Journal of Software for Algebra and Geometry

```
                              gap> g:= SymmetricGroup( 4 );
                              Sym( [ 1 .. 4 ] )
                              gap> tbl:= CharacterTable( g );;  HasIrr( tbl );
i5 : betti(t,Weights=>{1,0})
                              false
          0 1  2  3 4         gap> tblmod2:= CharacterTable( tbl, 2 );
o5 = total: 1 4 13 14 4       BrauerTable( Sym( [ 1 .. 4 ] ), 2 )
       0: 1  .  .  . .
       1: . 2  2  4 2         gap> tblmod2 = CharacterTable( tbl, 2 );
       2: . 2  5  6 .         true
       3: . . 4  . 2
       4: . . .  . 4          gap> tblmod2 = BrauerTable( tbl, 2 );
       5: . . 2  . .          true

o5 : Betti                    gap> tblmod2 = BrauerTable( tbl, 2 )
i6 : betti(t,Weights=>{0,     true

          0 1  2  3 4         gap> libtbl:= CharacterTable( "M" );
o6 = total: 1 4 13 14 4       CharacterTable( "M" )
       0: 1  .  .  . .        gap> CharacterTableRegular( libtbl, 2 );
                              BrauerTable( "M" )
       3: . . 4  . 2          gap> BrauerTable( libtbl, 2 );
       4: . . .  . 4          fail
       5: . . 2  . .
                              gap> CharacterTable( "Symmetric", 4 );
o6 : BettiTally               CharacterTable( "Sym(4)" )
i7 : t1 = betti(t,Weights=>{1,1})
                              gap> ComputedBrauerTables( tbl );
          0 1  2  3 4         [ , BrauerTable( Sym( [ 1 .. 4 ] ), 2 ) ]
o7 = total: 1 4 13 14 4       option(noprot);
       0: 1 .  .  . .
       1: . .  .  . .         timer=1;
       2: . .  .  . .
       3: . 2  .  . .         ring r2 = 32003,(x,y,z),dp;
       4: . .  .  . .
       5: . 2  .  . .         poly f=imap(r1,f);
       6: . .  1  . .         ideal j=jacob(f);
       7: . .  8  6 .         vdim(std(j));
       8: . .  4  8 4       ==> 536
                              vdim(std(j+f));
o7 : BettiTally             ==> 195
i8 : peek t1
                              timer=0;  // reset timer

o8 = BettiTally{(0, {0, 0}, 0) => 1 }
               (1, {2, 2}, 4) => 2
               (1, {3, 3}, 6) => 2
               (2, {3, 7}, 10) => 2
               (2, {4, 4}, 8) => 1
               (2, {4, 5}, 9) => 4
               (2, {5, 4}, 9) => 4
               (2, {7, 3}, 10) => 2
               (3, {4, 7}, 11) => 4
               (3, {5, 5}, 10) => 6
               (3, {7, 4}, 11) => 4
               (4, {7, 5}, 12) => 2
```

```
ring r1 = 32003,(x,y,z),ds;
int a,b,c,t=11,5,3,0;
poly f = x^a+y^b+z^(3*c)+x^(c+2)*y^(c-1)+x^
         x^(c-2)*y^c*(y^2+t*x)^2;
```

Real solutions to systems of polynomial equations in Macaulay2

Jordy Lopez Garcia, Kelly Maluccio, Frank Sottile and Thomas Yahl

Real solutions to systems of polynomial equations in Macaulay2

JORDY LOPEZ GARCIA, KELLY MALUCCIO, FRANK SOTTILE AND THOMAS YAHL

ABSTRACT: The Macaulay2 package `RealRoots` provides symbolic methods to study real solutions to systems of polynomial equations. It updates and expands an earlier package developed by Grayson and Sottile in 1999. We provide mathematical background and descriptions of the `RealRoots` package, giving examples which illustrate some of its implemented methods. We also prove a general version of Sylvester's theorem whose statement and proof we could not find in the literature.

