.

Here, isolated is taken with respect to the algebraic closure. This Bézout Theorem is a consequence of the refined Bézout Theorem of Fulton and MacPherson [11, §1.23].

A system of polynomial equations with fewer than this degree bound or Bézout number of solutions is called *deficient*, and there are well-defined classes of deficient systems that satisfy other bounds. For example, fewer monomials lead to fewer solutions, for which polyhedral bounds [4] on the number of solutions are often tighter (and no weaker than) the Bézout number, which applies when all monomials are present. When the polynomials come from geometry, determining the number of solutions is the central problem in enumerative geometry.

Date: 14 November 2000.

<sup>1991</sup> Mathematics Subject Classification. 12D10, 13P10, 14M15, 14M25, 14N10, 14P99, 14Q20, 65H20. Key words and phrases. Enumerative geometry, Grassmannian, Gröbner basis.

Research supported in part by NSF grant DMS-0070494.

Chapter in book: *Computations in Algebraic Geometry with Macaulay 2*, D. Eisenbud, D. Grayson, M. Stillmann, and B. Sturmfels, eds.

Symbolic computation can help compute the solutions to a system of equations that has only isolated solutions. In this case, the polynomials generate a zero-dimensional ideal I. The *degree* of I (dim<sub>k</sub> k[X]/I), which is the number of standard monomials in any term order gives an upper bound on the number of solutions, which is attained when I is radical.

**Example 1.1.2.** We illustrate this discussion with an example. Let  $f_1$ ,  $f_2$ ,  $f_3$ , and  $f_4$  be random quadratic polynomials in the ring  $\mathbb{F}_{101}[y_{11}, y_{12}, y_{21}, y_{22}]$ .

```
i1 : R = ZZ/101[y11, y12, y21, y22];
```

The ideal they generate has dimension 0 and degree  $16 = 2^4$ , which is the Bézout number.

```
i3 : I = ideal PolynomialSystem;
o3 : Ideal of R
i4 : dim I, degree I
o4 = (0, 16)
o4 : Sequence
```

If we restrict the monomials which appear in the  $f_i$  to be among

1,  $y_{11}$ ,  $y_{12}$ ,  $y_{21}$ ,  $y_{22}$ ,  $y_{11}y_{22}$ , and  $y_{12}y_{21}$ ,

then the ideal they generate again has dimension 0, but its degree is now 4.

If we further require that the coefficients of the quadratic terms sum to zero, then the ideal they generate now has degree 2.

In Example 4.4.2, we shall see how this last specialization is geometrically meaningful.

For us, enumerative geometry is concerned with enumerating geometric figures of some kind having specified positions with respect to general fixed figures. That is, counting the solutions to a geometrically meaningful system of polynomial equations. We use *Macaulay 2* to investigate some enumerative geometric problems from this point of view. The problem of enumeration will be solved by computing the degree of the (0-dimensional) ideal generated by the polynomials.

## 2. Solving systems of polynomials

We briefly discuss some aspects of solving systems of polynomial equations. For a more complete survey, see the relevant chapters in [6, 7].

Given an ideal I in a polynomial ring k[X], set  $\mathcal{V}(I) := \operatorname{Spec} k[X]/I$ . When I is generated by the polynomials  $f_1, \ldots, f_N, \mathcal{V}(I)$  gives the set of solutions in affine space to the system

(1) 
$$f_1(X) = \cdots = f_N(X) = 0$$

a geometric structure. These solutions are the *roots* of the ideal I. The degree of a zerodimensional ideal I provides an algebraic count of its roots. The degree of its radical counts roots in the algebraic closure, ignoring multiplicities.

2.1. Excess intersection. Sometimes, only a proper (open) subset of affine space is geometrically meaningful, and we want to count only the meaningful roots of I. Often the roots  $\mathcal{V}(I)$  has positive dimensional components that lie in the complement of the meaningful subset. One way to treat this situation of excess or improper intersection is to saturate I by a polynomial f vanishing on the extraneous roots. This has the effect of working in  $k[X][f^{-1}]$ , the coordinate ring of the complement of  $\mathcal{V}(f)$  [9, Exer. 2.3].

**Example 2.2.1.** We illustrate this with an example. Consider the following ideal in  $\mathbb{F}_{7}[x, y]$ .

i9 : R = ZZ/7[y, x, MonomialOrder=>Lex]; i10 : I = ideal (y<sup>3</sup>\*x<sup>2</sup> + 2\*y<sup>2</sup>\*x + 3\*x\*y, 3\*y<sup>2</sup> + x\*y - 3\*y);

```
ol0 : Ideal of R
```

Since the generators have greatest common factor y, I defines finitely many points together with the line y = 0. Saturate I by the variable y to obtain the ideal J of isolated roots.

i11 : J = saturate(I, ideal(y))

```
4 3 2
o11 = ideal (x + x + 3x + 3x, y - 2x - 1)
```

```
oll : Ideal of R \,
```

The first polynomial factors completely in  $\mathbb{F}_7[x]$ ,

i12 : factor(J\_0) o12 = (x - 2)(x + 1)(x + 2)(x)(1)o12 : Product

and so the isolated roots of I are (0, 1), (2, 5), (5, 4), and (6, 6).

Here, the extraneous roots came from a common factor in both equations. A less trivial example of this phenomenon will be seen in Section 5.2.

2.2. Elimination, rationality, and solving. Elimination theory can be used to study the roots of a zero-dimensional ideal  $I \subset k[X]$ . A polynomial  $h \in k[X]$  defines a map  $k[y] \to k[X]$  (by  $y \mapsto h$ ) and a corresponding projection h: Spec  $k[X] \twoheadrightarrow \mathbb{A}^1$ . The generator  $g(y) \in k[y]$  of the kernel of the map  $k[y] \to k[X]/I$  is called an *eliminant* and it has the property that  $\mathcal{V}(g) = h(\mathcal{V}(I))$ . When h is a coordinate function  $x_i$ , we may consider the eliminant to be in the polynomial ring  $k[x_i]$ , and we have  $\langle g(x_i) \rangle = I \cap k[x_i]$ . The most important result concerning eliminants is the Shape Lemma [2].

#### FRANK SOTTILE

**Shape Lemma.** Suppose h is a linear polynomial and g is the corresponding eliminant of a zero-dimensional ideal  $I \subset k[X]$  with  $\deg(I) = \deg(g)$ . Then the roots of I are defined in the splitting field of g and I is radical if and only if g is square-free.

Suppose further that  $h = x_1$  so that  $g = g(x_1)$ . Then, in the lexicographic term order with  $x_1 < x_2 < \cdots < x_n$ , I has a Gröbner basis of the form:

(2) 
$$g(x_1), x_2 - g_2(x_1), \dots, x_n - g_n(x_1),$$

where  $\deg(g) > \deg(g_i)$  for  $i = 2, \ldots, n$ .

When k is infinite and I is radical, an eliminant g given by a generic linear polynomial h will satisfy deg(g) = deg(I). Enumerative geometry counts solutions when the fixed figures are generic. We are similarly concerned with the generic situation of deg(g) = deg(I). In this case, eliminants provide a useful computational device to study further questions about the roots of I. For instance, the Shape Lemma holds for the ideal of Example 2.2.1. Its eliminant, which is the polynomial J\_0, factors completely over the ground field  $\mathbb{F}_7$ , so all four solutions are defined in  $\mathbb{F}_7$ . In Section 4.3, we will use eliminants in another way, to show that an ideal is radical.

Given a polynomial h in a zero-dimensional ring k[X]/I, the procedure eliminant(h, k[y]) finds a linear relation modulo I among the powers  $1, h, h^2, \ldots, h^d$  of h with d minimal and returns this as a polynomial in k[y]. This procedure is included in the Macaulay 2 package realroots.m2.

```
i13 : load "realroots.m2"
i14 : code eliminant
o14 = -- code for eliminant:
      -- realroots.m2:65-81
      eliminant = (h, C) \rightarrow (
            Z := C_0;
            A := ring h;
            assert( dim A == 0 );
            F := coefficientRing A;
            assert( isField F );
            assert( F == coefficientRing C );
            B := basis A;
            d := numgens source B;
            M := fold((M, i) -> M ||
                       substitute(contract(B, h^(i+1)), F),
                       substitute(contract(B, 1_A), F),
                       flatten subsets(d, d));
            N := ((ker transpose M)).generators;
P := matrix {toList apply(0..d, i -> Z^i)} * N;
                  (flatten entries(P))_0
            )
```

o14 : Net

Here, M is a matrix whose rows are the normal forms of the powers 1,  $h, h^2, \ldots, h^d$  of h, for d the degree of the ideal. The columns of the kernel N of **transpose** M are a basis of the linear relations among these powers. The matrix P converts these relations into polynomials. Since N is in column echelon form, the initial entry of P is the relation of minimal degree. (This method is often faster than naïvely computing the kernel of the map  $k[Z] \to A$  given by  $Z \mapsto h$ , which is implemented by eliminantNaive(h, Z).

