# CADECOM: Computer Algebra software for functional DECOMposition

Jaime Gutierrez and Rosario Rubio

Departamento de Matemáticas, Estadística y Computación
Facultad de Ciencias, Universidad de Cantabria
Santander E–39071, SPAIN
e-mail:{jaime, sarito}@matesco.unican.es

**Abstract.** In this paper we present the Maple package Cadecom which is designed for performing computations in rational function fields. The main objects that Cadecom deals with are multivariate rational functions over any computable field, and the key tool are the functional decomposition algorithms. The functional decomposition problem has many applications in computer science, engineering (CAGD), pure mathematics or robotics. We motivate the interest of this program package by presenting applications on computing roots, simplifying sine–cosine equations, integrating rational functions, computing subfields, computing Gröbner bases and reparametrizing parametric curves. We also include a short overview of the package from the Maple system point of view.

## 1 Introduction

The general functional decomposition problem can be stated as follows: given $f$ in a class of functions, we want to represent $f$ as a composition of two "simpler" functions $g$ and $h$ in the same class, i.e. $f = g \circ h = g(h)$. Although not every function can be decomposed in this manner, when such a decomposition does exist many problems become significantly simpler. Nowadays, this problem has become more important for the simplification of some algebraic objects/structures: polynomials, rational functions, sine–cosine equations or more generally multivariate rational functions module a polynomial ideal. Over the last ten years, there have been several new results in the area of polynomial decomposition, see the references in [8].

Univariate polynomial decomposition has applications in computer science, computational algebra, and robotics. In fact, computer algebra system such as AXIOM, MAPLE, MATHEMATICA and REDUCE support polynomial decomposition for univariate polynomials. However we do not know a program package dedicated to functional decomposition algorithms. In this paper we present the program package CADECOM (Computer Algebra software for functional DECOMposition) which is built on the computer algebra system MAPLE and designed for performing computations over rational function fields. The germ of Cadecom was a collection of procedures (c.f. [3]), which were designed as a help for the manipulation of univariate rational function fields.

The main objects that Cadecom deals with are multivariate rational functions over any computable field $K$, in the sense of the underlying computer algebra system Maple, that is, all the arithmetic operations have to be available in the system. Typically, a finite field $K = F_q$, or the rational numbers $K = Q$, or a finite algebraic extension $K(\alpha)$ of $K$, or a multivariate rational function field $K(x_1, \ldots, x_n)$.
The key tool of Cadecom are the functional decomposition algorithms. The main implementations are based on algorithms presented in [4, 9, 22] for decomposing univariate polynomial and rational functions; in [8] for decomposing multivariate polynomials in several ways; in [19] for reparametrizing parametric curves and in [10] for decomposing bivariate polynomials module the unit circle.
We motivate the importance of this program package by presenting some of the most interesting applications: computing roots, evaluating functions, simplifying sine–cosine equations, integrating rational functions, computing subfields, computing Gröbner bases and reparametrizing parametric curves. We describe the functionalities by examples, including the computation time on a personal computer Macintosh Centris 650.

The structure of the paper is as follows: In Section 2 we present some of the problems that can be simplified using the package and we illustrate them by some examples. In Section 3 we outline some aspects on Cadecom's procedures.

## 2 Motivation

In this section we present some applications of the package Cadecom and we illustrate them by some examples.

### 2.1 Evaluating Functions

Evaluation is a common calculation in mathematics. The evaluation of a function $f$ in a point requires, in the general case, $O(n)$ multiplications; but if $f$ is decomposable, it can be computed with $O(\sqrt{n})$ multiplications.

A rational function $f(x) \in K(x)$ is called *decomposable* if there exist two rational functions $g(x), h(x) \in K(x)$ with degree greater than one and such that $f(x) = g(h(x))$. The degree of a rational function is the maximum of the degree of numerator and the degree of the denominator.
For instance, suppose we want to evaluate the rational function

$$f = \frac{x^{35} + 5\,x^{28} + 10\,x^{21} - 3\,x^{19} + 10\,x^{14} - 3\,x^{12} + 5\,x^7 + 1}{x^{19} + x^{15} + x^{12}}$$

Using the `decomp` function in Cadecom package we get:

> `decomp`$(f, x)$;

$$\left[\frac{3\,x^4 - 1}{x^4\,(x-1)}, -\frac{x^3}{x^7+1}\right]$$

*time = 60.35 bytes = 7783850.*

Then, $f = g(h)$ where $h = -\dfrac{x^3}{x^7+1}$ and $g = \dfrac{3\,x^4-1}{x^4\,(x-1)}$.

Evaluation of multivariate polynomials can also be simplified via functional decomposition. A multivariate polynomial $f(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$ is *uni–multivariate decomposable* if there exist a univariate polynomial $g(y) \in K[y]$ and a multivariate polynomial $h(x_1,\ldots,x_n) \in K[x_1,\ldots,x_n]$ with total degree greater than one and such that $f(x_1,\ldots,x_n) = g(h(x_1,\ldots,x_n))$.

