Generalized Offsets as Envelopes of a One-parameter Set of Spheres

E. Hillgarter, G.Landsmann, J. Schicho, F.Winkler

Research Institute for Symbolic Computation

Johannes Kepler University

A-4040 Linz, Austria

(Received 22 December 1999)

A generalized offset of a parametrized curve $m(t)$ in $\mathbb{R}^n$ is the set of all points having a normal distance $r(t)$ from $m(t)$. Thus the concept covers the classical offsets (for $r(t) = const$) of plane curves as well as pipes and canal surfaces. In this paper we develop methods for generating a rational parametrization of generalized offsets of rational curves $m(t)$ with rational radius variation $r(t)$, in case such a parametrization exists. In addition we try to select those methods, which allow an implementation, that provides solutions in reasonable time.

1. Introduction

By a rational parametrization (with real coefficients) of a real algebraic hypersurface $H = \{x \in \mathbb{R}^n \mid F(x) = 0\}$ we mean an $n-$tupel of rational functions $(x_1, \ldots, x_n) \in \mathbb{R}(U_1, \ldots, U_{n-1})^n$ which defines a map with Zariski-dense image in H. If $\mathrm{dom}(x_j)$ denotes the domain of definition of x_j, i.e. the set of all points in $\mathbb{R}^{n-1}$ which are not in the zero set of the denominator of x_j, then $x \in \mathbb{R}(U_1, \ldots, U_{n-1})^n$ is a rational parametrization of H iff

$$\forall u \in \bigcap_{j=1}^{n} \mathrm{dom}(x_j)\big(F(x_1(u), \ldots, x_n(u)) = 0 \wedge \mathrm{rank}\frac{\partial x_j}{\partial u_i}(u) = n-1\big).$$

For $x = (x_1, \ldots, x_n) \in \mathbb{R}(U_1, \ldots, U_{n-1})^n$ with $\mathrm{rank}(\frac{\partial x_j}{u_i}) = n-1$ a simple verification shows that these conditions are fulfilled iff $F(x_1, \ldots, x_n) = 0$ is true in the field $\mathbb{R}(U_1, \ldots, U_{n-1})$. So a rational parametrization is given by one solution of the equation $F = 0$, which has the mentioned maximal rank property, in this field .

By the parametrization problem we mean the following:

PROBLEM 1.1. *Given a real algebraic hypersurface. Decide existence of a rational parametrization and - in the affirmative case - find one.*

Whereas the parametrization problem for a general real algebraic hypersurface is fairly complicated (Schicho, 95; Schicho, 97) and far from being solved algorithmically, the case $n = 2$ (i.e. the hypersurfaces are plane curves) is completely solved (Sendra & Winkler, 97) and for $n = 3$, (i.e. surfaces in $\mathbb{R}^3$) there has been considerable progress made in recent time (Schicho, 97).

In this paper we deal with the parametrization problem of a special class of hypersurfaces, which can be described as the envelope of a one-parameter family of spheres with centers moving along a rational curve $m(t)$ in real $n-$space and whose radii are allowed to vary according to a given rational function $r(t)$. For the special cases $n = 2$ and $n = 3$, which have priority with respect to application in CAGD, these hypersurfaces, known as offset curves and canal surfaces, resp., have received considerable attention in the literature (see the bibliography). While there are simple examples of plane rational curves whose offsets - even in the case $r = const$ - are of genus > 0 and thus do not possess any rational parametrization, we know from (Peternell & Pottmann, 97; Degen, 67) that rational parametrizations of canal surfaces always do exist. This shows that a general dimension approach for solving the parametrization problem for this surface class must fail. We therefore deal with the dimensions $n = 2$ and $n = 3$ separately. Nevertheless the dimension independent definition of this surface class leads to a uniform formulation of the methods used. This work has been partially supported by the Austrian Science Fund (FWF) under the Proj.Nr. P11160-TEC (HySax), Proj.Nr. P12662-TEC (Adjoints), and the special research area SFB F013, subprojects 03 and 04.

2. The General Envelope

Let $m_1(t), \ldots, m_n(t), r(t)$ be rational functions with coefficients in $\mathbb{R}$. The tupel $m = (m_1, \ldots, m_n)$ defines a rational parametrization of a curve in $\mathbb{R}^n$, which we call the spine curve in the sequel. Let F be the expression

$$F = \sum_{i=1}^{n} (x_i - m_i(t))^2 - r(t)^2$$

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

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

which is a smooth manifold of dimension n by the implicit function theorem. Consider the projection $p : M \longrightarrow \mathbb{R}^n, (x_1, \ldots, x_n, t) \mapsto (x_1, \ldots, x_n)$. Then the envelope E^n is the set of all critical values of p, that means

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

Because p is the restriction of the linear projection $\pi\colon \mathbb{R}^{n+1} \longrightarrow \mathbb{R}^n$, the tangent map $T_{(x,t)}(p)$ is just restriction of π to the tangent space $T_{(x,t)}(M)$ and the condition $\mathrm{rank}_{(x,t)}(p) < n$ amounts to $\frac{\partial F}{\partial t}(x,t) = 0$. Thus the envelope is given by

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

that is, the solutions in U of the system

$$\sum_{i=1}^{n} (x_i - m_i(t))^2 - r(t)^2 \quad = 0$$

$$\sum_{i=1}^{n}(x_i - m_i(t))\dot{m}_i(t) + r(t)\dot{r}(t) \quad = 0 \tag{2.1}$$

after elimination of t (the dot denotes differentiation with respect to t).

Our goal is to give conditions for the existence of a rational parametrization of E^n and - in the affirmative case - to present an algorithm to find such a parametrization.

Assume - for the moment - $n = 3$ and $r = const$. Let (T, N, B) denote the Frenet trihedron of the curve $m(t)$. Then the formula

$$X(t, \eta) = m(t) + r(\cos\eta N(t) + \sin\eta B(t))$$

represents a parametrization of a pipe surface which obviously is not rational. By using a generalized spherical coordinate system such a parametrization works in any dimension. So we see that there are no analytic obstacles for the existence of rational parametrizations of hypersurfaces coming from generalized envelopes. In their paper (Peternell & Pottmann, 97) Peternell and Pottmann use geometric methods cf. (Pottmann & Peternell, 98) to derive the existence of such parametrizations for canal surfaces. The natural approach is to first calculate an implicit representation and then to apply general methods for parametrizing real surfaces in $\mathbb{R}^3$ (Schicho, 97). Unfortunately the defining polynomial - coming as an output from any method in elimination theory - is in general too big to serve as an input for any actual existing parametrization algorithm. So, in the present paper, we try a different approach to overcome these difficulties. Instead of calculating the resultant, we work directly with the variety given by their input polynomials, and apply a sequence of appropriate transformations to them, until we arrive at a variety described by an equation in simplest possible form, birationally equivalent to the original one. Finding a rational parametrization of the latter and transforming back solves the parametrization problem for the former. So we first deal with the variety in $U \subseteq \mathbb{R}^{n+1}$ defined by system 2.1 (which is not a hypersurface), that means, we consider the algebraic set

$$\hat{E^n} = \{(x, t) \in U \mid F(x, t) = 0 \wedge \frac{\partial F}{\partial t}(x, t) = 0\}.$$

After performing the sequence of transformations, we look for a solution of the ultimate equation in an extension of $\mathbb{R}$ of appropriate transcendence degree. In case such a solution exists, application of the inverse transformations gives a parametrization of $\hat{E^n}$ and composition with the projection p parametrizes the envelope E^n rationally.

As remarked in the introduction, the methods for realizing this outlined strategy depend to a certain extent on the dimension of the ambient space $\mathbb{R}^n$.

There is one obvious simplification, which can be accomplished simultanously in any dimension $n \geq 2$, given by

$$x_i = m_i(t) + r(t)u_i \qquad 1 \leq i \leq n. \tag{2.2}$$

We view 2.2 as map $U \longrightarrow U$ given by

$$(x_1, \ldots, x_n, t) \mapsto \Big(\frac{x_1 - m_1(t)}{r(t)}, \ldots, \frac{x_n - m_n(t)}{r(t)}, t\Big)$$

which birationally transforms $\hat{E^n}$ to $\hat{E_1^n}$:

$$\hat{E_1^n} : \quad \begin{cases} \sum_{i=1}^{n} u_i^2 - 1 & = 0 \\ \sum_{i=1}^{n} \dot{m}_i(t)u_i + \dot{r}(t) & = 0 \end{cases} \tag{2.3}$$

The formal advantage of system 2.3 as compared to 2.1 is accompanied by a loss of geometrical clarity. While the former shows a sphere of radius $r(t)$ along the spine $m(t)$, and a hyperplane orthogonal to the tangent vector $\dot{m}(t)$, the latter represents just one (constant) sphere of radius 1, and a hyperplane, changing position in time t. As is the case in all algebraic considerations, the formal aspect is dominant. Thus we take 2.3 as the starting point, to be applied differently in different dimensions. We begin with the simplest case $n = 2$.

