Technical Report

Algorithms for Trigonometric Curves (Simplification, Implicitization, Parameterization)

Hoon Hong and Josef Schicho

Research Institute for Symbolic Computation

Johannes Kepler University

A-4040 Linz, Austria

e-mail: {hhong,jschicho}@risc.uni-linz.ac.at

www: http://www.risc.uni-linz/people/{hhong,jschicho}

(Received 27 February 1997)

A trigonometric curve is a real plane curve where each coordinate is given parametrically by a truncated Fourier series. The trigonometric curves frequently arise in various areas of mathematics, physics, and engineering. Some trigonometric curves can be also represented implicitly by bivariate polynomial equations. In this paper, we give algorithms for (a) simplifying a given parametric representation, (b) computing an implicit representation from a given parametric representation, and (c) computing a parametric representation from a given implicit representation.

1. Introduction

A trigonometric curve is a real plane curve where each coordinate is given parametrically by a trigonometric polynomial, that is, a truncated Fourier series:

$$\begin{aligned} x &= \sum_{k=0}^{m} a_k \cos(k\theta) + b_k \sin(k\theta) \\ y &= \sum_{k=0}^{n} c_k \cos(k\theta) + d_k \sin(k\theta) \end{aligned}$$

where $\theta \in [0, 2\pi]$. Figure 1 gives the picture of the following small examples:

Ex1: $x = \cos(5\theta)$
$y = \sin(7\theta)$

Ex2: $x = 2\cos(2\theta) + \sin(2\theta) + \sin(6\theta)$
$y = \cos(2\theta) + \sin(2\theta) + \cos(10\theta)$

Ex3: $x = \cos(\theta) - \sin(\theta) + \cos(2\theta) - \sin(2\theta) + \cos(3\theta) - \sin(3\theta) + \cos(4\theta) - \sin(4\theta)$
$y = \cos(\theta) + \sin(\theta) + \cos(2\theta) + \sin(2\theta) + \cos(3\theta) + \sin(3\theta) + \cos(4\theta) + \sin(4\theta)$.

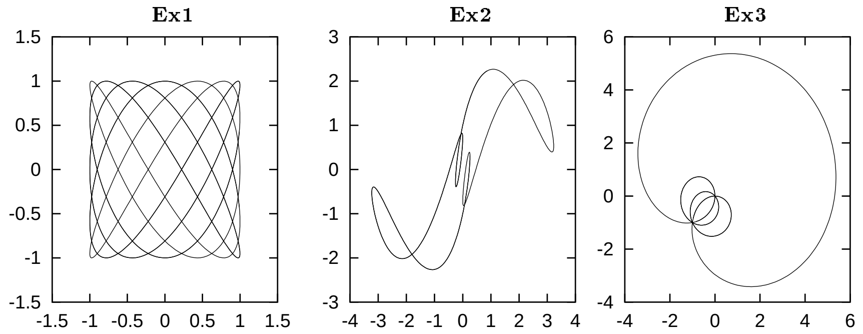

Figure 1. Example Trigonometric Curves

The class of trigonometric curves includes numerous classical curves such as Limacon of Pascal, Cardioid, Trifolium, Epi-cyloid, Hypo-cyloid, etc, as special cases. They also arise naturally in numerous areas such as linear differential equations, Fourier analysis, almost periodic functions (under the name of generalized trigonometric polynomials), representation of groups (utilizing its periodicity), electrical circuit analysis (Lissajous curves, as often shown on oscilloscopes), fracture mechanics (as the caustic pattern appearing when a fractured material is shone by a laser beam), etc. The class includes all bounded polynomial curves (i.e. images of a polynomial parameterization with bounded parameter interval). It is a subset of the class of rational curves (images of rational parameterizations). Algorithms for rational curves can be found in (Abhyankar and Bajaj, 1987), (Sendra and Winkler, 1991), (Schicho, 1992), (van Hoeij, 1994), (Mnuk *et al.*, 1995) (this system is also available by `http://ftp.risc.uni-linz.ac.at/pub/casa`), (Mnuk *et al.*, 1996), (van Hoeij, 1997).

The class of trigonometric curves has also been studied under different names (higher cycloid curves, higher planet motions) in (Wunderlich, 1947; Wunderlich, 1950; Pottmann, 1984). On the algebraic side, we mention (Gutierrez and Recio, 1995) which contains a method that allows to decompose a trigonometric polynomial (as a function).

In this paper, we give algorithms for (a) simplifying a given parametric representation, (b) computing an implicit representation from a given parametric representation, and (c) computing a parametric representation from a given implicit representation.

Simplification:

A trigonometric curve can have many different trigonometric parameterizations. Some of them are less economical than others, meaning that parts of the curve are traced unnecessarily often. A simple parameterization is one which traces the whole curve exactly once. Given a parameterization, the simplification problem asks for a simple equivalent parameterization (which may or may not exist).

To solve this problem, we adapt a technique introduced in (Binder, 1995; Binder, 1996) for polynomials to trigonometric polynomials. If no simplification exists, then we give an equivalent simple parameterization with polynomials. Furthermore, we prove that simple trigonometric parameterizations are unique up to change of phase and orientation. This is quite surprising, since the corresponding statement is false for polynomial parameterizations.

Implicitization:

It is quite obvious that a trigonometric curve is either algebraic or semi-algebraic. Given a parameterization of a curve, the implicitization problem asks for the polynomial equation of the curve, if the curve is algebraic. In the semi-algebraic case, we might ask for an equation and a set of inequalities. The problem becomes a lot simpler if we ignore isolated points (which we do).

One obvious approach is to rewrite $\cos(k\theta)$ and $\sin(k\theta)$ as polynomials in $\cos\theta$ and $\sin\theta$ and to parameterize $\cos\theta$ and $\sin\theta$ by the usual rational parameterization of a circle, obtaining a rational parameterization of the curve, and then implicitize the rational parameterization by using general methods such as Buchberger's Gröbner basis method (Buchberger, 1965; Buchberger, 1985; Gao and Chou, 1992; Kalkbrener, 1990; Hoffmann, 1989; Winkler, 1988), Collins' cylindrical algebraic decomposition method (Collins, 1975; Hong, 1990; Collins and Hong, 1991), Ritt-Wu's characteristic set method (Wu, 1986), and the resultants (Collins, 1967; Brown and Traub, 1971) etc.

However one can often devise a more efficient/simpler method for a particular problem class by taking advantage of its special structure. One such method was given by one of the authors (Hong, 1996; Hong, 1995) for a certain sub-class of trigonometric curves. The method requires one resultant computation with a factorization. In this paper, we give a method which is more general and efficient than the one (Hong, 1996; Hong, 1995) in that it works for arbitrary trigonometric curves and that it does not require factorization.

Parameterization:

Given the equation of an algebraic curve, the parameterization problem asks for a trigonometric parameterization. Obviously it is possible iff the curve is a trigonometric curve. It is easy to see that any trigonometric curve is a rational curve, i.e. has a parameterization in terms of rational functions. Thus we first compute a rational parameterization and then try to extract a trigonometric parameterization from it (when possible).

The trigonometric parameterization often covers the geometry of many interesting and important curves much better than the rational/polynomial parameterizations. This holds especially for closed curves. Also it turns out that different trigonometric parameterizations of an algebraic curve differ only by a linear parameter change. For instance, all trigonometric parameterizations of a circle have uniform speed (since we have one obvious uniform speed parameterization). Hence, trigonometric parameterizations have intrinsic character, in the sense that they depend only on the curve. The corresponding assertion for polynomial parameterization is obviously false.

In the following we give the details via definitions, examples, theorems, and algorithms for the above three problems. You will notice that much of harder proofs are *postponed* until the last section (titled Harder Proofs). There are two-fold reasons for this: (1) We expect that the reader will have an easier time at the first reading, without getting bombarded by technical details. (2) Many of the proofs are *inter-related*, and thus it is much more economical to put them in one place both for presentation and reading.