Given the multivariate polynomial $f \in K[x,y,z]$:

$$f = 3x^4y^2 + 6x^2y^3z + 18x^3y + 3z^2y^4 + 18zy^2x + 27x^2 + 6x^2y + 6zy^2 + 18x + 2$$

Using the `umdecompoly` function, we get:

> `umdecompoly`$(f,u)$;

$$\left[3u^2+6u+2, u = x^2y + zy^2 + 3x\right]$$

*time = 45.21 bytes = 5727569.*

### 2.2 Computing Roots

In general, the equation $f(x) = 0$ can be numerically solved more efficiently if $f$ is decomposable. Moreover, in the particular case when $f$ is a polynomial, it is easier to determine if the zeroes of $f$ can be expressed in terms of radicals. Suppose we want to find out all the roots of a polynomial $f$; if $f = g(h)$, in general, it would be more effective to compute the roots of $g$, say $\alpha$ and then solve the equations $h - \alpha$. For example, let

$$f = x^6 - 6x^5 - 17x^4 + 112x^3 + 67x^2 - 442x + 290$$

$f$ is an irreducible polynomial over $Q[x]$. But it is decomposable, this can be seen using the `decompoly` code:

> `decompoly`$(f,x)$;

$$\left[x^2+34x+290, x^3-3x^2-13x\right]$$

*time = 1.47, bytes = 133434.*

Now we can compute all the roots of $f$: first solve the equation $x^2+34x+290 = 0$: we have two roots $\alpha = -17+\sqrt{-1}$ and its conjugate $\overline{\alpha}$; then solve the equation $x^3-3x^2-13x-\alpha = 0$, we get three roots of $f$, $\beta_1, \beta_2$ and $\beta_3$. The other roots of $f$ are $\overline{\beta}_1, \overline{\beta}_2$ and $\overline{\beta}_3$. Summarizing, we can compute the roots of the polynomial $f$, with degree 6, solving a second order equation and a third order equation.

Sometimes you come across an irreducible and indecomposable univariate polynomial, but you can still simplify the polynomial equation. We say that a univariate polynomial $f(x) \in K[x]$ is *ideal decomposable* if there exist $g(x)$ and $h(x)$

in $K[x]$ forming a non–trivial decomposition, $g(h(x))$, i.e. $\deg h, \deg g < \deg f$, and so that $f(x)$ divides $g(h(x))$. The *ideal decomposition* problem is to decide if $f$ is ideal decomposable; and in the affirmative case compute $\bar{f}$, $g$ and $h$ such that $f\bar{f} = g(h)$ (c.f. [6]).

Suppose we want to compute the zeroes of the polynomial

$$f = x^6 + 9x^4 - 10^3 + 27x^2 + 90x + 52$$

with rational coefficients. First of all, we check that $f$ is irreducible and indecomposable. In fact, Maple was unable to compute symbolically the roots of this polynomial. The `idealdecompoly` function in Cadecom package give us:

$>$ `idealdecompoly`$(f, x)$;

$$\left[x^3 + 9x^2 + 27x + 22, \left[x^3 + 12x^2 + 1128x + 1144, x^3 + 3x^2 + 3x\right]\right]$$

*time = 567.22, bytes = 67838253.*

We have that $f\bar{f} = g(h)$ where

$$\bar{f} = x^3 + 9x^2 + 27x + 22, g = x^3 + 12x^2 + 1128x + 1144, \text{ and } h = x^3 + 3x^2 + 3x.$$

So, we have reduced the problem to compute the zeroes of two polynomial of degree 3.

### 2.3 Reparametrizing Parametric Curves

A parametrization $(g(t), h(t))$ of a parametric curve $f(x, y) = 0$ is called *faithful* if every point $(x_0, y_0)$ of the curve (except a finite number of them) corresponds to a unique value of the parameter $t_0$, that is, given a point $(x_0, y_0)$ of the curve, i.e. $f(x_0, y_0) = 0$, there exists a unique $t_0$ such that

$$x_0 = g(t_0),\ y_0 = h(t_0).$$

Not every algebraic curve is parametric, but if it is, there exists a faithful parametrization. The computation of a faithful parametrization is an important topic in Computer Aided Geometric Design (CAGD); see for example [7, 19].

In algebraic terms, a parametrization $(g(t), h(t))$ of a curve $f$ is faithful if and only if $K(g(t), h(t)) = K(t)$. In Cadecom there are implemented several procedures to test the faithfulness: for example, `TRfaithful` which is based on the concept of Taylor resultant introduce by Abhyancar around 1972 (see [1]). We can also find a faithful parametrization from a non-faithful one: for instance, using the procedure `netto` based on the constructive proof of the classical result of Lüroth's theorem or the procedure `sedeberg` based on the paper [19].