We do not intend to discuss the phenomenon of extraneous spheres, which arise at singular points of the curve $m(t)$. This is done - for constant distance offsets of plane curves - in the paper of Farouki and Neff (Farouki & Neff (2), 90). Consequently we always take the asumption $\dot{m} \neq 0$ as a hypothesis.

3. 2-dimensional Offsets

Here, the spine being a plane rational curve, system 2.1 reads

$$\begin{aligned} (x_1 - m_1(t))^2 + (x_2 - m_2(t))^2 &= r(t)^2 \\ (x_1 - m_1(t))\dot{m}_1(t) + (x_2 - m_2(t))\dot{m}_2(t) + r(t)\dot{r}(t) &= 0. \end{aligned} \tag{3.1}$$

In the special case $r = const$ the envelope - after elimination of extraneous circles - is called the offset curve of the plane curve (m_1, m_2), and the algebraic and analytic properties of the offset in dependence with the spine curve are studied extensively in (Farouki & Neff (2), 90)(Farouki & Neff (1), 90).

In the general case a rational parametrization of the (generalized) offset is a solution (x_1, x_2) of 3.1 in $\mathbb{R}(U)^2$. The transformation 2.2 is now given by

$$u = \frac{x_1 - m_1(t)}{r(t)}, \quad v = \frac{x_2 - m_2(t)}{r(t)}, \quad t = t$$

and applied to $\hat{E}^2$ yields $\hat{E}_1^2$ described by the system

$$\begin{aligned} u^2 + v^2 &= 1 \\ a(t)u + b(t)v &= d(t) \end{aligned} \tag{3.2}$$

with $a(t) = \dot{m}_1(t), b(t) = \dot{m}_2(t), d(t) = -\dot{r}(t)$. In order to parametrize $\hat{E}_1^2$ we must find a solution $\rho = (u(\Theta), v(\Theta), t(\Theta))$ of 3.2 in $\mathbb{R}(\Theta)^3$. First we try to parametrize $\hat{E}_1^2$ in accordance with the spine curve m, i.e. we set $t(\Theta) = \Theta$. This amounts to determining a solution (u, v) of 3.2 in $\mathbb{R}(t)^2$, treating a and b as constants.

We may assume $a, b \neq 0$. The general solution of the linear equation is given by $(d/2a + xb, d/2b - xa)$, $x \in \mathbb{R}(t)$. Plugging into the quadratic and generating a complete square by setting

$$x' = x + \frac{d(b^2 - a^2)}{2ab(a^2 + b^2)}$$

leads to

$$(a^2 + b^2)^2 x'^2 - (a^2 + b^2 - d^2) = 0 \tag{3.3}$$

Obviously this last equation has a solution in $\mathbb{R}(t)$ iff 3.2 has a solution in $\mathbb{R}(t)^2$. If x' is a solution then $(a^2 + b^2)x'$ solves

$$x''^2 = a^2 + b^2 - d^2 \tag{3.4}$$

On the other hand, a solution x'' of 3.4 immediately yields the solution $\frac{x''}{a^2+b^2}$ of 3.3. Thus, we see that the generalized offset has a rational parametrization in accordance with the spine curve, iff 3.4 has a nontrivial solution, and from such a solution (X', Y') we can compute the parametrization (x_1, x_2). Thus we are led to the following theorem.

THEOREM 3.1. *Let $m_1, m_2, r \in \mathbb{R}(t)$, $(\dot{m}_1, \dot{m}_2) \neq (0,0)$, $r \neq 0$. The generalized offset given by the data m_1, m_2, r admits a rational parametrization over $\mathbb{R}$ in accordance with (m_1, m_2) iff $\dot{m}_1{}^2 + \dot{m}_2{}^2 - \dot{r}^2$ is a square in $\mathbb{R}(t)$. If this is the case, i.e. $\dot{m}_1{}^2 + \dot{m}_2{}^2 - \dot{r}^2 = \rho^2$ for some $\rho(t) \in \mathbb{R}(t)$, then a rational parametrization of the offset curve is given by*

$$\begin{aligned} x_1 &= m_1 + r\frac{\dot{m}_2\rho - \dot{m}_1\dot{r}}{\dot{m}_1{}^2 + \dot{m}_2{}^2} \\ x_2 &= m_2 - r\frac{\dot{m}_2\dot{r} + \dot{m}_1\rho}{\dot{m}_1{}^2 + \dot{m}_2{}^2}. \end{aligned}$$

PROOF. As above write $a = \dot{m}_1, b = \dot{m}_2, d = -\dot{r}$.
The case $a \neq 0$ and $b \neq 0$ is done.

Now, without loss of generality, assume $a = 0, b \neq 0$. The transformation

$$u = \frac{x_1 - m_1}{r}, \quad v = \frac{x_2 - m_2}{r}$$

then leads to the system

$$\begin{aligned} u^2 + v^2 &= 1 \\ bv = d & \end{aligned}$$

which obviously is solvable iff $a^2 + b^2 - d^2$ is a square.

In any case the correctness of the parametrization formula is verified by a trivial calculation. □

From the special form of 3.2 (a conic and a line) we see that there are at most two such different special parametrizations of $\hat{E}^2$ and therefore of E^2 too.

So in the classical offset situation $n = 2, r = const$, we get the well known theorem, that an offset of a rationally parametrized spine curve m can be parametrized with the same parameter as m if and only if m is a pythagoreian hodograph. (Aigner, 97))

REMARK 3.1. *In the general situation we formally do the same manipulations as in the special case but consider them as rational transformations. The association*

$$\begin{pmatrix} x'' \\ t \end{pmatrix} = \begin{pmatrix} \frac{a(t)^2+b(t)^2}{b(t)} & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} u \\ v \\ t \end{pmatrix} + \begin{pmatrix} \frac{-a(t)d(t)}{b(t)} \\ 0 \end{pmatrix}$$

maps the variety

$$\hat{E_1^2} = \{(u, v, t) \in U \mid u^2 + v^2 = 1 \wedge a(t)u + b(t)v = d(t)\}$$

birationally onto

$$\hat{E_2^2} := \{(x'', t) \in \mathbb{R} \times V \mid x''^2 - (a(t)^2 + b(t)^2 - d(t)^2) = 0\}.$$

Its inverse is

$$\begin{pmatrix} u \\ v \\ t \end{pmatrix} = \begin{pmatrix} \frac{b(t)}{a(t)^2+b(t)^2} & 0 \\ \frac{-a(t)}{a(t)^2+b(t)^2} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x'' \\ t \end{pmatrix} + \begin{pmatrix} \frac{a(t)d(t)}{a(t)^2+b(t)^2} \\ \frac{b(t)d(t)}{a(t)^2+b(t)^2} \\ 0 \end{pmatrix}.$$

So from a rational parametrization $(x'', t) \in \mathbb{R}(\Theta)^2$ of $\hat{E}_2^2$, we can calculate a rational parametrization of E^2 :

$$\begin{aligned} x_1(\Theta) &= m_1(t(\Theta)) + r(t(\Theta)) \frac{\dot{m}_2(t(\Theta))x''(\Theta) - \dot{m}_1(t(\Theta))\dot{r}(t(\Theta))}{\dot{m}_1(t(\Theta))^2 + \dot{m}_2(t(\Theta))^2} \\ x_2(\Theta) &= m_2(t(\Theta)) - r(t(\Theta)) \frac{\dot{m}_2(t(\Theta))\dot{r}(t(\Theta)) + \dot{m}_1(t(\Theta))x''(\Theta)}{\dot{m}_1(t(\Theta))^2 + \dot{m}_2(t(\Theta))^2} \end{aligned}$$

Remark 3.2. *An alternative method would be to apply the inverse of the rational transformation*

$$\begin{pmatrix} s \\ t \end{pmatrix} \mapsto \begin{pmatrix} \frac{2s}{1+s^2} \\ \frac{s^2-1}{1+s^2} \\ t \end{pmatrix}$$

which on $\hat{E}_1^2$ is given by

$$\begin{pmatrix} u \\ v \\ t \end{pmatrix} \mapsto \begin{pmatrix} \frac{u}{1-v} \\ t \end{pmatrix}$$

and birationally maps $\hat{E}_1^2$ to E_2^2 :

$$(b(t) - d(t))s^2 + 2a(t)s - (b(t) + d(t)) = 0 \tag{3.5}$$

In order to find a parametrization of the generalized offset, we can apply standard techniques from algebraic curve theory to the plane curve 3.5 and - in case it is rational - go through the process of back transforming as mentioned earlier.

