Proceedings of the 3rd ASCM, 23–36
Aug. 6–8, 1998. Lanzhou


# Algebraic Factorization Applied to Geometric Problems

Dongming Wang[†] and Lihong Zhi[‡]

[†]LEIBNIZ–INPG, 46, avenue Félix Viallet, 38031 Grenoble Cedex, France
[‡]Institute of Systems Science, Academia Sinica, Beijing 100080, China

**Abstract.** This paper describes an optimized method for factorizing multivariate polynomials over algebraic extension fields. The proposed method is applied to solving several selected problems in automated geometry theorem proving, decomposition and implicitization of geometric objects, and verification of geometric conditions. Some performance comparisons between this and other related methods are reported. This work demonstrates the practical value and need of algebraic factorization in geometric problem-solving.

## 1. Introduction

Factoring multivariate polynomials over algebraic extension fields (or *algebraic factorization* for short) is one of the most difficult tasks in computer algebra. Algorithmic investigations on the subject, began in the middle 1970's (see [13, 18, 19] for example), have led to the revitalization of classical ideas and development of new and powerful techniques [1, 7, 8, 9]. Research efforts and technological advances have made factoring routines available and efficient on desktop. Our study on algebraic factorization started in 1984, motivated by the need of it in Wu's method [20, 21] for geometry theorem proving (GTP). Two different methods were proposed in [6] and [15] respectively and applied to GTP [16] and irreducible decomposition of algebraic varieties [14]. Investigations along this line have been furthered recently by the second author [23] who has been trying to work out an optimized algorithm by incorporating and improving different techniques. For some time we have observed that, in the algebraic treatment of problems with geometric background, it happens often that some polynomials are reducible over certain algebraic extension fields and their factorization may result in easy solutions to the problems. This paper evolves from an exploration of this observation. It is twofold: on one hand, the paper provides a set of selected geometric problems and explains how algebraic factorization can help solve such problems. On the other hand, the selected problems serve as a reasonable testbed for the efficiency and applicability of the different algorithms we are working with.

In the following section, we describe a hybrid factoring algorithm which has good overall performance according to our experiments. We shall indicate the cases in which other algorithms may perform better. In Sections 3, 4 and 5, different types of problems from geometry — including the non-existence of real MacLane $8_3$ configuration and the verification of Tam conditions for circle space — and their solutions making use of algebraic factorization will be presented. Some of these problems are computationally hard and unsolvable by other methods (without factorization). Timing statistics and comparisons among different factoring methods for some of the occurring polynomials will be given. The results of this paper demonstrate the practical value of our factoring methods and their implementation.

## 2. An Optimized Method of Factorization

Let $\boldsymbol{Q}$ denote the field of rational numbers, $\boldsymbol{Z}$ denote the ring of integers and $u_1, u_2, \ldots, u_d$ be a set of transcendental elements, abbreviated as $\boldsymbol{u}$. The transcendental extension field obtained from $\boldsymbol{Q}$ by adjoining the $u_i$ is denoted by $\boldsymbol{K}_0$, i.e., $\boldsymbol{K}_0 = \boldsymbol{Q}(u_1, \ldots, u_d)$. A finite ordered set $\mathbb{A}$ of polynomials is called an *ascending set* if it can be put in the form

$$[A_1(\boldsymbol{u}, y_1), A_2(\boldsymbol{u}, y_1, y_2), \ldots, A_r(\boldsymbol{u}, y_1, y_2, \ldots, y_r)]$$

with $A_i \in \boldsymbol{Q}[\boldsymbol{u}, y_1, \ldots, y_i]$, $\deg(A_i, y_i) > 0$ for each $i$, and $\deg(A_i, y_j) < \deg(A_j, y_j)$ for each pair $j < i$. Here $\deg(A_i, y_j)$ denotes the *degree* of $A_i$ in $y_j$ as usual. $\mathbb{A}$ is said to be *irreducible* if $A_i$ as a polynomial in $\boldsymbol{K}_{i-1}[y_i]$ is irreducible, where $\boldsymbol{K}_{i-1} = \boldsymbol{K}_{i-2}(\eta_{i-1})$ with $A_{i-1}$ as minimal polynomial of $\eta_{i-1}$ for each $i \geq 2$. The field

$\boldsymbol{K}_r$ is called an *algebraic extension field* of $\boldsymbol{K}_0$ defined by $\mathbb{A}$ (or simply by $A_1$ when $r = 1$). If $d = 0$ and thus $\boldsymbol{K}_0 = \boldsymbol{Q}$, then $\boldsymbol{K}_r$ is called an *algebraic number field*; otherwise it is called an *algebraic function field*. Sometimes, when $\mathbb{A}$ is specified as above, we simply write $\boldsymbol{K}_{i-1}(y_i)$ for $\boldsymbol{K}_i$ without explicitly introducing the algebraic element $\eta_i$.