You will notice that theorems/lemmas are labeled following the convention **X-Y** where

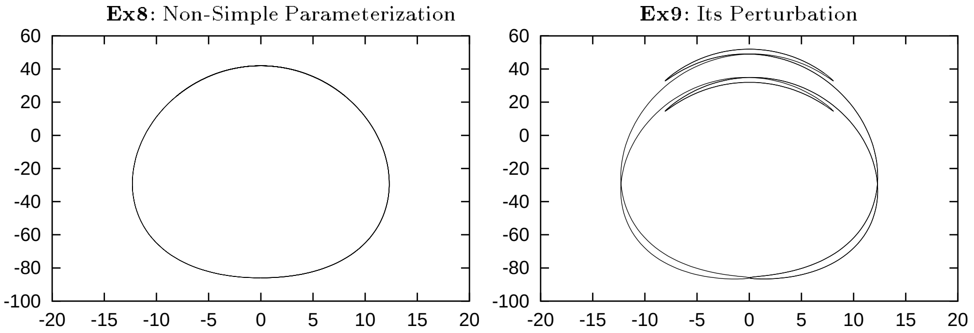

Figure 2. Non-Simple Parameterization and Its Perturbation

$$\mathbf{X} = \begin{cases} \text{S} & \text{for Simplification} \\ \text{I} & \text{for Implicitization} \\ \text{P} & \text{for Parameterization} \\ \text{H} & \text{for Harder proofs} \end{cases} \qquad \mathbf{Y} = \begin{cases} \text{EXI} & \text{for Existence check} \\ \text{HOW} & \text{for How to find when exist} \\ \text{UNI} & \text{for Uniqueness} \\ \text{ALG} & \text{for Algorithm correctness} \\ \text{AUX} & \text{for Auxiliary results.} \end{cases}$$

All the algorithms in this paper (and other related graphical tools) have been implemented in Maple / Java and are available on the world-wide-web site:

`http://www.risc.uni-linz.ac.at/people/hhong/software/trig/trig.html`

2. Simplification

A parameterization $t : [a, b] \rightarrow C$ is called *simple* iff at most finitely many points on C have more than one number in the preimage. Two parameterizations t and t' are called *equivalent* iff the images coincide. If t is a parameterization, and t' is an equivalent simple parameterization, then we say that t' is a *simplification* of t. Now we are ready to state the simplification problem.

Problem 2.1. (Simplification)
Input: A trigonometric parameterization $t : [0, 2\pi] \rightarrow C$.
Output: A trigonometric simplification $t' : [0, 2\pi] \rightarrow C$, if there exists one.

Before presenting the technical results, we would like to motivate them by the following examples:

Ex4: $x = \cos(\theta)$
$y = \sin(\theta)$

Ex5: $x = \cos(2\theta)$
$y = \sin(2\theta)$

Ex6: $x = \cos(\theta)$
$y = 0$

Ex7: $x = \cos(\theta) + \cos(3\theta)$
$y = 0$

Ex8: $x = -4\cos(\theta) - 6\cos(3\theta) + 6\cos(5\theta) + 3\cos(7\theta) + \cos(9\theta)$
$y = -56\cos(2\theta) - 33\cos(4\theta) - 12\cos(6\theta) + 10\cos(8\theta) + 4\cos(10\theta) + \cos(12\theta)$

Ex9: $x =$ the same as x in **Ex8**
$y = y$ in **Ex8** $+10\sin(\theta)$

where $\theta \in [0, 2\pi]$. The parameterization **Ex4** is already simple, since every point on the circle corresponds to exactly one value of the parameter θ. The parameterization **Ex5** is *not* simple, since every point on the circle corresponds to two values of the parameter θ. But it can be made simple trivially by removing 2 from $\cos(2\theta)$ and $\sin(2\theta)$, going back to **Ex4**.

In general it is obvious that one can always remove (factor out) the greatest common divisor (gcd) of all multiplicators of θ occurring in nonzero summands. Now a question arises: is the resulting parameterization always simple? The answer is no. A trivial counter example is given by **Ex6**. Furthermore, it is obvious that there does not exists a simple trigonometric parameterization for this curve.

But then, we observe that if we allow the domain to be restricted to $[0, \pi]$, then we can get a simple parameterization. Thus, a question arises: is it always possible to obtain a simple parameterization by restricting the domain (to a sub-interval of $[0, 2\pi]$). The answer is no. A trivial counter example is given by **Ex7**. By plotting the graph of $x(t)$, one will immediately observe this fact.

So far, we encountered two reasons for parameterization to be not simple: (1) there is a non-trivial gcd or (2) the curve is not closed. Thus, another question arises: is a curve simple if none of the two reasons hold? The answer is no again. A counter example is given by **Ex8**. Clearly the gcd is trivial and Figure 2 shows that the curve is also closed. But it turns out that the parameterization is not simple. This can be *guessed* from observing the behavior of a slightly perturbed one **Ex9** where y is increased by $10\sin(\theta)$. See the curve in Figure 2. One can also guess, rightly, from the perturbed curve that one cannot obtain a simple parameterization by restricting the interval for θ.

From these discussions, we end up with two non-trivial questions: (1) how can we decide whether there exists an equivalent simple trigonometric parameterization, (2) how can we compute one if exists. The following theorem helps answering the question (1).

THEOREM 2.1. (S-EXI) *Let $t : [0, 2\pi] \to C$ be a trigonometric parameterization. Then exactly one of the following two assertions is true:*
(a) *There exists a trigonometric simplification $t' : [0, 2\pi] \to C$.*
(b) *There exists a polynomial simplification $p : [a, b] \to C$.*

PROOF. Postponed to the last section. It is intuitively plausible that both cannot hold: the image of a simple polynomial parameterization has endpoints, while the image of a simple trigonometric parameterization has not. However, the endpoints may coincide. This is what happens in example **Ex8**. □

Thus, the question (1) is reduced to checking the existence of a polynomial simplification. For the moment, we assume that we can do this (this will be discussed below). Now, the following theorem answers the question (2).

Theorem 2.2. (S-how) *Let t be a trigonometric parameterization with a trigonometric simplification. Let g be the greatest common divisor of all multiplicators of θ occurring in nonzero summands of t. Let t' be the trigonometric parameterization obtained by replacing θ by θ/g, that is, factoring out g. Then, t' is a trigonometric simplification of t.*

Proof. It is obvious that t and t' is equivalent. The proof for the simplicity of t' is postponed. □

Based on these two theorems, we immediately obtain the following algorithm. The algorithm produces, as a *by-product*, a polynomial simplification when no trigonometric simplification exists.

Algorithm 2.1. (Simplify)

```
Input:    A trigonometric parameterization $t : [0, 2\pi] \to C$.
Output:   A trigonometric simplification $t' : [0, 2\pi] \to C$, if there exists one.
          A polynomial simplification $p : [a, b] \to$C, otherwise.

$p :=$ PolySimplify($t$).
If $p =$ NotExist then
    $g := gcd$ of all multiplicators of $\theta$ occurring in nonzero summands of $t$.
    $t' :=$ substitute $\theta$ by $\theta/g$ in $t$.
    Return $t'$.
Else
    Return $p$.
□
```

In the above, PolySimplify is an algorithm that is supposed to check whether a polynomial simplification exists and to find one if so. Now we will present one such algorithm. The main insight underlying the algorithm is the observation that the technique introduced in (Binder, 1995; Binder, 1996), for computing a Lüroth generator (see eg. (Winter, 1974) for Lüroth's theorem) of a function field with polynomials, can be modified/adapted for trigonometric polynomials.