Example 3.1. Consider the circle

$$m(t) = (\frac{2t}{1+t^2}, \frac{t^2-1}{1+t^2}), \ r = const.$$

$\dot{m}_1^2 + \dot{m}_2^2 - \dot{r}^2$ evaluates to $4/(1+t^2)^2$ and so we get a parametrization of the offset via theorem 3.1. The inner and outer offset at distance r is parametrized by

$$x_{1i} = \frac{2t(r+1)}{1+t^2} \quad x_{2i} = \frac{(t^2-1)(r+1)}{1+t^2}$$

$$x_{1o} = -\frac{2t(r-1)}{1+t^2} \quad x_{2o} = -\frac{(t^2-1)(r-1)}{1+t^2}$$

which are concentric circles.

Example 3.2. If we take the same data for m but the radius function $r = \frac{1}{t}$, we get

$$\dot{m}_1^2 + \dot{m}_2^2 - \dot{r}^2 = \frac{(t-1)(1+t)(3t^2+1)}{t^4(1+t^2)^2}$$

so theorem 3.1 is not applicable. Invoking equation 3.5 and simplifying yields

$$4s^2t^3 + s^2 + 2s^2t^2 + s^2t^4 - 4st^4 + 4st^2 - 4t^3 + 1 + 2t^2 + t^4$$

which can be seen to have genus 1. So there is no rational parametrization of the offset.

EXAMPLE 3.3. $m = (t^2, t^3)$, $r = const.$
Equaton 3.5 specialises to

$$3t^2s^2 + 4ts - 3t^2 = 0.$$

After ignoring the factor t we get the parametrization

$$t(\vartheta) = \frac{-4\vartheta}{3(\vartheta^2 - 1)}, \quad s(\vartheta) = s$$

which after back transformation gives us the rational parametrization of the offset:

$$x_1 = \frac{2\vartheta(8\vartheta + 8\vartheta^3 + 9r\vartheta^4 - 18r\vartheta^2 + 9r)}{9(\vartheta - 1)^2(1 + \vartheta)^2(1 + \vartheta^2)}$$

$$x_2 = \frac{-64\vartheta^3 - 64\vartheta^5 + 27r\vartheta^8 - 108r\vartheta^6 + 162r\vartheta^4 - 108r\vartheta^2 + 27r}{27(\vartheta - 1)^3(1 + \vartheta)^3(1 + \vartheta^2)}$$

4. Canal Surfaces

This is the case $n = 3$. The system 2.1 now reads

$$\begin{aligned} (X_1 - m_1(t))^2 + (X_2 - m_2(t))^2 + (X_3 - m_3(t))^2 - r(t)^2 &= 0 \\ (X_1 - m_1(t))\dot{m}_1(t) + (X_2 - m_2(t))\dot{m}_2(t) + (X_3 - m_3(t))\dot{m}_3(t) + r(t)\dot{r}(t) &= 0 \end{aligned} \quad (4.1)$$

A rational parametrization of $\hat{E}^3$ is given by a quadrupel

$$(x_1(\vartheta, \eta), x_2(\vartheta, \eta), x_3(\vartheta, \eta), t(\vartheta, \eta)) \in \mathbb{R}(\vartheta, \eta)^4$$

and projection to the first three coordinates gives a rational parametrization of E^3. From (Peternell & Pottmann, 97) we know, that rational parametrizations of canal surfaces do always exist. We use the following strategy:

1 Find a rational curve $\mathcal{C}$ on E^3
2 Construct a rational parametrization of E^3 with the aid of $\mathcal{C}$.

Of course we have to take care, that the curve $\mathcal{C}$ meets every characteristic circle of E^3, i.e. for every instant t_0 there is a $\vartheta(t_0) \in \mathbb{R}$ such that $(\mathcal{C}(\vartheta(t_0)), t_0)$ solves 4.1. Thus, contrary to the 2-dimensional situation, we do not search for a generally parametrized curve on $\hat{E}^3$ but for a curve parametrized in accordance with the spine. So after performing the transformation 2.2 to obtain

$$\begin{aligned} u_1^2 + u_2^2 + u_3^2 &= 1 \\ a_1(t)u_1 + a_2(t)u_2 + a_3(t)u_3 &= d(t) \end{aligned} \quad (4.2)$$

where we write a_i instead of $\dot{m}_i$ and d for $-\dot{r}$, we work in the vector space $\mathbb{R}(t)^3$ over the field $\mathbb{R}(t)$ of rational functions and treat a_1, a_2, a_3, d as constants. After having established a solution of 4.2, it would be possible to substitute back to get the curve c on E^3 and then - as proposed by Peternell/Pottmann (Peternell & Pottmann, 97) - reflecting every point of c on a pencil of planes to construct the desired parametrization of E^3. We prefer instead to build up a parametrization of the variety $\hat{E}_1^3$ and then lift it back to 4.1. This, of course, is just a matter of taste. Again we handle the case $a_1, a_2, a_3 \neq 0$ first. The general solution of the linear equation is

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} \frac{d}{3a_1} + x_1 a_2 \\ \frac{d}{3a_2} - x_1 a_1 + x_2 a_3 \\ \frac{d}{3a_3} \qquad - x_2 a_2 \end{pmatrix}$$

with $x_1, x_2 \in \mathbb{R}(t)$. Plugging into the quadratic expression and making the following substitutions:

$$\begin{array}{ll} \alpha_1 = a_1^2 + a_2^2 & \gamma_1 = \frac{2d}{3}\frac{a_2^2 - a_1^2}{a_1 a_2} \\ \alpha_2 = a_2^2 + a_3^2 & \gamma_2 = \frac{2d}{3}\frac{a_3^2 - a_2^2}{a_2 a_3} \\ \beta = -a_1 a_3 & \delta = \frac{d^2}{9}(\frac{1}{a_1^2} + \frac{1}{a_2^2} + \frac{1}{a_3^2}) - 1 \end{array}$$

we arrive at the equation

$$\alpha_1 x_1^2 + \alpha_2 x_2^2 + 2\beta x_1 x_2 + \gamma_1 x_1 + \gamma_2 x_2 + \delta = 0. \tag{4.3}$$

In order to construct a quadratic expression without linear terms we make the transformations

$$y_1 = x_1 + \frac{\gamma_1}{2\alpha_1}, y_2 = x_2$$

arriving at

$$\alpha_1 y_1^2 + 2\beta y_1 y_2 + \alpha_2 y_2^2 + (\gamma_2 - \frac{\beta\gamma_1}{\alpha_1})y_2 + \delta - \frac{\gamma_1^2}{4\alpha_1} = 0$$

and $z_1 = y_1 + \frac{\beta}{\alpha_1} y_2, z_2 = y_2$ to end up with

$$\alpha_1 z_1^2 + (\alpha_2 - \frac{\beta^2}{\alpha_1})z_2^2 + (\gamma_2 - \frac{\beta\gamma_1}{\alpha_1})z_2 + \delta - \frac{\gamma_1^2}{4\alpha_1} = 0.$$

Now, for simplicity, we set

$$\lambda = \alpha_2 - \frac{\beta^2}{\alpha_1} \qquad \mu = \gamma_2 - \frac{\beta\gamma_1}{\alpha_1} \qquad \nu = \delta - \frac{\gamma_1^2}{\alpha_1}.$$