Suppose we have an eliminant  $g(x_1)$  of a zero-dimensional ideal  $I \subset k[X]$  with  $\deg(g) = \deg(I)$ , and we have computed the lexicographic Gröbner basis (2). Then the roots of I

are

(3) 
$$\{(\xi_1, g_2(\xi_1), \dots, g_n(\xi_1)) \mid g(\xi_1) = 0\}$$

Suppose now that  $k = \mathbb{Q}$  and we seek floating point approximations for the (complex) roots of I. Following this method, we first compute floating point solutions to  $g(\xi) = 0$ , which give all the  $x_1$ -coordinates of the roots of I, and then use (3) to find the other coordinates. The difficulty here is that enough precision may be lost in evaluating  $g_i(\xi_1)$  so that the result is a poor approximation for the other components  $\xi_i$ .

2.3. Solving with linear algebra. We describe another method based upon numerical linear algebra. When  $I \subset k[X]$  is zero-dimensional, A = k[X]/I is a finite-dimensional k-vector space, and any Gröbner basis for I gives an efficient algorithm to compute ring operations using linear algebra. In particular, multiplication by  $h \in A$  is a linear transformation  $m_h : A \to A$  and the command regularRep(h) from realroots.m2 gives the matrix of  $m_h$  in terms of the standard basis of A.

i15 : code regularRep

```
o15 = -- code for regularRep:
    -- realroots.m2:97-102
    regularRep = f -> (
        assert( dim ring f == 0 );
        b := basis ring f;
        k := coefficientRing ring f;
        substitute(contract(transpose b, f*b), k)
        )
```

```
o15 : Net
```

Since the action of A on itself is faithful, the minimal polynomial of  $m_h$  is the eliminant corresponding to h. The procedure charPoly(h, Z) in realroots.m2 computes the characteristic polynomial det $(Z \cdot Id - m_h)$  of h.

```
i16 : code charPoly
```

```
o16 = -- code for charPoly:
    -- realroots.m2:108-116
    charPoly = (h, Z) -> (
        A := ring h;
        F := coefficientRing A;
        S := F[Z];
        Z = value Z;
        mh := regularRep(h) ** S;
        Idz := S_0 * id_(S^(numgens source mh));
        det(Idz - mh)
        )
```

o16 : Net

When this is the minimal polynomial (the situation of the Shape Lemma), this procedure often computes the eliminant faster than does eliminant, and for systems of moderate degree, much faster than naïvely computing the kernel of the map  $k[Z] \to A$  given by  $Z \mapsto h$ .

The eigenvalues and eigenvectors of  $m_h$  give another algorithm for finding the roots of I. The engine for this is the following result.

**Stickelberger's Theorem.** Let  $h \in A$  and  $m_h$  be as above. Then there is a one-to-one correspondence between eigenvectors  $\mathbf{v}_{\xi}$  of  $m_h$  and roots  $\xi$  of I, the eigenvalue of  $m_h$  on  $\mathbf{v}_{\xi}$  is the value  $h(\xi)$  of h at  $\xi$ , and the multiplicity of this eigenvalue (on the eigenvector  $\mathbf{v}_{\xi}$ ) is the multiplicity of the root  $\xi$ .

#### FRANK SOTTILE

Since the linear transformations  $m_h$  for  $h \in A$  commute, the eigenvectors  $\mathbf{v}_{\xi}$  are common to all  $m_h$ . Thus we may compute the roots of a zero-dimensional ideal  $I \subset k[X]$  by first computing floating-point approximations to the eigenvectors  $\mathbf{v}_{\xi}$  of  $m_{x_1}$ . Then the root  $\xi = (\xi_1, \ldots, \xi_n)$  of I corresponding to the eigenvector  $\mathbf{v}_{\xi}$  has *i*th coordinate satisfying

(4) 
$$m_{x_i} \cdot \mathbf{v}_{\xi} = \xi_i \cdot \mathbf{v}_{\xi}.$$

An advantage of this method is that we may use structured numerical linear algebra after the matrices  $m_{x_i}$  are precomputed using exact arithmetic. (These matrices are typically sparse and have additional structures which may be exploited.) Also, the coordinates  $\xi_i$ are *linear* functions of the floating point entries of  $\mathbf{v}_{\xi}$ , which affords greater precision than the non-linear evaluations  $g_i(\xi_1)$  in the method based upon elimination. While in principle only one of the deg(I) components of the vectors in (4) need be computed, averaging the results from all components can improve precision.

2.4. Real Roots. Determining the real roots of a polynomial system is a challenging problem with real world applications. When the polynomials come from geometry, this is the main problem of real enumerative geometry. Suppose  $k \subset \mathbb{R}$  and  $I \subset k[X]$  is zero-dimensional. If g is an eliminant of k[X]/I with  $\deg(g) = \deg(I)$ , then the real roots of g are in 1-1 correspondence with the real roots of I. Since there are effective methods for counting the real roots of a univariate polynomial, eliminants give a naïve, but useful method for determining the number of real roots to a polynomial system. (For some applications of this technique in mathematics, see [19, 22, 23].)

The classical symbolic method of Sturm, based upon Sturm sequences, counts the number of real roots of a univariate polynomial in an interval. When applied to an eliminant satisfying the Shape Lemma, this method counts the number of real roots of the ideal. This is implemented in *Macaulay 2* via the command SturmSequence(f) of realroots.m2

```
i17 : code SturmSequence
```

```
o17 = -- code for SturmSequence:
    -- realroots.m2:120-134
    SturmSequence = f -> (
        assert( isPolynomialRing ring f );
        assert( numgens ring f === 1 );
        R := ring f;
        assert( char R == 0 );
        x := R_0;
        n := first degree f;
        c := new MutableList from toList (0 .. n);
        if n >= 0 then (
            c#0 = f;
            if n >= 1 then (
                c#1 = diff(x,f);
                scan(2 .. n, i -> c#i = - c#(i-2) % c#(i-1));
            ));
        toList c)
```

o17 : Net

The last few lines of SturmSequence construct the Sturm sequence of the univariate argument f: This is  $(f_0, f_1, f_2, ...)$  where  $f_0 = f$ ,  $f_1 = f'$ , and for i > 1,  $f_i$  is the normal form reduction of  $-f_{i-2}$  modulo  $f_{i-1}$ . Given any real number x, the variation of f at x is the number of changes in sign of the sequence  $(f_0(x), f_1(x), f_2(x), ...)$  obtained by evaluating the Sturm sequence of f at x. Then the number of real roots of f over an interval [x, y] is the difference of the variation of f at x and at y.

The Macaulay 2 commands numRealSturm and numPosRoots (and also numNegRoots) use this method to respectively compute the total number of real roots and the number of positive roots of a univariate polynomial.

```
i18 : code numRealSturm
```

```
o18 = -- code for numRealSturm:
      -- realroots.m2:161-165
      numRealSturm = f \rightarrow (
           c := SturmSequence f;
           variations (signAtMinusInfinity \ c)
                 variations (signAtInfinity \ c)
           )
o18 : Net
i19 : code numPosRoots
o19 = -- code for numPosRoots:
      -- realroots.m2:170-174
      numPosRoots = f \rightarrow (
           c := SturmSequence f;
           variations (signAtZero \ c)
                - variations (signAtInfinity \ c)
           )
```

```
o19 : Net
```

These use the commands signAt\*(f), which give the sign of f at \*. (Here, \* is one of Infinity, zero, or MinusInfinity. Also variations(c) computes the number of sign changes in the sequence c.

o20 : Net

i21 : code traceForm

A more sophisticated method to compute the number of real roots which can also give information about their location uses the rank and signature of the symmetric trace form. Suppose  $I \subset k[X]$  is a zero-dimensional ideal and set A := k[X]/I. For  $h \in k[X]$ , set  $S_h(f,g) := \operatorname{trace}(m_{hfg})$ . It is an easy exercise that  $S_h$  is a symmetric bilinear form on A. The procedure traceForm(h) in realroots.m2 computes this trace form  $S_h$ .

o21 : Net

The value of this construction is the following theorem.

