Rational Univariate Representation

In [4] and [6], symbolic recipes apply linear algebra methods to zero-dimensional ideals. Recipes are also given in [1]. Our application is a 6R robot arm [3], [5]. Oversimplifying, we assume $\mathbb{C}$ as number field.

1 Stickelberger's Theorem

A Rational Univariate Representation (abbreviated by RUR) is

$$R = \left\{ p_0(T) = 0,\ x_i = \frac{p_i(T)}{q(T)}, i = 1, 2, \ldots, n \right\} \tag{1}$$

where $p_0, p_1, p_2, \ldots, p_n, q \in \mathbb{C}[T]$. This set R represents the coordinates of the zeroes of a solution set V, $\#V = D < \infty$, of some system of polynomials in $\mathbb{C}[\mathbf{x}]$. D is counted with multiplicities. The number of distinct zeroes in V is denoted by d.

Let the linear form $L(\mathbf{x})$ separate the zeroes: $L(\mathbf{z}_i) \neq L(\mathbf{z}_j)$, for $\mathbf{z}_i$, $\mathbf{z}_j \in V$ $i \neq j$. Consider the multiplication map

$$m_L : \mathbb{C}[\mathbf{x}]/I(V) \rightarrow \mathbb{C}[\mathbf{x}]/I(V) : h \mapsto ((h \cdot L) \rightarrow_{\mathcal{G}_>} r) \tag{2}$$

where $\rightarrow_{\mathcal{G}_>}$ represents the normal form algorithm implemented by the division algorithm using some Gröbner basis $\mathcal{G}_>$. The existence of a separating linear form is demonstrated by the following lemma:

Lemma 1.1 *If V has d distinct zeroes, then at least one of the*

$$u_i(x_1, x_2, x_3, \ldots, x_n) = x_1 + i x_2 + i^2 x_3 + \cdots + i^{n-1} x_n, \quad \text{for} \quad 0 \leq i \leq (n-1) \binom{d}{2} \tag{3}$$

is separating, i.e.: $\forall \mathbf{z}_j, \mathbf{z}_k \in V$, $j \neq k$, $u_i(\mathbf{z}_j) \neq u_i(\mathbf{z}_k)$.

Proof. For the pair $(\mathbf{z}_j, \mathbf{z}_k)$, $j \neq k$, of two distinct zeroes in V with components $\mathbf{z}_j = (z_{j1}, z_{j2}, \ldots, z_{jn})$ $\mathbf{z}_k = (z_{k1}, z_{k2}, \ldots, z_{kn})$, consider the bad situation when $u_t(\mathbf{z}_j) = u_t(\mathbf{z}_k)$, corresponding to

$$p(t) = (z_{j1} - z_{k1}) + (z_{j2} - z_{k2})t + \cdots + (z_{jn} - z_{kn})t^{n-1}. \tag{4}$$

Because $\mathbf{z}_j \neq \mathbf{z}_k$, $p \not\equiv 0$ and therefore p can have at most $n-1$ zeroes. So for each pair of zeroes of V we have at most $n-1$ bad choices for u_i and the number of pairs of zeroes is $d(d-1)/2$, yielding a total of at most $(n-1)d(d-1)/2$ nonseparating u_i's. But the set of u_i's consists of $(n-1)d(d-1)/2 + 1$ elements, so there is at least one separating u_i. □

If no variables separates the zeroes, then eliminating with any variable order will increase multiplicities.

Theorem 1.1 (Stickelberger's theorem) *The multiplication map m_L is a linear map with matrix M_L. The eigenvalues of M_L give values for $L(\mathbf{z})$, for all $\mathbf{z} \in V$, occurring with the same multipliciy $\mu_{\mathbf{z}}$.*

As a consequence of this theorem, we have that $p_0(T)$ is the characteristic polynomial of M_L:

$$p_0(T) = \det(M_L - T I_D) = \prod_{\mathbf{z} \in V} (T - L(\mathbf{z}))^{\mu_{\mathbf{z}}}, \tag{5}$$

with $\mu_{\mathbf{z}}$ the multiplicity of the root.

The trace of M_L is

$$\text{trace}(M_L) = \sum_{\mathbf{z} \in V} \mu_{\mathbf{z}} L(\mathbf{z}). \tag{6}$$

The determinant of M_L is

$$\det(M_L) = \prod_{\mathbf{z} \in V} L(\mathbf{z})^{\mu_{\mathbf{z}}}. \tag{7}$$

2 The Elbow Manipulator

The application in this section is based on [3], but following the original notation of [5].