Any element in $\boldsymbol{K}_r$ can be represented by a basis

$$\{{\eta_1}^{e_1} \cdots {\eta_r}^{e_r} : \ \ 0 \leq e_i < m_i \text{ for all } i\},$$

where $m_i$ is the degree of the minimal polynomial $A_i$ of $\eta_i$ in $y_i$. The *defect* of this basis for $\boldsymbol{K}_r$ is the largest denominator appearing in the representation of those algebraic functions whose monic minimal polynomials lie in $\boldsymbol{Z}[\boldsymbol{u}]$. The *discriminant* of the basis for $\boldsymbol{K}_r$ is

$$N_2 N_3 \cdots (\mathrm{dis}(A_1)) N_1 N_3 \cdots (\mathrm{dis}(A_2)) N_1 N_2 \cdots (\mathrm{dis}(A_3)) \cdots,$$

where $N_i$ is the norm map, i.e., the product of the images under the different embeddings from $\boldsymbol{K}_i$ to $\boldsymbol{K}_{i-1}$, and $\mathrm{dis}(A_i)$ denotes the discriminant of $A_i$ (which is defined to be the resultant of $A_i$ and its derivative $A_i'$ with respect to $y_i$). The following theorem can be easily proved (see [1]).

**Theorem 1**. The square of the defect of the basis for $\boldsymbol{K}_r$ divides its discriminant.

As we know, integer substitutions and Hensel lifting are efficient techniques for factorizing polynomial over finite fields, $\boldsymbol{Z}$ or algebraic number fields. In this section, we extend these techniques to factorize multivariate polynomials over algebraic function fields. We state the extended Hensel lemma below and refer to [22] for other details.

**Extended Hensel Lemma**. Let $F(x, x_2, \ldots, x_t)$ be a polynomial in $\boldsymbol{K}_r[x, x_2, \ldots, x_t]$ and $a_2, \ldots, a_t$ be a set of integers satisfying that

$$\deg(F(x, x_2, \ldots, x_t), x) = \deg(F(x, a_2, \ldots, a_t), x)$$

and $F(x, a_2, \ldots, a_t)$ is squarefree. Let a factorization of $F(x, a_2, \ldots, a_t)$ over $\boldsymbol{K}_r$ be

$$F(x, a_2, \ldots, a_t) \equiv G_1^{(0)}(x) \cdots G_m^{(0)}(x) \mod (U),$$

where $U = (x_2 - a_2, \ldots, x_t - a_t)$ denotes the ideal generated by $x_2 - a_2, \ldots, x_t - a_t$. Then for an arbitrary non-negative integer $k$, one can construct polynomials $G_1^{(k)}, \ldots, G_m^{(k)} \in \boldsymbol{K}_r[x, x_2, \ldots, x_t]$ such that

$$\begin{aligned} &F(x, x_2, \ldots, x_t) \equiv G_1^{(k)}(x, x_2, \ldots, x_t) \cdots G_m^{(k)}(x, x_2, \ldots, x_t) \mod (U^{k+1}), \\ &G_i^{(k)}(x, x_2, \ldots, x_t) \equiv G_i^{(0)}(x) \mod (U). \end{aligned}$$

By choosing $x$ as the main variable, one can write $F$ in the form

$$F = C_n x^n + \cdots + C_0$$

with $C_i \in \boldsymbol{K}_r[x_2, \ldots, x_t]$ for $i = 0, 1, \ldots, n$. $C_n$ is the leading coefficient of $F$ in $x$. With respect to $x$, the content of $F$ is the greatest common divisor of $C_0, \ldots, C_n$; $F$ is *primitive* if its content is 1. $F$ is said to be *squarefree* if it has no repeated factors. In [23] we have presented a method for the squarefree decomposition of polynomials over algebraic function fields. In what follows, $F$ is assumed to be squarefree, and primitive with respect to its main variable.

Now consider the factorization of a multivariate polynomial $F$ over the algebraic function field $\boldsymbol{K}_r$ which is defined by the irreducible ascending set $\mathbb{A}$. Through some transformations such as normalization and linear transformation, we can make the leading coefficients of $F$ and the polynomials in $\mathbb{A}$ to be in $\boldsymbol{Z}$.

The basic idea underlying the algorithm to be described is using suitable integer substitutions to first map $F$ to a univariate polynomial and $\boldsymbol{K}_r$ to an algebraic number field and then map the algebraic number field to a simple algebraic number field through linear transformation and characteristic sets computation [11, 20]. Part of this is done by devising a method similar to that given in [13]. The factors of the original polynomial $F$ are finally reconstructed by Hensel lifting and true factor test. Here we should note that the ascending set

which defines the extension field must be lifted along with the factors. Below we give an outline of the three main algorithms and present two examples to illustrate their main steps. Note that $\boldsymbol{\eta}$ stands for $\eta_1, \ldots, \eta_r$.