First it is easy to see that the set of all trigonometric polynomials with the usual $+$ and $\cdot$ forms an *integral domain*. One only needs to recall the elementary trigonometric identities:

$$\cos(\alpha)\cos(\beta) = \frac{\cos(\alpha+\beta)+\cos(\alpha-\beta)}{2}$$

$$\sin(\alpha)\cos(\beta) = \frac{\sin(\alpha+\beta)+\sin(\alpha-\beta)}{2}$$

$$\sin(\alpha)\sin(\beta) = \frac{\cos(\alpha+\beta)-\cos(\alpha-\beta)}{-2}$$

In order to apply Binder's method, we also need a concept of *division* for trigonometric polynomials. Let the *degree* of a non-zero trigonometric polynomial F be the largest multiplicator of θ occurring in nonzero summands of F (the degree of 0 is $-\infty$). The degree function gives the integral domain of trigonometric polynomials an interesting structure, namely it makes it *almost* Euclidean. First, we obviously have that

$$\deg(F{\cdot}G) = \deg F + \deg G.$$

Second, one can easily verify, using the above elementary trigonometric identities, that for any two non-zero trigonometric polynomials F and G there are two trigonometric polynomials Q and R, such that

$$F = G \cdot Q + R,$$

$$\deg R \leq \deg G.$$

There is at most one such pair (Q, R) with $\deg R < \deg G$. If there exists such a pair, we call Q and R the *quotient* and the *remainder* of $F : G$. Otherwise, we say that the quotient and remainder do not exist. The computation of quotient and remainder, if exists, is straightforward (almost same as with polynomials), and we leave it to the reader. Now we give a theorem corresponding to proposition 2.1 in (Binder, 1996)).

Theorem 2.3. (S-aux) *Let F and G be two trigonometric polynomials. Let Q and R be the quotient and remainder of $F : G$. Then*

(a) $\mathrm{R}[F, G] \subseteq \mathrm{R}[G, Q, R]$.

(b) $\mathrm{R}(F, G) = \mathrm{R}(G, Q, R)$.

Proof. The claim (a) is obvious from $F = G{\cdot}Q + R$. For the claim (b), the direction $\subseteq$ follows from (a). The proof of the direction $\supseteq$ is postponed to the last section. □

Repeated application of this theorem suggests the following algorithm for deciding the existence of a polynomial simplification. We will use the notation $t = (X, Y)$ where X and Y are the trigonometric polynomials in θ for x and y.

Algorithm 2.2. (Modified-Binder)

Input: A trigonometric parameterization $t = (X, Y)$.

Output: `Exist`, if t has a polynomial simplification.
`NotExist`, otherwise.

```
$S := \{X, Y\}$.
While $S$ contains at least two elements do
    Choose $F$ and $G$ such that $\deg F \geq \deg G$.
    If $\deg G = 0$ then
        Remove $G$ from $S$.
    $Q, R$ := quotient and remainder of $F : G$.
    If the quotient and remainder do not exist then
        Return NotExist.
    Remove $F$ from $S$.
    Add $R$ and $Q$ to $S$.
Return Exist.
```
□

Remark 2.1. There are three differences to Binder's algorithm (Binder, 1996): First, Binder uses polynomials instead of trigonometric polynomials. Second, Binder's algorithm never fails (the **If** statement is not there). Third, the output is the single element in S after termination of the while loop (and not simply `Exist`).

Remark 2.2. The formal similarity of Binder's technique to Euclid's algorithm for computing *gcd*s is astounding. Indeed, if we delete the phrases concerning Q, then we have Euclid's algorithm. Cf. also (Binder, 1995; Binder, 1996).

Now it is straightforward to extend the above algorithm so that it also reports a polynomial simplification in the positive case. For this, one only needs to remember the relationships among the input and the generated trigonometric polynomials. A set M will be used for storing these relationships.

Algorithm 2.3. (PolySimplify)

Input: A trigonometric parameterization $t = (X, Y)$.

Output: A polynomial simplification of t, if one exists,
`NotExist`, otherwise.

```
$F_1 := X$, $F_2 := Y$, $S := \{F_1, F_2\}$. $n := 2$.
$M := \{\}$.
While $S$ contains at least two elements do
    Choose $F_i$ and $F_j$ such that $\deg F_i \geq \deg F_j$.
    If $\deg F_j \leq 0$ then
        Remember this fact by adding to $M$ the equation $u_j = F_j$.
        Remove $F_j$ from $S$.
    Else
        $F_{n+1}, F_{n+2}$ := quotient and remainder of $F_i : F_j$.
        If the quotient and remainder do not exist then
            Return NotExist.
        Remember this relation by adding to $M$ the equation $u_i = u_j u_{n+1} + u_{n+2}$.
        Remove $F_i$ from $S$.
        Add $F_{n+1}$ and $F_{n+2}$ to $S$.
        $n := n + 2$.
Let $F_m$ be the only remaining element in $S$.
By successive substitution in $M$, get $P$ and $Q$ such that $u_1 = P(u_m)$ and $u_2 = Q(u_m)$.
                                        [ Now we know that $F_1 = P(F_m)$ and $F_2 = Q(F_m)$ ].
Compute $a = \min_\theta F_m(\theta)$ and $b = \max_\theta F_m(\theta)$.
Let $p$ be the polynomial parameterization given by $P$ and $Q$ over $[a, b]$.
Return $p$.
□
```

Remark 2.3. The bottleneck of the algorithm is the computation of the parameter interval $[a, b]$, since it involves the solution of algebraic equations. Let $G(x, y)$ be a bivariate polynomial such that $F_m(\theta) = G(\cos\theta, \sin\theta)$ (obtained by the de Moivre formula). Then we have to compute all solutions of the equation system

$$-\partial_x G(x, y)y + \partial_y G(x, y)x = x^2 + y^2 - 1 = 0$$

(there are only finitely many unless F_m is constant). Each solution is plugged into G. Then a and b are the minimum and the maximum of these values.

EXAMPLE 2.1. We show the result of applying the algorithm SIMPLIFY on several (nontrivial) examples given above.

Ex1: the input itself

Ex2: $x = 2\cos(\theta) + \sin(\theta) + \sin(3\theta)$
$y = \cos(\theta) + \sin(\theta) + \cos(5\theta)$

Ex3: the input itself

Ex8: $x = -4s^3 + 16s$
$y = 8s^4 - 64s^2 + 42$
over $[-2, 2]$ which is the range of $-\cos(\theta) - \cos(3\theta)$.

Ex9: the input itself

□

THEOREM 2.4. (S-ALG) *The algorithm* SIMPLIFY *is correct.*

PROOF. Termination is clear as soon as we know that MODIFIED BINDER terminates. This follows from the observation that the sum of the degrees of all nonzero trigonometric polynomials in S drops at least by 1 in any division step.

Correctness follows immediately from the theorems (S-EXI) and (S-HOW) and the correctness of the algorithm POLYSIMPLIFY, which we will show now. Clearly, we have $X = F_1 = P(F_m)$ and $Y = F_2 = Q(F_m)$, where F_m is the trigonometric polynomial which remains at the end. It follows that the output parameterization is indeed *equivalent* to the input parameterization t. By (S-AUX), F_m can be expressed as a rational function in X and Y. This implies that the returned parameterization (P, Q) has a rational inverse, and is consequently *simple*.

It remains to show that there exists no equivalent polynomial parameterization, if POLYSIMPLIFY returns NOTEXIST. The proof is involved, and thus we label this assertion with (S-SUB) and postpone the proof to the last section. □

REMARK 2.4. At the first glimpse, it seems that the computational complexity of the algorithm MODIFIED-BINDER is worse than that of Euclid's algorithm. But when the pivot elements are cleverly chosen, the contrary is the case. We choose F_i to be of largest degree, and F_j of degree as close as possible to $\frac{\mathrm{deg} F_i}{2}$. With this strategy, a trigonometric function is replaced by two trigonometric polynomials of approximately half the degree. See (Binder, 1995; Binder, 1996) for details.

Simplifications are not unique. For instance, we can modify a simplification by a phase change or by a change of orientation. The next theorem tells that all equivalent parameterizations can be obtained that way.