**Theorem 2.2.2** ([3, 18]). Suppose  $k \subset \mathbb{R}$  and I is a zero-dimensional ideal in  $k[x_1, \ldots, x_n]$ and consider  $\mathcal{V}(I) \subset \mathbb{C}^n$ . Then, for  $h \in k[x_1, \ldots, x_n]$ , the signature  $\sigma(S_h)$  and rank  $\rho(S_h)$ of the bilinear form  $S_h$  satisfy

$$\sigma(S_h) = \#\{a \in \mathcal{V}(I) \cap \mathbb{R}^n : h(a) > 0\} - \#\{a \in \mathcal{V}(I) \cap \mathbb{R}^n : h(a) < 0\}$$
  
$$\rho(S_h) = \#\{a \in \mathcal{V}(I) : h(a) \neq 0\}.$$

That is, the rank of  $S_h$  counts roots in  $\mathbb{C}^n - \mathcal{V}(h)$ , and its signature counts the real roots weighted by the sign of h (which is -1, 0, or 1) at each root. The command traceFormSignature(h) in realroots.m2 returns the rank and signature of the trace form  $S_h$ .

```
i22 : code traceFormSignature
```

```
o22 = -- code for traceFormSignature:
    -- realroots.m2:213-224
    traceFormSignature = h -> (
        A := ring h;
        assert( dim A == 0 );
        assert( char A == 0 );
        S := QQ[Z];
        TrF := traceForm(h) ** S;
        IdZ := Z * id_(S^(numgens source TrF));
        f := det(TrF - IdZ);
        << "The trace form S_h with h = " << h <<
        " has rank " << rank(TrF) << " and signature " <<
        numPosRoots(f) - numNegRoots(f) << endl
        )
```

```
o22 : Net
```

The Macaulay 2 command numRealTrace(A) simply returns the number of real roots of I, given  $\mathbf{A} = k[X]/I$ .

```
i23 : code numRealTrace
o23 = -- code for numRealTrace:
    -- realroots.m2:229-237
    numRealTrace = A -> (
        assert( dim A == 0 );
        assert( char A == 0 );
        S := QQ[Z];
        TrF := traceForm(1_A) ** S;
        IdZ := Z * id_(S^(numgens source TrF));
        f := det(TrF - IdZ);
        numPosRoots(f) -numNegRoots(f)
        )
```

```
o23 : Net
```

**Example 2.2.3.** We illustrate these methods on the following polynomial system.

i24 : R = QQ[x, y]; i25 : I = ideal (1 - x<sup>2</sup>\*y + 2\*x\*y<sup>2</sup>, y - 2\*x - x\*y + x<sup>2</sup>); o25 : Ideal of R The ideal I has dimension zero and degree 5. i26 : dim I, degree I o26 = (0, 5)

o26 : Sequence

We compare the two methods to compute the eliminant of x in the ring R/I.

```
i27 : A = R/I;
i28 : time g = eliminant(x, QQ[Z])
    -- used 0.03 seconds
o28 = Z - 5Z + 6Z + Z - 2Z + 1
o28 : QQ [Z]
i29 : time g = charPoly(x, Z)
    -- used 0.01 seconds
o29 = Z - 5Z + 6Z + Z - 2Z + 1
o29 : QQ [Z]
```

The eliminant has 3 real roots, which we test in two different ways.

i30 : numRealSturm(g), numRealTrace(A)

030 = (3, 3)

```
o30 : Sequence
```

We use Theorem 2.2.2 to isolate these roots in the x, y-plane.

i31 : traceFormSignature(x\*y);

The trace form S\_h with h = x\*y has rank 5 and signature 3

Thus all 3 real roots lie in the first and third quadrants (where xy > 0). We isolate these further.

i32 : traceFormSignature(x - 2);

The trace form  $S_h$  with h = x - 2 has rank 5 and signature 1

This shows that two roots lie in the first quadrant with x > 2 and one lies in the third. Finally, one of the roots lies in the triangle y > 0, x > 2, and x + y < 3.

i33 : traceFormSignature(x + y - 3);

The trace form S\_h with h = x + y - 3 has rank 5 and signature -1

Figure 1 shows these three roots (dots), as well as the lines x + y = 3 and x = 2.

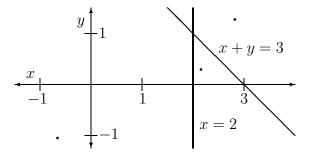


FIGURE 1. Location of roots

2.5. **Homotopy methods.** We describe symbolic-numeric *homotopy continuation methods* for finding approximate complex solutions to a system of equations. These exploit the traditional principles of conservation of number and specialization from enumerative geometry.

Suppose we seek the isolated solutions of a system F(X) = 0 where  $F = (f_1, \ldots, f_n)$  are polynomials in the variables  $X = (x_1, \ldots, x_N)$ . First, a homotopy H(X, t) is found with the following properties:

- 1. H(X, 1) = F(X).
- 2. The isolated solutions of the start system H(X, 0) = 0 are known.
- 3. The system H(X,t) = 0 defines finitely many (complex) curves, and each isolated solution of the original system F(X) = 0 is connected to an isolated solution  $\sigma_i(0)$  of H(X,0) = 0 along one of these curves.

Next, choose a generic smooth path  $\gamma(t)$  from 0 to 1 in the complex plane. Lifting  $\gamma$  to the curves H(X,t) = 0 gives smooth paths  $\sigma_i(t)$  connecting each solution  $\sigma_i(0)$  of the start system to a solution of the original system. The path  $\gamma$  must avoid the finitely many points in  $\mathbb{C}$  over which the curves are singular or meet other components of the solution set H(X,t) = 0.

Numerical path continuation is used to trace each path  $\sigma_i(t)$  from t = 0 to t = 1. When there are fewer solutions to F(X) = 0 than to H(X, 0) = 0, some paths will diverge or become singular as  $t \to 1$ , and it is expensive to trace such a path. The homotopy is *optimal* when this does not occur.

When N = n and the  $f_i$  are generic, set  $G(X) := (g_1, \ldots, g_n)$  with  $g_i = (x_i - 1)(x_i - 2) \cdots (x_i - d_i)$  where  $d_i := \deg(f_i)$ . Then the *Bézout homotopy* 

$$H(X,t) := tF(X) + (1-t)G(X)$$

is optimal. This homotopy furnishes an effective demonstration of the bound in Bézout's Theorem for the number of solutions to F(X) = 0.

When the polynomial system is deficient, the Bézout homotopy is not optimal. When n > N (often the case in geometric examples), the Bézout homotopy does not apply. In either case, a different strategy is needed. Present optimal homotopies for such systems all exploit some structure of the systems they are designed to solve. The current state-of-the-art is described in [27].

**Example 2.2.4.** The Gröbner homotopy [13] is an optimal homotopy that exploits a square-free initial ideal. Suppose our system has the form

 $F := g_1(X), \ldots, g_m(X), \Lambda_1(X), \ldots, \Lambda_d(X)$ 

where  $g_1(X), \ldots, g_m(X)$  form a Gröbner basis for an ideal I with respect to a given term order  $\prec, \Lambda_1, \ldots, \Lambda_d$  are linear forms with  $d = \dim(\mathcal{V}(I))$ , and we assume that the initial ideal in  $\prec I$  is square-free. This last, restrictive, hypothesis occurs for certain determinantal varieties.

As in [9, Chapter 15], there exist polynomials  $g_i(X, t)$  interpolating between  $g_i(X)$  and their initial terms  $in_{\prec}g_i(X)$ 

$$g_i(X;1) = g_i(X)$$
 and  $g_i(X;0) = \operatorname{in}_{\prec} g_i(X)$ 

so that  $\langle g_1(X,t),\ldots,g_m(X,t)\rangle$  is a flat family with generic fibre isomorphic to I and special fibre in I. The *Gröbner homotopy* is

$$H(X,t) := g_1(X,t), \ldots, g_m(X,t), \Lambda_1(X), \ldots, \Lambda_d(X).$$

Since  $\operatorname{in}_{\prec} I$  is square-free,  $\mathcal{V}(\operatorname{in}_{\prec} I)$  is a union of  $\operatorname{deg}(I)$ -many coordinate *d*-planes. We solve the start system by linear algebra. This conceptually simple homotopy is in general not efficient as it is typically overdetermined.

# 3. Some enumerative geometry

We use the tools we have developed to explore the enumerative geometric problems of cylinders meeting 5 general points and lines tangent to 4 spheres.

3.1. Cylinders meeting 5 points. A cylinder is the locus of points equidistant from a fixed line in  $\mathbb{R}^3$ . The Grassmannian of lines in 3-space is 4-dimensional, which implies that the space of cylinders is 5-dimensional, and so we expect that 5 points in  $\mathbb{R}^3$  will determine finitely many cylinders. That is, there should be finitely many lines equidistant from 5 general points. The question is: How many cylinders/lines, and how many of them can be real?

Bottema and Veldkamp [5] show there are 6 *complex* cylinders and Lichtblau [16] observes that if the 5 points are the vertices of a bipyramid consisting of 2 regular tetrahedra sharing a common face, then all 6 will be real. We check this reality on a configuration with less symmetry (so the Shape Lemma holds).