**Algorithm** FactorA.

Input: An irreducible ascending set $\mathbb{A} = [A_1(\boldsymbol{u}, y_1), \ldots, A_r(\boldsymbol{u}, y_1, \ldots, y_r)]$ that defines the algebraic function field $\boldsymbol{Q}(\boldsymbol{u}, \boldsymbol{\eta})$ and a squarefree polynomial $F(\boldsymbol{u}, \boldsymbol{\eta}, x_1, \ldots, x_t) \in \boldsymbol{Q}(\boldsymbol{u}, \boldsymbol{\eta})[x_1, \ldots, x_t]$.

Output: An irreducible factorization of $F$ over $\boldsymbol{Q}(\boldsymbol{u}, \boldsymbol{\eta})$.

Step 1. Choose two sets of lucky integers $\boldsymbol{b} = (b_1, \ldots, b_d)$ and $\boldsymbol{a} = (a_2, \ldots, a_t)$, and let

$$F^{(0)} := F(\boldsymbol{b}, \boldsymbol{\eta}, x_1, \boldsymbol{a}),$$
$$\mathbb{A}^{(0)} := [A_1(\boldsymbol{b}, y_1), \ldots, A_r(\boldsymbol{b}, y_1, \ldots, y_r)].$$

Step 2. Use UFactorA to factorize $F^{(0)}(\boldsymbol{\eta}, x_1)$ over $\boldsymbol{Q}(\boldsymbol{\eta})$ defined by $\mathbb{A}^{(0)}$:

$$F^{(0)} \equiv G_1^{(0)}(\boldsymbol{\eta}, x_1) \cdots G_m^{(0)}(\boldsymbol{\eta}, x_1) \mod (U, \mathbb{A}^{(0)}),$$

where $U = (u_1 - b_1, \ldots, u_d - b_d, x_2 - a_2, \ldots, x_t - a_t)$.

Step 3. Apply Hensel lifting for the factors $G_i^{(0)}$ and $\mathbb{A}^{(0)}$ such that

$$F \equiv G_1^{(\delta)}(\boldsymbol{u}, \boldsymbol{\eta}, x_1, \ldots, x_t) \cdots G_m^{(\delta)}(\boldsymbol{u}, \boldsymbol{\eta}, x_1, \ldots, x_t) \mod (U^{\delta+1}, \mathbb{A}^{(\delta)}),$$
$$\mathbb{A} \equiv \mathbb{A}^{(\delta)} \mod (U^{\delta+1}).$$

Step 4. When $\delta > \deg(F, \boldsymbol{u}) + \sum_{i=2}^{t} \deg(F, x_i) + \sum_{i=1}^{r} \deg(A_i, \boldsymbol{u})$ (where the degree in $\boldsymbol{u}$ is meant the *total degree*), use TrueFactor test to obtain

$$F = G_1(\boldsymbol{u}, \boldsymbol{\eta}, x_1, \ldots, x_t) \cdots G_s(\boldsymbol{u}, \boldsymbol{\eta}, x_1, \ldots, x_t).$$

In step 1 of FactorA, the two sets of lucky integers $\boldsymbol{b} = (b_1, \ldots, b_d)$ and $\boldsymbol{a} = (a_2, \ldots, a_t)$ are chosen to satisfy the following two conditions:

1) $F^{(0)} = F(\boldsymbol{b}, \boldsymbol{\eta}, x_1, \boldsymbol{a})$ remains squarefree and $\deg(F^{(0)}, x_1) = \deg(F, x_1)$.

2) $\mathbb{A}^{(0)} = [A_1(\boldsymbol{b}, y_1), \ldots, A_r(\boldsymbol{b}, y_1, \ldots, y_r)]$ is still an irreducible ascending set.

For the first condition, we only need to choose $\boldsymbol{a}$ and $\boldsymbol{b}$ such that

$$\mathrm{res}_{x_1}(F, F')(\boldsymbol{b}, x_1, \boldsymbol{a}) \neq 0.$$

Here and later on $\mathrm{res}_x$ denotes the resultant of the polynomials with respect to the variable $x$. It is more difficult to choose $\boldsymbol{b}$ such that the ascending set remains irreducible. However, there is a lot of freedom according to the following Hilbert irreducibility theorem.

**Theorem 2**. Let $P(y_1, \ldots, y_s, x_1, \ldots, x_t)$ be irreducible in $\boldsymbol{Z}[y_1, \ldots, y_s, x_1, \ldots, x_t]$ and $U(N)$ denote the number of $s$-tuples $(b_1, \ldots, b_s) \in \boldsymbol{Z}^s$ such that $|b_i| \leq N$ for $1 \leq i \leq s$ and $P(b_1, \ldots, b_s, x_1, \ldots, x_t)$ is reducible in $\boldsymbol{Z}[x_1, \ldots, x_t]$. Then there exist constants $a$ and $c$ (depending on $P$) such that $U(N) \leq c(2N+1)^{s-a}$ and $0 < a < 1$.

According to this theorem and the primitive element theory, there exist an infinite number of specializations of $\boldsymbol{u}$ which keep the irreducibility of the ascending set $\mathbb{A}$.