INTRODUCTION. Understanding the number of real solutions to systems of polynomial equations is fundamental for real algebraic geometry and for applications of algebraic geometry. In 1999, Grayson and Sottile [4] developed the *Macaulay*2 package `realroots` for this purpose. That package had limited functionality, was not documented, and not all of its implemented methods were compatible with modern releases of *Macaulay*2.

The *Macaulay*2 package `RealRoots` expands and modernizes `realroots`, superseding it. `RealRoots` implements symbolic methods for studying real solutions to polynomial systems. This note provides some mathematical background and examples of methods from the package. Its three sections each describe related methods.

Section 1 describes methods for counting and isolating real roots of univariate polynomials, as well as methods for determining if a polynomial is Hurwitz-stable. We give an extension of Sylvester's theorem that we could not find in the literature and sketch its proof.

Section 2 describes methods involving elimination that reduce a zero-dimensional system of multivariate polynomials to a univariate polynomial for solving, studying the number of real solutions, or addressing other arithmetic questions, such as Galois groups.

Section 3 describes a further method for studying zero-dimensional systems based on the trace symmetric form.

1. REAL ROOTS OF UNIVARIATE POLYNOMIALS. Let $f \in \mathbb{R}[x]$ be a polynomial. It has the form

$$f = c_k x^{a_k} + \cdots + c_1 x^{a_1} + c_0 x^{a_0},$$

---

where $a_k > \cdots > a_1 > a_0 \geq 0$ are integers and $c_i \in \mathbb{R}$ is nonzero for each $i = 0, \ldots, k$. Let

$$\mathrm{var}(c_0, \ldots, c_k) := \#\{1 \leq i \leq k \mid c_{i-1}c_i < 0\}$$

be the number of variations in sign of the coefficients of f. Descartes' rule of signs [5] gives an upper bound for the number of positive real roots of f.

Theorem 1 (Descartes' rule of signs). *The number, r, of positive real roots of f, counted with multiplicity, is at most* $\mathrm{var}(c_0, \ldots, c_k)$ *and the difference* $\mathrm{var}(c_0, \ldots, c_k) - r$ *is even.*

Given any sequence $c = (c_0, \ldots, c_k)$, the *variation* $\mathrm{var}(c)$ of c is the number of variations in sign after removing all zero terms.

```
i1 : loadPackage("RealRoots");
i2 : variations {2, -3, 0, -8, 12, 0, 0, 8, -12, 0}
o2 = 3
```

For a sequence of polynomials $f_\bullet = (f_0, \ldots, f_k)$ in $\mathbb{R}[x]$ and $a \in \mathbb{R}$, $\mathrm{var}(f_\bullet, a)$ is the variation in the sequence $(f_0(a), \ldots, f_k(a))$. We extend this to $a \in \{\pm\infty\}$ by taking $f(\infty)$ to be the leading coefficient of $f(x)$ and $f(-\infty)$ to be the leading coefficient of $f(-x)$.

Given a polynomial $f \in \mathbb{R}[x]$ of degree k, consider its sequence of derivatives,

$$\delta f := (f(x), f'(x), f''(x), \ldots, f^{(k)}(x)).$$

For $a < b$ in $\mathbb{R} \cup \{\pm\infty\}$, let $r(f, a, b)$ be the number of roots of f in the interval $(a, b]$, counted with multiplicity. Budan and Fourier [5, Chapter 2] generalized Descartes' rule.