So the equation writes

$$\alpha_1 z_1^2 + \lambda z_2^2 + \mu z_2 + \nu = 0.$$

With the substituion $x'_1 = z_1, x'_2 = z_2 + \frac{\mu}{2\lambda}$ we get

$$\alpha_1 x_1'^2 + \lambda x_2'^2 + \nu - \frac{\mu^2}{4\lambda} = 0.$$

Calculating the coefficients gives

$$(a_1^2 + a_2^2)x_1'^2 + \frac{a_2^2(a_1^2 + a_2^2 + a_3^2)}{a_1^2 + a_2^2}x_2'^2 + \frac{d^2 - (a_1^2 + a_2^2 + a_3^2)}{a_1^2 + a_2^2 + a_3^2} = 0,$$

which is equivalent to

$$(a_1^2 + a_2^2)^2(a_1^2 + a_2^2 + a_3^2)x_1'^2 + a_2^2(a_1^2 + a_2^2 + a_3^2)^2 x_2'^2 + (d^2 - (a_1^2 + a_2^2 + a_3^2))(a_1^2 + a_2^2) = 0,$$

and transforms to

$$(a_1^2 + a_2^2 + a_3^2)y_1'^2 + y_2'^2 + (d^2 - (a_1^2 + a_2^2 + a_3^2))(a_1^2 + a_2^2) = 0 \tag{4.4}$$

via the substitution $y_1' = (a_1^2 + a_2^2)x_1', \ y_2' = a_2(a_1^2 + a_2^2 + a_3^2)x_2'$.
So the assignment $(u_1, u_2, u_3) \longleftrightarrow (x_1, x_2)$ constitutes a birational mapping connecting the variety of the system 4.2 with the variety 4.3 whereas $(x_1, x_2) \longleftrightarrow (y_1', y_2')$ defines an affine transformation from 4.3 to 4.4:

$$y_1' = (a_1^2 + a_2^2)x_1 - a_1 a_3 x_2 + \frac{d(a_2^2 - a_1^2)}{3a_1 a_2}$$

$$y_2' = a_2(a_1^2 + a_2^2 + a_3^2)x_2 + \frac{d(2a_3^2 - a_1^2 - a_2^2)}{3a_3}$$

$$x_1 = \frac{1}{a_1^2 + a_2^2}y_1' + \frac{a_1 a_3}{a_2(a_1^2 + a_2^2)(a_1^2 + a_2^2 + a_3^2)}y_2' + \frac{d(2a_1^2 - a_2^2 - a_3^2)}{3a_1 a_2(a_1^2 + a_2^2 + a_3^2)}$$

$$x_2 = \frac{1}{a_2(a_1^2 + a_2^2 + a_3^2)}y_2' + \frac{d(a_1^2 + a_2^2 - 2a_3^2)}{3a_2 a_3(a_1^2 + a_2^2 + a_3^2)}$$

Because $(u_1, u_2, u_3) \longleftrightarrow (x_1, x_2)$ is actually polynomial, the points of the varieties 4.2 and 4.4 are in one-one correspondence under the association $(u_1, u_2, u_3) \longleftrightarrow (y_1', y_2')$.

For convenience we list the chain of transformations connecting equations 4.1 and 4.4:

$$4.1 \longleftrightarrow 4.2: \qquad u_i = \frac{X_i - m_i}{r} \qquad X_i = m_i + r u_i \qquad (1 \le i \le 3)$$

$$4.2 \longleftrightarrow 4.3: \qquad \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} \frac{d}{3a_1} + x_1 a_2 \\ \frac{d}{3a_2} - x_1 a_1 + x_2 a_3 \\ \frac{d}{3a_3} \qquad - x_2 a_2 \end{pmatrix} \qquad \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{3a_1 u_1 - d}{3a_1 a_2} \\ \frac{d - 3a_3 u_3}{3a_2 a_3} \end{pmatrix}$$

$$4.3 \longleftrightarrow 4.4: \quad \begin{cases} \begin{pmatrix} y_1' \\ y_2' \end{pmatrix} = \begin{pmatrix} a_1^2 + a_2^2 & -a_1 a_3 \\ 0 & a_2(a_1^2 + a_2^2 + a_3^2) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} + \begin{pmatrix} \frac{d(a_2^2 - a_1^2)}{3a_1 a_2} \\ \frac{d(2a_3^2 - (a_1^2 + a_2^2))}{3a_3} \end{pmatrix} \\ \\ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} \frac{1}{a_1^2 + a_2^2} & \frac{a_1 a_3}{a_2(a_1^2 + a_2^2)(a_1^2 + a_2^2 + a_3^2)} \\ 0 & \frac{1}{a_2(a_1^2 + a_2^2 + a_3^3)} \end{pmatrix} \begin{pmatrix} y_1' \\ y_2' \end{pmatrix} + \begin{pmatrix} \frac{d(2a_1^2 - a_2^2 - a_3^2)}{3a_1 a_2(a_1^2 + a_2^2 + a_3^2)} \\ \frac{d(a_1^2 + a_2^2 - 2a_3^2)}{3a_2 a_3(a_1^2 + a_2^2 + a_3^2)} \end{pmatrix} \end{cases}$$

Equation 4.4 is the keypoint in this approach. Several methods for finding a solution are treated in the sequel.

Assume we have constructed a solution $(y_1'(t), y_2'(t)) \in \mathbb{R}(t)^2$ of 4.4. Transforming back yields a solution $u(t) = (u_1(t), u_2(t), u_3(t))$ of 4.2 in $\mathbb{R}(t)^3$. Now for a fixed $t_0 \in \mathbb{R}$ let $g_{t_0}(\eta)$ be a 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

$$g_{t_0}(\lambda) = u(t_0) + \lambda[M(t_0) - u(t_0) + \eta(u(t_0) - M(t_0)) \times a(t_0)] \tag{4.5}$$

where $M(t_0)$ denotes the center of that circle in 3-space, which is the real solution of 4.2 for $t = t_0$, i.e.

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

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

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

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

$$(t, \eta) \mapsto u(t) - 2\frac{\langle u(t), v(t, \eta)\rangle}{||v(t, \eta)||^2} v(t, \eta) \tag{4.6}$$

defines a rational parametrization of the variety in 3-space given by 4.2. The canal surface E^3 is now parametrized by

$$X(t, \eta) = m(t) + r(t)\Big(u(t) - 2\frac{\langle u(t), v(t, \eta)\rangle}{||v(t, \eta)||^2} v(t, \eta)\Big). \tag{4.7}$$

The parametrizing map 4.7 is - in addition to arguments which violate our general demand on the spine curve - not defined for those $t_0 \in \mathbb{R}$ for which $v(t_0, \eta) = 0$. It is immediately seen that for such numbers t_0 the plane $\langle a(t_0), X\rangle = d(t_0)$ is tangent to the sphere $||u|| = 1$ and $||\dot{m}(t_0)|| = |\dot{r}(t_0)|$. For a pipe surface this would cause a singularity on the spine and thus an extraneous sphere.

Now we describe methods for finding solutions of equation 4.4 in $\mathbb{R}(t)^2$, which may be done most conveniently in a projective setting. So after homogenization we obtain the equation

$$(a_1^2 + a_2^2 + a_3^2)y_1'^2 + y_2'^2 + (d^2 - a_1^2 - a_2^2 - a_3^2)(a_1^2 + a_2^2)y_3'^2 = 0. \tag{4.8}$$

which will be treated in two different ways. The first one is by application of a projective transformation, the second by invoking a generalization of the Legendre Theorem from number theory.

Equation 4.8 has the solution $p = ((a_3+d)i : -(a_1^2+a_2^2+a_3^2+a_3 d) : 1)$ in $\mathbb{P}^2(\mathbb{C}(t))$. One might try to use this point to parametrize all complex solutions of 4.8 and then select the real ones from all the solutions. Unfortunately this procedure leads to an equation similar to the original one, so we try a different approach. If we apply a projective transformation in order to force the variety to contain the circular point at infinity $q = (1 : i : 0)$, then in the new coordinates we get an equation of the form

$$az_1'^2 + bz_1'z_2' + cz_2'^2 + z_3'(\ldots) = 0$$

and because q is a solution we conclude that $a = c$ and $b = 0$.