If the axial line has direction  $\mathbf{V}$  and contains the point  $\mathbf{P}$  (and hence has parameterization  $\mathbf{P} + t\mathbf{V}$ ), and if r is the squared radius, then the cylinder is the set of points  $\mathbf{X}$ satisfying

$$0 = r - \left\| \mathbf{X} - \mathbf{P} - \frac{\mathbf{V} \cdot (\mathbf{X} - \mathbf{P})}{\|\mathbf{V}\|^2} \mathbf{V} \right\|^2.$$

Expanding and clearing the denominator of  $\|\mathbf{V}\|^2$  yields

(5) 
$$0 = r \|\mathbf{V}\|^2 + [\mathbf{V} \cdot (\mathbf{X} - \mathbf{P})]^2 - \|\mathbf{X} - \mathbf{P}\|^2 \|\mathbf{V}\|^2.$$

We consider cylinders containing the following 5 points, which form an asymmetric bipyramid.

```
i34 : Points = {{2, 2, 0}, {1, -2, 0}, {-3, 0, 0},

{0, 0, 5/2}, {0, 0, -3}};

Suppose that \mathbf{P} = (0, y_{11}, y_{12}) and \mathbf{V} = (1, y_{21}, y_{22}).

i35 : R = QQ[r, y11, y12, y21, y22];

i36 : P = matrix{{0, y11, y12}};

o36 : Matrix R <--- R

i37 : V = matrix{{1, y21, y22}};

o37 : Matrix R <--- R

We construct the ideal given by evaluating the polynomial (5) at each of the five points.

i38 : Points = matrix Points ** R;
```

o39 : Ideal of R

This ideal has dimension 0 and degree 6.

i40 : dim I, degree I

040 = (0, 6)

o40 : Sequence

There are 6 real roots, and they correspond to real cylinders (with r > 0).

i41 : A = R/I; numPosRoots(charPoly(r, Z))

042 = 3

3.2. Lines tangent to 4 spheres. We now ask for the lines having a fixed distance from 4 general points. Equivalently, these are the lines mutually tangent to 4 spheres. Since the Grassmannian of lines is four-dimensional, we expect there to be only finitely many such lines. Macdonald, Pach, and Theobald [17] show that there are indeed 12 lines, and that all 12 may be real. This problem makes geometric sense over any field k not of characteristic 2, and the derivation of the number 12 is also valid for algebraically closed fields not of characteristic 2.

A sphere in  $k^3$  is  $\mathcal{V}(q(1, \mathbf{x}))$ , where q is a quadratic form on  $k^4$  and  $\mathbf{x} \in k^3$ . If our field does not have characteristic 2, then there is a symmetric  $4 \times 4$  matrix M such that  $q(\mathbf{u}) = \mathbf{u}M\mathbf{u}^t$ .

A line  $\ell$  having direction V and containing the point P is tangent to the sphere defined by q when the univariate polynomial in s

$$q((1, \mathbf{P}) + s(0, \mathbf{V})) = q(1, \mathbf{P}) + 2s(1, \mathbf{P})M(0, \mathbf{V})^{t} + s^{2}q(0, \mathbf{V}),$$

has a double root. Thus its discriminant vanishes, giving the equation

(6) 
$$((1,\mathbf{P})M(0,\mathbf{V})^t)^2 - (1,\mathbf{P})M(1,\mathbf{P})^t \cdot (0,\mathbf{V})M(0,\mathbf{V})^t = 0.$$

The matrix M of the quadratic form q of the sphere with center (a, b, c) and squared radius r is constructed by Sphere(a,b,c,r).

i43	:	Sphere	= (a,	b, c, r)	-> (							
		-	matri	ix{{a^2 +	$b^{2} + c^{2}$	- r	,-	-a	,-	-b	,-c	},
				{	-a		,	1	,	0	, 0	},
				{	-b		,	0	,	1	, 0	},
				{	-c		,	0	,	0	, 1	}}
			);									

If a line  $\ell$  contains the point  $\mathbf{P} = (0, y_{11}, y_{12})$  and  $\ell$  has direction  $\mathbf{V} = (1, y_{21}, y_{22})$ , then tangentTo(M) is the equation for  $\ell$  to be tangent to the quadric  $uMu^T = 0$  determined by the matrix M.

The ideal of lines having distance  $\sqrt{5}$  from the four points (0,0,0), (4,1,1), (1,4,1), and (1,1,4) has dimension zero and degree 12.

Thus there are 12 lines whose distance from those 4 points is  $\sqrt{5}$ . We check that all 12 are real.

i48 : A = R/I;

i49 : numRealSturm(eliminant(y11 - y12 + y21 + y22, QQ[Z]))

o49 = 12

Since no eliminant given by a coordinate function satisfies the hypotheses of the Shape Lemma, we took the eliminant with respect to the linear form  $y_{11} - y_{12} + y_{21} + y_{22}$ .

This example is an instance of Lemma 3 of [17]. These four points define a regular tetrahedron with volume V = 9 where each face has area  $A = \sqrt{3^5}/2$  and each edge has length  $e = \sqrt{18}$ . That result guarantees that all 12 lines will be real when  $e/2 < r < A^2/3V$ , which is the case above.

## 4. Schubert calculus

The classical Schubert calculus of enumerative geometry concerns linear subspaces having specified positions with respect to other, fixed subspaces. For instance, how many lines in  $\mathbb{P}^3$  meet four given lines? (See Example 4.4.2.) More generally, let 1 < r < n and suppose that we are given general linear subspaces  $L_1, \ldots, L_m$  of  $k^n$  with dim  $L_i = n - r + 1 - l_i$ . When  $l_1 + \cdots + l_m = r(n - r)$ , there will be a finite number  $d(r, n; l_1, \ldots, l_m)$  of r-planes in  $k^n$  which meet each  $L_i$  non-trivially. This number may be computed using classical algorithms of Schubert and Pieri (see [15]).

The condition on r-planes to meet a fixed (n-r+1-l)-plane non-trivially is called a *(special) Schubert condition*, and we call the data  $(r, n; l_1, \ldots, l_m)$  *(special) Schubert data*. The *(special) Schubert calculus* concerns this class of enumerative problems. We give two polynomial formulations of this special Schubert calculus, consider their solutions over  $\mathbb{R}$ , and end with a question for fields of arbitrary characteristic.

4.1. Equations for the Grassmannian. The ambient space for the Schubert calculus is the Grassmannian of r-planes in  $k^n$ , denoted  $\mathbf{G}_{r,n}$ . For  $H \in \mathbf{G}_{r,n}$ , the rth exterior product of the embedding  $H \to k^n$  gives a line

$$k \simeq \wedge^r H \longrightarrow \wedge^r k^n \simeq k^{\binom{n}{r}}$$

This induces the Plücker embedding  $\mathbf{G}_{r,n} \hookrightarrow \mathbb{P}^{\binom{n}{r}-1}$ . If H is the row space of an r by n matrix, also written H, then the Plücker embedding sends H to its vector of  $\binom{n}{r}$  maximal minors. Thus the r-subsets of  $\{0, \ldots, n-1\}$ ,  $\mathbb{Y}_{r,n} := \mathtt{subsets}(\mathbf{n}, \mathbf{r})$ , index Plücker coordinates of  $\mathbf{G}_{r,n}$ . The Plücker ideal of  $\mathbf{G}_{r,n}$  is therefore the ideal of algebraic relations among the maximal minors of a generic r by n matrix.

We create the coordinate ring  $k[p_{\alpha} \mid \alpha \in \mathbb{Y}_{2,5}]$  of  $\mathbb{P}^9$  and the Plücker ideal of  $\mathbf{G}_{2,5}$ . The Grassmannian  $\mathbf{G}_{r,n}$  of *r*-dimensional subspaces of  $k^n$  is also the Grassmannian of *r*-1-dimensional affine subspaces of  $\mathbb{P}^{n-1}$ . Macaulay 2 uses this alternative indexing scheme.

i50 : R = ZZ/101[apply(subsets(5,2), i -> p\_i )];

i51 : I = Grassmannian(1, 4, R)
o51 = ideal (p p - p p + p t + p p , p , p ...
{2, 3} {1, 4} - {1, 3} {2, 4} + {1, 2} {3, 4} + {2, 3} ...
o51 : Ideal of R
This projective variety has dimension 6 and degree 5
i52 : dim(Proj(R/I)), degree(I)
o52 = (6, 5)

```
o52 : Sequence
```

#### FRANK SOTTILE

This ideal has an important combinatorial structure [26, Example 11.9]. We write each  $\alpha \in \mathbb{Y}_{r,n}$  as an increasing sequence  $\alpha \colon \alpha_1 < \cdots < \alpha_r$ . Given  $\alpha, \beta \in \mathbb{Y}_{r,n}$ , consider the two-rowed array with  $\alpha$  written above  $\beta$ . We say  $\alpha \leq \beta$  if each column weakly increases. If we sort the columns of an array with rows  $\alpha$  and  $\beta$ , then the first row is the meet  $\alpha \wedge \beta$  (greatest lower bound) and the second row the join  $\alpha \vee \beta$  (least upper bound) of  $\alpha$  and  $\beta$ . These definitions endow  $\mathbb{Y}_{r,n}$  with the structure of a distributive lattice. Figure 2 shows  $\mathbb{Y}_{2.5}$ .

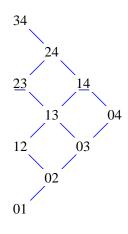


FIGURE 2.  $\mathbb{Y}_{2,5}$ 

We give  $k[p_{\alpha}]$  the degree reverse lexicographic order, where we first order the variables  $p_{\alpha}$  by lexicographic order on their indices  $\alpha$ .