Now let us have a look at the fourth step in FactorA. It is obvious that the degree of any factor of $F$ is less than the degree of $F$ in $\boldsymbol{x}$, but this is not true for the degree in $\boldsymbol{u}$. Consider, for example, the factorization

$$F = x^2 - u = (x + u^2 y)(x - u^2 y)$$

over the extension field $\boldsymbol{Q}(u, y)$ defined by the minimal polynomial $u^3 y^2 - 1$. In J. A. Abbott's Ph.D thesis [1], a possible upper bound for the degree in $\boldsymbol{u}$ was given, but unfortunately the bound is often too large and Abbott's proof based on Trager's algorithm [13] is not complete.

We also need to worry about the case where $\boldsymbol{u}$ appears in the denominators of the coefficients of the factors. This may be seen, for example, from the factorization

$$F = x^2 - u = \left(x - \frac{a}{u}\right)\left(x + \frac{a}{u}\right)$$

over the extension field $\boldsymbol{Q}(u, a)$ defined by $a^2 - u^3$. Because of these two cases, it is necessary to distinguish $\boldsymbol{x}$ from $\boldsymbol{u}$ and perform the TrueFactor test. After multiplied by the *defect*, the factors will belong to $\boldsymbol{Q}(\boldsymbol{\eta})[\boldsymbol{u}, x_1, \ldots, x_t]$, so FactorA will terminate when $\delta$ is big enough. We refer to [23] for the details of TrueFactor test.

**Algorithm** UFactorA.

Input: An irreducible ascending set $\mathbb{A} = [A_1(y_1), \ldots, A_r(y_1, \ldots, y_r)]$ that defines $\boldsymbol{Q}(\boldsymbol{\eta})$ and a squarefree polynomial $F(\boldsymbol{\eta}, x) \in \boldsymbol{Q}(\boldsymbol{\eta})[x]$.

Output: An irreducible factorization of $F$ over $\boldsymbol{Q}(\boldsymbol{\eta})$.

Step 1. Select a set of integers $\boldsymbol{c} = (c_1, \ldots, c_r)$ such that the characteristic set $\mathbb{C}$ of $\mathbb{A} \cup \{w - c_1 y_1 - \cdots - c_r y_r\}$ under the variable ordering $w \prec y_1 \prec \cdots \prec y_r$ is irreducible and quasilinear (that is, the first polynomial in $\mathbb{C}$ is irreducible over $\boldsymbol{Q}$ and all the other polynomials in $\mathbb{C}$ are linear with respect to their main variables).

Step 2. Normalize $\mathbb{C}$ so that it becomes the form $\mathbb{C} = [C_0(w), y_1 - C_1(w), \ldots, y_r - C_r(w)]$.

Step 3. Let $F^*(w, x) := F(C_1(w), \ldots, C_r(w), x)$ and apply Factor to $F^*(\xi, x)$ over $\boldsymbol{Q}(\xi)$:

$$F^* = F_1(\xi, x) \cdots F_s(\xi, x),$$

where $\xi$ has minimal polynomial $C_0(w)$.

Step 4. Substitute $\xi = \sum_{i=1}^{r} c_i \eta_i$ for $\xi$ in each $F_i$.

Step 5. Return $F = F_1(\boldsymbol{\eta}, x) \cdots F_s(\boldsymbol{\eta}, x)$.

**Theorem 3**. The probability of success for the selection of the integers $c_i$ in step 1 of UFactorA is 1.

We refer to [5] for a proof of this theorem.

**Algorithm** Factor.

Input: A monic minimal polynomial $m(y)$ of $\alpha$ and a squarefree polynomial $F(\alpha, x) \in \boldsymbol{Q}(\alpha)[x]$.

Output: An irreducible factorization of $F$ over $\boldsymbol{Q}(\alpha)$.

Step 1. Choose a positive integer $s$ and compute

$$G(\alpha, x) := F(\alpha, x - s\alpha),$$
$$R(x) := \mathrm{res}_y(G(y, x), m(y)).$$

Step 2. If $R(x)$ is squarefree then go to step 3. Otherwise, compute over $\boldsymbol{Q}$ an irreducible factorization

$$F_1(x) \cdots F_k(x) = R(x)/\gcd(R(x), R'(x)).$$

If $k = 1$ then go to step 1 (trying another integer $s$) else compute

$$G_i := \gcd(F(x), F_i(x + s\alpha))$$

and factorize $F/(G_1 \cdots G_k)$ and each $G_i$ over $\boldsymbol{Q}(\alpha)$ using Factor:

$$G_i(\alpha, x) = G_{i1}(\alpha, x) \cdots G_{im_i}(\alpha, x), \quad 1 \le i \le k,$$
$$F(\alpha, x)/[G_1(\alpha, x) \cdots G_k(\alpha, x)] = G_{01}(\alpha, x) \cdots G_{0m_0}(\alpha, x);$$

then return

$$F = \prod_{\substack{1 \le j \le m_i \\ 0 \le i \le k}} G_{ij}(\alpha, x)$$

and the algorithm terminates.