Suppose we are given the parametrization

$$(g,h)=\left(\frac{t^6+3t^4+675t^2+2745-64t^3-2352t}{(2t-7)^3},\frac{(2t-7)(t^2+1)}{t^4+26t^2+295-168t}\right).$$

of the plane algebraic curve $f(x,y)=y^3x^2+16y^3x+280y^3+144y^2+18y^2x-x-8$. In Cadecom we get:

> k:=`sedeberg`$([g,h],t)$;

$$k=\frac{31557-8980t+127t^2}{13t^2-202t+720}$$

*time = 0.40, bytes = 83230.*

In order to find a faithful parametrization of $f$ from $(g,h)$, we call `lcomp` procedure:

> g':=`lcomp`$(k,g,t)$;

$$g'=9\frac{-10055829104+678164228t-15210262t^2+112525t^3}{-2048383+629031t-64389t^2+2197t^3}$$

*time = 1.85, bytes = 226074.*

> h':=`lcomp`$(k,h,t)$;

$$h'=\frac{570230-71197t+1313t^2}{20256874-926792t+11215t^2}$$

*time = 1.12, bytes = 142782.*

Then $(g',h')$ is a faithful parametrization of the algebraic curve defined by the polynomial $f$.

Another interesting test over parametric curves is to decide if a parametrization is quasi–polynomial. A parametrization $(g(t),h(t))$ is *quasi–polynomial* if the union field $K(g(t),h(t))$ contains a non–constant polynomial. To simplify this kind of parametrization we can use decomposition polynomial algorithms which are very fast. We can test it using cadecom function `quasipol`.

Given the plane algebraic curve, $-31+140y^3x+296x-99y-92yx^2-4x^2+196y^2x^2-100y^3x^2-117y^2+672y^2x-49y^3+764xy=0$, by the parametrization

$$(g,h)=\left(\frac{t^6+3t^4+3t^2+2}{2t^2-4},\frac{t^4-5}{t^4+6t^2+9}\right).$$

> `quasipol`$([g,h],t)$;

`true`

*time = 2.72, bytes = 196062.*

### 2.4 Computing Gröbner Bases

Gröbner bases computation can also be reduced via multivariate decomposition. For multivariate decomposition there exist several definitions of decomposable, see [8]. For Gröbner bases we are interesting in multi–univariate decomposable polynomial, since this decomposition is compatible with Gröbner bases computation:

Given $G$ be a reduced Gröbner basis —under some term ordering— of the ideal generated by $H$, where $H$ is a finite set of polynomials in the variables $x_1, \ldots, x_n$; let $\Theta$ be a polynomial map, that is, $\Theta = (\theta_1, \ldots, \theta_n)$ is a list of $n$ polynomials in the variables $x_1, \ldots, x_n$. Now, we consider two new polynomial sets: $H^*$ and $G^*$, obtained from $H$ and $G$, respectively, by replacing $x_i$ with $\theta_i$. A natural question that arises is: *Under which circumstances is $G^*$ the reduced Gröbner basis of the ideal generated by $H^*$ under the same term ordering?* In [11] the authors give a complete answer: this happens if and only if the composition by $\Theta$ is "compatible" with the term ordering and $\Theta$ is a list of permuted univariate and monic polynomials. Similar results were obtained in [12] for Gröbner bases. This problem has two natural applications. One of them is in the computation of reduced Gröbner bases of the ideal generated by composed polynomials: so, in order to compute a reduced Gröbner basis of $H^*$, we first compute a reduced Gröbner basis $G$ of $H$ and carry out the composition on $G$, obtaining a reduced Gröbner basis of $H^*$. This appears to be more efficient than computing a reduced Gröbner basis of $H^*$ directly. On the other hand, the opposite application is decomposing the input polynomials $f \in H$ as $f = g(\theta_1(x_1), \ldots, \theta_n(x_n))$, where $\theta_i(x_i)$ is an univariate polynomial in the variable $x_i$, and then check if the composition by $\Theta = (\theta_1, \ldots, \theta_n)$ is "compatible" with the term ordering.

We say that a multivariate polynomial $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ is *multi–univariate* if there exist a multivariate polynomial $g \in K[x_1, \ldots, x_n]$ and univariate polynomials $h_i(x_i) \in K[x_i]$ with degree greater than 1 such that $f = g(h_1, \ldots, h_n)$.