THEOREM 2.5. (S-UNI) *A trigonometric simplification of a trigonometric parameterization t is unique up to phase change and orientation change.*

PROOF. Postponed to the last section. □

Remark 2.5. The property simple is closely related to the property proper of rational parameterizations. Over the complex numbers, a rational parameterization is simple iff it is proper. For details, consult (Sederberg, 1986). We will see that a similar statement also holds for real trigonometric parameterizations (see (H-aux-5)).

3. Implicitization

An *implicitization* of a curve is an irreducible bivariate polynomial whose zero set is equal to the curve plus maybe some isolated points. It is unique up to multiplication with a nonzero constant. Not every curve has an implicitization. Now we are ready to state the implicitization problem.

Problem 3.1. (Implicitization)
Input: A trigonometric parameterization t.
Output: An implicitization for t, if there exists one.

Example 3.1. The circle given by $x = \cos(\theta)$ and $y = \sin(\theta)$ obviously has an implicitization: $x^2 + y^2 - 1$. But the line segment given by $x = \cos(\theta)$ and $y = 0$ does *not* have an implicitization. □

The following theorem shows how to check the existence of the implicitization. It extends the earlier Theorem (S-exi).

Theorem 3.1. (I-exi) *Let $t : [0, 2\pi] \to C$ be a trigonometric parameterization. The following are equivalent.*

(a) *t has an implicitization.*
(b) *t has a trigonometric simplification.*
(c) *t has no polynomial simplification.*

Proof. (a)→(c): Assume, indirectly, that t has an implicitization F, and a polynomial simplification $p = (P, Q) : [a, b] \to C$. The univariate polynomial $F(P(s), Q(s))$ must vanish identically, since it is zero on $[a, b]$. Therefore, the zero set of F is not bounded, since it contains $(P(s), Q(s))$ for arbitrary large s. On the other hand, C is compact, hence bounded, and F cannot be an implicitization of C. The proof for (c)→(b) and (b)→(a) is postponed to the last section. □

Next, we study how to find the implicitization when exists. Let $t : [0, 2\pi] \to C$ be a trigonometric parameterization. Substituting all terms $\cos(m\theta)$ and $\sin(m\theta)$ by $\frac{z^m + z^{-m}}{2}$ and $\frac{z^m - z^{-m}}{2i}$, we obtain a parameterization $t_c : S^1 \to C$ where S^1 is the unit circle of the complex plane. We call this the *complex form* of the parameterization t.

Example 3.2. The complex form of the parameterization $x = \cos(\theta)$ and $y = \sin(\theta)$ is obviously $x = \frac{z + z^{-1}}{2}$ and $y = \frac{z - z^{-1}}{2i}$. □

Note that a complex form of the parameterization has the form

$$z \mapsto \left(\frac{P(z)}{z^m}, \frac{Q(z)}{z^n}\right),$$

where P and Q are polynomials with complex coefficients of degree $2m$ and $2n$, respectively. Both polynomials have the property that their reverse (the reverse of P is $z^{2m}P(1/z)$) is equal to their conjugate. Vice versa, any parameterization of such a form can be converted into a trigonometric parameterization, by substituting $z = \cos\theta + i\sin\theta$.

Theorem 3.2. (I-how-1) *Let $(\frac{P(z)}{z^m}, \frac{Q(z)}{z^n})$ be the complex form of a simple trigonometric parameterization t. Then*

$$R(x, y) = \mathrm{resultant}_z(P(z) - z^m x, Q(z) - z^n y)$$

is the implicitization of t.

Proof. Postponed to the last section. □

Remark 3.1. In (Hong, 1996; Hong, 1995), one of the authors has shown a similar result for *nested circular* parameterizations. These are trigonometric parameterizations such that all pairs $a\cos(n\theta) + b\sin(n\theta)$, $a'\cos(n\theta) + b'\sin(n\theta)$ occurring in X, Y satisfy $b = -a'$, $b' = a$.

Remark 3.2. It can be shown that the following converse of theorem (I-exi) is also true: when the resultant is the implicitization, then the parameterization is simple.

Now we are ready to give an algorithm to solve the implicitization problem as stated above. But what shall we return when it turns out that the input trigonometric parameterization does not have an implicitization? By Theorem (I-exi), in this case, there exists a simple polynomial parameterization. Now by Tarski's quantifier elimination theorem, we see immediately that the curve is semi-algebraic, i.e. it can be defined by an equation and some *inequalities*. Thus, it will be nice to compute those inequalities.

We say that a triple $(R, S, [a, b])$, where R is an irreducible polynomial, S is a rational function and $[a, b]$ is an real interval, is a *semi-implicitization* of a curve C iff the set

$$\{(x, y) \mid R(x, y) = 0,\ a \le S(x, y) \le b\}$$

is equal to the curve C minus at most finitely many exceptional points for which $S(x, y)$ is not defined.

Theorem 3.3. (I-how-2) *Let $p = (P(s), Q(s)) : [a, b] \rightarrow C$ be a polynomial birational parameterization. Let $R(x, y)$ be the resultant of P and Q and let $R_0(x, y) + R_1(x, y)s$ be the first subresultant of $P(s) - x$ and $Q(s) - y$ with respect to s. Then (R, $-R_0/R_1$, $[a, b]$) is a semi-implicitization of p.*

Proof. Postponed to the last section. □

From the above three theorems, we immediately obtain the following algorithm for implicitization (or semi-implicitization).

Algorithm 3.1. (Implicitization)

```
Input:    A trigonometric parameterization $t$.
Output:   An implicitization of $t$, if it exists.
          A semi-implicitization of $t$, otherwise.
```

```
$q$ := SIMPLIFY($t$).
If $q$ is a trigonometric parameterization then
    $(P(z)/z^m, Q(z)/z^n)$ := complex form of $q$.
    $R$:= resultant$_z(P(z) - z^m x, Q(z) - z^n y)$.
    Return $R$.
Else (thus $q$ is a polynomial parameterization)
    Let $q$ is given by $(P, Q)$ over $[a, b]$.
    $R$:= resultant$_s(P(s) - x, Q(s) - y)$.
    $R_0 + sR_1$:= sub$_1$resultant$_s(P(s) - x, Q(s) - y)$.
    Return ( $R$, $-R_0/R_1$, $[a, b]$ ).
□
```

EXAMPLE 3.3. We show the result of applying the algorithm IMPLICITIZE on several (non-trivial) examples given above.

Ex1: $4096x^{14} - 14336x^{12} + 19712x^{10} - 13440x^8 + 4704x^6 - 784x^4 + 49x^2 + 256y^{10} - 640y^8 + 560y^6 - 200y^4 + 25y^2 - 1$

Ex2: $256x^{10} - 5760x^8 + 4224x^7y - 640y^2x^6 + 33760x^6 - 53184x^5y + 35392x^4y^2 - 9176x^4 - 12864y^3x^3 + 7832x^3y + 2736x^2y^4 - 2912x^2y^2 + 477x^2 - 320y^5x + 504y^3x - 208xy + 16y^6 - 32y^4 + 20y^2 - 4$

Ex3: $x^8 + 4y^2x^6 - 20x^6 - 40x^5 - 60x^4y^2 - 20x^4 + 6y^4x^4 - 40yx^4 - 80y^2x^3 - 80x^3y - 60x^2y^4 - 40x^2y^2 + 4y^6x^2 - 80x^2y^3 - 32yx^2 - 32xy^2 - 40y^4x - 80y^3x - 20y^4 - 20y^6 - 40y^5 + y^8$

Ex8: $310632 - 172y - 130y^2 - 2752x^2 - 32x^2y - y^3 + 2x^4$
$-2 \leq \frac{-x(86+y)}{2(-688-8y+x^2)} \leq 2$

Ex9: Aborted after 10 minutes on Maple running on a sun workstation. The output is expected to be huge.

