Symbolic Parametrization of Pipe and Canal Surfaces

Günter Landsmann, Josef Schicho, Franz Winkler, Erik Hillgarter
Research Institute for Symbolic Computation
Johannes Kepler University
A-4040 Linz, Austria
{landsmann, schicho, winkler, hillgarter}@risc.uni-linz.ac.at

ABSTRACT

A canal surface $\mathcal{S}$, generated by a parametrized curve $m(t)$, in $\mathbb{R}^3$ is the envelope of the set of spheres with radius $r(t)$ centered at $m(t)$. This concept generalizes the classical offsets (for $r(t) = const$) of plane curves. In this paper we develop elementary symbolic methods for generating a rational parametrization of canal surfaces generated by rational curves $m(t)$ with rational radius variation $r(t)$. In a pipe surface $r(t)$ is constant.

1. INTRODUCTION

Given a space curve $m(t)$ and a real-valued function $r(t)$, the *canal surface* with *spine curve* m and radius variation r is the envelope of the family of spheres centered at $m(t)$ with radius $r(t)$. A canal surface with constant radius function is called a *pipe surface*. Pipe surfaces have many practical applications, such as shape reconstruction or robotic path planning; canal surfaces come up in CAGD contexts mainly as transition surfaces between pipes. As today CAD systems prefer rational function representations, the natural question is whether a pipe or canal surface is rational and how to find a rational parametrization. While - considering the analogous problem in dimension 2 - one can construct simple examples of plane rational curves with nonrational offsets, it turns out that canal surfaces with rational spine curve and rational radius function are in general rational [10]. To be precise, they admit rational parametrizations of their real components. We want to compute such parametrizations.

Many subproblems in the parametrization process are treated in the literature on real algebraic geometry, see e.g. [2] or [1]. In this paper we are concerned with the problem of achieving such a parametrization by elementary algebraic methods, and also with the problem of parametrizing in a coefficient field of lowest possible degree.

A straightforward approach is to construct the implicit equation and apply Schicho's algorithm [13] for the parametrization of implicitly given surfaces. However, the implicit equation is usually much more complex than the representation of the surface by r and m.

As we will see in Section 3, the problem can be reduced to the parametrization problem for a surface with an equation which is quadratic in two of the three variables. It is well-known that parametrizations for this class of surfaces can be computed by an algorithm given in [12]. But the equations derived in Section 3 have a special structure. In this paper, we devise a more efficient and simpler method that takes advantage of this structure.

Our method is to apply a sequence of appropriate transformations, until we arrive at a variety described by an equation in simplest possible form, rationally equivalent to the original one. Finding a rational parametrization of the latter and transforming back solves the parametrization problem for the former.

In the case of plane algebraic curves, the parametrization problem ultimately reduces to the problem of finding a "good" point on the given curve, see [14],[15]. In the case of pipe and canal surfaces we determine a "good" curve on the surface.

As in [10] the parametrization problem is reduced to the problem of finding a representation of a rational function as a sum of two squares. This is a special case of Hilbert's 17^{th} problem. Over the real algebraic numbers there exists a simple algorithm. We describe a procedure for deciding this problem over $\mathbb{Q}$.

This work has been supported by the Austrian Science Fund (FWF) under the Proj.Nr. P11160-TEC (HySax), and the special research area SFB F013, subprojects 03 and 04.

2. CANAL SURFACES

Let $m_1(t), m_2(t), m_3(t), r(t)$ be rational functions with coefficients in $\mathbb{R}$. The tuple $m = (m_1, m_2, m_3)$ defines a rational parametrization of a curve in $\mathbb{R}^3$. Let F be the expression

$$F(x_1, x_2, x_3, t) = \sum_{i=1}^{3}(x_i - m_i(t))^2 - r(t)^2$$

and let Z denote the union of the zero sets of the denominators of m_1, m_2, m_3, r and of the numerator of r. Set $V = \mathbb{R} - Z$, $U = \mathbb{R}^3 \times V$. Then F being regular on U defines the set

$$M = \{(x_1, x_2, x_3, t) \in U \mid F(x_1, x_2, x_3, t) = 0\}$$

ISSAC 2000, St. Andrews, Scotland
©2000 ACM 1-58113-218-2/ 00/ 0008 $5.00

which is a smooth manifold of dimension 3 by the Implicit Function Theorem. Consider the projection

$$p : M \longrightarrow \mathbb{R}^3, (x_1, x_2, x_3, t) \mapsto (x_1, x_2, x_3).$$

Then the envelope E^3 is the set of all critical values of p, that means

$$E^3 = \{x \in \mathbb{R}^3 \mid \exists t\colon (x, t) \in M \text{ and } \operatorname{rank}_{(x,t)}(p) < 3\}.$$

Since p is the restriction of the linear projection $\pi\colon \mathbf{R}^4 \longrightarrow \mathbb{R}^3$, the tangent map $T_{(x,t)}(p)$ is just restriction of π to the tangent space $T_{(x,t)}(M)$ and the condition $\operatorname{rank}_{(x,t)}(p) < 3$ amounts to $\frac{\partial F}{\partial t}(x, t) = 0$. Thus the envelope is given by

$$E^3 = \{x \in \mathbb{R}^3 \mid \exists t\colon (x, t) \in U \wedge F(x, t) = 0 \wedge \frac{\partial F}{\partial t}(x, t) = 0\}.$$

that is, the solutions in U of the system

$$\begin{aligned} \sum_{i=1}^{3}(x_i - m_i(t))^2 - r(t)^2 &= 0 \\ \sum_{i=1}^{3}(x_i - m_i(t))\dot{m}_i(t) + r(t)\dot{r}(t) &= 0 \end{aligned} \tag{1}$$

after elimination of t (the dot denotes differentiation with respect to t). The associated canal surface $\mathcal{S}$ can now be defined as the closure of E^3.