Theorem 2 (Budan and Fourier). *The inequality* $r(f, a, b) \leq \mathrm{var}(\delta f, a) - \mathrm{var}(\delta f, b)$ *holds, and the difference* $\mathrm{var}(\delta f, a) - \mathrm{var}(\delta f, b) - r(f, a, b)$ *is even.*

Descartes' rule is when $a = 0$ and $b = \infty$. Let us consider an example.

```
i3 : R = QQ[x];
i4 : f = x*(2*x - 3)*(x^4 - 2)^2
      10     9     6      5     2
o4 = 2x   - 3x  - 8x  + 12x  + 8x  - 12x
i5 : budanFourierBound(f, 0, infinity)
o5 = 3
i6 : budanFourierBound(f, -2, 1)
o6 = 7
```

Note that $r(f, 0, \infty) = r(f, -2, 1) = 3$, as the real roots of f are $-\sqrt[4]{2}, -\sqrt[4]{2}, 0, \sqrt[4]{2}, \sqrt[4]{2}, \frac{3}{2}$.

In contrast to these bounds, Sylvester's theorem determines the actual number of real roots, and more. The *Sylvester sequence*, $\mathrm{Syl}(f, g)$ of polynomials $f, g \in \mathbb{R}[x]$ is the sequence $(f_0, f_1, \ldots, f_k)$ of nonzero polynomials, where $f_0 := f$, $f_1 := f' \cdot g$, and for $i \geq 1$,

$$f_{i+1} := -1 \cdot \mathrm{remainder}(f_{i-1}, f_i),$$

the negative remainder term in the division of f_{i-1} by f_i. The last nonzero remainder is $f_k = \gcd(f, f'g)$. Observe that for each $1 \leq i \leq k$, there exists $q_i \in \mathbb{R}[x]$ such that

$$f_{i-1} = q_i(x)f_i(x) - f_{i+1}(x). \tag{1}$$

The *reduced Sylvester sequence* $g_\bullet = (g_0, \ldots, g_k)$ is obtained by dividing each term in the Sylvester sequence by $f_k = \gcd(f, f'g)$, so that $g_i f_k = f_i$ for each i. Note that $g_k = 1$, and elements of the reduced Sylvester sequence satisfy (1) with g_j replacing f_j.

Theorem 3 (Sylvester). *Let $f, g \in \mathbb{R}[x]$ and suppose that $g_\bullet$ is the reduced Sylvester sequence of f and g. For $a < b$ in $\mathbb{R} \cup \{\pm\infty\}$,*

$$\mathrm{var}(g_\bullet, a) - \mathrm{var}(g_\bullet, b) = \#\{\zeta \in (a, b] \mid f(\zeta) = 0 \text{ and } g(\zeta) > 0\} - \#\{\zeta \in [a, b) \mid f(\zeta) = 0 \text{ and } g(\zeta) < 0\}.$$

Observe the different roles that the endpoints $\{a, b\}$ play in this formula.

Proof. In [1, Theorem 2.55], Sylvester's theorem is stated and proven when f does not vanish at a or at b, and it is in terms of the Sylvester sequence $\mathrm{Syl}(f, g)$. That proof proceeds by studying $\mathrm{var}(\mathrm{Syl}(f, g), t)$ as t increases from a to b, noting that it may only change when t passes a root of some element of the Sylvester sequence. Since multiplying a sequence by a nonzero number $f_k(t)$ does not change its variation, the proof in [1] establishes this refined version when f does not vanish at a or at b. We proceed with the general case.

Let $g_\bullet$ be the reduced Sylvester sequence of f and g. The variation $\mathrm{var}(g_\bullet, t)$ may only change when t passes a root $\zeta \in [a, b]$ of some g_i in $g_\bullet$. Observe that ζ cannot be a root of two consecutive elements of $g_\bullet$. If it were, then by (1) and induction, it is a root of all elements of $g_\bullet$, and thus of $g_k = 1$, which is a contradiction. Suppose that $g_i(\zeta) = 0$ for some $i \geq 1$. By (1) again, $g_{i-1}(x)$ and $g_{i+1}(x)$ have opposite signs for x near ζ, and thus g_{i-1}, g_i, g_{i+1} do not contribute to any change in $\mathrm{var}(g_\bullet, t)$ for t near ζ. This remains true if $\zeta = a$ and t increases from a or if $\zeta = b$ and t approaches b.