Step 3. Factorize $R$ over $\boldsymbol{Q}$:

$$R(x) = H_1(x) \cdots H_l(x).$$

If $l = 1$ then return $F$ and the algorithm terminates.

Step 4. For $i = 1, \ldots, l$ do:

$$\begin{aligned} H_i(\alpha, x) &:= \gcd(H_i(x), G(\alpha, x)), \\ G(\alpha, x) &:= G(\alpha, x)/H_i(\alpha, x), \\ H_i(\alpha, x) &:= H_i(\alpha, x + s\alpha) \end{aligned}$$

over $\boldsymbol{Q}(\alpha)$.

Step 5. Return $F = H_1(\alpha, x) \cdots H_l(\alpha, x)$.

**Theorem 4**. For any $F(\alpha, x) \in \boldsymbol{Q}(\alpha)[x]$ there are only finitely many integers $s$ that make $R(x)$, the norm of $F(\alpha, x - s\alpha)$ over $\boldsymbol{Q}(\alpha)$, not squarefree. If $R(x)$ is squarefree and $H_1(x) \cdots H_k(x)$ is a complete factorization of $R(x)$ over $\boldsymbol{Q}$, then $\prod_{i=1}^{k} \gcd(F(\alpha, x - s\alpha), H_i(x))$ is a complete factorization of $F(\alpha, x - s\alpha)$ over $\boldsymbol{Q}(\alpha)$.

For a proof of this theorem, refer to [13].

**Example 1**. Factorize

$$F = x^2 + r^2ax - rax - aby^2 + ry^2 - r^2aby - raby - r^4$$

over $\boldsymbol{Q}(r, a, b)$ defined by $\mathbb{A} = [a^2 - r, b^2 - ab + r]$.

Step 1. Pick the substitution value 2 for $r$ and 1 for $y$; then $F$ and $\mathbb{A}$ are mapped to

$$F^{(0)} = x^2 + 2ax - 7ab - 14 \quad \text{and} \quad \mathbb{A}^{(0)} = [a^2 - 2, b^2 - ab + 2],$$

respectively. $\mathbb{A}^{(0)}$ is still an irreducible ascending set.

Step 2. Computing a characteristic set of $\mathbb{A}^{(0)} \cup \{w - b\}$ under the variable ordering $w \prec a \prec b$, we get

$$[w^4 + 2w^2 + 4, 2a + w^3, b - w].$$

Substitution of $a = -w^3/2, b = w$ in $F^{(0)}$ yields

$$F^{(0)} = (x + w - 2w^3)(x + w^3 - w)$$

over $\boldsymbol{Q}(w)$ defined by $w^4 + 2w^2 + 4$, so $F = (x + b + 4a)(x - b - 2a)$ over $\boldsymbol{Q}(a, b)$ defined by $\mathbb{A}^{(0)}$.

Step 3. Hensel lifting $\mathbb{A}^{(0)}$ and the two factors of $F^{(0)}$, we have

$$\begin{aligned} F &\equiv (x + by + 4ra - 4a)(x - by - ra) \mod (r - 2, y - 1)^2, \\ \mathbb{A} &\equiv [a^2 - r, b^2 - ab + r] \mod (r - 2, y - 1)^2, \\ F &\equiv (x + by + r^2a)(x - by - ra) \mod (r - 2, y - 1)^3, \\ \mathbb{A} &\equiv [a^2 - r, b^2 - ab + r] \mod (r - 2, y - 1)^3. \end{aligned}$$

Step 4. The factor $x - by - ra$ remains unchanged during the lifting, so with test it is found to be a true factor of $F$. Thus, we have

$$F = (x + by + r^2a)(x - by - ra)$$

over $\boldsymbol{Q}(r, a, b)$ defined by $\mathbb{A}$.

**Example 2**. Factorize $F = x^2 - y + 1$ over $\boldsymbol{K} = \boldsymbol{Q}(y, a)$ defined by $\mathbb{A} = [a^2 - (y - 1)^3]$.

Step 1. Pick the substitution value 0 for $y$; then $F$ and $\mathbb{A}$ are mapped to

$$F^{(0)} = x^2 + 1 \quad \text{and} \quad \mathbb{A}^{(0)} = [a^2 + 1]$$

respectively. The ascending set $\mathbb{A}^{(0)}$ is still irreducible.