□

THEOREM 3.4. (I-ALG) *The algorithm* implicitize *is correct.*

PROOF. This follows easily from (I-EXI), (I-HOW-1), (I-HOW-2), and the fact that the polynomial simplifications produced by *simplify* are birational (has a rational inverse), which was proved in the proof of (S-ALG). □

4. Parameterization

Let $S \subset \mathrm{R}^2$ be a set given by an irreducible bivariate polynomial equation. We say that t is a *parameterization* of S iff the image is contained in S, the difference is finite, and the parameterization is not constant (to exclude the degenerate case when S is a finite set). Now we are ready to state the parameterization problem.

PROBLEM 4.1. (PARAMETERIZATION)
Input: An irreducible bivariate polynomial $F(x, y)$.
Output: A trigonometric parameterization t for the zero set of F, if there exists one.

As a stepping stone towards a trigonometric parameterization, we introduce a new concept and recall some known concepts. We say that t is a *partial parameterization* of S iff the image of t is an infinite subset of S. A *rational parameterization* is a partial function $r : (-\infty,\infty]\to C$, defined on almost all points of $(-\infty,\infty]$, which can be expressed in terms of rational functions. Here, we say that r is defined at $s\in(-\infty,\infty]$ iff the limes' of the two rational functions exist for s. A rational parameterization which has rational inverse is also called a *birational parameterization*. It is easy to show that the image of a birational parameterization is algebraic (the parameter can be produced for almost all points fulfilling the same equation).

Theorem 4.1. (P-exi-1) *Let S be an algebraic set, given by an irreducible equation. If S has a partial trigonometric parameterization, then it also has a birational parameterization.*

Proof. By substituting $\theta := 2\mathrm{arctan}s$, we get a partial rational parameterization (P,Q). The field $\mathrm{R}(P,Q)$ is a subfield of $\mathrm{R}(s)$ not equal to R. By Lüroth's theorem, this field is equal to $\mathrm{R}(F)$, for a suitable rational function F. Consequently, we have $P = P'(F)$, $Q = Q'(F)$, and $F = G(P,Q)$ for suitable rational functions P', Q', G. Then, (P',Q') is a rational parameterization of C with rational inverse G. □

The following theorem provides a criterion for a curve to be trigonometric, in terms of a birational parameterization.

Theorem 4.2. (P-exi-2) *Let $r = (P,Q) : (-\infty,\infty]\to C$ be a birational parameterization of a curve C. Let a be the number of parameters for which r is not defined. Let b be the number of complex, but not real numbers for which the limes of P or Q is not defined. The following are equivalent.*

(a) *C has a simple trigonometric parameterization.*

(b) *C has a trigonometric parameterization.*

(c) *$a = 0$ and $b = 2$.*

Proof.

(a)$\to$(b): Trivial.

(c)$\to$(a): We write $P = P_n/P_d$ and $Q = Q_n/Q_d$, with P_d and Q_d monic. Since r is defined at ∞, we have $\mathrm{deg}P_d\leq\mathrm{deg}P_n$ and $\mathrm{deg}Q_d\leq\mathrm{deg}Q_n$. Since $a = 0$ and $b = 2$, the equation $P_dQ_d = 0$ has exactly two complex roots, which must be a conjugated pair. Therefore, we have $P_d = N^m$ and $Q_d = N^n$ for a suitable irreducible quadratic polynomial N. With a linear parameter change, we can achieve that $N = s^2+1$. Now, we substitute $s = i\frac{z-1}{z+1}$ in P and Q. This parameter change transforms the real line to the unit circle in the complex plane. After expanding and shortening, we obtain two rational functions of the form $P'(z)/z^m$, $Q'(z)/z^n$, where $\mathrm{deg}P' = 2m$, $\mathrm{deg}Q' = 2n$, and both polynomials are equal to the conjugate of their reverse. Hence, we obtained the complex form of a trigonometric parameterization.

(b)$\to$(c): Postponed to the last section. □

Remark 4.1. The integer a is the number of asymptotes of C. The integer b has no obvious geometric meaning.

To decide the existence, of a partial parameterization, we use a well-known criterion for the existence of polynomial parameterizations.

THEOREM 4.3. (P-AUX) *Let $r = (P, Q) : (-\infty, \infty] \rightarrow C$ be a birational parameterization of a curve C. Let a be the number of parameters for which r is not defined. Let b be the number of complex, but not real numbers for which the limes of P or Q is not defined. The following are equivalent:*

(a) *C has a birational polynomial parameterization.*

(b) *C has a partial polynomial parameterization.*

(c) *$a = 1$ and $b = 0$.*

PROOF.

(a)→(b): Trivial.

(c)→(a): (This is known, but a proof is included because we use the construction in the algorithm.) We again write $P = P_n/P_d$ and $Q = Q_n/Q_d$, with P_d and Q_d monic. If r is not defined at ∞, then P_d and Q_d do not have any complex roots, which means that they are equal to one: r is already a polynomial parameterization. In the other case, we have $\deg P_d \leq \deg P_n$ and $\deg Q_d \leq \deg Q_n$. Since $a = 1$ and $b = 2$, the equation $P_d Q_d = 0$ has one real root and no other complex root. With a linear parameter change, we can achieve that this root is 0, so that $P_d = s^m$ and $Q_d = s^n$. But then, P and Q can be written as polynomials in $\frac{1}{s}$.

(b)→(c): See (Abhyankar, 1990; Manocha and Canny, 1991). It also follows by (H-AUX-1) in the last section of this paper. □

THEOREM 4.4. (P-EXI-3) *Let C be an algebraic curve that has no trigonometric parameterization. Then C has a partial trigonometric parameterization iff it has a polynomial parameterization.*

PROOF.

←: By plugging an arbitrary trigonometric polynomial into the polynomial parameterization, we get a partial trigonometric parameterization.

→: Let t be a partial, but not full trigonometric parameterization with image $C' \subset C$. Then C' must be semi-algebraic and not algebraic. By (I-EXI), t has a polynomial simplification, which is at the same time a partial polynomial parameterization of C. By (P-AUX), C has a polynomial parameterization. □

Now, we are ready to give an algorithm that solves the parameterization problem. In case when there is no trigonometric parameterization, the algorithm, as almost by-products, tries to produce other parameterizations such as rational or polynomial. We assume a subalgorithm BIRATIONAL which computes a birational parameterization, if one exists. See (Alonso *et al.*, 1995; Sendra and Winkler, 1997; Recio and Sendra, 1997), for such an algorithm.

ALGORITHM 4.1. (PARAMETERIZE)

Input: A bivariate irreducible polynomial F.

Output: A trigonometric parameterization for the zero set of F, if one exists, else
A polynomial parameterization for the zero set of F, if one exists, else

```
        A rational parameterization for the zero set of $F$, if one exists, else
        NotExist otherwise.

$r$ := Birational($F$).
If $r$ = NotExist then
    Return NotExist.
Let $r = (P(s), Q(s))$, $P = P_n/P_d$, and $Q = Q_n/Q_d$.
$N$ := greatest squarefree divisor of $P_dQ_d$.

If $\deg N = 2$ and
        $\deg P_n \leq \deg P_d$ and
        $\deg Q_n \leq \deg Q_d$ and
        discriminant($N$) $< 0$ then
    Let $N = as^2 + bs + c$.
    Substitute $s := \sqrt{4ac - b^2}/(2a)s - b/(2a)$ in $P$ and $Q$.
    Substitute $s := i(z - 1)/(z + 1)$ in $P$ and $Q$.
    $X, Y$ := the trigonometric forms of $P, Q$.
    Return $(X, Y)$ as a trigonometric parameterization.

If $\deg N = 1$ and
        $\deg P_n \leq \deg P_d$ and
        $\deg Q_n \leq \deg Q_d$ and
    Let $N = as + b$.
    Substitute $s := (s - b)/a$ in $P$ and $Q$.
    Substitute $s := 1/s$ in $P$ and $Q$.
    Return $(P, Q)$ as a polynomial parameterization.

If $\deg N = 0$ then
    Return $(P, Q)$ as a polynomial parameterization.

Return $r$ as a rational parameterization.
□
```