Suppose we want to find the Gröbner basis of the ideal generated by

$$
\begin{aligned}
(g, h) = (&-94038\,y + 1707\,y^6 + 320\,x^9 - 720\,x^7 + 540\,x^5 + 61452\,y^2 - 4800\,x^6 \\
&+11082\,x - 8808\,y^3x + 864\,x^8 + 54\,x^2y^6 + 648\,x^2y^4 + 20484\,y^4 - 4428\,y^5 \\
&-738\,y^7 - 270\,y^7x - 15\,y^9x + 20\,y^9x^3 - 1020\,x^3y^6 - 36720\,x^3y^2 4128\,x^6y \\
&-12240\,x^3y^4 + 1152\,x^6y^4 + 3456\,x^6y^2 + 96\,x^6y^6 + 27540\,xy^2 + 765\,xy^6 \\
&+9180\,xy^4 + 256\,x^{12} + 1944\,x^2y^2 - 24529\,y^3 - 33408\,xy - 5184\,x^4y^2 \\
&+45354\,x^3y - 144\,x^4y^6 - 768\,x^{10} + 42684 - 1728\,x^4y^4 + 6633\,x^4 \\
&-2457\,x^2 - 1920\,x^9y + 2322\,x^2y - 14911\,x^3 - 1032\,x^4y^3 - 6192\,x^4y \\
&+4320\,x^7y - 3240\,x^5y + 387\,x^2y^3 - 320\,x^9y^3 + 11879\,x^3y^3 + 720\,x^7y^3 \\
&-1620\,y^5x - 540\,x^5y^3 - 41\,y^9 + 688\,x^6y^3 + 360\,y^7x^3 + 2160\,y^5x^3, \\
&-2898\,y - 20\,y^6 - 720\,y^2 + 736\,x^6 + 3030\,x - 330\,y^3x - 240\,y^4 + 108\,y^5 \\
&+18\,y^7 - 267\,y^3 - 1980\,xy + 2640\,x^3y - 1104\,x^4 + 414\,x^2 - 270\,x^2y \\
&-4040\,x^3 + 120\,x^4y^3 + 720\,x^4y - 45\,x^2y^3 + 440\,x^3y^3 + 5363 + y^9 \\
&-80\,x^6y^3 - 480\,x^6y),
\end{aligned}
$$

the Maple V (release 5) function `gbasis` was not able to compute it -after two days or work- but if we use `mudecompoly` function we get

> `mudecompoly`($g$);

$$[-15673\,y + 7424\,xy + 688\,x^2y - 320\,x^3y + 42684 - 14776\,x - 4368\,x^2 + 320\,x^3 \\ +256\,x^4 + 1707\,y^2 - 1020\,xy^2 + 96\,x^2y^2 - 41\,y^3 + 20\,y^3x, [y^3 + 6\,y, -3/4\,x + x^3]]$$

*time = 7.60, bytes = 492534.*

> `lmdecompoly`($[y^3 + 6\,y, -3/4\,x + x^3], h$);

$$-483\,y + 440\,xy - 80\,x^2y + 5363 - 4040\,x + 736\,x^2 - 20\,y^2 + y^3$$

*time = 3.45, bytes = 257258.*

Now, we can compute the Gröbner basis of the ideal generated by

$$(g', h') = (-15673\,y + 7424\,xy + 688\,x^2y - 320\,x^3y + 42684 - 14776\,x - 4368\,x^2 \\ +320\,x^3 + 256\,x^4 + 1707\,y^2 - 1020\,xy^2 + 96\,x^2y^2 - 41\,y^3 + 20\,y^3x, \\ -483\,y + 440\,xy - 80\,x^2y + 5363 - 4040\,x + 736\,x^2 - 20\,y^2 + y^3)$$

> G:=`gbasis`($[g', h']$,`plex`($x, y$));

$$G = 17928427558923\,y + 69652831043084\,y^2 - 50521292884496\,y^3 \\ +6589152\,y^{10} - 124688\,y^{11} - 203979830\,y^9 + 1039\,y^{12} + 17619477962188\,y^4 \\ -3821455949733\,y^5 - 57443632170\,y^7 + 560626353463\,y^6 + 4127863857\,y^8, \\ 8339747697261257196327729573560342832 0\,x - 130766609289177 \\ +3619129950872006044740306311819759 9\,y^{11} \\ -4042379725979571674708750716525995067\,y^{10} \\ +1958739460962737338410561321574665998 79\,y^9 \\ -5472783196174854894651618542646887950369\,y^8 \\ +9811340651742878318277256733604249185496 6\,y^7 \\ -1181032358591884169753128118627836046029776\,y^6 \\ +9645518018879286632169470532178440050271479\,y^5 \\ -5229203951039543617068557758322390206222927 2\,y^4 \\ +1749919470694363131883749700501394607012649 40\,y^3 \\ -2895185824790298432943475592949753189132723 96\,y^2 \\ -1052735602612379866970515925868849301993076 0\,y \\ +5411119488787725126351318046490242454354176 83]$$

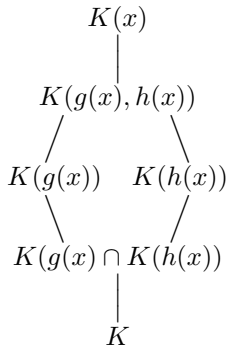
*time = 12.20, bytes = 6460538.*

The Gröbner basis of $(g, h)$ is $\{f(-3/4\,x + x^3, y^3 + 6\,y) \mid f \in G\}$.

### 2.5 Computing Subfields

A classical issue in Algebra is to describe the lattice of fields related to subfields $K(g)$ and $K(h)$, where $g, h$ are two univariate rational functions. In other words,

to determine the union field, the intersection field or compute the intermediate subfields $F$: $K(g) \subset F \subset K(x)$. We know that there exists only a finite number of them, since by Lüroth's theorem every field $F$ is generated by one rational function $f(x) \in K(x)$, i.e. $F = K(f)$. The following diagram illustrates this:




In order to construct symbolically this lattice, we use the Cadecom procedures `maxcomponent` or `netto` (to compute the union field ) and `inters` (to compute the intersection field) for rational functions and `maxcompoly1, maxcompoly2` and `interspol` for polynomials. Again we have distinguished between rational functions and polynomials since for polynomials we have faster algorithms. Each procedure for rational functions calls the respective polynomial one when the input is a polynomial.