Our goal is to develop an elementary, symbolic implementable algorithm which calculates a rational parametrization of $\mathcal{S}$. To this aim we apply an appropriate sequence of transformations to the variety (1).

3. TRANSFORMATIONS

A first simplification gives the substitution

$$x_i = m_i(t) + r(t)u_i \qquad (1 \le i \le 3). \tag{2}$$

We may consider (2) as a map $U \longrightarrow U$ given by

$$(x_1, x_2, x_3, t) \mapsto \Big(\frac{x_1 - m_1(t)}{r(t)}, \frac{x_2 - m_2(t)}{r(t)}, \frac{x_3 - m_3(t)}{r(t)}, t\Big)$$

which birationally transforms (1) to

$$\begin{aligned} \sum_{i=1}^{3} u_i^2 - 1 &= 0 \\ \sum_{i=1}^{3} \dot{m}_i(t)u_i + \dot{r}(t) &= 0. \end{aligned} \tag{3}$$

For fixed t this describes a circle in $\mathbb{R}^3$ arising as the intersection of a sphere and a plane.

¿From now on we work in projective space. We define the abbreviations $a_j = \dot{m}_j(t),\ (1 \le j \le 3)$ and $d = -\dot{r}(t)$ and then pass to the homogeneous system

$$\begin{aligned} u_1^2 + u_2^2 + u_3^2 - u_0^2 &= 0 \\ a_1u_1 + a_2u_2 + a_3u_3 - du_0 &= 0 \end{aligned} \tag{4}$$

which we treat as a system of equations in $\mathbb{P}^3(\mathbb{R}(t))$. The general solution of the linear equation is

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_0 \end{pmatrix} = \begin{pmatrix} a_2x_1 & & \\ -a_1x_1 + a_3x_2 & & \\ & -a_2x_2 + dx_3 & \\ & & a_3x_3 \end{pmatrix}$$

with $x_1, x_2, x_3 \in \mathbb{R}(t)$. Plugging into the sphere yields the quadratic form

$$\varphi = A_1x_1^2 + A_2x_2^2 + A_3x_3^2 - 2Bx_1x_2 - 2Cx_2x_3 \tag{5}$$

with

$$A_1 = a_1^2 + a_2^2 \quad A_2 = a_2^2 + a_3^2 \quad A_3 = d^2 - a_3^2$$
$$B = a_1a_3 \qquad C = da_2.$$

Applying standard techniques and defining the notation

$$s_2 = a_1^2 + a_2^2,\ s_3 = s_2 + a_3^2$$

we derive the equation

$$(d^2 - a_3^2)y_1^2 + (d^2 - s_3)y_2^2 + s_2y_3^2 = 0. \tag{6}$$

Obviously this equation has the complex solution

$$p = (i : 1 : 1).$$

We now apply a real projective transformation T that maps p to the circular point at infinity $q = (1 : i : 0)$. Writing the equation in the new coordinates as

$$az_1^2 + bz_2^2 + cz_1z_2 + z_3(\dots) = 0$$

would imply that

$$a - b + ci = 0.$$

We may therefore derive an equation in simplest possible form. To this end we choose the matrix of T^{-1} as

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

After some standard manipulations we arrive at the equation

$$Z_1^2 + Z_2^2 + (d^2 - s_3)s_2Z_3^2 = 0. \tag{7}$$

The essence of these technical transformations can be described as follows:

First we replace the quadratic form (5) by

$$\psi = A_1A_3^2\varphi.$$

In matrix notation we obtain

$$\psi = \begin{pmatrix} A_1^2A_3^2 & -A_1A_3^2B & 0 \\ -A_1A_3^2B & A_1A_2A_3^2 & -A_1A_3^2C \\ 0 & -A_1A_3^2C & A_1A_3^3 \end{pmatrix}.$$

Then with the aid of the matrix

$$g = \begin{pmatrix} \frac{a_1}{s_2a_2(d^2-a_3^2)} & \frac{1}{s_2(d^2-a_3^2)} & \frac{-a_1}{a_2(d^2-a_3^2)} \\ \frac{1}{a_2a_3(d^2-a_3^2)} & 0 & \frac{-s_2}{a_2a_3(d^2-a_3^2)} \\ \frac{1}{(d-a_3)(d^2-a_3^2)a_3} & 0 & \frac{a_3d-s_3}{(d-a_3)(d^2-a_3^2)a_3} \end{pmatrix}$$

we pass to the equivalent quadratic form

$$\eta = g^T\psi g$$

which proves to be the left hand side of (7). Obviously we have to make the assumptions

$$a_2, a_3, d^2 - a_3^2 \neq 0.$$

A simple study of cases shows, that we always may arrive at the quadratic form (7). If some of the denominators happen to be 0 then an adapted backtransformation will be needed (see [6] for computational details).