**Theorem 4.4.1.** The reduced Gröbner basis of the Plücker ideal with respect to this degree reverse lexicographic term order consists of quadratic polynomials

$$g(\alpha,\beta) = p_{\alpha} \cdot p_{\beta} - p_{\alpha \vee \beta} \cdot p_{\alpha \wedge \beta} + lower terms in \prec,$$

for each incomparable pair  $\alpha, \beta$  in  $\mathbb{Y}_{r,n}$ , and all lower terms  $\lambda p_{\gamma} \cdot p_{\delta}$  in  $g(\alpha, \beta)$  satisfy  $\gamma \leq \alpha \wedge \beta$  and  $\alpha \vee \beta \leq \delta$ .

The form of this Gröbner basis implies that the standard monomials are the sortable monomials, those  $p_{\alpha}p_{\beta}\cdots p_{\gamma}$  with  $\alpha \leq \beta \leq \cdots \leq \gamma$ . Thus the Hilbert function of  $\mathbf{G}_{r,n}$  may be expressed in terms of the combinatorics of  $\mathbb{Y}_{r,n}$ . For instance, the dimension of  $\mathbf{G}_{r,n}$  is the rank of  $\mathbb{Y}_{r,n}$ , and its degree is the number of maximal chains. From Figure 2, these are 6 and 5 for  $\mathbb{Y}_{2,5}$ , confirming our previous calculations.

Since the generators  $g(\alpha, \beta)$  are linearly independent, this Gröbner basis is also a minimal generating set for the ideal. The displayed generator in o51,

$$p_{\{2,3\}}p_{\{1,4\}} - p_{\{1,3\}}p_{\{2,4\}} - p_{\{1,2\}}p_{\{3,4\}}$$

is g(23, 14), and corresponds to the underlined incomparable pair in Figure 2. Since there are 5 such incomparable pairs, the Gröbner basis has 5 generators. As  $\mathbf{G}_{2,5}$  has codimension 3, it is not a complete intersection. This shows how the general enumerative problem from the Schubert calculus gives rise to an overdetermined system of equations in this global formulation.

The Grassmannian has a useful system of local coordinates given by  $\operatorname{Mat}_{r,n-r}$  as follows (7)  $Y \in \operatorname{Mat}_{r,n-r} \longmapsto \operatorname{rowspace} [I_r : Y] \in \mathbf{G}_{r,n}.$  Let L be a (n - r + 1 - l)-plane in  $k^n$  which is the row space of a n - r + 1 - l by n matrix, also written L. Then L meets  $X \in \mathbf{G}_{r,n}$  non-trivially if

maximal minors of 
$$\begin{bmatrix} L \\ X \end{bmatrix} = 0.$$

Laplace expansion of each minor along the rows of X gives a linear equation in the Plücker coordinates. In the local coordinates (substituting  $[I_r : Y]$  for X), we obtain multilinear equations of degree min $\{r, n-r\}$ . These equations generate a prime ideal of codimension l.

Suppose each  $l_i = 1$  in our enumerative problem. Then in the Plücker coordinates, we have the Plücker ideal of  $\mathbf{G}_{r,n}$  together with r(n-r) linear equations, one for each (n-r)-plane  $L_i$ . By Theorem 4.4.1, the Plücker ideal has a square-free initial ideal, and so the Gröbner homotopy of Example 2.2.4 may be used to solve this enumerative problem.

**Example 4.4.2.**  $\mathbf{G}_{2,4} \subset \mathbb{P}^5$  has equation

(8) 
$$p_{\{1,2\}}p_{\{0,3\}} - p_{\{1,3\}}p_{\{0,2\}} + p_{\{2,3\}}p_{\{0,1\}} = 0$$

The condition for  $H \in \mathbf{G}_{2,4}$  to meet a 2-plane L is the vanishing of

(9) 
$$p_{\{1,2\}}L_{34} - p_{\{1,3\}}L_{24} + p_{\{2,3\}}L_{14} + p_{\{1,4\}}L_{23} - p_{\{2,4\}}L_{13} + p_{\{3,4\}}L_{12},$$

where  $L_{ij}$  is the (i, j)th maximal minor of L.

If  $l_1 = \cdots = l_4 = 1$ , we have 5 equations in  $\mathbb{P}^5$ , one quadratic and 4 linear, and so by Bézout's Theorem there are two 2-planes in  $k^4$  that meet 4 general 2-planes non-trivially. This means that there are 2 lines in  $\mathbb{P}^3$  meeting 4 general lines. In local coordinates, (9) becomes

$$L_{34} - L_{14}y_{11} + L_{13}y_{12} - L_{24}y_{21} + L_{23}y_{22} + L_{12}(y_{11}y_{22} - y_{12}y_{21})$$

This polynomial has the form of the last specialization in Example 1.1.2.

4.2. Reality in the Schubert calculus. Like the other enumerative problems we have discussed, enumerative problems in the special Schubert calculus are fully real in that all solutions can be real [21]. That is, given any Schubert data  $(r, n; l_1, \ldots, l_m)$ , there exist subspaces  $L_1, \ldots, L_m \subset \mathbb{R}^n$  such that each of the  $d(r, n; l_1, \ldots, l_m)$  r-planes that meet each  $L_i$  are themselves real.

This result gives some idea of which choices of the  $L_i$  give all *r*-planes real. Let  $\gamma$  be a fixed rational normal curve in  $\mathbb{R}^n$ . Then the  $L_i$  are linear subspaces osculating  $\gamma$ . More concretely, suppose that  $\gamma$  is the standard rational normal curve,  $\gamma(s) = (1, s, s^2, \ldots, s^{n-1})$ . Then the *i*-plane  $L_i(s) := \langle \gamma(s), \gamma'(s), \ldots, \gamma^{(i-1)}(s) \rangle$  osculating  $\gamma$  at  $\gamma(s)$  is the row space of the matrix given by oscPlane(i, n, s).

(In o55, the exponents of s are displayed in line:  $s^2$  is written s2. Macaulay 2 uses this notational convention to display matrices efficiently.)

**Theorem 4.4.3** ([21]). For any Schubert data  $(r, n; l_1, \ldots, l_m)$ , there exist real numbers  $s_1, s_2, \ldots, s_m$  such that there are  $d(r, n; l_1, \ldots, l_m)$  r-planes that meet each osculating plane  $L_i(s_i)$ , and all are real.

The inspiration for looking at subspaces osculating the rational normal curve to study real enumerative geometry for the Schubert calculus is the following very interesting conjecture of Boris Shapiro and Michael Shapiro, or more accurately, extensive computer experimentation based upon their conjecture [19, 22, 23, 28].

**Shapiros's Conjecture.** For any Schubert data  $(r, n; l_1, \ldots, l_m)$  and for all real numbers  $s_1, s_2, \ldots, s_m$  there are  $d(r, n; l_1, \ldots, l_m)$  r-planes that meet each osculating plane  $L_i(s_i)$ , and all are real.

In addition to Theorem 4.4.3, (which replaces the quantifier *for all* by *there exist*), the strongest evidence for this Conjecture is the following result of Eremenko and Gabrielov [10].

**Theorem 4.4.4.** Shapiros's Conjecture is true when either r or n - r is 2.

We test an example of this conjecture for the Schubert data  $(3, 6; 1^3, 2^3)$ , (where  $a^b$  is a repeated b times). The algorithms of the Schubert calculus predict that  $d(3, 6; 1^3, 2^3) = 6$ . The function spSchub(r, L, P) computes the ideal of r-planes meeting the row space of L in the Plücker coordinates  $P_{\alpha}$ .

We are working in the Grassmannian of 3-planes in  $\mathbb{C}^6$ .

i57 : R = QQ[apply(subsets(6,3), i -> p\_i )];

The ideal *I* consists of the special Schubert conditions for the 3-planes to meet the 3planes osculating the rational normal curve at the points 1, 2, and 3, and to also meet the 2-planes osculating at 4, 5, and 6, together with the Plücker ideal Grassmannian(2, 5, R). Since this is a 1-dimensional homogeneous ideal, we add the linear form  $p_{0,1,5}$ - 1 to make the ideal zero-dimensional. As before, Grassmannian(2, 5, R) creates the Plücker ideal of  $G_{3,6}$ .

```
o58 : Ideal of R
```

This has dimension 0 and degree 6, in agreement with the Schubert calculus.

i59 : dim I, degree I

059 = (0, 6)

o59 : Sequence

As expected, all roots are real.

i60 : A = R/I; numRealSturm(eliminant(p\_{2,3,4}, QQ[Z]))

061 = 6

There have been many checked instances of this conjecture [22, 23, 28], and it has some geometrically interesting generalizations [24].