Suppose we want to compute the lattice of the fields $K(g)$ and $K(h)$ for $g = x^4$ and $h = \dfrac{x}{1-x^2}$. The computation in Cadecom:

$>$ `maxcomponent`$([g, h], x)$;

$$x$$

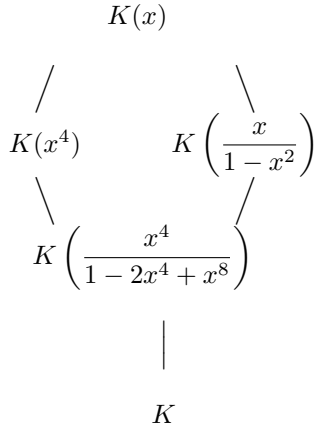
*time = 0.75, bytes = 67650,*

$>$ `inters`$(g, h, x)$;

$$\frac{x^4}{1 - 2x^4 + x^8}$$

*time = 5.52, bytes = 295662.*

Then the subfield lattice is:




Another subfield computation problem is the calculation of all the fields $F$ which contains $K(f)$. For this computation we use the function `intermediate`. Moreover, we can order the subfields under inclusion relation using the procedure `intermtree`. In the particular case when the field $K(f)$ contains a non-constant polynomial, we can use the procedure `intermpol` (c.f. [2]). Of course, this code is much faster than the previous one.
In this example, we want to compute all intermediate subfields ordered with respect to inclusion. Suppose

$$f = \frac{2x^4 - 2x^3 - 8x - 1}{4x^4 + 2x^3 - 16x + 1},$$

if we compute $F$ such that $Q(f) \subset F \subset Q(x)$ there is no proper intermediate field, but if we compute $F$ such that $Q(\alpha)(f) \subset F \subset Q(\alpha)(x)$ where $\alpha^3 = 2$ we get an intermediate field.

> `intermtree`$(f, x)$;

$$[\,]$$

*time = 0.77, bytes = 89630.*

> `alias(alpha=RootOf`$(Z^3 - 2))$ :
`intermtree`$(f, x, \alpha)$;

$$\left[\frac{\alpha x(\alpha x - 2)}{\alpha x + 1}\right]$$

*time = 29.88, bytes = 2285522.*

### 2.6 Simplifying Sine–Cosine Equations

By a *sine–cosine* equation we will understand a polynomial equality $f(s, c) = 0$, with $f$ in the quotient ring $K[s, c]/(s^2 + c^2 - 1)$, and where $K$ is a field of

characteristic zero (typically, a numerical field such as the rational numbers field $Q$ or a field of parameters $Q(x_1, \ldots, x_m)$).

Therefore, when we write $f(s, c)$ we regard this sine–cosine polynomial expression $f(s, c) = 0$ as implicitly univariate in some unknown angle $\theta$ such that:

$$s = sin(\theta),\ c = cos(\theta).$$

We are interested in simplifying or solving equations of the sort $f(s, c) = 0$; and thus, equivalently, for solving or simplifying systems

$$f(s, c) = 0$$
$$s^2 + c^2 - 1 = 0.$$

Polynomial systems, where the variables are interpreted as trigonometric functions of unknown angles, are quite ubiquitous, arising, for instance, in electrical networking, in molecular kinematics and in concrete situations, like in tilting effects on a double pendulum. Here, our applications will be taken from the field of robot kinematics. Besides refering to the many situations described in the recent book of [13], we will sketch, for the sake of being self-contained, an example of the role of sine–cosine systems in robotics:

Given a robot arm with six revolute joints, i.e. a $6R$ robot, the *inverse kinematics* problem is to find the values of the different joint angles (with respect to some standard way of measuring them) that place the tip (or hand) of the robot at some desired position and orientation.
So, the inverse kinematics problem amounts to solving a non-linear polynomial system where the unknowns are the sines and cosines :

$$\{s_i = sin(\theta_i), c_i = cos(\theta_i), i = 1, \ldots, 6\}$$

of the six joint angles:

$$\{\theta_i, i = 1, \ldots, 6\}.$$

The solution of such systems, in general, is quite involved, and depends on the particular geometry of the robot. After decades of research, a symbolic solution (though not in closed form) for the general $6R$ manipulator inverse kinematics system has been found (see [14, 17]). By a clever elimination method it turns out that in this system $\theta_3$ can be determined as the solution of a 16–degree polynomial in the tangent of $\theta_3/2$; then $\theta_1$ and $\theta_2$ are found by solving a system of sine–cosine polynomials, linear in these trigonometric functions, with coefficients in $\theta_3$. Of course, the determining 16–degree polynomial can be also expressed as a 8–degree polynomial in the sine and cosine of $\theta_3$. However, the degree of this solution, together with the complexity of its coefficients, which may contain thousand of terms (c.f. [20]), limits the practical use of this approach.