Step 2. Applying UFactorA to $F^{(0)}$, one gets

$$F \equiv (x-a)(x+a) \mod (y, \mathbb{A}^{(0)}).$$

Step 3. Hensel lifting $\mathbb{A}^{(0)}$ and the two factors of $F^{(0)}$ proceeds as follows:

$$\begin{aligned}
&F \equiv (x-a-ay)(x+a+ay) \mod (y^2, \mathbb{A}),\\
&\mathbb{A} \equiv [a^2-3y+1] \mod (y^2),\\
&F \equiv (x-a-ay-ay^2)(x+a+ay+ay^2) \mod (y^3, \mathbb{A}),\\
&\mathbb{A} \equiv [a^2+3y^2-3y+1] \mod (y^3),\\
&F \equiv (x-a-ay-ay^2-ay^3)(x+a+ay+ay^2+ay^3) \mod (y^4, \mathbb{A}),\\
&\mathbb{A} \equiv [a^2-y^3+3y^2-3y+1] \mod (y^4).
\end{aligned}$$

Step 4. TrueFactor test: Let $D$ be the greatest factor whose square divides the discriminant of the basis for $\boldsymbol{K}$, i.e., $\mathrm{dis}(a^2-(y-1)^3) = -4(y-1)^3$; clearly $D = y-1$. Take one (or the product) of the above two factors, e.g.,

$$F_1 = (x-a-ay-ay^2-ay^3).$$

Then, we have

$$F_1^* = DF_1 = (y-1)F_1 \equiv x(y-1)+a \mod (y^4, \mathbb{A}).$$

A simple test shows that $F_1^*/D = x + a/(y-1)$ can divide $x^2 - y + 1$. Therefore, we obtain the following factorization

$$F = \left(x - \frac{a}{y-1}\right)\left(x + \frac{a}{y-1}\right)$$

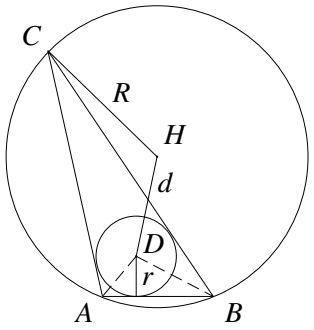
over $\boldsymbol{K}$.

The above method is an extension of P. S. Wang's method [18]. His method is restricted to algebraic number fields, while ours can also factorize multivariate polynomial over algebraic function fields. Wang made use of factorization over finite fields. In our method, factorization is performed over the integers because of the inefficient coefficient bound in the case of algebraic function fields.

## 3. Proving Geometric Theorems

Following Wu [20], one may express a theorem in elementary (unordered) geometry be means of a set $\mathbb{H}$ of polynomials for its hypothesis and, without loss of generality, a single polynomial $C$ for its conclusion. Proving the theorem amounts to deciding whether any zero of $\mathbb{H}$ is a zero of $C$, and if not, which parts of the zeros of $\mathbb{H}$ are zeros of $C$. An elementary version of Wu's method [20] proceeds by computing first a characteristic set $\mathbb{C}$ of $\mathbb{H}$ and then the pseudo-remainder $R$ of $C$ with respect to $\mathbb{C}$. If $R \equiv 0$, then the theorem is proved to be true under the subsidiary condition $J \neq 0$, where $J$ is the product of the initials of the polynomials in $\mathbb{C}$. A large number of geometric theorems can be proved effectively in this way. However, if $R$ happens to be non-zero, one cannot immediately tell whether the theorem is false or not; in this case, one has to examine the reducibility of $\mathbb{C}$ and to perform further decompositions [3, 16, 20]. $\mathbb{C}$ is reducible often when some geometric ambiguities such as bisection of angles and contact of circles are involved in the theorem [21]. To test the irreducibility of $\mathbb{C}$ or to decompose $\mathbb{C}$ into irreducible ascending sets, it is necessary to factorize polynomials over successive algebraic extension fields. In [16] was presented a set of geometric theorems whose automated proofs may require algebraic factorization. Here we give two other examples — Poncelet's theorem and the non-existence of real $8_3$ configuration.

**Example 3** (Poncelet's theorem). Let $R$ be the radius of the circumscribed circle and $r$ the radius of the inscribed circle of an arbitrary triangle, and let $d$ be the distance between the centers of the two circles. Show that $R^2 - 2Rr = d^2$.




Let the arbitrary triangle be $ABC$, the incenter and circumcenter of $\triangle ABC$ be $D$ and $H$, and the points be located as

$$O(0,0),\quad A(x_1,0),\quad B(x_2,0),\quad C(0,x_3),\quad D(x_4,x_5),\quad H(x_6,x_7).$$

Then the hypothesis of the theorem may be expressed as

$$\begin{aligned}
&H_1 = x_3(x_5^2 - x_4^2) - 2x_1(x_4 - x_1)x_5 + x_1x_3(2x_4 - x_1) = 0, && \% \quad \angle BAD = \angle DAC\\
&H_2 = x_3(x_5^2 - x_4^2) - 2x_2(x_4 - x_2)x_5 + x_2x_3(2x_4 - x_2) = 0, && \% \quad \angle ABD = \angle DBC\\
&H_3 = (x_2 - x_1)(2x_6 - x_2 - x_1) = 0, && \% \quad H \text{ is the circumcenter}\\
&H_4 = 2x_3x_7 - 2x_2x_6 - x_3^2 + x_2^2 = 0, && \% \quad \text{of } \triangle ABC\\
&H_5 = r^2 - x_5^2 = 0, && \% \quad r^2 = |OD|^2\\
&H_6 = R^2 - x_7^2 - (x_6 - x_1)^2 = 0, && \% \quad R^2 = |AH|^2\\
&H_7 = d^2 - (x_7 - x_5)^2 - (x_6 - x_4)^2 = 0. && \% \quad d^2 = |DH|^2
\end{aligned}$$

With the above algebraic formulation, Poncelet's theorem is not always true because $D$ can also be an excenter of $\triangle ABC$ and so can $r, R, d$ be negative. It is not easy to distinguish the incenter from the excenters and to deal with positiveness without using inequalities. We want to see for which components the above formulation of Poncelet's theorem is true.