We now suppose that $g_0(\zeta) = 0$, and thus $g_1(\zeta) \neq 0$. Then $f(\zeta) = 0$. Let m be the multiplicity of the root ζ of f so that

$$f = (x - \zeta)^m h, \quad \text{with } h(\zeta) \neq 0.$$

If $g(\zeta) = 0$, then $(x - \zeta)^m$ divides $f'g$ and thus f_k, and so $g_0 = f/f_k$ does not vanish at ζ. Thus, $g(\zeta) \neq 0$.

Notice that $h_0 := f/(x - \zeta)^{m-1}$ and $h_1 := f'g/(x - \zeta)^{m-1}$ have the same signs for x near ζ as do g_0 and g_1. A computation reveals that $h_1 = mhg + (x - \zeta)h'g$. Choose $\epsilon > 0$ so that ζ is the only root of any element in $g_\bullet$ lying in the interval $[\zeta - \epsilon, \zeta + \epsilon]$. Then

x	$h_0(x)$	$h_1(x)$
$\zeta - \epsilon$	$-\epsilon h(\zeta - \epsilon)$	$mh(\zeta - \epsilon)g(\zeta - \epsilon) - \epsilon h'(\zeta - \epsilon)g(\zeta - \epsilon)$
ζ	0	$mh(\zeta)g(\zeta)$
$\zeta + \epsilon$	$\epsilon h(\zeta - \epsilon)$	$mh(\zeta + \epsilon)g(\zeta + \epsilon) + \epsilon h'(\zeta + \epsilon)g(\zeta + \epsilon)$

Suppose that $g(\zeta) > 0$. Then the sign of h_1 on $[\zeta - \epsilon, \zeta + \epsilon]$ is opposite to the sign of $h_0(\zeta - \epsilon)$, but the same as the sign of $h_0(\zeta + \epsilon)$. Thus the variation $\mathrm{var}(g_\bullet, t)$ decreases by 1 as t passes from $\zeta - \epsilon$ to ζ, but is unchanged as t passes from ζ to $\zeta + \epsilon$.
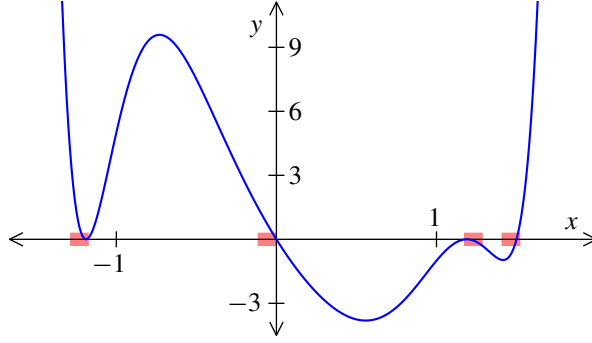
Figure 1. Graph of f.

Suppose that $g(\zeta) < 0$. Then the sign of h_1 on $[\zeta - \epsilon, \zeta + \epsilon]$ is the same as the sign of $h_0(\zeta - \epsilon)$, but opposite to the sign of $h_0(\zeta + \epsilon)$. Thus the variation $\mathrm{var}(g_\bullet, t)$ is unchanged as t passes from $\zeta - \epsilon$ to ζ, but increases by 1 as t passes from ζ to $\zeta + \epsilon$.

Now consider the variation $\mathrm{var}(g_\bullet, t)$ for $t \in [a, b]$. This may only change at a number $\zeta \in [a, b]$ if $f(\zeta) = 0$. If $g(\zeta) > 0$ and $\zeta \neq b$, then it decreases by 1. If $g(\zeta) < 0$ and $\zeta \neq a$, then it increases by 1. It is otherwise unchanged. This completes the proof. □

The *Sturm sequence* of a polynomial $f \in \mathbb{R}[x]$ is the Sylvester sequence $\mathrm{Syl}(f, 1)$. The *reduced Sturm sequence* of f is the reduced Sylvester sequence of f and 1.