4. THE CONSTRUCTION OF A RATIONAL CURVE

In order to find a rational parametrization of the canal surface $\mathcal{S}$ we first need a rational curve $\mathcal{C}$ on $\mathcal{S}$, which then can be used as a basis for parametrizing the whole surface by a reflection process. Finding the curve $\mathcal{C}$ amounts to presenting a nontrivial solution of (7) in $\mathbb{P}^2(\mathbb{R}(t))$. In affine coordinates

$$z_1 = \frac{Z_1}{Z_3},\ z_2 = \frac{Z_2}{Z_3}$$

this is done if we are able to find a presentation of the term $s_2(s_3 - d^2)$ as a sum of two squares. We formulate the following lemma:

Lemma 1. *Let $F \in \mathbb{R}[t]$ be a polynomial with real coefficients. Then F is indefinite (i.e. $\exists x, y \in \mathbb{R}$ with $F(x) < 0 < F(y)$) if and only if F has a real linear factor of odd multiplicity.*

Proof. Assume $F = (t-a)^d G$ with $a \in \mathbb{R},\ G(a) \neq 0,\ d$ odd. Then by continuity of G we see the existence of elements x, y with $F(x) < 0 < F(y)$. Conversely write F as $L_1^{d_1} \cdots L_r^{d_r} Q_1^{e_1} \cdots Q_s^{e_s}$ with L_i linear and Q_j quadratic irreducible and assume all d_i even. Then from the fact that $Q_1^{e_1} \cdots Q_s^{e_s}$ has no real roots and $L_i^{d_i} \geq 0$ we conclude that F must be definite. □

Corollary 1. *Let ρ be in $\mathbb{R}(t)$. Then ρ is a sum of two squares if and only if $\rho = \frac{F}{G}$ with $F, G \in \mathbb{R}[t]$, $F \geq 0$ and G is a square in $\mathbb{R}[t]$.*

Proof. If ρ is a sum of two squares then

$$\rho = \sigma^2 + \tau^2 = \left(\frac{P}{Q}\right)^2 + \left(\frac{R}{S}\right)^2 = \frac{(PS)^2 + (QR)^2}{(QS)^2}.$$

Conversely assume $\rho = \frac{F}{G}$ with $F \geq 0$ and $G = H^2$. ¿From the lemma we know that every linear factor of F in $\mathbb{R}[t]$ has even multiplicity, so F is a product $Q_1^{e_1} \cdots Q_t^{e_t}$ with $Q_i = a_i t^2 + b_i t + c_i,\ a_i > 0$ and $b_i^2 - 4a_i c_i \leq 0$. Every quadratic Q_i can be written as a sum of two squares:

$$Q_i = \left(\sqrt{a}_i t + \frac{b_i}{2\sqrt{a}_i}\right)^2 + \overline{\sqrt{c_i - \frac{b_i^2}{4a_i}}}^{\,2}.$$

If $g = a^2 + b^2$ and $h = c^2 + d^2$ are terms decomposed in a sum of two squares, then the formula

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \qquad (8)$$

shows, that their product joins this property. We conclude that $F = A^2 + B^2$, hence

$$\rho = \left(\frac{A}{H}\right)^2 + \left(\frac{B}{H}\right)^2.$$

□

We may now formulate the following theorem:

Theorem 1. *Equation (7) has a solution in $\mathbb{P}^2(\mathbb{R}(t))$ if and only if for all $x \in \mathbb{R}$ lying in the domain of definition of a_1, a_2, a_3, d we have $a_1(x)^2 + a_2(x)^2 + a_3(x)^2 \geq d(x)^2$.*

Proof. Assume $z_1^2 + z_2^2 + s_2(d^2 - s_3)z_3^2 = 0$ with (z_1, z_2, z_3) in $\mathbb{R}(t)^3 \setminus 0$. Then $z_3 \neq 0$ and the assertion is obvious. Conversely, if for all $x \in \mathbb{R}$ lying in the domain of definition of a_1, a_2, a_3, d we have $a_1(x)^2 + a_2(x)^2 + a_3(x)^2 \geq d(x)^2$, then - with obvious notation - the relation

$$a_1^2 + a_2^2 + a_3^2 - d^2 = \frac{A_1^2}{B_1^2} + \frac{A_2^2}{B_2^2} + \frac{A_3^2}{B_3^3} - \frac{D^2}{E^2} =$$

$$\frac{(A_1B_2B_3E)^2 + (B_1A_2B_3E)^2 + (B_1B_2A_3E)^2 - (B_1B_2B_3D)^2}{(B_1B_2B_3E)^2}$$

shows that the numerator of the expression $a_1^2 + a_2^2 + a_3^2 - d^2$ is nonnegative for all real x while its denominator is a square. Thus Corollary 1 shows, that it is a sum of two squares and by the formula (8) we get a solution of (7). □