For this purpose, let us order the variables as $x_1 \prec \cdots \prec x_7 \prec r \prec R \prec d$ and split $\{H_1, \ldots, H_7\}$ into two polynomial sets $\mathbb{H}'$ and $\mathbb{H}''$ according to the obvious factorization of $H_5$ (for simplifying the computation). Using Wu's method [20], we compute a characteristic set $\mathbb{C}'$ of $\mathbb{H}'$, and $\mathbb{C}''$ of $\mathbb{H}''$; during the computation, two factors $x_2 - x_1$ and $x_1$ are removed. The pseudo-remainder of the conclusion-polynomial $G = d^2 - R^2 + 2Rr$ is non-zero with respect to both $\mathbb{C}'$ and $\mathbb{C}''$, so we have to examine the reducibility of $\mathbb{C}'$ and $\mathbb{C}''$.

One may find that $\mathbb{C}_1$ differs from $\mathbb{C}_2$ only by their fifth polynomials

$$\begin{aligned}
C_5' &= 2(x_4 - x_2 - x_1)r - x_3(2x_4 - x_2 - x_1),\\
C_5'' &= 2(x_4 - x_2 - x_1)r + x_3(2x_4 - x_2 - x_1).
\end{aligned}$$

The first, sixth and seventh polynomials in $\mathbb{C}'$ and in $\mathbb{C}''$ are

$$\begin{aligned}
C_1' = C_1'' &= 4x_4^4 - 8(x_2 + x_1)x_4^3 - 4(x_3^2 - x_2^2 - 3x_1x_2 - x_1^2)x_4^2 + 4(x_2 + x_1)(x_3^2 - x_1x_2)x_4 - (x_2 + x_1)^2x_3^2,\\
C_6' = C_6'' &= 4x_3^2R^2 - x_3^4 - (x_2^2 + x_1^2)x_3^2 - x_1^2x_2^2,\\
C_7' = C_7'' &= 4x_3^2(x_4 - x_2 - x_1)d^2 - 8x_3^2x_4^3 + 12(x_2 + x_1)x_3^2x_4^2 + [3x_3^4 - 12x_1x_2x_3^2 - 5(x_2^2 + x_1^2)x_3^2 - x_1^2x_2^2]x_4\\
&\quad - (x_2 + x_1)x_3^4 - (x_2 + x_1)^3x_3^2 - x_1^2(x_2 + x_1)x_2^2.
\end{aligned}$$

The other polynomials in $\mathbb{C}'$ and $\mathbb{C}''$ are all linear in their main variables. We thus need to factorize $C_6' = C_6''$ over the extension field $\boldsymbol{K} = \boldsymbol{Q}(x_1, \ldots, x_4)$ defined by the irreducible polynomial $C_1' = C_1''$. The factorization may be found as follows

$$C_6' = C_6'' = (2x_3R - 2x_4^2 + 2x_2x_4 + 2x_1x_4 + x_3^2 - x_1x_2)(2x_3R + 2x_4^2 - 2x_2x_4 - 2x_1x_4 - x_3^2 + x_1x_2).$$

It took 1.65 CPU seconds using Factor A in Maple V.3 on an Alpha station 600.

It may be verified that $C_7' = C_7''$ is irreducible over $\boldsymbol{K}$. Therefore, $\mathbb{C}'$ can be decomposed into two irreducible ascending sets: the pseudo-remainder of $G$ is zero with respect to one of them, and non-zero with respect to the other. The same conclusion holds for $\mathbb{C}''$.

The non-constant factors of the initials of the polynomials in $\mathbb{C}'$ and $\mathbb{C}''$ are $x_3$ and $x_4 - x_2 - x_1$. Hence, under the subsidiary conditions $(x_2 - x_1)x_3(x_4 - x_2 - x_1) \neq 0$ (i.e., $\triangle ABC$ does not degenerate into a line and is not isosceles), the algebraic form of Poncelet's theorem is true for two non-degenerate components and false for the other two. Geometrically, the theorem is true generically when $D$ is the incenter of $\triangle ABC$ and the variables $r$ and $R$ take the same sign.

Remark that the irreducible decompositions for the examples in this paper were computed by using the CharSets package [17]. The following theorem is interesting because it is true over the reals but not the complexes.