The question remains for which numbers  $0 \le d \le d(r, n; l_1, \ldots, l_m)$  do there exist real planes  $L_i$  with  $d(r, n; l_1, \ldots, l_m)$  r-planes meeting each  $L_i$ , and exactly d of them are real. Besides Theorem 4.4.3 and the obvious parity condition, nothing is known in general. In every known case, every possibility occurs—which is not the case in all enumerative problems, even those that are fully real<sup>1</sup>. Settling this (for d = 0) has implications for linear systems theory [19].

4.3. Transversality in the Schubert calculus. A basic principle of the classical Schubert calculus is that the intersection number  $d(r, n; l_1, \ldots, l_m)$  has enumerative significancethat is, for general linear subspaces  $L_i$ , all solutions appear with multiplicity 1. This basic principle is not known to hold in general. For fields of characteristic zero, Kleiman's Transversality Theorem [14] establishes this principle. When r or n-r is 2, then Theorem E of [20] establishes this principle in arbitrary characteristic. We conjecture that this principle holds in general; that is, for arbitrary infinite fields and any Schubert data, if the planes  $L_i$  are in general position, then the resulting zero-dimensional ideal is radical.

We test this conjecture on the enumerative problem of Section 4.2, which is not covered by Theorem E of [20]. The function testTransverse(F) tests transversality for this enumerative problem, for a given field F. It does this by first computing the ideal of the enumerative problem using random planes  $L_i$ .

and the Plücker ideal of the Grassmannian  $G_{3,6}$  Grassmannian(2, 5, R).) Then it adds a random (inhomogeneous) linear relation 1 + random(1, R) to make the ideal zerodimensional for generic  $L_i$ . When this ideal is zero dimensional and has degree 6 (the expected degree), it computes the characteristic polynomial g of a generic linear form. If g has no multiple roots, 1 == gcd(g, diff(Z, g)), then the Shape Lemma guarantees that the ideal was radical. testTransverse exits either when it computes a radical ideal, or after limit iterations (which is set to 5 for these examples), and prints the return status.

```
i63 : testTransverse = F -> (
    R := F[apply(subsets(6, 3), i -> q_i)];
    continue := true;
    j := 0;
    limit := 5;
    while continue and (j < limit) do (
        j = j + 1;
        I := fold((J, i) -> J +
            spSchub(3, randL(R, 6, 3, 1), q) +
            spSchub(3, randL(R, 6, 3, 2), q),
        Grassmannian(2, 5, R) +
            ideal (1 + random(1, R)),
            {0, 1, 2});
        if (dim I == 0) and (degree I == 6) then (
            lin := promote(random(1, R), (R/I));
        g := charPoly(lin, Z);
        continue = not(1 == gcd(g, diff(Z, g)));
        ));
    if continue then << "Failed for the prime " << char F <<
        " with " << j << " iterations" << endl;
        if not continue then << "Succeeded for the prime " << char F <<
            char F << " in " << j << " iteration(s)" << endl;
        if <</pre>
```

<sup>&</sup>lt;sup>1</sup>For example, of the 12 rational plane cubics containing 8 real points in  $\mathbb{P}^2$ , either 8, 10 or 12 can be real, and there are 8 points with all 12 real [8, Proposition 4.7.3].

Since 5 iterations do not show transversality for  $\mathbb{F}_2$ ,

```
i64 : testTransverse(ZZ/2);
```

```
Failed for the prime 2 with 5 iterations
```

we can test transversality in characteristic 2 using the field with four elements,  $\mathbb{F}_4 = GF$  4.

i65 : testTransverse(GF 4); Succeeded for the prime 2 in 3 iteration(s) We do find transverselity for F

We do find transversality for  $\mathbb{F}_7$ .

);

i66 : testTransverse(ZZ/7); Succeeded for the prime 7 in 2 iteration(s)

We have tested transversality for all primes less than 100 in every enumerative problem involving Schubert conditions on 3-planes in  $k^6$ . These include the problem above as well as the problem of 42 3-planes meeting 9 general 3-planes.<sup>2</sup>

# 5. The 12 lines: reprise

The enumerative problems of Section 3 were formulated in local coordinates (7) for the Grassmannian of lines in  $\mathbb{P}^3$  (Grassmannian of 2-dimensional subspaces in  $k^4$ ). When we formulate the problem of Section 3.2 in the global Plücker coordinates of Section 4.1, we find some interesting phenomena. We also consider some related enumerative problems.

5.1. Global formulation. A quadratic form q on a vector space V over a field k not of characteristic 2 is given by  $q(\mathbf{u}) = (\varphi(\mathbf{u}), \mathbf{u})$ , where  $\varphi \colon V \to V^*$  is a symmetric linear map, that is  $(\varphi(\mathbf{u}), \mathbf{v}) = (\varphi(\mathbf{v}), \mathbf{u})$ . Here,  $V^*$  is the linear dual of V and  $(\cdot, \cdot)$  is the pairing  $V \otimes V^* \to k$ . The map  $\varphi$  induces a quadratic form  $\wedge^r q$  on the *r*th exterior power  $\wedge^r V$  of V through the symmetric map  $\wedge^r \varphi \colon \wedge^r V \to \wedge^r V^* = (\wedge^r V)^*$ . The action of  $\wedge^r V^*$ on  $\wedge^r V$  is given by

(10) 
$$(\mathbf{x}_1 \wedge \mathbf{x}_2 \wedge \cdots \wedge \mathbf{x}_r, \ \mathbf{y}_1 \wedge \mathbf{y}_2 \wedge \cdots \wedge \mathbf{y}_r) = \det |(\mathbf{x}_i, \mathbf{y}_j)|,$$

where  $\mathbf{x}_i \in V^*$  and  $\mathbf{y}_i \in V$ .

When we fix isomorphisms  $V \simeq k^n \simeq V^*$ , the map  $\varphi$  is given by a symmetric  $n \times n$  matrix M as in Section 3.2. Suppose r = 2. Then for  $\mathbf{u}, \mathbf{v} \in k^n$ ,

$$\wedge^2 q(\mathbf{u} \wedge \mathbf{v}) = \det \left[ \begin{array}{cc} \mathbf{u} M \mathbf{u}^t & \mathbf{u} M \mathbf{v}^t \\ \mathbf{v} M \mathbf{u}^t & \mathbf{v} M \mathbf{v}^t \end{array} \right] ,$$

which is Equation (6) of Section 3.2.

**Proposition 5.5.1.** A line  $\ell$  is tangent to a quadric  $\mathcal{V}(q)$  in  $\mathbb{P}^{n-1}$  if and only if its Plücker coordinate  $\wedge^2 \ell \in \mathbb{P}^{\binom{n}{2}-1}$  lies on the quadric  $\mathcal{V}(\wedge^2 q)$ .

Thus the Plücker coordinates for the set of lines tangent to 4 general quadrics in  $\mathbb{P}^3$  satisfy 5 quadratic equations: The single Plücker relation (8) together with one quadratic equation for each quadric. Thus we expect the Bézout number of  $2^5 = 32$  such lines. We check this.

The procedure randomSymmetricMatrix(R, n) generates a random symmetric  $n \times n$  matrix with entries in the base ring of R.

i67 : randomSymmetricMatrix = (R, n) -> (
 entries := new MutableHashTable;
 scan(0..n-1, i -> scan(i..n-1, j ->

<sup>&</sup>lt;sup>2</sup>After this was written, we discovered an elementary proof of transversality for the enumerative problems  $d(r, n; 1^{r(n-r)})$ , where the conditions are all codimension 1 [25].

The procedure tangentEquation(r, R, M) gives the equation in Plücker coordinates for a point in  $\mathbb{P}^{\binom{n}{r}-1}$  to be isotropic with respect to the bilinear form  $\wedge^r M$  (R is assumed to be the coordinate ring of  $\mathbb{P}^{\binom{n}{r}-1}$ ). This is the equation for an *r*-plane to be tangent to the quadric associated to M.

```
i68 : tangentEquation = (r, R, M) -> (
    g := matrix {gens(R)};
    (entries(g * exteriorPower(r, M) * transpose g))_0_0
);
```

We construct the ideal of lines tangent to 4 general quadrics in  $\mathbb{P}^3$ .

o70 : Ideal of R

As expected, this ideal has dimension 0 and degree 32.

```
i71 : dim Proj(R/I), degree I
```

```
o71 = (0, 32)
o71 : Sequence
```

5.2. Lines tangent to 4 spheres. That calculation raises the following question: In Section 3.2, why did we obtain only 12 lines tangent to 4 spheres? To investigate this, we generate the global ideal of lines tangent to the spheres of Section 3.2.

```
o72 : Ideal of R \,
```

We compute the dimension and degree of  $\mathcal{V}(I)$ .

i73 : dim Proj(R/I), degree I

073 = (1, 4)

o73 : Sequence

The ideal is not zero dimensional; there is an extraneous one-dimensional component of zeroes with degree 4. Since we found 12 lines in Section 3.2 using the local coordinates (7), the extraneous component must lie in the complement of that coordinate patch, which is defined by the vanishing of the first Plücker coordinate,  $p_{\{0,1\}}$ . We saturate I by  $p_{\{0,1\}}$  to obtain the desired lines.

i74 : Lines = saturate(I, ideal (p\_{0,1}));

o74 : Ideal of R

This ideal does have dimension 0 and degree 12, so we have recovered the zeroes of Section 3.2.

i75 : dim Proj(R/Lines), degree(Lines)
o75 = (0, 12)
o75 : Sequence

We investigate the rest of the zeroes, which we obtain by taking the ideal quotient of I and the ideal of lines. As computed above, this has dimension 1 and degree 4.

i76 : Junk = I : Lines; o76 : Ideal of R i77 : dim Proj(R/Junk), degree Junk o77 = (1, 4)

o77 : Sequence

We find the support of this extraneous component by taking its radical.

```
i78 : radical(Junk)
```

o78 : Ideal of R  $\,$ 

From this, we see that the extraneous component is supported on an imaginary conic in the  $\mathbb{P}^2$  of lines at infinity.