Remark 1. *We may rephrase Corollary 1 as: ρ is expressible as a sum of two squares if and only if ρ admits a representation as $\rho = \frac{F}{G}$ with both $F, G \geq 0$.*

5. THE SURFACE PARAMETRIZATION

Assume, that we are given a solution $(z_1 : z_2 : z_3)$ of (7). Transforming back yields a solution $(u_1 : u_2 : u_3 : u_0)$ of (4). We now change back to affine coordinates by replacing u_j by $\frac{u_j}{u_0}$ $(1 \leq j \leq 3)$. Now for a fixed $t_0 \in \mathbb{R}$ let $g_{t_0}(\eta)$ be the pencil of lines lying in the plane $\langle a(t_0), X\rangle = d(t_0)$ and passing through $u(t_0)$. We may realize this as

$$g_{t_0}(\lambda) = u(t_0) + \lambda[M(t_0) - u(t_0) + \eta(u(t_0) - M(t_0)) \times a(t_0)]$$

where $M(t_0)$ denotes the center of that circle in 3-space, which is the real solution of (3) for $t = t_0$, i.e.

$$M(t_0) = \frac{d(t_0)}{||a(t_0)||^2} a(t_0),$$

λ parametrizes points on a line which itself depends on the parameter η.

After a stretching of the parameter ($\lambda := \frac{\lambda}{||a(t_0)||^2}$) we obtain

$$\bar{g}_{t_0}(\eta)(\lambda) = u + \lambda[da - ||a||^2 u - \eta(da - ||a||^2 u) \times a]\Big|_{t=t_0} =$$

$$= u(t_0) + \lambda v(t_0, \eta).$$

Intersecting $\bar{g}_{t_0}(\eta)$ and the sphere $u_1^2 + u_2^2 + u_3^2 = 1$, ignoring the solution $\lambda = 0$ (which represents the point $u(t_0)$) gives

$$\lambda = -\frac{2\langle u(t_0), v(t_0, \eta)\rangle}{||v(t_0, \eta)||^2}.$$

Therefore the expression

$$(t, \eta) \mapsto u(t) - 2\frac{\langle u(t), v(t, \eta)\rangle}{||v(t, \eta)||^2} v(t, \eta) \qquad (9)$$

defines a rational parametrization of the variety (3). The canal surface $\mathcal{S}$ is now parametrized by

$$X(t, \eta) = m(t) + r(t)\left(u(t) - 2\frac{\langle u(t), v(t, \eta)\rangle}{||v(t, \eta)||^2} v(t, \eta)\right). \quad (10)$$

We observe that this parametrization of $\mathcal{S}$ makes use of the spine curve parameter t. We say that such a parametrization is in accordance with the spine curve. The following theorem is now obvious:

Theorem 2. *The canal surface given by the spine curve $m(t) = (m_1(t), m_2(t), m_3(t))$ and the radius function $r(t)$ with $m_1(t), m_2(t), m_3(t), r(t) \in \mathbb{R}(t)$ admits a rational parametrization over the reals in accordance with the spine if and only if $\dot{m}_1(x)^2 + \dot{m}_2(x)^2 + \dot{m}_3(x)^2 \geq \dot{r}(x)^2$ for almost all $x \in \mathbb{R}$.*

In general the rational function $\rho := \dot{m}_1(t)^2 + \dot{m}_2(t)^2 + \dot{m}_3(t)^2 - \dot{r}(t)^2$ needs not to be positive for almost all real values t. In this case we have to restrict ourselves to intervals on which $\rho \geq 0$ and to reparametrize the spine curve, so that in the new setting of the parameter the condition $\rho \geq 0$ is valid on the whole real axis. If e.g. ρ is positive on $[a, b] \subset \mathbb{R}$, we can apply the reparametrization $t = \frac{b\theta^2 + a}{\theta^2 + 1}$. In case $\rho \geq 0$ on $[a, \infty)$ we can use $t = \theta^2 + a$. Obviously, then, each point of the curve component under consideration is passed twice, violating properness of the parametrization, so restriction to the positive real axis is necessary.

We are now in a position to formulate the following algorithm for finding a real rational parametrization of canal surfaces:

Algorithm CANAL_SURFACE

in: $m_1(t), m_2(t), m_3(t), r(t)$;
out: $X_1(t, \eta), X_2(t, \eta), X_3(t, \eta)$;

1. Compute $\rho(t) = \sum_{j=1}^{3} \dot{m}_j(t)^2 - \dot{r}(t)^2$.
2. Choose an interval (a, b) on which $\rho \geq 0$.
3. If $(a, b) \neq \mathbb{R}$ then reparametrize $t\colon = t(\theta)$, so that $\rho(\theta) \geq 0$.
4. Compute a decomposition $\rho = \sigma^2 + \tau^2$.
5. Set $z_1 := \dot{m}_1\sigma + \dot{m}_2\tau \quad z_2 := \dot{m}_1\tau - \dot{m}_2\sigma$.
6. Apply the inverse transformations to get a curve $\mathcal{C}$ on the variety (3).
7. Compute a surface parametrization of (3) with the aid of the curve $\mathcal{C}$ according to formula (9).
8. Compute a rational parametrization of the canal surface according to formula (10).