To be precise, let $A \in \mathrm{GL}_3(\mathbb{R}(t))$, with the property $Ap = q$, $B = A^{-1}$. Solving a linear system we see that we can choose

$$A = \begin{pmatrix} 0 & 0 & 1 \\ \frac{1}{a_3+d} & 0 & 0 \\ 0 & 1 & a_1^2+a_2^2+a_3^2+a_3 d \end{pmatrix} \quad B = \begin{pmatrix} 0 & a_3+d & 0 \\ -(a_1^2+a_2^2+a_3^2+a_3 d) & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

(we ignore the case $a_3+d=0$ which at once gives the solution $(0 : a_1^2+a_2^2 : 1)$.) Plugging in the new variables $(z_1', z_2', z_3')^T = A(y_1', y_2' y_3')^T$ gives

$$(a_1^2+a_2^2+a_3^2)(a_3+d)^2(z_1'^2+z_2'^2) + z_3'^2 - 2(a_1^2+a_2^2+a_3^2+a_3 d)z_1' z_3' = 0.$$

Now the substitution

$$x_1'' = z_1' - \frac{a_1^2+a_2^2+a_3^2+a_3 d}{(a_1^2+a_2^2+a_3^2)(a_3+d)^2} z_3', \ x_2'' = z_2', \ x_3'' = z_3'$$

leads to

$$(a_1^2+a_2^2+a_3^2)(a_3+d)^2 x_1''^2 + (a_1^2+a_2^2+a_3^2)(a_3+d)^2 x_2''^2 + x_3''^2 - \frac{(a_1^2+a_2^2+a_3^2+a_3 d)^2}{(a_1^2+a_2^2+a_3^2)(a_3+d)^2} x_3''^2 = 0$$

which is equivalent to

$$(a_1^2+a_2^2+a_3^2)^2(a_3+d)^4 x_1''^2 + (a_1^2+a_2^2+a_3^2)^2(a_3+d)^4 x_2''^2 + (a_1^2+a_2^2)(d^2-a_1^2-a_2^2-a_3^2)x_3''^2$$

Finally with substitution

$$y_1'' := (a_1^2+a_2^2+a_3^2)(a_3+d)^2 x_1'', \ y_2'' := (a_1^2+a_2^2+a_3^2)(a_3+d)^2 x_2'', \ y_3'' := x_3''$$

we end up with

$$y_1''^2 + y_2''^2 = (a_1^2+a_2^2)(a_1^2+a_2^2+a_3^2-d^2)y_3''^2 \tag{4.9}$$

The varieties 4.8 and 4.9 are connected by the projective transformation

$$\begin{pmatrix} y_1' \\ y_2' \\ y_3' \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{(a_1^2+a_2^2+a_3^2)(a_3+d)} & 0 \\ \frac{-(a_1^2+a_2^2+a_3^2+a_3 d)}{(a_1^2+a_2^2+a_3^2)(a_3+d)^2} & 0 & \frac{(a_1^2+a_2^2)(d^2-a_1^2-a_2^2-a_3^2)}{(a_1^2+a_2^2+a_3^2)(a_3+d)^2} \\ \frac{1}{(a_1^2+a_2^2+a_3^2)(a_3+d)^2} & 0 & \frac{a_1^2+a_2^2+a_3^2+a_3 d}{(a_1^2+a_2^2+a_3^2)(a_3+d)^2} \end{pmatrix} \begin{pmatrix} y_1'' \\ y_2'' \\ y_3'' \end{pmatrix}$$

$$\begin{pmatrix} y_1'' \\ y_2'' \\ y_3'' \end{pmatrix} = \begin{pmatrix} 0 & -(a_1^2+a_2^2+a_3^2+a_3 d) & (a_1^2+a_2^2)(d^2-a_1^2-a_2^2-a_3^2) \\ (a_1^2+a_2^2+a_3^2)(a_3+d) & 0 & 0 \\ 0 & 1 & a_1^2+a_2^2+a_3^2+a_3 d \end{pmatrix} \begin{pmatrix} y_1' \\ y_2' \\ y_3' \end{pmatrix}$$

In affine coordinates equation 4.9 is

$$y_1''^2 + y_2''^2 = (a_1^2+a_2^2)(a_1^2+a_2^2+a_3^2-d^2) \tag{4.10}$$

Essentially the same methods apply to the case, where one of the expressions a_1, a_2, a_3 is zero. Again we arrive at equation 4.10, but we have to be careful during back transformation, to avoid zero denominators. If e.g. $a_3 = 0$ - we can therefor assume $a_1, a_2 \neq 0$ - then we may proceed in the following manner:
The system 4.2 is birationally equivalent to

$$y_1'^2 + (a_1^2+a_2^2)y_2'^2 + a_2^2(d^2-a_1^2-a_2^2) = 0 \tag{4.11}$$

via the formulas

$$\begin{pmatrix} y_1' \\ y_2' \end{pmatrix} = \begin{pmatrix} (a_1^2+a_2^2)u_1 - da_1 \\ a_2 - u_3 \end{pmatrix} \qquad \begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} \frac{y_1'+da_1}{a_1^2+a_2^2} \\ \frac{da_2^2-a_1y_1'}{a_2(a_1^2+a_2^2)} \\ \frac{y_2'}{a_2} \end{pmatrix}$$

In case $d=0$ we have to solve equation

$$y_1'^2 + (a_1^2+a_2^2)y_2'^2 = (a_1^2+a_2^2)a_2^2.$$

But in this case we have simpler solution: recall that $a_i = \dot{m}_i$ and $d = -\dot{r}$. Thus a cross section of the canal surface is given by $c(t) = (m_1(t), m_2(t), m_3 - r)$. In this way we obtain rational parametrizations of pipe surfaces for all plane rational parametrizable curves.

If $d \neq 0$, then equation 4.11 transforms to 4.10 by

$$\begin{pmatrix} y_1'' \\ y_2'' \\ y_3'' \end{pmatrix} = \begin{pmatrix} 0 & a_1^2+a_2^2 & a_2(d^2-a_1^2-a_2^2) \\ d & 0 & 0 \\ 0 & 1 & -a_2 \end{pmatrix} \begin{pmatrix} y_1' \\ y_2' \\ y_3' \end{pmatrix}$$

whose inverse is given by

$$\begin{pmatrix} y_1' \\ y_2' \\ y_3' \end{pmatrix} = \begin{pmatrix} 0 & \frac{1}{d} & 0 \\ \frac{1}{d^2} & 0 & 1-\frac{a_1^2+a_2^2}{d^2} \\ \frac{1}{a_2d^2} & 0 & \frac{-a_1^2-a_2^2}{a_2d^2} \end{pmatrix} \begin{pmatrix} y_1'' \\ y_2'' \\ y_3'' \end{pmatrix}.$$

In each case we arrive at equation 4.10. Solving this equation is obviously the same as giving a presentation of $(a_1^2+a_2^2)(a_1^2+a_2^2+a_3^2-d^2)$ as sum of two squares. The next corollary says, that this problem can easily be solved:

Lemma 4.1. *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 4.1. *Let F be in $\mathbb{R}[t]$. Then F is a sum of two squares in $\mathbb{R}[t]$ iff $F \geq 0$ (i.e. $F(x) \geq 0 \forall x \in \mathbb{R}$).*

Proof. Assume $F \geq 0$. 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 $b_i^2 - 4a_ic_i \leq 0$. Every quadratic Q_i can be written as

$$Q_i = (\sqrt{a_i}t + \frac{b_i}{2\sqrt{a_i}})^2 + \sqrt{c_i - \frac{b_i^2}{4a_i}}^2$$

thus it is a sum of two squares.

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

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \tag{4.12}$$

shows, that their product is a sum of two squares too. □

COROLLARY 4.2. *Let ρ be in $\mathbb{R}(t)$. Then ρ is a sum of two squares iff $\rho = \frac{F}{G}$ with $F, G \in \mathbb{R}[t]$ and $F \geq 0$ and G is a square in $\mathbb{R}[t]$.*

PROOF. If ρ is a sum of two squares then

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

Conversely if $\rho = \frac{F}{G}$ with $F \geq 0$ and $G = H^2$ then $F = A^2 + B^2$ by the previous corollary and thus $\rho = \left(\frac{A}{H}\right)^2 + \left(\frac{B}{H}\right)^2$. □

Thus we are led to the following theorem:

THEOREM 4.1. *Equation 4.10 has a solution $(y_1'', y_2'') \in \mathbb{R}(t)^2$ iff for all $x \in \mathbb{R}$ not zero of the denominator of any 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 we have a solution $(y_1'', y_2'') \in \mathbb{R}(t)^2$ of 4.10. Then the relation

$$a_1^2 + a_2^2 + a_3^2 - d^2 = \frac{y_1''^2 + y_2''^2}{a_1^2 + a_2^2}$$

shows the correctness of the assertion. 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

$$\begin{aligned} a_1^2 + a_2^2 + a_3^2 - d^2 &= \frac{A_1^2}{B_1^2} + \frac{A_2^2}{B_2^2} + \frac{A_3^2}{B_3^3} - \frac{D^2}{E^2} = \\ = \quad & \frac{(A_1 B_2 B_3 E)^2 + (B_1 A_2 B_3 E)^2 + (B_1 B_2 A_3 E)^2 - (B_1 B_2 B_3 D)^2}{(B_1 B_2 B_3 E)^2} \end{aligned}$$

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 4.2 shows, that it is a sum of two squares and by the formula 4.12 given in the proof of corollary 4.1 we once get a solution of 4.10. □

We therefore may formulate the following theorem:

THEOREM 4.2. *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 $x \in \mathbb{R}$.*

If the condition stated in the theorem is fulfilled, we can find a parametrization by first factorizing the numerator of $\dot{m}_1^2 + \dot{m}_2^2 + \dot{m}_3^2 - \dot{r}^2$ in $\mathbb{R}[t]$ and then generate a solution of 4.10 by iterated application of formula 4.12, and after this, transforming back to get a solution of 4.1.