The elbow manipulator is a spatial robot arm with three links, of lengths L_2, L_3, and L_4. Abbreviating the sines and cosines of the angles θ_i respectively by $s_i = \sin(\theta_i)$ and $c_i = \cos(\theta_i)$, for $i = 1, 2, \ldots, 6$, the successive transformations from one coordinate frame to the next are described by

$$\begin{pmatrix} c_1 & 0 & s_1 & 0 \\ s_1 & 0 & -c_1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_2 & -s_2 & 0 & c_2 L_2 \\ s_2 & c_2 & 0 & s_2 L_2 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_3 & -s_3 & 0 & c_3 L_3 \\ s_3 & c_3 & 0 & s_3 L_3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$
$$\cdot \begin{pmatrix} c_4 & 0 & -s_4 & c_4 L_4 \\ s_4 & 0 & c_4 & s_4 L_4 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_5 & 0 & s_5 & 0 \\ s_5 & 0 & -c_5 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} c_6 & -s_6 & 0 & 0 \\ s_6 & c_6 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} n_x & o_x & a_x & p_x \\ n_y & o_y & a_y & p_y \\ n_z & o_z & a_z & p_z \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad (8)$$

where the matrix at the right of (8) represents the position and orientation of the hand of the robot: $\mathbf{p} = (p_x, p_y, p_z)$ is the position of the origin at the hand, and the tree unit vectors $\mathbf{n} = (n_x, n_y, n_z)$, $\mathbf{o} = (o_x, o_y, o_z)$ and $\mathbf{a} = (a_x, a_y, a_z)$ are respectively called the normal, orientation, and approach vector, related to each other by the cross product $\mathbf{n} = \mathbf{o} \times \mathbf{a}$. In addition to (8), we have the usual relations between the angles, given by

$$c_i^2 + s_i^2 = 1, \quad i = 1, 2, \ldots, 6. \quad (9)$$

Taking one as the value for the three lengths L_2, L_3, and L_4, in [3], the following examples for the matrix at the right of (8) are proposed:

$$\begin{pmatrix} 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 8 \\ 0 & 0 & 1 & 12 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{2}{3} & \frac{1}{3} & \frac{2}{3} & \frac{7}{9} \\ \frac{-1}{3} & \frac{-2}{3} & \frac{2}{3} & \frac{2}{9} \\ \frac{1}{3} & \frac{-2}{3} & \frac{-1}{3} & \frac{5}{9} \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} \frac{3}{7} & \frac{6}{7} & \frac{2}{7} & \frac{1}{9} \\ \frac{2}{7} & \frac{-3}{7} & \frac{6}{7} & \frac{2}{9} \\ \frac{6}{7} & \frac{-2}{7} & \frac{-3}{7} & \frac{4}{9} \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad (10)$$

For these five choices the number of complex solutions equals 8 for each instance, while the number of real solutions equals 0, 4, 4, 8, and 8 respectively.

3 Removing Multiplicities

The *radical* of an ideal I, denoted by $\sqrt{I}$, consists of all polynomial in I with removed multiplicities. For example, if $I = \langle x^2 \rangle$, then $\sqrt{I} = \langle x \rangle$. The quotient ring $A = \mathbb{C}[\mathbf{x}]/\langle I \rangle$ is a finite dimensional vector space. For any h in the quotient ring, we define the *h-trace bilinear form* (TrB):

$$\mathrm{TrB}_h : A \times A \rightarrow \mathbb{C} : (f, g) \mapsto \mathrm{trace}(L_{fgh}) \quad (11)$$

and the *Hermite quadratic form* Q_h:

$$Q_h : A \rightarrow \mathbb{C} : f \mapsto \mathrm{trace}(L_{f^2 h}). \quad (12)$$

The kernel of Q_1 is

$$\ker(Q_1) = \{ \ f \in A \mid \forall g \in A : \mathrm{TrB}_1(f, g) = 0 \ \}. \quad (13)$$

Theorem 3.1 $p \in \sqrt{I} \Leftrightarrow p \in ker(Q_1)$

The proof is based on the formula for the trace:

$$\mathrm{TrB}_1(f, g) = \sum_{\mathbf{z} \in V} \mu_{\mathbf{z}} f(\mathbf{z}) g(\mathbf{z}) = 0, \quad \forall g \in A. \quad (14)$$

For $h = 1$, we write TrB_1 as TrM.