To understand the geometry behind this computation, observe that the sphere with radius r and center (a, b, c) has homogeneous equation

$$(x - wa)^{2} + (y - wb)^{2} + (z - wc)^{2} = r^{2}w^{2}$$

At infinity, w = 0, this has equation

$$x^2 + y^2 + z^2 = 0.$$

The extraneous component is supported on the set of tangent lines to this imaginary conic. Aluffi and Fulton [1] studied this problem, using geometry to identify the extraneous ideal and the excess intersection formula [12] to obtain the answer of 12. Their techniques show that there will be 12 isolated lines tangent to 4 quadrics which have a smooth conic in common.

When the quadrics are spheres, the conic is the imaginary conic at infinity. Fulton asked the following question: Can all 12 lines be real if the (real) four quadrics share a real conic? We answer his question in the affirmative in the next section.

5.3. Lines tangent to real quadrics sharing a real conic. We consider four quadrics in  $\mathbb{P}^3_{\mathbb{R}}$  sharing a non-singular conic, which we will take to be at infinity so that we may use local coordinates for  $\mathbf{G}_{2,4}$  in our computations. The variety  $\mathcal{V}(q) \subset \mathbb{P}^3_{\mathbb{R}}$  of a nondegenerate quadratic form q is determined up to isomorphism by the absolute value of the signature  $\sigma$  of the associated bilinear form. Thus there are three possibilities, 0, 2, or 4, for  $|\sigma|$ .

When  $|\sigma| = 4$ , the real quadric  $\mathcal{V}(q)$  is empty. The associated symmetric matrix M is conjugate to the identity matrix, so  $\wedge^2 M$  is also conjugate to the identity matrix. Hence  $\mathcal{V}(\wedge^2 q)$  contains no real points. Thus we need not consider quadrics with  $|\sigma| = 4$ .

When  $|\sigma| = 2$ , we have  $\mathcal{V}(q) \simeq S^2$ , the 2-sphere. If the conic at infinity is imaginary, then  $\mathcal{V}(q) \subset \mathbb{R}^3$  is an ellipsoid. If the conic at infinity is real, then  $\mathcal{V}(q) \subset \mathbb{R}^3$  is a hyperboloid of two sheets. When  $\sigma = 0$ , we have  $\mathcal{V}(q) \simeq S^1 \times S^1$ , a torus. In this case,  $\mathcal{V}(q) \subset \mathbb{R}^3$  is a hyperboloid of one sheet and the conic at infinity is real.

Thus either we have 4 ellipsoids sharing an imaginary conic at infinity, which we studied in Section 3.2; or else we have four hyperboloids sharing a real conic at infinity, and there are five possible combinations of hyperboloids of one or two sheets sharing a real conic at infinity. This gives six topologically distinct possibilities in all.

20

**Theorem 5.5.2.** For each of the six topologically distinct possibilities of four real quadrics sharing a smooth conic at infinity, there exist four quadrics having the property that each of the 12 lines in  $\mathbb{C}^3$  simultaneously tangent to the four quadrics is real.

*Proof.* By the computation in Section 3.2, we need only check the five possibilities for hyperboloids. We fix the conic at infinity to be  $x^2 + y^2 - z^2 = 0$ . Then the general hyperboloid of two sheets containing this conic has equation in  $\mathbb{R}^3$ 

(11) 
$$(x-a)^2 + (y-b)^2 - (z-c)^2 + r = 0,$$

(with r > 0). The command Two(a,b,c,r) generates the associated symmetric matrix.

The general hyperboloid of one sheet containing the conic  $x^2 + y^2 - z^2 = 0$  at infinity has equation in  $\mathbb{R}^3$ 

(12) 
$$(x-a)^2 + (y-b)^2 - (z-c)^2 - r = 0$$

(with r > 0). The command One(a,b,c,r) generates the associated symmetric matrix.

i80 : One = (a, b, c, r) -> ( matrix{{a^2 + b^2 - c^2 - r ,-a ,-b , c }, { -a , 1 , 0 , 0 }, { -b , 0 , 1 , 0 }, { c , 0 , 0 ,-1 }} );

We consider *i* quadrics of two sheets (11) and 4-i quadrics of one sheet (12). For each of these cases, the table below displays four 4-tuples of data (a, b, c, r) which give 12 real lines. (The data for the hyperboloids of one sheet are listed first.)

i		Dat	ta	
0	(5, 3, 3, 16),	(5, -4, 2, 1),	(-3, -1, 1, 1),	(2, -7, 0, 1)
1	(3, -2, -3, 6),	(-3, -7, -6, 7),	(-6, 3, -5, 2),	(1, 6, -2, 5)
2	(6, 4, 6, 4),	(-1, 3, 3, 6),	(-7, -2, 3, 3),	(-6, 7, -2, 5)
3	(-1, -4, -1, 1),	(-3, 3, -1, 1),	(-7, 6, 2, 9),	(5, 6, -1, 12)
4	(5, 2, -1, 25),	(6, -6, 2, 25),	(-7, 1, 6, 1),	(3, 1, 0, 1)

We test each of these, using the formulation in local coordinates of Section 3.2. i81 : R = QQ[y11, y12, y21, y22];

21

```
i85 : numRealSturm(charPoly(promote(y22, R/I), Z))
o85 = 12
o86 : Ideal of R
i87 : numRealSturm(charPoly(promote(y22, R/I), Z))
087 = 12
i88 : I = ideal (tangentTo(One(-1,-4,-1, 1))
                     tangentTo(Two(-3, 3, -1, 1)),
tangentTo(Two(-7, 6, 2, 9)),
tangentTo(Two( 5, 6, -1, 12)));
o88 : Ideal of R
i89 : numRealSturm(charPoly(promote(y22, R/I), Z))
089 = 12
i90 : I = ideal (tangentTo(Two( 5, 2,-1,25))
                     tangentTo(Two(6, 2, -6, 2, 25)),
tangentTo(Two(-7, 1, 6, 1)),
tangentTo(Two(3, 1, 0, 1)));
o90 : Ideal of R
i91 : numRealSturm(charPoly(promote(y22, R/I), Z))
091 = 12
```

In each of these enumerative problems, we have checked that every possible number of real solutions (0, 2, 4, 6, 8, 10, or 12) can occur.

5.4. Generalization to higher dimensions. We consider lines tangent to quadrics in higher dimensions. First, we reinterpret the action of  $\wedge^r V^*$  on  $\wedge^r V$  described in (10) as follows. The vectors  $\mathbf{x}_1, \ldots, \mathbf{x}_r$  and  $\mathbf{y}_1, \ldots, \mathbf{y}_r$  define maps  $\alpha \colon k^r \to V^*$  and  $\beta \colon k^r \to V$ . The matrix  $[(\mathbf{x}_i, \mathbf{y}_j)]$  is the matrix of the bilinear form on  $k^r$  given by  $\langle \mathbf{u}, \mathbf{v} \rangle := (\alpha(\mathbf{u}), \beta(\mathbf{v}))$ . Thus (10) vanishes when the bilinear form  $\langle \cdot, \cdot \rangle$  on  $k^r$  is degenerate.

Now suppose that we have a quadratic form q on V given by a symmetric map  $\varphi \colon V \to V^*$ . This induces a quadratic form and hence a quadric on any r-plane H in V (with  $H \not\subset \mathcal{V}(q)$ ). This induced quadric is singular when H is tangent to  $\mathcal{V}(q)$ . Since a quadratic form is degenerate only when the associated projective quadric is singular, we see that H is tangent to the quadric  $\mathcal{V}(q)$  if and only if  $(\wedge^r \varphi(\wedge^r H), \wedge^r H) = 0$ . (This includes the case  $H \subset \mathcal{V}(q)$ .) We summarize this argument.