Corollary 4 (Sturm's theorem). *Let $f \in \mathbb{R}[x]$ and $a < b$ in $\mathbb{R} \cup \{\pm\infty\}$. Let $g_\bullet$ be the reduced Sturm sequence of f. Then the number of zeros of f in the interval $(a, b]$ equals $\mathrm{var}(g_\bullet, a) - \mathrm{var}(g_\bullet, b)$.*

Using the reduced Sylvester sequence of f and -1, we obtain the number of zeros of f in $[a, b)$. Let us continue with the same polynomial $f = x(2x - 3)(x^4 - 2)^2$ as before.

```
i7 : sylvesterCount(f, x^2 - 1, -2, 3)

o7 = 2

i8 : sturmCount(f)

o8 = 4
```

Calling `sturmCount(f)` without endpoints a, b returns the total number of real roots of f.

Figure 1 shows the graph of f in a neighborhood of its real roots. Note that $x^2 - 1$ is negative only at the root 0.

An application of Sturm's theorem is to give *isolating intervals*, which are disjoint intervals each containing exactly one real root of f. Our implementation gives a list of pairs $\{p, q\}$ such that $(p, q]$ contains a unique root of f and $q - p$ is less than a user-provided tolerance. The numbers p, q are dyadic, lying in $\mathbb{Z}\left[\frac{1}{2}\right]$, as they are found in a binary search.

```
i9 : realRootIsolation(f, 1/5)
```

$$o9 = \left\{\left\{-\frac{165}{128}, -\frac{75}{64}\right\}, \left\{-\frac{15}{128}, 0\right\}, \left\{\frac{75}{64}, \frac{165}{128}\right\}, \left\{\frac{45}{32}, \frac{195}{128}\right\}\right\}$$

These isolating intervals are shaded in Figure 1.

Thomas [6] observed that recursively iterating Sturm's theorem on $f_k = \gcd(f, f')$ can be used to give the number of real roots of f, counted with multiplicity. This same idea may be used to extend Sylvester's theorem to give the count with multiplicity.

```
i10 : sturmCount(f, -1, 2, Multiplicity => true)
o10 = 4
```

A polynomial $f \in \mathbb{R}[x]$ is *Hurwitz-stable* if its complex roots all have negative real parts. All solutions to the system of constant coefficient ordinary differential equations

$$\dot{y} = Ay$$

are asymptotically stable ($\lim_{t \to \infty} y(t) = 0$) when all eigenvalues ζ of A have negative real part, equivalently when the characteristic polynomial of A is Hurwitz-stable.

Given a polynomial $f = c_k x^k + c_{k-1} x^{k-1} + \cdots + c_0$, let H be the matrix

$$\begin{pmatrix} c_{k-1} & c_{k-3} & \cdots & 0 & 0 \\ c_k & c_{k-2} & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & c_2 & c_0 \end{pmatrix}.$$

For $1 \le i \le k$, the *Hurwitz determinant* Δ_i is the i-th principal minor of H.

Theorem 5 (Hurwitz [3]). *Suppose that $c_k > 0$. Then f is Hurwitz-stable if and only if each Hurwitz determinant $\Delta_1, \ldots, \Delta_k$ is positive.*

`RealRoots` implements both the Hurwitz matrix and this test for Hurwitz-stability.

```
i11 : hurwitzMatrix(x^4 + 5*x^3 + 7*x^2 + 11*x + 13)

o11 = | 5 11 0   0  |
      | 1 7   13 0  |
      | 0 5   11 0  |
      | 0 1   7  13 |
             4         4
o11 : Matrix QQ  <--- QQ
i12 : isHurwitzStable(x^4 + 5*x^3 + 7*x^2 + 11*x + 13)
o12 = false
i13 : isHurwitzStable(x^4 + 9*x^3 + 7*x^2 + 5*x + 3)
o13 = true
```

2. ELIMINATION. Elimination is a classical symbolic method often used to solve systems of equations involving multivariate polynomials. Geometrically, it gives the image of a variety under a polynomial map, such as a coordinate projection. `RealRoots` implements methods for zero-dimensional ideals that reduce their study to that of univariate polynomials.