In general the rational function $\rho := \dot m_1(t)^2 + \dot m_2(t)^2 + \dot m_3(t)^2 - \dot r(t)^2$ need not be positive for almost all real values t. In this case we have to restrict ourselves to intervals, on which $\rho \geq 0$ holds, and reparametrize the spine curve. If e.g. ρ is positive on $[a,b] \subset \mathbb{R}$, we can apply the reparametrization $t = \frac{b\vartheta^2+a}{\vartheta^2+1}$. In case $\rho \geq 0$ on $[a,\infty)$ we can use $t = \vartheta^2 + a$. Thus we may formulate the following algorithm:

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 intervall (a,b) on which $\rho \geq 0$.
3 If $(a,b) \neq \mathbb{R}$ then reparametrize $t := t(s)$, so that $\rho(s) \geq 0$.
4 Compute a decomposition $\rho = \sigma^2 + \tau^2$.
5 Set $y_1'' := \dot m_1\sigma + \dot m_2\tau \quad y_2'' := \dot m_1\tau - \dot m_2\sigma$.
6 Apply the inverse transformations to get a curve $\mathcal{C}$ on the variety 4.2.
7 Compute a surface parametrization of 4.2 with the aid of the curve $\mathcal{C}$ according to formula 4.6.
8 Compute a rational parametrization of the canal surface according to formula 4.7.

EXAMPLE 4.1. $m = (t, t^2, t^3), r = const$. Equation 4.10 is now

$$y_1''^2 + y_2''^2 = (1+4t^2)(1+4t^2+9t^4)$$

Factorization and application of the corollary gives

$$\begin{aligned}(1+4t^2+9t^4) &= (3t^2-\sqrt{2}t+1)(3t^2+\sqrt{2}t+1) = \left((\sqrt{3}t-\tfrac{1}{\sqrt{6}})^2+\sqrt{\tfrac{5}{6}}^2)((\sqrt{3}t+\tfrac{1}{\sqrt{6}})^2+\sqrt{\tfrac{5}{6}}^2\right) \\ &= ((\sqrt{3}t-\tfrac{1}{\sqrt{6}})(\sqrt{3}t+\tfrac{1}{\sqrt{6}})+\sqrt{\tfrac{5}{6}}\sqrt{\tfrac{5}{6}})^2+(\sqrt{3}t-\tfrac{1}{\sqrt{6}})\sqrt{\tfrac{5}{6}}-\sqrt{\tfrac{5}{6}}(\sqrt{3}t+\tfrac{1}{\sqrt{6}}))^2 \\ &= (3t^2+\tfrac{2}{3})^2+(\tfrac{\sqrt{5}}{3})^2\end{aligned}$$

Consequently

$$(1+4t^2)(1+4t^2+9t^4) = \left((3t^2+\tfrac{2}{3})1+\tfrac{\sqrt{5}}{3}2t\right)^2+\left((3t^2+\tfrac{2}{3})2t-\tfrac{\sqrt{5}}{3}1\right)^2 = \left(3t^2+\tfrac{2\sqrt{5}}{3}t+\tfrac{2}{3}\right)^2+\left(6t^3+\tfrac{4}{3}t-\tfrac{\sqrt{5}}{3}\right)^2$$

So a solution of 4.9 is given by

$$\left(3t^2+\frac{2\sqrt{5}}{3}t+\frac{2}{3} : -6t^3-\frac{4}{3}t+\frac{\sqrt{5}}{3} : 1\right).$$

Transforming back yields

$$\begin{pmatrix} y_1' \\ y_2' \\ y_3' \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{5}-18t^3-4t)}{9(1+4t^2+9t^4)t^2} \\ \frac{21t^2+5+2t\sqrt{5}}{-27t^4} \\ \frac{21t^2+5+2t\sqrt{5}+27t^4}{27(1+4t^2+9t^4)t^4} \end{pmatrix}$$

We set $y_1' := \frac{y_{1,}}{y_3'}$, $y_2' := \frac{y_2'}{y_3'}$ to get a solution of 4.4. Generating the solution of 4.2 yields

$$\begin{pmatrix} u_1 \\ u_2 \\ u_3 \end{pmatrix} = \begin{pmatrix} \frac{-3t^2(9t^2+5)}{21t^2+5+2t\sqrt{5}+27t^4} \\ \frac{-3t^2(6t+\sqrt{5})}{21t^2+5+2t\sqrt{5}+27t^4} \\ \frac{21t^2+5+2t\sqrt{5}}{21t^2+5+2t\sqrt{5}+27t^4} \end{pmatrix}$$

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

$$\begin{pmatrix} c_1(t) \\ c_2(t) \\ c_3(t) \end{pmatrix} = \begin{pmatrix} t - 3\frac{rt^2(9t^2+5)}{21t^2+5+2t\sqrt{5}+27t^4} \\ t^2 - 3\frac{rt^2(6t+\sqrt{5})}{21t^2+5+2t\sqrt{5}+27t^4} \\ t^3 + \frac{r(21t^2+5+2t\sqrt{5})}{21t^2+5+2t\sqrt{5}+27t^4} \end{pmatrix}$$

Not using the last result, by applying formula 4.6 we get a rational parametrization $(U_1(t,\eta), U_2(t,\eta), U_3(t,\eta))$ of $\hat{E}_1^3$:

$$U_1 = -\frac{(243\eta^2t^7+243\eta^2t^5+108\eta t^4+87\eta^2t^3-27t^3+18\eta t^3\sqrt{5}+84\eta t^2+8\eta t\sqrt{5}+15t\eta^2-15t+20\eta)t}{(9\eta^2t^4+4\eta^2t^2+\eta^2+1)(21t^2+5+2t\sqrt{5}+27t^4)}$$

$$U_2 = -\frac{162\eta^2t^7+27\eta^2t^6\sqrt{5}-162\eta t^6+72\eta^2t^5-90\eta t^4+12\eta^2t^4\sqrt{5}-18t^3+18\eta^2t^3+3\eta^2t^2\sqrt{5}-3t^2\sqrt{5}-42\eta t^2-4\eta t\sqrt{5}-10\eta}{(9\eta^2t^4+4\eta^2t^2+\eta^2+1)(21t^2+5+2t\sqrt{5}+27t^4)}$$

$$U_3 = \frac{189\eta^2t^6-108\eta t^5+18\eta^2t^5\sqrt{5}+129\eta^2t^4+8\eta^2t^3\sqrt{5}-24\eta t^3-21t^2+6\eta t^2\sqrt{5}+41\eta^2t^2+2\eta^2t\sqrt{5}-2t\sqrt{5}+5\eta^2-5}{(9\eta^2t^4+4\eta^2t^2+\eta^2+1)(21t^2+5+2t\sqrt{5}+27t^4)}$$

Now a parametrization of the pipe surface is given by the formulas

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

Example 4.2. [Viviani's temple] This space curve is defined as the intersaction of a sphere of radius $2a$ and a circular cylinder of radius a:

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

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

$$c_1(t) = \frac{N_1}{D_1}, \quad c_2(t) = \frac{N_2}{D_2} \quad c_3(t) = \frac{N_3}{D_3}$$

where

$$\begin{aligned} N_1 &= (-1+t^2)(8a\sqrt{2}t^3 - 16a\sqrt{2}t^5 - 2a\sqrt{2} - 14a\sqrt{2}t^4 + 14a\sqrt{2}t^2 - 4a + 8a\sqrt{2}t^7 \\ &\quad +2at^6\sqrt{2} + 4at^8 + 3rt^4\sqrt{2} + 3rt^6\sqrt{2} + rt^8\sqrt{2} - 4rt^3 + 4rt^5 + 4rt^7 + rt^2\sqrt{2} - 4rt) \\ N_2 &= (1-t^2)(-16a\sqrt{2}t^4 + 16at^6\sqrt{2} + 4at\sqrt{2} + 4a\sqrt{2}t^5 - 24a\sqrt{2}t^3 + 8at^7 + 8at^5 \\ &\quad +8at^3 + 8at + 10rt^4 + 4rt^6 - rt^8 + 4rt^2 - 3rt^2\sqrt{2} - 3rt^4\sqrt{2} - rt^6\sqrt{2} - r - r\sqrt{2}) \\ N_3 &= (-16a\sqrt{2}t^4 + 16at^6\sqrt{2} + 4at\sqrt{2} + 4a\sqrt{2}t^5 - 24a\sqrt{2}t^3 + 8at^7 + 8at^5 + 8at^3 + 8at \end{aligned}$$

$$-4r\sqrt{2}t^3+4r\sqrt{2}t^7+r\sqrt{2}-5rt^2\sqrt{2}-5rt^4\sqrt{2}+rt^6\sqrt{2}+r+4rt^2+6rt^4+4rt^6+rt^8)$$

$$\begin{aligned} D_1 &= D2 \;=\; (1+t^2)^2(-4\sqrt{2}t^3+4\sqrt{2}t^5+\sqrt{2}+\sqrt{2}t^4-6\sqrt{2}t^2+2t^6+2t^4+2t^2+2) \\ D_3 &= (1+t^2)(-4\sqrt{2}t^3+4\sqrt{2}t^5+\sqrt{2}+\sqrt{2}t^4-6\sqrt{2}t^2+2t^6+2t^4+2t^2+2) \end{aligned}$$

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

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 4.1. For symbolic treatment of step 4 in the algorithm **CANAL_SURFACE**, the following variant of the problem arises:

PROBLEM 4.1. 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 4.2) Actually, computability of k is not enough for solving this problem. We have to assume at least that we can solve problem 4.1 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 (Davenport & Trager, 81)). Problem 4.1 is a special case of the problem solved in (Hillgarter, 96; Hillgarter & Winkler, 98). 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 4.3. *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

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

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 4.1. 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.

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 (Abbot, 88; Landau, 85; Lenstra, 82; Wang, 76) 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 perfomance 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 4.12. This leads to the following algorithm for the solution of problem 4.1.

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;
    Γ:= 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 4.3. 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 $\mathbf{Q}$. 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 its negative as square roots of -1 modulo F. At this step, we know that a solution exists. Because the leading coefficient is 1^2+0^2, we set

$$X := x_0 + x_1t + x_2t^2 + t^3, Y := y_0 + y_1t + y_2t^2.$$

The coefficients of remainder($X-RY,F$) are

$$-1/19\,y_2 + \frac{10}{19}\,y_0 + \frac{3}{19}\,y_1, -\frac{17}{19}\,y_2 - \frac{25}{19}\,y_1 - \frac{39}{19}\,y_0 + 1,$$

$$\frac{25}{19}\,y_2 + \frac{73}{19}\,y_0 + \frac{39}{19}\,y_1 + x_2, -\frac{21}{19}\,y_2 - \frac{94}{19}\,y_0 - \frac{51}{19}\,y_1 + x_1,$$

$$x_0 + \frac{35}{19}y_1 + \frac{20}{19}y_2 + \frac{47}{19}y_0, -\frac{7}{19}y_0 - \frac{5}{19}y_2 - \frac{4}{19}y_1$$

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

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

5. The General Case

After discussion of the problem in dimensions $n = 2, 3$ we propose the following approach for handling the general case:

Starting from 2.1 and applying the transformation 2.2 we consider the system 2.3 whose set of zeroes is $\hat{E_1^n}$. Again we set $a_j = \dot{m}_j(t),\ d = -\dot{r}(t)$.

LEMMA 5.1. *The variety given by the system*

$$\begin{aligned} u_1^2 + \cdots + u_n^2 &= 1 \\ a_1(t)u_1 + \cdots + a_n(t)u_n &= d(t) \quad (n \geq 2) \end{aligned}$$

transforms birationally to

$$\alpha_1(t)y_1^2 + \cdots + \alpha_{n-1}(t)y_{n-1}^2 + \beta_n(t) = 0$$

where

$$\alpha_k(t) = \frac{\sum_{j=1}^{k+1} a_j(t)^2}{\sum_{j=1}^{k} a_j(t)^2} \quad (1 \leq k \leq n-1) \quad \textit{and} \quad \beta_n(t) = \frac{d(t)^2 - \sum_{j=1}^{n} a_j(t)^2}{\sum_{j=1}^{n} a_j(t)^2}.$$

PROOF. By linear algebra motivation we use the map

$$\begin{aligned} u_1 &= x_1 a_2(t) \\ u_2 &= -x_1 a_1(t) + x_2 a_3(t) \\ u_3 &= -x_2 a_2(t) + x_3 a_4(t) \\ &\vdots \\ u_{n-1} &= -x_{n-2} a_{n-2}(t) + x_{n-1} a_n(t) \\ u_n &= \frac{d(t)}{a_n(t)} - x_{n-1} a_{n-1}(t) \\ t &= t \end{aligned}$$

With the abbreviations

$$A_k := a_k(t)^2 + a_{k+1}(t)^2 \quad (1 \leq k < n) \quad B_k := a_k(t) a_{k+2}(t) \quad (1 \leq k < n-1)$$

we derive

$$\sum_{k=1}^{n-1} A_k x_k^2 - 2\sum_{k=1}^{n-2} B_k x_k x_{k+1} - 2\frac{d a_{n-1}}{a_n} x_{n-1} + \frac{d^2}{a_n^2} - 1 = 0.$$

We define recursively

$$\tilde{\alpha}_1 := A_1 \quad \tilde{\alpha}_{j+1} := A_{j+1} - \frac{B_j^2}{\tilde{\alpha}_j} \quad (1 \leq j < n-1)$$

and

$$\beta_n := \frac{d^2(\tilde\alpha_{n-1} - a_{n-1}^2) - a_n^2\tilde\alpha_{n-1}}{a_n^2\tilde\alpha_{n-1}}.$$

Then the transformation

$$z_k = x_k - \frac{B_k}{\tilde\alpha_k}x_{k+1} \quad (1 \le k < n-1) \quad z_{n-1} = x_{n-1} - \frac{a_{n-1}d}{\tilde\alpha_{n-1}a_n} \tag{5.1}$$

leads to the equation

$$\sum_{j=1}^{n-1} \tilde\alpha_j z_j^2 + \beta_n = 0.$$

This is easy to see for $n = 2$. For $n + 1$ we get

$$\begin{aligned} &\sum_{k=1}^{n} A_k x_k^2 - 2\sum_{k=1}^{n-1} B_k x_k x_{k+1} - 2\frac{da_n}{a_{n+1}}x_n + \frac{d^2}{a_{n+1}^2} - 1 = \\ = \;& \sum_{k=1}^{n-1} A_k x_k^2 - 2\sum_{k=1}^{n-2} B_k x_k x_{k+1} - 2\frac{da_{n-1}}{a_n}x_{n-1} + \frac{d^2}{a_n^2} - 1 + \\ &+A_n x_n^2 - 2B_{n-1}x_{n-1}x_n + 2\frac{da_{n-1}}{a_n}x_{n-1} - \frac{d}{a_n^2} - 2\frac{da_n}{a_{n+1}}x_n + \frac{d^2}{a_{n+1}^2} \end{aligned}$$

By induction hypothesis this is

$$\begin{aligned} &\sum_{k=1}^{n-2} \tilde\alpha_k z_k^2 + \tilde\alpha_{n-1}(x_{n-1} - \frac{a_{n-1}d}{\tilde\alpha_{n-1}a_n})^2 + \beta_n + \\ &+A_n x_n^2 - 2B_{n-1}x_{n-1}x_n + 2\frac{da_{n-1}}{a_n}x_{n-1} - \frac{d}{a_n^2} - 2\frac{da_n}{a_{n+1}}x_n + \frac{d^2}{a_{n+1}^2} \end{aligned}$$

where $z_k = x_k - \frac{B_k}{\tilde\alpha_k}x_{k+1} \quad (1 \le k < n-1)$. Now with

$$z_{n-1} = x_{n-1} - \frac{B_{n-1}}{\tilde\alpha_{n-1}}x_n$$

this yields

$$\sum_{k=1}^{n-2} \tilde\alpha_k z_k^2 + \tilde\alpha_{n-1}\big(z_{n-1}^2 - \frac{B_{n-1}^2}{\tilde\alpha_{n-1}^2}x_n^2\big) + A_n x_n^2 - 2\frac{a_n d}{a_{n+1}}x_n + \frac{d^2}{a_{n+1}^2} - 1$$