4 Newton Identities

A polynomial p in one variable x defined by its roots x_1, x_2, x_3, and x_4, written as a monic polynomial:

$$\begin{aligned}
p(x) &= (x-x_1)(x-x_2)(x-x_3)(x-x_4) & (15)\\
&= x^4 - (x_1+x_2+x_3+x_4)x^3 & (16)\\
&\quad + (x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4)x^2 & (17)\\
&\quad - (x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4)x & (18)\\
&\quad + x_1x_2x_3x_4 & (19)\\
&= x^4 - e_1(x_1,x_2,x_3,x_4)x^3 + e_2(x_1,x_2,x_3,x_4)x^2 - e_3(x_1,x_2,x_3,x_4)x + e_4(x_1,x_2,x_3,x_4). & (20)
\end{aligned}$$

The polynomials e_1, e_2, e_3, and e_4 are the elementary symmetric polynomials.

Substituting the roots x_1, x_2, x_3, and x_4 into $p(x) = x^4 - e_1x^3 + e_2x^2 - e_3x + e_4$ gives

$$\begin{aligned}
0 = p(x_1) &= x_1^4 - e_1x_1^3 + e_2x_1^2 - e_3x_1 + e_4, & (21)\\
0 = p(x_2) &= x_2^4 - e_1x_2^3 + e_2x_2^2 - e_3x_2 + e_4, & (22)\\
0 = p(x_3) &= x_3^4 - e_1x_3^3 + e_2x_3^2 - e_3x_3 + e_4, & (23)\\
0 = p(x_4) &= x_4^4 - e_1x_4^3 + e_2x_4^2 - e_3x_4 + e_4. & (24)
\end{aligned}$$

Adding the four relations above leads to

$$0 = s_4 - e_1s_3 + e_2s_2 - e_3s_1 + 4e_4, \qquad (25)$$

where s_1, s_2, s_3, and s_4 are the power sums:

$$\begin{aligned}
s_1 &= x_1+x_2+x_3+x_4, & (26)\\
s_2 &= x_1^2+x_2^2+x_3^2+x_4^2, & (27)\\
s_3 &= x_1^3+x_2^3+x_3^3+x_4^3, & (28)\\
s_4 &= x_1^4+x_2^4+x_3^4+x_4^4. & (29)
\end{aligned}$$

So we can express the power sums in terms of the elementary symmetric polynomials:

$$\begin{aligned}
s_1 &= e_1, & (30)\\
s_2 &= e_1s_1 - 2e_2, & (31)\\
s_3 &= e_1s_2 - e_2s_1 + 3e_3, & (32)\\
s_4 &= e_1s_3 - e_2s_2 + e_3s_1 - 4e_4. & (33)
\end{aligned}$$

The relations above allow the derivations of the power sums from the coefficients of a monic polynomial. Writing the Newton identities in another way:

$$\begin{aligned}
e_1 &= s_1, & (34)\\
2e_2 &= e_1s_1 - s_2, & (35)\\
3e_3 &= e_1s_2 - e_2s_1 + s_3, & (36)\\
4e_4 &= e_1s_3 - e_2s_2 + e_3s_1 - s_4, & (37)
\end{aligned}$$

we see that, given the power sums of the roots, we can derive the coefficients of the monic polynomial that vanishes at those roots.

5 Application of the Newton Identities

We follow [4] and [6] and we derive an expression for the characteristic polynomial p_0. The trace of L^i is

$$s_i = \sum_{\mathbf{z} \in V} \mu_{\mathbf{z}} L^i(\mathbf{z}). \tag{38}$$

If

$$p_0(T) = \sum_{i=0}^{D} b_i T^{D-i}, \quad D = \#V, \quad b_i \in \mathbb{C}[\mathbf{x}], \tag{39}$$

then

$$\frac{p_0'(T)}{p_0(T)} = \sum_{\mathbf{z} \in V} \frac{\mu_{\mathbf{z}}}{T - L(\mathbf{z})} = \sum_{j \geq 0} \frac{\mathrm{trace}(L^j)}{T^{j+1}}. \tag{40}$$

Then

$$p_0'(T) = \sum_{l=0}^{D-1} \sum_{j=0}^{D-l-1} \mathrm{trace}(L^j) b_l T^{D-l-j-1}. \tag{41}$$

Identification of the formula obtained above with the derivative of (39) gives Newton's formula:

$$(D-i) b_i = \sum_{j=0}^{i} \mathrm{trace}(L^j) b_{i-j}. \tag{42}$$

This leads to a linear system to find the coefficients b_i of p_0.

After the computation of the characteristic polynomial $p_0(T)$ of the multiplication map m_L where L is separating for the d solutions in V.