Example 4.1. Consider the trigonometric parameterization **Ex3** again:

$$\begin{aligned} x &= \cos(\theta) - \sin(\theta) + \cos(2\theta) - \sin(2\theta) + \cos(3\theta) - \sin(3\theta) + \cos(4\theta) - \sin(4\theta) \\ y &= \cos(\theta) + \sin(\theta) + \cos(2\theta) + \sin(2\theta) + \cos(3\theta) + \sin(3\theta) + \cos(4\theta) + \sin(4\theta). \end{aligned}$$

Recall that the algorithm Implicitize generated the polynomial:

$$x^8 + 4y^2x^6 - 20x^6 - 40x^5 - 60x^4y^2 - 20x^4 + 6y^4x^4 - 40yx^4 - 80y^2x^3 - 80x^3y - 60x^2y^4 - \\ 40x^2y^2 + 4y^6x^2 - 80x^2y^3 - 32yx^2 - 32xy^2 - 40y^4x - 80y^3x - 20y^4 - 20y^6 - 40y^5 + y^8$$

Now we would like to get back a trigonometric parameterization from this bivariate polynomial, using the algorithm Parameterize. We first compute a birational parameterization, obtaining:

$$x = \frac{-576 - 19872s^2 + 23328s - 360s^6 + 1080s^5 + 6480s^4 - 10080s^3}{-8000s + 10000 + 6400s^2 - 2720s^3 + 1096s^4 - 272s^5 + 64s^6 - 8s^7 + s^8}$$

$$y = \frac{-15168 + 14304s - 24s^7 + 96s^6 + 2088s^5 - 4560s^4 - 13440s^3 + 16704s^2}{-8000s + 10000 + 6400s^2 - 2720s^3 + 1096s^4 - 272s^5 + 64s^6 - 8s^7 + s^8}$$

Continuing with the subsequent steps of the algorithm PARAMETERIZE, we obtain:

$$\begin{aligned} x &= \cos(\theta) - \sin(\theta) - \cos(2\theta) - \sin(2\theta) - \cos(3\theta) + \sin(3\theta) + \cos(4\theta) + \sin(4\theta) \\ y &= -\cos(\theta) - \sin(\theta) - \cos(2\theta) + \sin(2\theta) + \cos(3\theta) + \sin(3\theta) + \cos(4\theta) - \sin(4\theta). \end{aligned}$$

Note that this trigonmetric paramaterization is different from the original one **Ex3**. But we note that it can be obtained by replacing θ with $-\theta - \pi/2$. Thus it is the same as the original one upto the orientation and the phase. □

THEOREM 4.5. (P-ALG) *The algorithm* parameterize *is correct.*

PROOF. This follows immediately from (P-EXI-1), the correctness of BIRATIONAL, (P-EXI-2), (P-AUX), and the proofs of (P-EXI-2) and (P-AUX).

The statement (P-EXI-3) is not needed for the correctness proof. It just gives the additional information that the algorithm BIRATIONAL can also be used to decide the existence of partial trigonometric parameterizations and to compute one if exists (by substituting an arbitrary trigonometric polynomial for the parameter in a polynomial parameterization). □

It is easy to see that there are infinitely many trigonometric parameterizations of an algebraic set S when one exists. But the following theorems tells that they are "essentially" the same parameterizations.

THEOREM 4.6. (P-UNI) *A trigonometric parameterization of an algebraic set S is unique up to linear parameter change.*

PROOF. Let t_1, t_2 be two trigonometric parameterizations of S. By (I-EXI), both have simplifications t_1' and t_2', which can be obtained by linear parameter change by (S-HOW). Now, the images of t_1 and t_2 are closed connected sets which differ by a finite set of points, and so they coincide. Therefore, all parameterizations are equivalent. By (S-UNI), t_1' and t_2' differ only by a linear parameter change. □

COROLLARY 4.1. (P-COR) *Any trigonometric parameterization of a circle has uniform speed.*

PROOF. By (P-UNI), since we have an obvious uniform speed parameterization of the circle. □

5. Harder Proofs

Let C be an algebraic curve. We denote by $\alpha(C)$ the number of real infinite places of C (i.e. the number of asymptotes) and by $\beta(C)$ the number of complex, but not real infinite places of C. If C has a birational parameterization, then these integers coincide with the numbers occurring in (P-EXI-2) and (P-EXI-3).

LEMMA 5.1. (H-AUX-1) *Let $f : C \to C'$ be a polynomial map, not necessarily almost surjective. Then*

$$\alpha(C) + \beta(C) \geq \alpha(C') + \beta(C').$$

In case of equality, f maps each infinite place of C to an infinite place of C', and the preimage of any infinite place of C' is a single infinite place of C.

PROOF. The action of f on places is surjectiv, and it cannot happen that a finite place is mapped to an infinite place. Hence each infinite place of C' has at least one infinite place of C in its preimage. In the equality case, there is exactly one. Moreover, we have no more other infinite places of C that can be mapped to finite places of C'. □

PROOF. (P-EXI-2). (b)→(c): If C is trigonometric, then there is a polynomial map from the unit circle S_0 to C. By (H-AUX-1), we have

$$\alpha(C) + \beta(C) \leq \alpha(S_0) + \beta(S_0) = 2.$$

Since C is bounded, we have $\alpha(S_0) = 0$. Now, $\beta(C)$ must be an even number, since complex infinite points appear in conjugate pairs. Also, it is positive, because the total number of asymptotes cannot be zero. It remains only $\beta = 2$. □

We introduce the maps

$$m_n : S_0 \to S_0, (\cos\theta, \sin\theta) \mapsto (\cos(n\theta), \sin(n\theta)).$$

These maps are polynomial (by the de Moivre formulae). The next lemma is equivalent to (P-COR). But, we cannot use (P-COR) to prove the lemma.

LEMMA 5.2. (H-AUX-2) *Let $f : S_0 \to S_0$ be a polynomial map. Then there is an integer n and a rotation or reflection e, such that $f = e \circ m_n$.*

PROOF. By (H-AUX-1), the inverse image of any of the two complex infinite places is one of the two infinite places.

Let $g : S^1 \to S_0$ be the rational parameterization $z \mapsto (\frac{z^2+1}{2z}, \frac{z^2-1}{2iz})$. It is birational, its inverse is $(u, v) \mapsto u + iv$. It maps the places $z = 0$ and $z = \infty$ to the two complex places of S_0.

We consider the rational map $f' := g^{-1} \circ f \circ g$. There are two cases.

Case 1: The preimage of the place $z = 0$ is the place $z = 0$, and the preimage of the place $z = \infty$ is the place $z = \infty$. Then f' is given by a polynomial whose only zero is zero, i.e. a polynomial of the form az^n. Since f' maps the complex unit circle to the complex unit circle, we have $|a| = 1$. Then, f is $e \circ m_n$, where e is the rotation corresponding to the multiplication with the complex number a.

Case 2: The preimage of the place $z = 0$ is the place $z = \infty$, and the preimage of the place $z = \infty$ is the place $z = 0$. Left to the reader. □

The next lemma allows to construct polynomial maps.

LEMMA 5.3. (H-AUX-3) *Let S_0 be the unit circle. Let $f : S_0 \to C$ be a polynomial map. Let $g : C' \to C$ be a birational polynomial map. Suppose that*

$$\alpha(C) + \beta(C) = \alpha(C') + \beta(C').$$

Then $g^{-1} \circ f$ is a polynomial map.

PROOF. Polynomial maps map finite places to finite places. Since the number of infinite places is the same for C and C', and g acts bijectively on places, the map g^{-1} also maps finite places to finite places. Then the composite $r := g^{-1} \circ f$ also maps finite places to finite places. Then, the components R_1, R_2 of r map finite places to finite values. By a well-known theorem (theorem VI.3 in (Bourbaki, 1964)), R_1 and R_2 are integral over the function ring. But the function ring of S_0 is integrally closed, hence R_1 and R_2 are polynomial functions. Thus, r is polynomial. □

Let $t : [0, 2\pi] \rightarrow C$ be a trigonometric parameterization. Then there is a polynomial map $t_a : S_0 \rightarrow C$, such that $t = t_a \circ s_0$, where $s_0 : [0, 2\pi] \rightarrow S_0$ is the standard parameterization $(\cos\theta, \sin\theta)$. We call it the *algebraic form* of t.