6. EXAMPLES

Example 1. $m = (t, t^2, t^3), r = 1 - t^2$. *Equation (7) is now*

$$Z_1^2 + Z_2^2 = (1 + 9t^4)(1 + 4t^2)Z_3^2$$

Consequently

$$(1 + 4t^2)(1 + 9t^4) = (1 + 6t^3)^2 + (2t - 3t^2)^2$$

and a solution of (7) is given by

$$(1 + 6t^3, 2t - 3t^2, 1).$$

Transforming into a solution of (3) yields

$$(u_1, u_2, u_3) = (0, 1, 0) \tag{11}$$

Now - for the sake of visualization - we can write down the parametrization of the curve $\mathcal{C}$ which by a reflection process on planes would cover the whole canal surface:

$$(\mathcal{C}_1(t), \mathcal{C}_2(t), \mathcal{C}_3(t)) = (t, 1, t^3)$$

From (10) we obtain a rational parametrization $(U_1(t, \eta), U_2(t, \eta), U_3(t, \eta))$ of the $u-$surface:

$$\begin{array}{rcl}
N_1 & = & \left(27\,t^5\eta + 12\,t^3\eta + 3\,t\eta + 2\right) t \\
N_2 & = & 81\,t^8\eta^2 + 72\,t^6\eta^2 + 34\,t^4\eta^2 - 9\,t^4 + 8\,t^2\eta^2 \\
 & & +4\,t^2 + \eta^2 - 1 \\
N_3 & = & 9\,t^4\eta - 6\,t^3 + 4\,t^2\eta + \eta \\
D_{1,2,3} & = & 81\,t^8\eta^2 + 72\,t^6\eta^2 + 34\,t^4\eta^2 + 9\,t^4 + 8\,t^2\eta^2 \\
 & & +4\,t^2 + \eta^2 + 1
\end{array}$$

where $U_i = \frac{N_i}{D_i}$. Now a parametrization of the canal surface is given by the formulas

$$X_i(t, \eta) = m_i(t) + r(t)U_i(t, \eta).$$

Example 2. *[Viviani's temple] This space curve is defined as the intersection of a sphere of radius $2a$ and a circular cylinder of radius a:*

$$\begin{array}{rcl}
x^2 + y^2 + z^2 & = & 4a^2 \\
(x - a)^2 + y^2 & = & a^2
\end{array}$$

Its rational parametrization can be given by

$$m(t) = \begin{pmatrix} \frac{2a(1-t^2)^2}{(1+t^2)^2} \\ \frac{4at(1-t^2)}{(1+t^2)^2} \\ \frac{4at}{1+t^2} \end{pmatrix}.$$

It turns out, that the term

$$\dot{m}_1^2 + \dot{m}_2^2 + \dot{m}_3^2 = 32\frac{a^2(t^4 + 1)}{(1 + t^2)^4},$$

thus, it can be written as

$$\left(4\frac{\sqrt{2}at^2}{(1 + t^2)^2}\right)^2 + \left(4\frac{\sqrt{2}a}{(1 + t^2)^2}\right)^2.$$

If we set $r = const$, then we obtain a rational curve on the pipe surface

$$\mathcal{C}_1(t) = \frac{N_1}{D_1}, \quad \mathcal{C}_2(t) = \frac{N_2}{D_2} \quad \mathcal{C}_3(t) = \frac{N_3}{D_3}$$

where

$$\begin{array}{rcl}
N_1 & = & \left(t^2 - 1\right)(4\,at^{10} + \sqrt{2}rt^{10} - 8\,\sqrt{2}at^9 + 4\,rt^9 + 4\,at^8 \\
 & & -2\,\sqrt{2}at^8 - 28\,\sqrt{2}rt^8 + 8\,\sqrt{2}at^7 - 8\,\sqrt{2}rt^7 + 8\,rt^7 \\
 & & +12\,\sqrt{2}at^6 + 70\,\sqrt{2}rt^6 + 8\,\sqrt{2}at^5 + 56\,\sqrt{2}rt^5 \\
 & & -28\,\sqrt{2}rt^4 - 8\,\sqrt{2}at^3 - 8\,rt^3 - 56\,\sqrt{2}rt^3 - 4\,at^2 \\
 & & -12\,\sqrt{2}at^2 + \sqrt{2}rt^2 + 8\,\sqrt{2}rt - 4\,rt - 4\,a + 2\,\sqrt{2}a) \\
N_2 & = & -\left(t^2 - 1\right)(-rt^{10} + 8\,at^9 + 8\,\sqrt{2}rt^9 - 16\,\sqrt{2}at^8 \\
 & & +3\,rt^8 + \sqrt{2}rt^8 + 16\,at^7 - 4\,\sqrt{2}at^7 - 56\,\sqrt{2}rt^7 \\
 & & +14\,rt^6 - 28\,\sqrt{2}rt^6 + 16\,at^5 + 20\,\sqrt{2}at^5 + 56\,\sqrt{2}rt^5 \\
 & & +16\,\sqrt{2}at^4 + 14\,rt^4 + 70\,\sqrt{2}rt^4 + 20\,\sqrt{2}at^3 + 16\,at^3 \\
 & & -8\,\sqrt{2}rt^3 + 3\,rt^2 - 28\,\sqrt{2}rt^2 - 4\,\sqrt{2}at + 8\,at \\
 & & +\sqrt{2}r - r) \\
N_3 & = & rt^8 + 8\,at^7 - 4\,\sqrt{2}rt^7 - 16\,\sqrt{2}at^6 + 4\,rt^6 - \sqrt{2}rt^6 \\
 & & -4\,\sqrt{2}at^5 + 8\,at^5 + 16\,\sqrt{2}at^4 + 6\,rt^4 + 5\,\sqrt{2}rt^4 \\
 & & +8\,at^3 + 24\,\sqrt{2}at^3 + 4\,\sqrt{2}rt^3 + 5\,\sqrt{2}rt^2 + 4\,rt^2 \\
 & & -4\,\sqrt{2}at + 8\,at - \sqrt{2}r + r \\
D_1 & = & D_2 = \left(t^2 + 1\right)^3 (2\,t^6 - 4\,\sqrt{2}t^5 - \sqrt{2}t^4 + 2\,t^4 \\
 & & +4\,\sqrt{2}t^3 + 2\,t^2 + 6\,\sqrt{2}t^2 + 2 - \sqrt{2}) \\
D_3 & = & \left(t^2 + 1\right)(2\,t^6 - 4\,\sqrt{2}t^5 - \sqrt{2}t^4 + 2\,t^4 + 4\,\sqrt{2}t^3 \\
 & & +2\,t^2 + 6\,\sqrt{2}t^2 + 2 - \sqrt{2})
\end{array}$$