**Theorem 5.5.3.** Let  $\varphi: V \to V^*$  be a linear map with resulting bilinear form  $(\varphi(\mathbf{u}), \mathbf{v})$ . Then the locus of r-planes in V for which the restriction of this form is degenerate is the set of r-planes H whose Plücker coordinates are isotropic,  $(\wedge^r \varphi(\wedge^r H), \wedge^r H) = 0$ , with respect to the induced form on  $\wedge^r V$ .

When  $\varphi$  is symmetric, this is the locus of r-planes tangent to the associated quadric in  $\mathbb{P}(V)$ .

We explore the problem of lines tangent to quadrics in  $\mathbb{P}^n$ . From the calculations of Section 5.1, we do not expect this to be interesting if the quadrics are general. (This is

borne out for  $\mathbb{P}^4$ : we find 320 lines in  $\mathbb{P}^4$  tangent to 6 general quadrics. This is the Bézout number, as deg  $\mathbf{G}_{2,5} = 5$  and the condition to be tangent to a quadric has degree 2.) This problem is interesting if the quadrics in  $\mathbb{P}^n$  share a quadric in a  $\mathbb{P}^{n-1}$ . We propose studying such enumerative problems, both determining the number of solutions for general such quadrics, and investigating whether or not it is possible to have all solutions be real.

We use Macaulay 2 to compute the expected number of solutions to this problem when r = 2 and n = 4. We first define some functions for this computation, which will involve counting the degree of the ideal of lines in  $\mathbb{P}^4$  tangent to 6 general spheres. Here, X gives local coordinates for the Grassmannian, M is a symmetric matrix, tanQuad gives the equation in X for the lines tangent to the quadric given by M.

**nSphere** gives the matrix M for a sphere with center V and squared radius  $\mathbf{r}$ , and V and  $\mathbf{r}$  give random data for a sphere.

We construct the ambient ring, local coordinates, and the ideal of the enumerative problem of lines in  $\mathbb{P}^4$  tangent to 6 random spheres.

```
o100 : Sequence
```

The expected numbers of solutions we have obtained in this way are displayed in the table below. The numbers in boldface are those which are proven.

n	2	3	4	5	6
# expected	4	12	24	48	96

# Acknowledgements

We thank Dan Grayson and Bernd Sturmfels; Some of the procedures in this chapter were written by Dan Grayson and the calculation in Section 5.2 is due to Bernd Sturmfels.

# INDEX

Macaulay 2, 3, 4, 7, 15, 18 Aluffi, P., 23 artinian, see also ideal, zero-dimensional, 2 Bézout number, 1, 21, 26 Bézout Theorem, 1, 11, 17 bilinear form, 21 signature, 8, 23 symmetric, 8 Bottema, O., 12 cylinder, 12 discriminant, 13 eliminant, 4-6, 14 elimination theory, 4 ellipsoid, 23 enumerative geometry, 1, 3, 4, 10, 11, 14 real, 7, 18 enumerative problem, 3, 11, 14, 20 fully real, 17, 19 Eremenko, A., 18 field algebraically closed, 1, 13 splitting, 4 Fulton, W., 23 Gabrielov, A., 18 Gröbner basis, 4 reduced, 15 Grassmannian, 12–14, 26 local coordinates, 16 not a complete intersection, 16 Grayson, D., 27 Hilbert function, 15 homotopy Bézout, 11 Gröbner, 11, 17 optimal, 11 homotopy continuation, 10 hyperboloid, 23, 24 ideal degree, 2, 3 radical, 2, 4, 19 zero-dimensional, 2, 18, 22 initial ideal square-free, 11, 17 Lichtblau, D., 12 Macdonald, I., 13

Pach, J., 13 Plücker coordinate, 15, 20, 21, 26 Plücker embedding, 15 Plücker ideal, 15 polynomial equations, 1, 3 deficient, 1 overdetermined, 16 quadratic form, 13, 21 rational normal curve, 17, 18 saturate, 3, 22 Schubert calculus, 14, 17–19 Shape Lemma, 4, 19 Shapiro, B., 18 Shapiro, M., 18 Shapiros's Conjecture, 18 solving polynomial equations, 3 real solutions, 6 via eigenvectors, 6 via elimination, 4 via numerical homotopy, 10 sphere, 13, 22, 26 Stickelberger's Theorem, 6 Sturm sequence, 7 Sturmfels, B., 27 symbolic computation, 2

Theobald, Th., 13 trace form, 8

Veldkamp, G., 12

#### References

- [1] P. Aluffi and W. Fulton, 2000. Private Communication.
- [2] E. Becker, M. G. Marinari, T. Mora, and C. Traverso. The shape of the Shape Lemma. In *Proceedings* ISSAC-94, pages 129–133, 1993.
- [3] E. Becker and Th. Wöermann. On the trace formula for quadratic forms. In Recent advances in real algebraic geometry and quadratic forms (Berkeley, CA, 1990/1991; San Francisco, CA, 1991), pages 271–291. Amer. Math. Soc., Providence, RI, 1994.
- [4] D. N. Bernstein. The number of roots of a system of equations. Funct. Anal. Appl., 9:183–185, 1975.
- [5] O. Bottema and G.R. Veldkamp. On the lines in space with equal distances to n given points. Geometrie Dedicata, 6:121–129, 1977.
- [6] A. M. Cohen, H. Cuypers, and H. Sterk, editors. Some Tapas of Computer Algebra. Springer-Varlag, 1999.
- [7] D. Cox, J. Little, and D. O'Shea. Ideals, Varieties, Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra. UTM. Springer-Verlag, New York, 1992.
- [8] A. Degtyarev and V. Kharlamov. Topological properties of real algebraic curves: du côté de chez Rokhlin. www.arXiv.org/math.AG/0004134, 2000.
- D. Eisenbud. Commutative Algebra With a View Towards Algebraic Geometry. Number 150 in GTM. Springer-Verlag, 1995.
- [10] A. Eremenko and A. Gabrielov. Rational functions with real critical points and B. and M. Shapiro conjecture in real enumerative geometry. MSRI preprint 2000-002.
- [11] W. Fulton. Intersection Theory. Number 2 in Ergebnisse der Math. Springer-Verlag, 1984.
- [12] W. Fulton and R. MacPherson. Intersecting cycles on an algebraic variety. In P. Holm, editor, *Real and Complex Singularities*, pages 179–197. Oslo, 1976, Sijthoff and Noordhoff, 1977.
- [13] B. Huber, F. Sottile, and B. Sturmfels. Numerical Schubert calculus. J. Symb. Comp., 26(6):767–788, 1998.
- [14] S. Kleiman. The transversality of a general translate. Compositio Math., 28:287–297, 1974.
- [15] S. Kleiman. and D. Laksov. Schubert calculus. Amer. Math. Monthly, 79:1061–1082, 1972.
- [16] D. Lichtblau. Finding cylinders through 5 points in  $\mathbb{R}^3$ . mss., danl@wolfram.com, 2000.
- [17] I.G. Macdonald, J. Pach, and Th. Theobald. Common tangents to four unit balls in ℝ<sup>3</sup>. Discr. Comput. Geom., to appear, 2000.
- [18] P. Pedersen, M.-F. Roy, and A. Szpirglas. Counting real zeros in the multivariate case. In Computational Algebraic Geometry (Nice, 1992), pages 203–224. Birkhäuser Boston, Boston, MA, 1993.
- [19] J. Rosenthal and F. Sottile. Some remarks on real and complex output feedback. Systems Control Lett., 33(2):73-80, 1998. For a description of the computational aspects, see http://www.nd.edu/~rosen/pole/.
- [20] F. Sottile. Enumerative geometry for the real Grassmannian of lines in projective space. Duke Math. J., 87(1):59–85, 1997.
- [21] F. Sottile. The special Schubert calculus is real. ERA of the AMS, 5:35–39, 1999.
- [22] F. Sottile. The conjecture of Shapiro and Shapiro. An archive of computations and computer algebra scripts, http://www.expmath.org/extra/9.2/sottile, 2000.
- [23] F. Sottile. Real Schubert calculus: Polynomial systems and a conjecture of Shapiro and Shapiro. Exper. Math., 9:161–182, 2000.
- [24] F. Sottile. Some real and unreal enumerative geometry for flag manifolds. Mich. Math. J, 48:573–592, 2000.
- [25] F. Sottile. Elementary transversality in the schubert calculus in any characteristic. math.AG/0010319, 2000.
- [26] Bernd Sturmfels. Gröbner Bases and Convex Polytopes, volume 8 of University Lecture Series. American Math. Soc., Providence, RI, 1996.
- [27] J. Verschelde. Polynomial homotopies for dense, sparse, and determinantal systems. MSRI preprint 1999-041, 1999.
- [28] J. Verschelde. Numerical evidence of a conjecture in real algebraic geometry. Exper. Math., 9:183–196, 2000.

DEPARTMENT OF MATHEMATICS AND STATISTICS, UNIVERSITY OF MASSACHUSETTS, AMHERST, MA, 01003, USA

*E-mail address*: sottile@math.umass.edu *URL*: http://www.math.umass.edu/~sottile