Let $\mathbb{K}$ be a field and $I \subseteq \mathbb{K}[x_1, \ldots, x_n]$ be a zero-dimensional ideal with scheme $\mathcal{V}(I) \subseteq \mathbb{K}^n$. The Artinian ring

$$R := \mathbb{K}[x_1, \ldots, x_n]/I$$

is a vector space over $\mathbb{K}$ of dimension $d := \text{degree}(I)$, and $\#\mathcal{V}(I) \leq d$. The ring R acts on itself by multiplication. For $f \in R$, let m_f be the operator of multiplication by f: for $g \in R$, $m_f(g) = fg$. By Stickelberger's theorem [2], the eigenvalues of m_f are the values of f at the points of $\mathcal{V}(I)$, and the multiplicity of the eigenvalue λ is the sum of the multiplicities in $\mathcal{V}(I)$ of the inverse images, $f^{-1}(\lambda) \cap \mathcal{V}(I)$.

The (univariate) eliminant g of I with respect to f is the minimal polynomial of m_f. When f is a variable, e.g., $f = x_1$, we have that g is the monic generator of the univariate ideal $I \cap \mathbb{K}[x_1]$. In general, the eliminant generates the kernel of the map $\mathbb{K}[Z] \to R$, where $Z \mapsto f$. The function `regularRepresentation` computes a matrix representing m_f with respect to the standard basis for R. The function `univariateEliminant` returns the minimal polynomial of m_f, with respect to a user-chosen variable (or the default Z).

```
i14 : S = QQ[x,y]
i15 : I = ideal(x^2*y^2-3*x^2-3*y^2+5,-3*x^2*y+2*x*y+4*x*y^2+1)
i16 : f = x + y
i17 : regularRepresentation(f, I)
o17 = (| 1 x x2 xy xy2 y y2 y3 |, | 0 0 1/3    -1/3 -35/4 0 0 -105/16 |)
                                  | 1 0 5/3    0    0     0 0 -1/4    |
                                  | 0 1 -2/3   0    21/4  0 0 63/16   |
                                  | 0 1 -5/3   -2/3 0     1 0 -5/4    |
                                  | 0 0 19/9   7/3  1/2   0 1 23/24   |
                                  | 1 0 -20/9  0    1/4   0 0 -19/48  |
                                  | 0 0 -2/3   0    21/4  1 0 269/48  |
                                  | 0 0 4/3    0    0     0 1 1/2     |
o17 : Sequence
i18 : g = univariateEliminant(f, I)
        8        7         6       5         4         3          2
o18 = 1296Z  - 432Z  - 38223Z  - 4806Z  + 209784Z  + 14172Z  - 430242Z ...
o18 : QQ[Z]
```

The eliminant g of I with respect to f defines the image of the scheme $\mathcal{V}(I)$ under f. When g has degree equal to the degree of I, then f is an isomorphism and thus g may be used to study the scheme $\mathcal{V}(I)$. For example, when both are reduced, g and R have the same Galois group over $\mathbb{K}$. While the eliminant a *priori* only tells us about $f(\mathcal{V}(I))$, when f is *separating* (injective on the points of $\mathcal{V}(I)$), it tells us more about those points. In our running example, both g and I have degree eight. (For I, note that this is the cardinality of the basis in o17.) We see that g is reduced and has four real roots.

```
i19 : T = ring(g)
i20 : gens gb ideal(g, diff(Z,g))
o20 = | 1 |
i21 : sturmCount(g)
o21 = 4
```

Thus $\mathcal{V}(I)$ is reduced and consists of eight points, exactly four of which are real.