from which we can easily generate a parametrization of the pipe surface by the process described above.

7. RATIONAL FUNCTIONS AS SUMS OF SQUARES

The problem in the algorithm **CANAL_SURFACE** is the fact that it requires factorization of univariate polynomials into linear and quadratic irreducible factors in step 4. This is no problem numerically, but a symbolic factorization of that kind is very difficult to find. Suppose, for instance, that we need to factor a degree 7 polynomial with 7 real roots which has the symmetric group S_7 as its Galois group. Then the smallest field containing such a factorization has degree 5040, and it is virtually impossible to do calculations in this field. It is therefore desirable to find a solution of the equation in step 4 within the rationals. If this is not possible, then we recommend to convert to numeric polynomials and proceed as in the proof of Corollary 1. For symbolic treatment of step 4 in the algorithm **CANAL_SURFACE**, the following variant of the problem arises:

Problem 1. *Let k be a computable field of characteristic zero. Let $F \in k(t)$. Decide if F is the sum of two rational functions. If yes, find $X, Y \in k(t)$, such that $X^2 + Y^2 = F$.*

It is easy to reduce to the case where F is a polynomial: in order to represent a fraction as a sum of two squares, expand the denominator to square and represent the numerator as a sum of two squares. (See also Corollary 1) Actually, computability of k is not enough for solving this problem. We have to assume at least that we can solve problem 1 for constants. If k is the field of rationals, then we can use Fermat's Theorem: c is a sum of two squares if and only every prime occuring with an odd exponent in the numerator or in the denominator is congruent 1 modulo 4. In the affirmative case, a representation can be found easily. We also make the convenient assumption that k has computable factorization. This property is shared by most computable fields occuring in practical computations, for instance all finitely generated fields (see [4]). Problem 1 is a special case of the problem solved in [5, 7]. However, the solution given there is not efficient enough for our purpose. Here we give a more efficient solution for this special case. By suitable scaling of the unknowns X, Y, we can reduce to the case that F is squarefree. Then, the following theorem solves the decision problem.

Theorem 3. *Let k be a field where -1 is not a square. Let F be a squarefree polynomial in $k[t]$. Then F is a sum of two squares of rational functions if and only if F is a sum of two squares of polynomials if and only if the following conditions are fulfilled.*

1. *F has even degree.*
2. *The leading coefficient of F is a sum of two squares.*
3. *-1 is a square in the ring $k[t]/\langle F\rangle$.*

Proof. Assume the existence of two rational functions X, Y such that $X^2 + Y^2 = F$. We may write X as at^m plus terms of lower order, and Y as bt^n plus terms of lower order. Assume $m \geq n$ without loss of generality. Because -1 is not a square, there is no cancellation in order $2m$ in the sum $X^2 + Y^2$. Therefore, $\deg(F) = 2m$, and $\mathrm{lcoeff}(F) = a^2 + b^2$ if $m = n$, and $\mathrm{lcoeff}(F) = a^2$ if $m > n$. In order to show the third condition, assume that $X = \frac{P}{D}$ and $Y = \frac{Q}{D}$, where $P, Q, D \in k[t]$ without common divisor. Then we have $P^2 + Q^2 = D^2 F$. Any irreducible common divisor of Q and F must also divide P. Since it cannot divide D, its square divides F. But F is squarefree, therefore Q and F are relatively prime. It follows that Q is invertible in $k[t]/\langle F\rangle$, whence $-1 = (P/Q)^2$ in $k[t]/\langle F\rangle$. Now, assume that the three conditions above are fulfilled, i.e. $-1 \equiv R(t)^2 (\mathrm{mod} F)$ and $\deg(F) = 2m$ and $\mathrm{lcoeff}(F) = a^2 + b^2$, for suitable R, m, a, b. Let X, Y be indeterminate polynomials of formal degree m, with coefficients $x_m, \ldots, x_0$, $y_m, \ldots, y_0$. The condition