The substitution

$$z_n = x_n - \frac{a_n d}{\tilde\alpha_n a_{n+1}}$$

gives

$$\sum_{k=1}^{n-1} \tilde\alpha_k z_k^2 + \tilde\alpha_n\big(z_n^2 - \frac{d^2a_n^2}{\tilde\alpha_n^2 a_{n+1}^2}\big) + \frac{d^2}{a_{n+1}^2} - 1$$

which finally computes to

$$\sum_{k=1}^{n} \tilde\alpha_k z_k^2 + \beta_{n+1}.$$

A straightforward induction shows that

$$\tilde{\alpha}_k = \frac{a_k^2 \sum_{j=1}^{k+1} a_j^2}{\sum_{j=1}^{k} a_j^2} \quad (1 \leq k < n)$$

After this the β_n is easily seen to be of the claimed form. Now with the transformation

$$y_j = a_j(t) z_j \qquad (1 \leq j \leq n-1)$$

the last equation becomes

$$\alpha_1(t) y_1^2 + \cdots + \alpha_{n-1}(t) y_{n-1}^2 + \beta_n(t) = 0. \tag{5.2}$$

□

Now we consider the solution set of equation 5.2 in $\mathbb{P}^{n-1}(\mathbb{C}(t))$.

THEOREM 5.1. *Let G_n denote the expression*

$$G_n = \sum_{j=1}^{n-1} \alpha_j y_j^2 + \beta_n y^2 \qquad (n \geq 2).$$

If $(y_1 : \cdots : y_{n-1} : y)$ is a solution of $G_n = 0$ then $(y_1 : \cdots : y_{n-1} : \frac{d a_{n+1}}{\sum_{j=1}^{n+1} a_j^2} y : y)$ solves the equation $G_{n+1} = 0$.

PROOF. We use the symbol s_n as an abbreviation for $\sum_{j=1}^{n} a_j^2$.
Assume $G_n(y_1 : \cdots : y_{n-1} : y) = 0$. This means

$$\alpha_1 y_1^2 + \cdots + \alpha_{n-1} y_{n-1}^2 + \beta_n y^2 = 0.$$

It follows

$$\alpha_1 y_1^2 + \cdots + \alpha_{n-1} y_{n-1}^2 + \alpha_n \left(\frac{d a_{n+1}}{s_{n+1}} y\right)^2 + \beta_{n+1} y^2 = \alpha_n \frac{d^2 a_{n+1}^2}{s_{n+1}^2} y^2 + \beta_{n+1} y^2 - \beta_n y^2 =$$

$$= y^2 \left(\frac{s_{n+1}}{s_n} \frac{d^2 a_{n+1}^2}{s_{n+1}^2} + \frac{d^2 - s_{n+1}}{s_{n+1}} - \frac{d^2 - s_n}{s_n}\right) = \frac{y^2 d^2}{s_n s_{n+1}} (a_{n+1}^2 + s_n - s_{n+1}) = 0.$$

□

The last theorem allows to construct from any solution of $G_n = 0$ solutions of $G_m = 0$ for $m > n$. From chapter 5 we derive the solution

$$\left(\frac{a_3 + d}{a_1^2 + a_2^2} i : \frac{a_1^2 + a_2^2 + a_3^2 + a_3 d}{a_1(a_1^2 + a_2^2 + a_3^2)} : \frac{1}{a_1}\right)$$

of G_3 in $\mathbb{P}^2(\mathbb{C}(t))$. Thus we get the solution

$$\left(\frac{a_3 + d}{a_1^2 + a_2^2} i : \frac{a_1^2 + a_2^2 + a_3^2 + a_3 d}{a_1(a_1^2 + a_2^2 + a_3^2)} : \frac{d a_4}{(a_1^2 + a_2^2 + a_3^2 + a_4^2) a_1} : \frac{1}{a_1}\right)$$

of G_4 in $\mathbb{P}^3(\mathbb{C}(t))$.

References

ABBOT,J.A. (1988) *Factorisation of Polynomials over Algebraic Number Fields*, Univ. of Bath, England, 1988.

ABHYANKAR, S. S., BAJAJ, C. (1986). *Automatic parametrization of curves and surfaces i: Conics and conicoids.* Technical report, Computer Science Department, Purdue University, West Lafayette, IN 47907.

AIGNER, K. (1997) *Symbolic Computation of and with Offset Curves.* Master paper, Research Institute for Symbolic Computation, Johannes Kepler Universität Linz.

DAVENPORT,J.H., TRAGER,B.M. (1981). *Factorization over finitely generated fields.* SYMSAC '81: Proceedings of the 1981 ACM Symposium on Symbolic and Algebraic Computation, Association for Computing Machinery.

DEGEN, W. (1967) *On the projective differential geometry of surfaces that are generated by a one parameter family of conics.* Math. Ann. **170**, 1-36.

FAROUKI, R.T., NEFF, C.A. (1990) *Analytic properties of plane offset curves.* Computer Aided Geometric Design **7**, 83-99.

FAROUKI, R.T., NEFF, C.A. (1990) *Algebraic properties of plane offset curves.* Computer Aided Geometric Design **7**, 101-127.

GREENBERG, M.J. (1969) *Lectures on forms in many variables.* Benjamnin 1969.

HARTSHORNE, R. (1977) *Algebraic Geometry.* Graduate Texts in Mathematics, New York, Springer-Verlag.

HILLGARTER, E. (1996) *Rational Points on Conics.* RISC-Linz Report 96-34.

HILLGARTER, E., WINKLER, F. (1998) *Points on Algebraic Curves and the Parametrization Problem.* In: Automated Deduction in Geometry, D. Wang and L. Fariñas and H.Shi, Ed. Springer, pp. 185–203.

IRELAND, K., ROSEN,M. (1982) *A Classical Introduction to Modern Number Theory.* Graduate Texts in Mathematics, Springer-Verlag, New York Heidelberg Berlin.

LANDAU,S. (1985) *Factoring Polynomials over Algebraic Number Fields.* sicomp **14/1**, feb.1985, 184-195.

LENSTRA, A.K. (1982) *Factoring Polynomials over Algebraic Number Fields.* Stichting Mathematisch Centrum, Kruislaan 413 1098 SJ Amsterdam", nov.1982.

MAEKAWA, T., PATRIKALAKIS, N.M., SAKKALIS, T. (1998) *Analysis and applications of pipe surfaces.* Computer Aided Geometric Design **15**, 437-458.

MNUK, M. (1995) *Algebraic and Geometric Approach to Paramtrization of Rational Curves.* PhD thesis, Univ. Linz.

PETERNELL, M., POTTMANN, H. (1997) *Computing Rational Parametrizations of Canal Surfaces.* J.Symbolic Computation **23**, 255-266.

POTTMANN, H., PETERNELL, M. (1998) *Applications of Laguerre geometry in CAGD.* Computer Aided Geometric Design **15** (1998) 165-186.

RECIO, T., SENDRA, J.R. (1997) *Real Reparametrizations of Real Curves.* J.Symbolic Computation **23**, 241-254.

SCHICHO, J. (1995) *Rational Parametrization of Algebraic Surfaces.* PhD thesis, Univ. Linz.

SCHICHO, J. (1997) *Rational Parametrization of Surfaces.* J.Symbolic Computation **26**, 1-30.

SCHICHO, J. (1998) *Rational Parameterization of Real Algebraic Surfaces.* ISSAC **98**, 302-308, ACM Press.

SENDRA, J.R., WINKLER, F. (1991) *Symbolic Parametrization of Curves.* J.Symbolic Computation **12**, 607-631.

SENDRA, J.R., WINKLER, F. (1997) *Parametrization of Algebraic Curves over Optimal Field Extensions.* J. Symbolic Computation **23**, 191-207.

WANG, P.S. (1976) *Factoring Multivariate Polynomials over Algebraic Number Fields.* mathcomp **32/144**, oct.1976, 324- 336.

WINKLER, F. (1996) *Polynomial Algorithms in Computer Algebra.* Texts and Monographs in Symbolic Computation, Springer Wien New York.