A useful variant of the eliminant is a *rational univariate representation* of a zero-dimensional ideal I [1, Section 11.4]. This is a triple (f, χ, ϕ) where f is a linear form that is separating for $\mathcal{V}(I)$, χ is the characteristic polynomial of m_f — which retains the multiplicities of points of $\mathcal{V}(I)$, if not their scheme

structure — and ϕ is a rational map $\phi\colon \mathbb{K} \to \mathbb{K}^n$ that restricts to a bijection between the roots of χ and the points of $\mathcal{V}(I)$.

```
i22 : (f, ch, ph) = rationalUnivariateRepresentation(I);

i23 : f

o23 = x + y

i24 : ch
```

$$o24 = Z^8 - \frac{1}{3}Z^7 - \frac{4247}{144}Z^6 - \frac{89}{24}Z^5 + \frac{8741}{54}Z^4 + \frac{1181}{108}Z^3 - \frac{71707}{216}Z^2 - \frac{2051}{324}Z + \frac{6044}{27}$$

```
i25 : ph
```

$$o25 = \{\frac{864Z^7 + 21348Z^6 - 6066Z^5 - 231771Z^4 - 17610Z^3 + 701286Z^2 + 6986}{5184Z^7 - 1512Z^6 - 114669Z^5 - 12015Z^4 + 419568Z^3 + 21258Z^2 - 430} \cdots$$

```
o25 : List
```

3. TRACE SYMMETRIC FORM.

The remaining methods in `RealRoots` are linear-algebraic and may be used to count the points of $\mathcal{V}(I)$ over any field and to count real points of $\mathcal{V}(I)$ according to the sign of another polynomial, similar to Sylvester's Theorem 3. We demonstrate how this may be used for real root location.

A symmetric bilinear form S in a real vector space R has two basic invariants, its rank $\rho(S)$ and its signature $\sigma(S)$. If we choose a basis for R and thus a corresponding matrix M representing S, then M will be symmetric, and therefore diagonalizable with all eigenvalues real. The rank $\rho(M)$ of M is its number of nonzero eigenvalues, and its signature is the difference

$$\sigma(M) := \#\{\text{positive eigenvalues of } M\} - \#\{\text{negative eigenvalues of } M\}.$$

Sylvester's law of inertia asserts that the rank and signature are independent of the choice of basis, and therefore are invariants of the symmetric form S.

Let $\mathbb{K}$ be any field, let $I \subset \mathbb{K}[x_1, \ldots, x_n]$ be a zero-dimensional ideal, and set $R := \mathbb{K}[x_1, \ldots, x_n]/I$, an Artinian ring. For $f \in R$ (or in $\mathbb{K}[x_1, \ldots, x_n]$), multiplication by f induces an endomorphism m_f of R as in Section 2. For $h \in R$ (or in $\mathbb{K}[x_1, \ldots, x_n]$), we define the symmetric bilinear *trace form*, S_h on R by $S_h(f, g) := \text{trace}(m_{fgh})$. The significance of the trace form is the following theorem:

Theorem 6 [1, Theorem 4.72]. *Suppose that $\mathbb{K}$ is a subfield of $\mathbb{R}$ and $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is a zero-dimensional ideal with scheme $\mathcal{V}(I) \subset \mathbb{C}^n$. For $h \in \mathbb{K}[x_1, \ldots, x_n]$, the rank and signature of the trace form S_h satisfy*

$$\rho(S_h) = \#\{z \in \mathcal{V}(I) \mid h(z) \neq 0\} \quad and \quad \sigma(S_h) = \#\{z \in \mathcal{V}(I) \cap \mathbb{R} \mid h(z) > 0\} - \#\{z \in \mathcal{V}(I) \cap \mathbb{R} \mid h(z) < 0\}. \quad (2)$$

If $\mathbb{K}$ is any field with algebraic closure $\overline{\mathbb{K}}$ and $\mathcal{V}(I)$ is a subscheme of $\overline{\mathbb{K}}^n$, then the rank of the trace form S_h satisfies (2).