$$X \equiv RY (\mathrm{mod} F)$$

is equivalent to a system Γ of $2m$ homogeneous linear equations in the indeterminates $x_m, \ldots, y_0$. Let z be a new variable. The system

$$\Gamma \cup \{x_m - az = 0, y_m - bz = 0\}$$

is a linear homogeneous system of $2m+2$ equations in $2m+3$ indeterminates. Therefore, it has a nontrivial solution. Let $(\xi_m, \ldots, \xi_0, \eta_m, \ldots, \eta_0, \zeta)$ be a nontrivial solution. Let X_0, Y_0 be the polynomials obtained by plugging the solution into the indeterminate coefficients. We claim that

$$X_0^2 + Y_0^2 = \zeta^2 F.$$

Proof: we have $X_0 \equiv RY_0 (\mathrm{mod} F)$ by construction. Hence

$$0 \equiv (X_0 - RY_0)(X_0 + RY_0) \equiv X_0^2 - R^2 Y_0^2 \equiv X_0^2 + Y_0^2 (\mathrm{mod} F).$$

The formal degree of $X_0^2 + Y_0^2$ is $2m$, hence $X_0^2 + Y_0^2$ is a scalar multiple of F. The claim follows now by comparison of the leading coefficients on both sides. Next, we claim that $\zeta \neq 0$. Suppose, indirectly, that $\zeta = 0$. Then $X_0^2 + Y_0^2 = 0$ by the above claim. This implies a cancellation in leading coefficients in the sum $X_0^2 + Y_0^2$, which is impossible because -1 is not a square. Now, we have found a representation

$$F = (X_0/\zeta)^2 + (Y_0/\zeta)^2$$

as sum of squares of two polynomials. The existence of a representation as sum of two polynomials trivially implies the existence of a representation as sum of two rational functions. □

Remark 2. *If -1 is a square, then*

$$F = \left(\frac{F+1}{2}\right)^2 + \left(\frac{F-1}{2\sqrt{-1}}\right)^2,$$

hence any polynomial is a sum of two squares.

Remark 3. *The equivalence of representations by rational functions and representations by polynomials is true in much greater generality. [11]*

To emphasize the role of Theorem 3 for practical computability, we specialize it to the rationals:

Corollary 2. *Let F be a squarefree polynomial with rational coefficients. Then F is a sum of two squares in $\mathbb{Q}(t)$ if and only if F is a sum of two squares in $\mathbb{Q}[t]$ if and only if*

1. *F has even degree.*
2. *The leading coefficient of F is a sum of two squares.*
3. *-1 is a square in $\mathbb{Q}[t]/\langle F\rangle$.*

Algorithmically, the problem of deciding whether -1 is a square modulo F (and computing $\sqrt{-1}$ in the affirmative case) can be reduced to the problem of factoring polynomials over algebraic extensions (see [3, 8, 9, 16] for algorithmic solutions of this problem). By the Chinese Remainder Theorem, it suffices to solve this problem for each irreducible factor of F. And for irreducible F, the problem is equivalent to the factorization of $x^2 + 1$ in the field extension defined by an algebraic number with minimal polynomial F. For performance reasons, it is better not to use the Chinese Remainder Theorem in order to compute $\sqrt{-1}$ in $k[t]/\langle F\rangle$, but to compute representations of the irreducible factors of F as sums of two squares, and to use the product formula (8). This leads to the following algorithm for the solution of Problem 1.

Algorithm TWO_SQUARES(F)

```
if deg$F$ is odd or lcoeff($F$) is not a sum of two squares then
    return(NotExist) and exit;
if $F$ is irreducible then
    $m := \deg(F)/2$;
    $(a, b)$:= two numbers such that $a^2 + b^2 = \mathrm{lcoeff}(F)$
    $X := x_0 + \ldots + x_{m-1}t^{m-1} + at^m$;
    $Y := y_0 + \ldots + y_{m-1}t^{m-1} + bt^m$;
    $k' := k[t]/\langle F\rangle$;
    if $x^2 + 1$ is irreducible over $k'$ then
        return(NotExist) and exit;
    $R$:= a polynomial such that $R(t)^2 + 1 = 0$ in $k'$;
    $Z$:= the remainder of $X - RY$ modulo $F$;
    $\Gamma$:= the linear system obtained by setting
    all coefficients of $Z$ to be zero;
    solve($\Gamma \cup \{x_m = a, y_m = b\}$);
    return($X, Y$);
else
    factor($F$);
    $(X, Y)$:= two constants such that $X^2 + Y^2 = \mathrm{lcoeff}(F)$
    for each $G$ in the list of monic factors do
        $(Z, W)$:= $TwoSquares(G)$;
        $(X, Y) := (XZ + YW, XW - YZ)$;
    return($X, Y$);
```