For any $v \in A$, we define

$$g_L(v, T) = \sum_{\mathbf{z} \in V} \mu_{\mathbf{z}} v(\mathbf{z}) \prod_{\substack{y \in V(p_0) \\ y \neq L(\mathbf{z})}} (T - y). \tag{43}$$

Since

$$\frac{g_L(v, L(\mathbf{z}))}{g_L(1, L(\mathbf{z}))} = \frac{\displaystyle \sum_{\mathbf{z} \in V} \mu_{\mathbf{z}} v(\mathbf{z}) \prod_{\substack{y \in V(p_0) \\ y \neq L(\mathbf{z})}} (L(\mathbf{z}) - y)}{\displaystyle \sum_{\mathbf{z} \in V} \mu_{\mathbf{z}} \prod_{\substack{y \in V(p_0) \\ y \neq L(\mathbf{z})}} (L(\mathbf{z}) - y)} = v(\mathbf{z}), \tag{44}$$

as v becomes a coordinate x_i we have:

$$x_i = \frac{g_L(x_i, T)}{g_L(1, T)}, \quad i = 1, 2, \ldots, n. \tag{45}$$

Note

$$g_L(1, T) = \frac{p_0'(T)}{\mathrm{GCD}(p_0'(T), p_0(T))}. \tag{46}$$

If all roots occur with multiplicity one, the denominator $g_L(1, T)$ is just the derivative of $p_0(T)$. To compute $g_L(v, T)$, we define $\bar{p}_0(T) = p_0(T)/\mathrm{GCD}(p_0'(T), p_0(T))$, and

$$g_L(v, T) = \sum_{j=0}^{d-1} \sum_{k=0}^{d-j-1} \mathrm{trace}(v L^j) a_i T^{d-j-k-1}, \quad \bar{p}_0 = \sum_{i=0}^{d} a_i T^{d-i}. \tag{47}$$

Then we set $q(T) = g_L(1, T)$ and $p_i(T) = g_L(x_i, T)$ and obtain a representation for (1).

6 Algorithms to Compute a RUR

Algorithms to compute a rational univariate representation can be found in [4] and [6].

As example, taken from [4], consider the `katsura3` system:

$$f(\mathbf{x}) = \left\{ \begin{array}{l} 2x_1^2 + 2x_2^2 + 2x_3^2 + x_4^2 - x_4 = 0 \\ 2x_1x_2 + 2x_2x_3 + 2x_3x_4 - x_3 = 0 \\ 2x_1x_3 + x_3^2 + 2x_2x_4 - x_2 = 0 \\ 2x_1 + 2x_2 + 2x_3 + x_4 - 1 = 0. \end{array} \right. \quad (48)$$

Using $x_4 > x_3 > x_2 > x_1$ in the computation of a Gr̈obner basis with lexicographic term order gives a univariate polynomial in x_1. Since all solutions of that polynomial in x_1 are distinct, we say that the variable x_1 is separating. We can use this polynomial in x_1 thus as the polynomial p_0 in the rational univariate representation:

$$\begin{array}{r} p_0(T) = 128304T^8 - 93312T^7 + 15552T^6 + 3144T^4 - 1120T^4 + 36T^3 + 15T^2 - T \\ q(T) = 7185024T^7 - 4572288T^6 + 653184T^5 + 110040T^4 - 31360T^3 + 756T^2 + 210T - 7 \\ p_2(T) = 699840T^7 - 449712T^6 + 74808T^5 + 1956T^4 - 1308T^3 + 174T^2 - 18T \\ p_3(T) = 303264T^7 - 314928T^6 + 113544T^5 - 9840T^4 - 3000T^3 + 564T^2 - 12T \\ p_4(T) = 3872448T^7 - 2607552T^6 + 408528T^5 + 63088T^4 - 20224T^3 + 540T^2 + 172T - 7 \end{array} \quad (49)$$

The polynomial $p_1(T)$ is omitted since for this case, the roots of $p_0(T)$ give the values for x_1.

There are two advantages of using a RUR over the shape lemma:
(1) the size of the coefficients is usually much less;
(2) one does not need a Gröbner basis with respect to the lexicographical term order.

In [4], Recipe VII gives an algorithm to compute a rational univariate representation of a zero dimensional ideal, given a Gröbner basis.

Algorithm 6.1 *Rational Univariate Representation*

Input: $\mathcal{G}_>$, a Gröbner basis for an ideal I with term order $>$, $\#V(I) = D < \infty$.
Output: a rational univariate representation for $V(\sqrt{I})$.

compute $\mathcal{N}_>$ the basis vector for the quotient ring;
let $D = \#\mathcal{N}_> = \#V(I)$, counted with multiplicities;
compute TrM and deduce $d = \#$distinct zeroes;
choose a separating element u as one of the u_i's;
compute for m from 1 to D: trace(u^m) and use u to form $p_0(T)$;
compute $\bar{p}_0$ for $\sqrt{I}$, if deg($\bar{p}_0$) $< d$ then choose another u;
for j from 1 to D
  for i from 0 to d
    compute trace($x_j u^i$) and deduce $g_u(x_j, T)$;
set $q(T) = g_u(1, T)$ and $p_i = g_u(x_i, T)$, $i = 1, 2, \ldots, n$.