The rank of the trace form S_1 is used in `rationalUnivariateRepresentation` to certify that a linear form is separating.
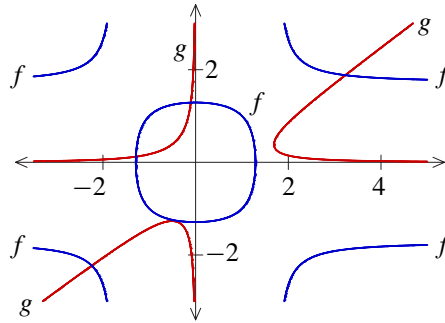
Figure 2. Two real curves.

We demonstrate how this may be used to study the number and location of real zeroes, using the ideal I of Section 2. Let

$$f := x^2y^2 - 3x^2 - 3y^2 + 5 \quad \text{and} \quad g := -3x^2y + 4xy^2 + 2xy + 1.$$

These define two curves in $\mathbb{R}^2$, shown in Figure 2. While they have eight complex points in common, only four are real.

```
i26 : traceCount(I)
o26 = 8
i27 : realCount(I)
o27 = 4
```

We saw this in Section 2, following o21. When $h = 1$, the rank and signature of the trace form S_1 count the complex and real points of $\mathcal{V}(I)$, respectively, and these are implemented as `traceCount(I)` and `realCount(I)`. Thus the possible tangency that we see in the third quadrant is only a near miss.

To see this in another way, consider the signature of the trace form S_{y^2+2y},

```
i28 : signature traceForm(y^2 + 2*y, I)
o28 = 4
```

As this equals the number of real points of $\mathcal{V}(I)$ and $y^2 + 2y < 0$ for $-2 < y < 0$, there are no real points of $\mathcal{V}(I)$ in that horizontal strip, which includes the apparent "near tangency" in Figure 2.

SUPPLEMENT. The online supplement contains version 1.0 of `RealRoots`.

REFERENCES.

[1] S. Basu, R. Pollack, and M.-F. Roy, *Algorithms in real algebraic geometry*, 2nd ed., Algorithms and Computation in Mathematics **10**, Springer, Berlin, 2006. MR Zbl

[2] D. A. Cox, "Stickelberger and the eigenvalue theorem", pp. 283–298 in *Commutative algebra*, edited by I. Peeva, Springer, Cham, 2021. MR Zbl

[3] A. Hurwitz, "Ueber die Bedingungen, unter welchen eine Gleichung nur Wurzeln mit negativen reellen Theilen besitzt", *Math. Ann.* **46**:2 (1895), 273–284. MR Zbl

[4] F. Sottile, "From enumerative geometry to solving systems of polynomials equations", pp. 101–129 in *Computations in algebraic geometry with Macaulay* 2, edited by D. Eisenbud et al., Algorithms Comput. Math. **8**, Springer, Berlin, 2002. MR Zbl

[5] F. Sottile, *Real solutions to equations from geometry*, University Lecture Series **57**, American Mathematical Society, Providence, RI, 2011. MR Zbl

[6] J. M. Thomas, "Sturm's theorem for multiple roots", *Natl. Math. Mag.* **15**:8 (1941), 391–394. MR Zbl

JORDY LOPEZ GARCIA:

jordy.lopez@tamu.edu
Department of Mathematics, Texas A&M University, College Station, TX, United States

KELLY MALUCCIO:

kmaluccio@gmail.com
Department of Mathematics, Austin Community College, Austin, TX, United States

FRANK SOTTILE:

sottile@tamu.edu
Department of Mathematics, Texas A&M University, College Station, TX, United States

THOMAS YAHL:

tyahl@wisc.edu
Department of Mathematics, University of Wisconsin-Madison, Madison, WI, United States