Example 3. *We want to represent the polynomial*

$$F = t^6 - 2t^5 + 6t^4 - 14t^3 + 19t^2 - 14t + 5$$

as a sum of two squares. The polynomial is irreducible over $\mathbb{Q}$*. Its degree is 6, and the leading coefficient is 1, so the first two conditions are fulfilled. The third condition can be checked using computer algebra: Maple returns*

$$R = \frac{7}{19}t^5 - \frac{10}{19}t^4 + \frac{39}{19}t^3 - \frac{73}{19}t^2 + \frac{94}{19}t - \frac{47}{19}$$

and $-R$ *as square roots of* -1 *modulo* F*. At this step we know that a solution exists. Since the leading coefficient is* $1^2 + 0^2$*, we set*

$$X := x_0 + x_1 t + x_2 t^2 + t^3, Y := y_0 + y_1 t + y_2 t^2.$$

The coefficients of remainder$(X - RY, F)$ *(in ascending order) are:*

$$\mathit{x0} + \frac{47}{19}\,\mathit{y0} + \frac{35}{19}\,\mathit{y1} + \frac{20}{19}\,\mathit{y2}, \quad \mathit{x1} - \frac{94}{19}\,\mathit{y0} - \frac{51}{19}\,\mathit{y1} - \frac{21}{19}\,\mathit{y2}$$

$$\mathit{x2} + \frac{73}{19}\,\mathit{y0} + \frac{39}{19}\,\mathit{y1} + \frac{25}{19}\,\mathit{y2}, \quad -\frac{39}{19}\,\mathit{y0} - \frac{25}{19}\,\mathit{y1} - \frac{17}{19}\,\mathit{y2} + 1$$

$$\frac{10}{19}\,\mathit{y0} + \frac{3}{19}\,\mathit{y1} - \frac{1}{19}\,\mathit{y2}, \quad -\frac{7}{19}\,\mathit{y0} - \frac{4}{19}\,\mathit{y1} - \frac{5}{19}\,\mathit{y2}.$$

Setting them to zero yields the unique solution

$$y_0 = -1, y_1 = 3, y_2 = -1, x_0 = -2, x_1 = 2, x_2 = -1$$

and hence the representation

$$F = (t^3 - t^2 + 2t - 2)^2 + (-t^2 + 3t - 1)^2$$

8. REFERENCES

[1] Benedetti, R., and Risler, J.-J. *Real Algebraic and Semi-Algebraic Sets.* Actualit´es Math´ematiques. Hermann, Paris, 1990.

[2] Bochnak, J., Coste, M., and Roy, M.-F. *Géometrie Algébrique Réelle.* Springer, 1987.

[3] Bradford, J. A. R., and Davenport, J. Factorisation of polynomials: old ideas and recent results. In *Trends in Computer Algebra* (1988), R. Janssen, Ed., vol. 296 of *Lecture Notes in Computer Science*, Springer, p. 81.

[4] Davenport, J. H., and Trager, B. M. Factorization over finitely generated fields. In *SYMSAC '81: Proceedings of the 1981 ACM Symposium on Symbolic and Algebraic Computation* (1981), P. Wang, Ed., Association for Computing Machinery, p. 200.

[5] Hillgarter, E. Rational points on conics. Master's thesis, RISC Linz, 1996.

[6] Hillgarter, E., Landsmann, G., Schicho, J., and Winkler, F. Generalized offsets as envelopes of an one-parameter set of spheres. Tech. Rep. 99-20, RISC-Linz, Univ. Linz, A-4040 Linz, 1999.

[7] Hillgarter, E., and Winkler, F. Points on Algebraic Curves and the Parametrization Problem. In *Automated Deduction in Geometry*, D. Wang and L. Fariñas and H.Shi, Ed. Springer, 1997, pp. 185–203.

[8] Landau, S. Factoring polynomials over algebraic number fields. *SIAM Journal on Computing 14*, 1 (Feb. 1985), 184–195.

[9] Lenstra, A. K. Factoring polynomials over algebraic number fields. Tech. rep., Stichting Mathematisch Centrum, Kruislaan 413 1098 SJ Amsterdam, Nov. 1982.

[10] Peternell, M., and Pottmann, H. Computing rational parametrizations of canal surfaces. *Journal of Symbolic Computation 23* (1997), 255–266.

[11] Pfister, A. *Quadratic Forms with Applications to Algebraic Geometry and Topology*, vol. 217 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 1995.

[12] Schicho, J. Rational parameterization of real algebraic surfaces. In *ISSAC-98* (1998), ACM Press, pp. 302–308.

[13] Schicho, J. Rational parametrization of surfaces. *J. Symb. Comp. 26*, 1 (July 1998), 1–30.

[14] Sendra, J., and Winkler, F. Symbolic parametrization of curves. *Journal of Symbolic Computation 12*, 6 (1991), 607–632.

[15] Sendra, J., and Winkler, F. Parametrization of algebraic curves over optimal field extensions. *Journal of Symbolic Computation 23*, 2/3 (1997), 191–208.

[16] Wang, P. S. Factoring multivariate polynomials over algebraic number fields. *Math. Comp. 32*, 144 (Oct. 1976), 324–336.