In Maple, we compute a rational univariate representation as follows:

```
[> f := [2*x[1]^2 + 2*x[2]^2 + 2*x[3]^2 + x[4]^2 - x[4],
        2*x[1]*x[2] + 2*x[2]*x[3] + 2*x[3]*x[4] - x[3],
        2*x[1]*x[3] + x[3]^2 + 2*x[2]*x[4] - x[2],
        2*x[1] + 2*x[2] + 2*x[3] + x[4] - 1];
[> v := x[4],x[3],x[2],x[1];
[> Groebner[Basis](f,plex(v));
[> Groebner[RationalUnivariateRepresentation](f,v,output=factored);
```

7 Exercises

1. Construct an example of a solution set V in two variables and $\#V > 1$ where all except for one choice of the u_i's fail to be separating.

2. Use a lexicographic term order to compute a Gröbner basis for the system in (48). How many decimal places does the largest coefficient in this basis have? Compare with the size of the coefficients in (49).

3. Use Maple's `Groebner[RationalUnivariateRepresentation]` on the example (48).

4. Create a Maple worksheet to define the polynomial system in (8), for general choices of the position. Solve the system using the choices in (10), either by Maple or by Sage.Singular.

5. Consider the system (from [4]):

$$f(\mathbf{x}) = \begin{cases} 24x_1x_2 - x_1^2 - x_2^2 - x_1^2x_2^2 - 13 = 0 \\ 24x_2x_3 - x_2^2 - x_3^2 - x_2^2x_3^2 - 13 = 0 \\ 24x_3x_1 - x_3^2 - x_1^2 - x_3^2x_1^2 - 13 = 0. \end{cases} \quad (50)$$

   (a) Solve the system to verify that none of the variables is separating.
   (b) Find a separating element of the form as u_i in (3) an run through the steps of Algorithm 6.1. Use a Maple worksheet or a Sage notebook to guide the computations.
   (c) Use the builtin commands in Maple or Sage to compute a rational univariate representation. Compare the output with the outcome of the step-by-step execution of Algorithm 6.1.

6. Consider the following modification (suggested in [2]) of the cyclic 5-roots problem:

$$f(\mathbf{x}) = \begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1 = 0 \\ x_1x_2x_3 + x_2x_3x_4 + x_3x_4x_5 + x_4x_5x_1 + x_5x_1x_2 = 0 \\ x_2x_3x_4 + x_2x_3x_4x_5 + x_3x_4x_5x_1 + x_4x_5x_1x_2 + x_5x_1x_2x_3 = 0 \\ x_1x_2x_3x_4x_5 - 1 = 0. \end{cases} \quad (51)$$

   where the monomial $x_1x_2x_3x_4$ in the original cyclic 5-roots system is replaced by $x_2x_3x_4$. Compute a Gröbner basis with the graded lexicographical order to determine the number of roots of this modified cyclic 5-roots system. Compute a rational univariate representation for this system. Compare the size of the coefficients between the lexicographical Gröbner basis (shape lemma) and the RUR.

References

[1] R.M. Corless. Groebner bases and matrix eigenproblems. *SIGSAM Bulletin*, 30(4):26–32, 1996.

[2] J.C. Faugère, P. Gianni, D. Lazard, and T. Mora. Efficient computation of zero-dimensional Gröbner bases by change of ordering. *Journal of Symbolic Computation*, 16(4):329–344, 1993.

[3] M.-J. Gonzalez-Lopez and L. Gonzalez-Vega. Project 3. The inverse kinematics problem in robotics. In *Some Tapas of Computer Algebra*, volume 4 of *Algorithms and Computation in Mathematics*, pages 305–310. Springer-Verlag, 1999.

[4] L. Gonzalez-Vega, F. Rouillier, and M.-F. Roy. Chapter 2. Symbolic recipes for polynomial system solving. In *Some Tapas of Computer Algebra*, volume 4 of *Algorithms and Computation in Mathematics*, pages 34–65. Springer-Verlag, 1999.

[5] R.P. Paul. *Robot Manipulators: Mathematics, Programming, and Control.* The MIT Press, 1981.

[6] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communication, and Computing*, 9(5):433–461, 1999.