In practice, the control of a robot requires the solution of the kinematic problem to be of low degree, so that the joint angles can be quickly found. Thus, it is of primordial interest to simplify, when possible, such a univariate sine–cosine equation. The recent paper [10] contains several methods for solving or simplifying sine–cosine equations.

Although $K[s, c]/(s^2 + c^2 - 1)$ is not a unique factorization domain, we can still look for lower degree factors of $f$. More precisely, factoring $f$ over the

domain $K[s,c]/(s^2+c^2-1)$ essentially means: finding sine–cosine polynomials $g(s,c), h(s,c)$, verifying $f = gh$ modulo $s^2+c^2-1$, plus the conditions: $deg(f) > deg(g)$ and $deg(f) > deg(h)$, in order to avoid trivial factorizations.

The following example is an irreducible sine–cosine polynomial with coefficients over the rational function field $Q(a,b)$.

$f = 70 + 21060\,b - 2\,b^5cs + 2\,ac^2 - 10530\,b^2s + 256\,c^5a^2 - 35\,bs + 8960\,ac^3 + 2947200\,c^3a^2 - 4912\,sa + 2456\,ab - 627536\,c^3a^2s - 256\,c^5ba + 12636000\,bsac - 256\,b^5c^4sa - 1200\,c^3bsa - ac^2bs - c^3b^6 + b^6c + 2695680\,bac^3 + c^2b^2s - 2\,c^2b + 42000\,sac - 2947200\,a^2c + 1200\,c^4b^5a - 1200\,b^5c^2a - 2456\,c^2ab.$

We are looking for a factorization of the sine–cosine polynomial $f$ over the field $Q(a,b)$. Then we use the Cadecom procedure

> `scfacpol` $(f,s,c)$;

$$\left[1,\ \frac{ac^2}{2} - \frac{c^2b}{2} - \frac{b^5cs}{2} + 5265\,b + \frac{35}{2} - 1228\,sa,\ 512\,ac^3 + 2400\,sac + 4 - 2\,bs\right]$$

*time : 0.88, bytes 94331.*

The natural notion of decomposability for sine–cosine polynomials $f(s,c)$ states, therefore, the existence of a standard polynomial $g(x)$ and of a sine–cosine polynomial $h(s,c)$, such that

$$f(s,c) = g(h(s,c)) \text{ modulo } s^2+c^2-1.$$

As in the case of factorization, we look for composition factors which are simpler than the given polynomial.

The following example is uni-multivariate indecomposable sine–cosine polynomial with coefficients in the rational function field $Q(a,b,m,n)$.

$$\begin{aligned} f = {} & -21662\,c + 3938\,cs + 114874\,c^2s - 260864\,c^2 - 121438\,c^3 + 22022\,c^3bs \\ & -547515\,c^5s + 934\,c^2sb + 71415\,c^6b + 12420\,c^4sb - 6210\,c^5a^2 - 8078\,c^3b \\ & +135\,c^6a^2b^2 + 540\,c^5a^2b + 556830\,c^3s - 12420\,c^4a^2s + 142830\,c^5 + 8078\,c^3a^2 \\ & -934\,c^2a^2s - 22022\,c^3a^2s + 3105\,c^5a^4s + 135\,c^4a^4s + 5001\,n^7 - 71415\,c^4s \\ & -71415\,c^6a^2 - 270\,c^4a^2sb + 135\,c^4b^2s - 90\,c^2b - 467 - 467\,c^4a^4 + 934\,c^4a^2b \\ & +90\,ca^5b - 934\,c^3a^7b - 934\,c^3a^2m^3 + 934\,c^3b^2a^5 + 934\,c^3bm^3 - 22022\,c^2sm^3 \\ & +8078\,c^2a^5b + 90\,c^2a^2 - 71415\,c^5a^5b + 259463\,c^4 + b^2 - 6210\,c^4m^3 \\ & -6210\,c^4a^5b - 467\,c^2a^{10}b^2 - 934\,cm^3s - 6210\,c^5a^2bs - 270\,c^5a^2bm^3 \\ & +270\,c^3a^2m^3s + 270\,c^4a^7bm^3 + 270\,c^3a^7bs + 6210\,c^4a^7sb + 135\,c^5b^3a^5 \\ & -934\,c^2a^5bm^3 - 934\,ca^5bs + 135\,c^5a^9b + 135\,c^5a^4m^3 - 270\,c^5a^7b^2 - 540\,c^4a^7b \\ & -540\,c^4a^2m^3 + 135\,c^4a^2m^6 - 22022\,c^2sa^5b + 8078\,c^2m^3 - 467\,c^2m^6 \\ & -270\,c^3m^6 + 45\,c^3m^9 + 71820\,c^4a^2 - 6210\,c^4b^2sa^5 + 45\,c^3a^{15}b^3 + 540\,c^4bm^3 \\ & -270\,c^5a^4 + 45\,c^6a^6 - 71820\,c^4b - 270\,c^5b^2 + 135\,c^4a^{12}b^2 - 45\,c^6b^3 \\ & +6210\,c^3sa^5bm^3 + 71820\,c^3a^5b - 270\,c^3bm^3s - 270\,c^4b^2a^5m^3 - 270\,c^3a^{10}b^2 \\ & -12420\,c^3sm^3 + 3105\,c^3sm^6 - 6210\,c^4bsm^3 + 540\,c^4b^2a^5 - 135\,c^4b^3a^{10} \\ & -135\,c^4bm^6 + 135\,c^2m^6s + 270\,c^2a^5bm^3s + 135\,c^3a^{10}b^2m^3 + 135\,c^2a^{10}b^2s \\ & +135\,c^3a^5bm^6 + 90\,cm^3 + 6210\,c^5b - 540\,c^3a^5bm^3 - 12420\,c^3sa^5b \\ & -467\,c^4b^2 - 135\,c^6a^4b + 3105\,c^5b^2s + 135\,c^5b^2m^3 + 6210\,c^4a^2sm^3 \\ & -71415\,c^5m^3 + 71820\,c^3m^3 - 270\,c^3b^2a^5s + 3105\,c^3sa^{10}b^2. \end{aligned}$$