If the algebraic form is birational, then we also say that t is a birational trigonometric parameterization (which is a little bit sloppy because the functions involved are transcendental). Since the map g in the proof of (H-AUX-1) is birational, a trigonometric parameterization is birational iff its complex form is birational.

LEMMA 5.4. (H-AUX-4) *Let C be an algebraic curve which has a at least a partial trigonometric parameterization. Then one of the following holds.*

(a) *C has a birational trigonometric parameterization, $\alpha(C) = 0$, $\beta(C) = 2$.*

(b) *C has a birational polynomial parameterization, $\alpha(C) = 1$, $\beta(C) = 0$.*

PROOF. By (H-AUX-1), we have $\alpha(C)+\beta(C) \leq 2$. Since $\beta(C)$ is even and $\alpha(C)+\beta(C) > 0$, we have three possibilities.

$\alpha(C) = 0$, $\beta(C) = 2$. Then C has a birational trigonometric parameterization by (P-EXI-2).

$\alpha(C) = 2$, $\beta(C) = 0$. Then the algebraic form of a trigonometric parameterization maps the two complex infinite places of S_0 to the two real places of C. This is impossible, because the two complex places are conjugated and can only be mapped to the same real place.

$\alpha(C) = 1$, $\beta(C) = 0$. Then C has a birational polynomial parameterization by (P-AUX). □

LEMMA 5.5. (H-AUX-5) *A trigonometric parameterization is simple iff it is birational.*

PROOF. $\leftarrow$: Obvious.

$\rightarrow$: Let $t : [0, 2\pi] \rightarrow C$ be simple and birational. Let S be its zero set of the equation of C (i.e. the Zariski closure of C). This set has at least a partial trigonometric parameterization. By (H-AUX-4), we distinguish two cases.

Case 1: S has a birational trigonometric parameterization t', and $\alpha(S) = 0$, $\beta(C) = 2$. By (H-AUX-3), the rational map $u := (t'_a)^{-1} \circ t_a : S_0 \rightarrow S_0$ is polynomial. By (H-AUX-2), u factors into $e \circ m_n$ for suitable e, n. Since u is simple, we have $n = 1$, and u is birational. Thus, t_a is also birational.

Case 2: S has a birational polynomial parameterization p, and $\alpha(S) = 1$, $\beta(C) = 0$. By (H-AUX-3), the rational map $u := p^{-1} \circ t_a : S_0 \rightarrow (-\infty, \infty)$ is polynomial. It is also simple. But one cannot have a simple polynomial map from the circle to the line by topological reasons. This case is therefore impossible. □

PROOF. (S-UNI). Let t, t' be two simple parameterizations of the same curve C. By (H-AUX-5), both are birational. The parameter change is $t_a^{-1} \circ t'_a$, which is also birational and polynomial by (H-AUX-3). By (H-AUX-2), it is either a rotation or a reflection, which means a phase change or an orientation change in terms of angles. □

PROOF. (S-HOW). Let t be a parameterization, and let t' be a simplification for t. By (H-AUX-5), t'_a is birational. By (H-AUX-3) and (P-EXI-2), $(t'_a)^{-1} \circ t_a$ is polynomial, and by (H-AUX-2) we can write $t_a = t'_a \circ e \circ m_n$ for suitable integer n and rotation or reflection e. Then, $t'' := t'_a \circ e$ is a simplification of t_a. Moreover, we get t from t'' by multiplying the angle with n. □

PROOF. (I-EXI). (c)→(b): For $t : [0, 2\pi] \to C$, we construct either a trigonometric simplification or a polynomial simplification. Let S be the Zariski-closure of C. By (H-AUX-4), S has either a birational trigonometric parameterization or a birational polynomial parameterization.

If S has a simple trigonometric parameterization t', then the map $u := (t'_a)^{-1} \circ t_a$ is polynomial by (H-AUX-3). By (H-AUX-2), all polynomial maps from S_0 to itself are surjectiv. It follows that t and t' have the same image, and t' is a simplification for t.

If S has a simple polynomial parameterization p, then the map $u := p^{-1} \circ t_a$ is polynomial by (H-AUX-3). The image of u is an interval $[a, b]$, and $p : [a, b] \to C$ is a polynomial simplification for t.

(b)→(a): Let $t : [0, 2\pi]$ be a simple trigonometric parameterization. By (H-AUX-5), it is birational. If S is the Zariski closure of C, then the inverse of t_a is defined for almost all points of S. Thus, the equation of S is an implicitization of C. □

PROOF. (S-EXI). Follows immediately from (I-EXI). □

LEMMA 5.6. (H-AUX-6) *Let $t = (F, G) : [0, 2\pi] \to C$ be a trigonometric parameterization with a polynomial simplification. Then there is a polynomial simplification $p = (P, Q)$ and a trigonometric polynomial H, such that $F = P(H)$, $G = Q(H)$, and $\mathrm{R}(F, G) = \mathrm{R}(H)$.*

PROOF. Let S be Zariski closure of C. By (P-AUX), it has a birational polynomial parameterization $p = (P, Q)$. By (H-AUX-3), the map $p^{-1} \circ t_a$ is polynomial. Then the map $p^{-1} \circ t : [0, 2\pi] \to \infty$ is a trigonometric polynomial H. Then P, Q, H satisfy the required identities. □

PROOF. (S-AUX). We have to show $\mathrm{R}(F, G) = \mathrm{R}(G, Q, R)$, where Q and R are quotient and remainder of the trigonometric division $F : G$. We distinguish two cases.

Case 1: The trigonometric parameterization (F, G) has a polynomial simplification. By (H-AUX-6), $f(H) = F$, $g(H) = G$, and $\mathrm{R}(F, G) = \mathrm{R}(H)$ for a suitable trigonometric polynomial H and suitable polynomials f, g. Let q and r by quotient and remainder of the polynomial division $f : g$. Suppose that $\deg H = r$, $\deg f = m$, $\deg g = n$. Then $F = Gq(H) + r(H)$ and $\deg r(H) < \deg G$. By the uniqueness of trigonometric quotient and remainder, we have $Q = q(H)$ and $R = r(H)$. Hence, $Q, R \in \mathrm{R}(H) = \mathrm{R}(F, G)$.

Case 2: The trigonometric parameterization $t = (F, G)$ has no polynomial simplification. Let n be the greatest common divisor of all multiplicators of θ occurring in nonzero summands of F or G. By (I-EXI) (or S-EXI)) and (S-HOW), there is a trigonometric simplification t', such that $t = t' \circ m_n$. By (H-AUX-5), t' is birational. Hence,

$\mathrm{R}(F,G)=\mathrm{R}(\cos(n\theta),\sin(n\theta))$. On the other side, n divides all multiplicators of θ occurring in nonzero summands of Q and R. Thus, $Q,R\in\mathrm{R}(H)=\mathrm{R}(F,G)$. □

PROOF. (S-SUB). Suppose, indirectly, that $t=(F,G):[0,2\pi]\to C$ has a polynomial simplification, but POLYSIMPLIFY answers `NotExist`. By (H-AUX-6), there is a trigonometric polynomial H, such that $K:=\mathrm{R}(H)=\mathrm{R}(F,G)$. If r is a rational function with a denominator of positive degree, then $r(H)$ cannot be a trigonometric polynomial, because it has poles in the complex plane. Therefore, all trigonometric polynomials contained in K are of the form $f(H)$ with polynomial f.