We are interested in a decomposition of $f$ modulo the unit circle over the field $Q(a, b, n, m)$. We use the Cadecom primitive `scdecpol`.

> `scdecpol` $(f, s, c)$;

$$\left[\left[b^2 + 5001\,n^7 + \left(45\,b - 45\,a^2\right)x + \left(-467\,b^2 + 934\,a^2b - 467\,a^4\right)x^2 + \left(-45\,b^3 + 135\,a^2b^2 - 135\,a^4b + 45\,a^6\right)x^3,\ \frac{1}{b-a^2}(c^2b - c^2a^2 - 23\,cs - ca^5b + 2\,c - cm^3 - s)\right]\right]$$

*time: 6.68, bytes: 557710.*

### 2.7 Integrating

Assume we want to integrate an indefinite integral of the form:

$$\int f(x)h(x)dx$$

where $f, h$ are rational functions. If the $\int h$ is a suitable leftcomponent of $f$, we can simplify the integral; i.e. if the there exists a rational function $g$ such that $f = g\left(\int h\right)$. If we call $y = \int h$, then $dy = d(\int h) = h(x)dx$. Therefore,

$$\int f(x)h(x)dx = \int g(y)dy.$$

If such $g$ exists satisfying some additional conditions, then the previous integral is reduced to the integral of a rational function, which is simpler.
The computation of the left component can be made with the function `lcomp` for rational functions and `lcompoly` for polynomials. Suppose we want to integrate

$$\int \frac{x^2}{x^6 + x^3 + 1}dx = \frac{1}{3}\int \frac{(x^3)'}{x^6 + x^3 + 1}dx.$$

$h = 3x^2$ and $\int h = x^3$ is a left component of $f = \dfrac{1}{x^6 + x^3 + 1}$:

> `lcomp` $\left(x^3, \dfrac{1}{x^6 + x^3 + 1}, x\right)$;

$$\frac{1}{1 + x + x^2}$$

*time = 0.97, bytes = 104210.*

Thus

$$\int \frac{x^2}{x^6 + x^3 + 1}dx = \frac{1}{3}\int \frac{1}{x^2 + x + 1}dx$$

$$= \frac{2}{9}\sqrt{3}\arctan\left(\frac{1}{3}(2x + 1)\sqrt{3}\right).$$

### 2.8 Other Applications

The computation of a decomposition was conjectured to be computationally hard: the security of a cryptographic protocol was based on its hardness (c.f. [5]), but it was broken by Berkovits and Lidl & Niederreiter.

We have seen that decomposition can be applied in many other topics and the main aim is simplification. In the following we highlight others: the $n$–partition problem (see [15]), the problem of characterizing the class of automorphisms of $K[x_1, \ldots, x_n]$ and computing their inverses (see [21, 9]).

## 3 Cadecom Package

Cadecom is an ordinary Maple package of about 3 megabytes, it has been developed at Departamento de Matemáticas, Estadística y Computación in Universidad de Cantabria over the last years, starting in 1992, by a research group under the direction of the first author. Several grants by Spanish Ministerio de Educación have been instrumental for reaching this stage of the system. Many people have contributed to Cadecom in different ways. The first version of this package was called FRAC(=Funciones RACionales) [3] and it was mainly implemented by Dr. Alonso.

The package is loaded via the `with` function. Each function is put into a separate file to be loaded via `readlib` into Maple session. Generally, functions are loaded at the time of their first invocation, in order to save memory. There are more than 80 auxilary functions and 42 of them are principal. The library also contains a Maple help; you can load it with `?function;` or `help(function);` commands. We also have included in the library the sypnosis of the procedures and some other extra information. The procedures in Cadecom work over the ground field, that is, the field generated by the coefficients of the input. In some of the procedures you can also work in other fields; you just need to add an argument $K$ to work in such field. For instance, if you type

```
> ?decomp;
```

**decomp - decompose a rational function**

**Calling sequence:**
`decomp`$(f, x)$
`decomp`$(f, x, K)$

**Parameters:**
$f$ – multivariate rational function
$x$ – a variable
$K$ – a field extension over which to decompose

**Description:**

– The procedure `decomp` computes a complete decomposition of $f$ with respect to the variable $x$, following the algorithm in [4].
– If the input is a polynomial calls `decompoly` function.
– If a third argument is given the decomposition is made over $K$, otherwise computes the decomposition in the ground field.

**Examples:** (We omit them)

**See Also:**
rcomp,Brcomp,lcomp,decompoly

The examples have been tested on a personal computer Macintosh Centris 650 in the system MapleV Release 5. We wrote down low degree functions in order to illustrate what the procedures may be used for. To give an idea of about the performance of our implementation, it is important to highlight that you can decompose instantaneously polynomials of degree 50 in a SUN machine. Moreover, the authors were able to decomposing sine–cosine equations of eight-degree with hundred of digits in the coefficients, which were highly complex terms, within 20 seconds of CPU time on an SUN machine. Therefore, we think that our package can now be a useful tool for solving sine–cosine equations.

The package Cadecom is available by anonymous ftp from `ftp.hall.matesco.unican.es` or by e-mail from the authors.

**Acknowledgments**

This research is partially supported by the National Spanish project PB97-0346 and "Acción Integrada Alemana-Española" HA1997-0124.

## References

1. S. Abhyankar, C. Bajaj: *Computations with algebraic curves.* ISSAC–89 L.N.C.S., Springer–Verlag no. 358, 1989, pp. 274–284.
2. C. Alonso: *Desarrollo análisis e implementación de algoritmos para la manipulación de variedades paramétricas.* Ph. dissertation, Dep. Math. and Computing, Universidad de Cantabria, 1994.
3. C. Alonso, J. Gutierrez, T. Recio: *Frac: A Maple package for computing in the rational function field K(X).* Proc. of Maple Summer Workshop and Symposium'94. Birkhäuser, 1994, pp.107–115.
4. C. Alonso, J. Gutierrez, T. Recio: *A rational function decomposition algorithm by near–separated polynomials.* J. Symbolic Comput. **19**, 1995, pp.527–544.
5. J.J. Cade: *A new public–key which allows signatures.* Proc. 2nd SIAM Conf. on Appl. Linear Algebra, raleigh NC, 1985.
6. D. Casperson, D.Ford, J. McKay: *Ideal decompositions and subfields.* J. Symbolic Comput, **21**, 1996, 133–137.
7. G. Farin: *Curves and surfaces for computer aided geometric design.* Academic Press, Boston, 1998.

8. J. von zur Gathen, J. Gutierrez, R. Rubio: *On multivariate polynomial decomposition.* Computer Algebra in Scientific Computing, CASC'99, 1999, pp.463–478.
9. J. Gutierrez: *A polynomial decomposition algorithm over factorial domains.* Compt. Rendues Math. Acad. **XIII–2**, 1991, pp 437–452.
10. J. Gutierrez, T. Recio: *Advances on the simplification of sine–cosine equations.* J. Symbolic Comput. **26**, 1998, pp.31–70.
11. J. Gutierrez, R. Rubio: *Reduced Gröbner Basis Under Composition.* J. Symbolic Comput, **26**, 1998, 433–444.
12. H. Hong: *Gröbner Basis Under Composition I.* J. Symbolic Comput. **25**, 1998, pp.643–663.
13. P. Kovács: *Rechnergestützte symbolische Roboterkinematik.* Vieweg Verlag. 1993.
14. H-Y. Lee, C.-G. Liang: *A new vector theory for the Analysis of Spatial Mechanisms.* Mechanisms and Machine Theory, **23-3**, 1988, pp.209-217.
15. A.K. Lenstra, H.W. Lenstra, L. Lovasz: *Factoring polynomials with rational coefficients.* Math. Ann. 261, 1982, pp.515–534.
16. F. Ollivier: *Inversibility of rational mappings and structural identifiability in automatics.* Proc. ISSAC'89, ACM, 1989, pp. 43-53.
17. M. Raghavan, B. Roth: *Kinematic Analysis of the 6R Manipulator of General Geometry.* Proc. Intl. Symposium on Robotic Research, Tokyo. 1989, pp. 314-320.
18. A. Schinzel: *Selected Topics on Polynomials.* Ann Arbor, University Michigan Press, 1982.
19. T.W. Sederberg: *Improperly parametrized rational curves.* Computed Aided Geometric Design, **3**, 1986, pp.67–75.
20. R. Selfridge: *Analysis of 6 Link Revolute Arms.* Mechanism and Machine Theory. **24-1**, 1989, pp.1-8.
21. D. Shannon, M. Sweedler: *Using Gröbner basis to determine algebra membership, split surjective algebra homomorphisms, determine birational equivalence.* J. Symbolic Comput, **6**, 1988, pp. 267-273.
22. R. Zippel: *Rational Function Decomposition* Proc. of ISSAC-91. ACM press, 1991, 1–6.