Since POLYSIMPLIFY answers `NotExist`, K contains two trigonometric functions F', G' of the same degree, which cannot be reduced with respect to each other. This means that their leading binomials are linearly independant. On the other side, any leading binomial of a trigonometric polynomial in K is a multiple of the leading binomial of $H^{n/r}$, where r is the degree of H. This is a contradiction. □

PROOF. (I-HOW-1). Recall the notation of (I-HOW-1): $(\frac{P(z)}{z^m},\frac{Q(z)}{z^n})$ is the complex form of a simple trigonometric parameterization t, and $R(x,y):=\mathrm{resultant}_z(P(z)-z^mx,Q(z)-z^ny)$. Let F be the implicitization of t, which exists by (I-EXI). For any point (x,y) on the curve, the two polynomials $P(z)-z^mx$ and $Q(z)-z^ny$ have a common complex solution. Therefore, R vanishes on (x,y). Therefore, F divides R.

Let x_0 be generic (i.e. transcendental over all coefficients of the involved polynomials). Then $P(z)-z^mx_0$ has $2m$ different complex solutions $z_1,\ldots,z_{2m}$. Because t is birational by (H-AUX-5), t_c is simple over the complex numbers, and the points $t_c(z_1),\ldots,t_c(z_{2m})$ in C^2 are all different. Thus, $F(x_0,y)$ has $2m$ complex solutions. We have $\deg_y(F)=2m$. Analogously, we can show that $\deg_x(F)=2n$.

On the other hand, we have $\deg_y(R)\leq 2m$ and $\deg_x(R)\leq 2n$. Therefore, $R=cF$ for a nonzero constant c. □

PROOF. (I-HOW-2). Recall the notation of (I-HOW-1): $p=(P(s),Q(s)):[a,b]\to C$ is a polynomial birational parameterization, $R(x,y)$ is the resultant and $R_0(x,y)+R_1(x,y)s$ is the first subresultant of $P(s)-x$ and $Q(s)-y$ with respect to s. The proof that R is the equation of C is completely analogous to the proof of (I-HOW-1). In order to show that (R, $-R_0/R_1$, $[a,b]$) is a semi-implicitization, we show that $-R_0/R_1$ represents a rational inverse to p.

Let K be the quotient field of $\mathrm{R}[x,y]/(R)$ (i.e. the function field of C). Over K, the polynomials $P(s)-x$ and $Q(s)-y$ have a linear gcd, and its unique solution represents the rational function $p^{-1}:C\to\mathrm{R}$. (This is a general way to invert rational functions, e.g. in (Schicho, 1995).) Note that the gcd is the last nonvanishing polynomial in the polynomial remainder sequence of $P(s)-x,Q(s)-y$ (over K). Then, by a theorem of Collins and Habicht (see (Habicht, 1948; Collins, 1967)), the first subresultant of $P(s)-x,Q(s)-y$ (still over K) is the gcd.

Subresultants commute with homomorphisms. Therefore, R_0+R_1s is linear modulo R, and $-R_0/R_1$ represents the rational function p^{-1}. □

References

Abhyankar, S. S. (1990). *Algebraic Geometry for Scientists and Engineers.* Number 35 in Mathematical Surveys and Monographs. American Mathematical Society, Providence, Rhode Island.

Abhyankar, S. S., Bajaj, B. (1987). Automatic parametrization of curves and surfaces III. *Computer Aided Geometric Design*, **5-4**:309–323.

Alonso, C., Gutierrez, J., Recio, T. (1995). Reconsidering algorithms for real parametric curves. *Applicable Algebra in Engineering, Communication and Computing*, **6**:345–352.

Binder, F. (1995). Polynomial Decomposition. Master's thesis, University of Linz.

Binder, F. (1996). Fast Computations in the Lattice of Polynomial Rational Function Fields. In *ISSAC-96*, pages 43–48. ACM Press.

Bourbaki, N. (1964). *Commutative algebra.* Hermann.

Brown, W. S., Traub, J. F. (1971). On Euclid's algorithm and the theory of subresultants. *Journal ACM*, **18**(4):505–514.

Buchberger, B. (1965). *An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal.* PhD thesis, Universitat Innsbruck, Institut fur Mathematik. German.

Buchberger, B. (1985). Groebner bases: An algorithmic method in polynomial ideal theory. In Bose, N. K., editor, *Recent Trends in Multidimensional Systems Theory*, chapter 6. D. Riedel Publ. Comp.

Collins, G. E. (1967). Subresultants and reduced polynomial remainder sequences. *Journal ACM*, **14**:128–142.

Collins, G. E. (1975). Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. In *Lecture Notes In Computer Science*, pages 134–183. Springer-Verlag, Berlin. Vol. 33.

Collins, G. E., Hong, H. (1991). Partial cylindrical algebraic decomposition for quantifier elimination. *Journal of Symbolic Computation*, **12**(3):299–328.

Gao, X.-S., Chou, S.-C. (1992). Implicitization of Rational Parametric Equations. *J. Symb. Comput.*, **14**: pages 459–470.

Gutierrez, J., Recio, T. (1995). Advances on the simplification of sine-cosine equations. Technical Report 1/1995, Dept. Matematicas y Computacion. Universidad de Cantabria.

Habicht, V. W. (1948). Eine verallgemeinerung des sturmschen wurzelzahlverfahrens. *Comm. Math. Helvetici*, **21**:99–116.

Hoffmann, C. M. (1989). *Geometric and Solid Modelling – an Introduction.* Morgan Kauffmann Publisher, San Mateo, California.

Hong, H. (1990). *Improvements in CAD-based Quantifier Elimination.* PhD thesis, The Ohio State University.

Hong, H. (1995). Implicitization of curves parameterized by generalized trigonometric polynomials. In *Proceedings of Applied Algebra, Algebraic Algorithms and Error Correcting Codes (AAECC-11)*, pages 285–296.

Hong, H. (1996). Implicitization of nested circular curves. *Journal of Symbolic Computation.* To appear.

Kalkbrener, M. (1990). Implicitization of Rational Curves and Surfaces. In Sakata, editor, *Lect. Notes in Comp. Sci. 508, AAECC-8*, Tokyo, Japan.

Manocha, D., Canny, J. (1991). Rational curves with polynomial parametrization. *Computer Aided Geometric Design*, pages 12–19.

Mnuk, M., Sendra, J. R., Winkler, F. (1996). On the complexity of parametrizing curves. *Beitr. Algebra und Geometrie*, **37/2**.

Mnuk, M., Wall, B., Winkler, F. (1995). CASA Reference Manual. Technical Report 95-02, RISC-Linz.

Pottmann, H. (1984). On the geometry of higher planet motion. *Mh. Math.*, **97**:141–156. in german.

Recio, T., Sendra, J. R. (1997). Real parametrizations of real curves. *Journal of Symbolic Computation.* to appear.

Schicho, J. (1992). On the choice of pencils in the parametrization of curves. *Journal of Symbolic Computation*, **14**(6):557–576.

Schicho, J. (1995). *Rational parametrization of surfaces.* PhD thesis, RISC Linz.

Sederberg, T. W. (1986). Improperly parametrized rational curves. *Computer Aided Geometric Design*, **3**:67–75.

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

Sendra, J., Winkler, F. (1997). Parametrization of algebraic curves over optimal field extensions. *Journal of Symbolic Computation.* to appear.

van Hoeij, M. (1994). Computing parametrizations of rational algebraic curves. In *ISSAC-94*, pages 187–190. ACM Press.

van Hoeij, M. (1997). Rational parametrizations of rational algebraic curves. *Journal of Symbolic Computation.* to appear.

Winkler, F. (1988). A p-adic approach to the computation of grobner bases. *J. Symb. Comp.*, **6(2-3)**:287–304.

Winter, D. J. (1974). *The structure of fields.* Springer.

Wu, W. T. (1986). Basic principles of mechianical theorem proving in elementary geometries. *Journal of Automated Reasoning*, **2**:221–252.

Wunderlich, W. (1947). Higher cycloid curves. *Österr. Ing. Arch.*, **1**:277–296.
Wunderlich, W. (1950). Approximation with higher cycloid curves. *Österr. Ing. Arch.*, **4**:3–11.