**Example 4** (MacLane $8_3$; see [4] and references therein). Let $A, B, C, D, E, F, G, H$ be eight points such that the following eight triples are collinear: $A, B, D; B, C, E; C, D, F; D, E, G; E, F, H; F, G, A; G, H, B; H, A, C$. Then all the other triples are also collinear (i.e., all the eight points lie on the same line).

We take the coordinates for the points as

$$A(0,0),\quad B(1,0),\quad D(u,0),\quad C(x_1,y_1),\quad E(x_2,y_2),\quad F(x_3,y_3),\quad G(x_4,y_4),\quad H(x_5,y_5).$$

Then the hypothesis and conclusion of the theorem may be expressed as follows

$$\begin{aligned}
&H_1 = x_2y_1 - x_1y_2 + y_2 - y_1 = 0, && \% \quad \mathsf{col}(B,C,E)\\
&H_2 = x_1y_3 - u(y_3 - y_1) - x_3y_1 = 0, && \% \quad \mathsf{col}(C,D,F)\\
&H_3 = x_2y_4 - u(y_4 - y_2) - x_4y_2 = 0, && \% \quad \mathsf{col}(D,E,G)\\
\text{HYP:}\quad &H_4 = x_2(y_3 - y_5) + x_3(y_5 - y_2) + x_5(y_2 - y_3) = 0, && \% \quad \mathsf{col}(E,F,H)\\
&H_5 = x_4y_3 - x_3y_4 = 0, && \% \quad \mathsf{col}(F,G,A)\\
&H_6 = y_5 - y_4 + x_5y_4 - x_4y_5 = 0, && \% \quad \mathsf{col}(G,H,B)\\
&H_7 = x_1y_5 - y_1x_5 = 0; && \% \quad \mathsf{col}(H,A,C)
\end{aligned}$$

$$\text{CON:}\quad y_1 = y_2 = y_3 = y_4 = y_5 = 0. \qquad \% \quad \mathsf{col}(A,B,C,D,E,F,G,H)$$

Hereinabove, $\mathsf{col}(A, B, C, \ldots)$ means that the points $A, B, C, \ldots$ are collinear.

Computing an irreducible decomposition of $\{H_1, \ldots, H_7\}$ with respect to the variable ordering $u \prec y_1 \prec \cdots \prec y_5 \prec x_1 \prec \cdots \prec x_5$, one may get eighteen irreducible ascending sets $\mathbb{C}_1, \ldots, \mathbb{C}_{18}$, for which

- $\mathbb{C}_1 = [y_1, y_2, y_3, y_4, y_5] = 0$ implies that the eight points are collinear;
- $\mathbb{C}_2 = [u, y_3, y_4, y_5, x_2y_1 - x_1y_2 + y_2 - y_1, x_3, x_4, x_5] = 0$ implies that $A = D = F = G = H$ and $B, C, E$ are collinear;
- $\mathbb{C}_3 = [y_2, y_3, y_4, y_5, x_2 - 1, x_3 - u, x_5] = 0$ implies that $A = H, B = E, D = F$ and $G$ are collinear.

The other 12 irreducible ascending sets, which only involve linear polynomials, correspond to some degenerate cases which can be derived from the above two cases through a cyclic permutation.

Now let us look at the three irreducible ascending sets $\mathbb{C}_{16}, \mathbb{C}_{17}, \mathbb{C}_{18}$, in which the first polynomials are quadratic. $\mathbb{C}_{16}$ is reproduced as follows

$$\begin{aligned}
\mathbb{C}_{16} = [&u^2 - u + 1, uy_2 - 2y_2 + y_1, uy_3 - 2y_3 + y_1, uy_4 - 3y_4 + y_1, uy_5 + y_5 - uy_1,\\
&ux_2 - 2x_2 + x_1 - u + 1, ux_3 - 2x_3 + x_1 + 1, ux_4 - 3x_4 + x_1 + 1, ux_5 + x_5 - ux_1].
\end{aligned}$$

Let $\alpha$ be a root of $u^2 - u + 1$ and $\beta = (\alpha + 1)/3$; then

$$A(0,0),\quad B(1,0),\quad C(0,1),\quad D(\alpha,0),\quad E(\frac{2-\alpha}{3},\beta),\quad F(\beta,\beta),\quad G(\frac{2+\alpha}{7},\frac{2+\alpha}{7}),\quad H(0,\beta)$$

give a non-degenerate complex zero of $\mathbb{C}_{16}$, under which the eight points are not collinear. So the theorem is not true over the field of complex numbers.

It is easy to verify that the theorem is not true for $\mathbb{C}_{17}$ and $\mathbb{C}_{18}$ over the complexes. Now consider the theorem for the component $\mathbb{C}_{17}$ over the reals (the same discussion is valid for the component $\mathbb{C}_{18}$). The first polynomial in $\mathbb{C}_{17}$ is

$$C_1 = [(u^2 - u + 1)y_2^2 + (u-2)y_1y_2 + y_1^2]y_3^2 - u(2uy_2 - y_2 + y_1)y_1y_2y_3 + u^2y_1^2y_2^2.$$

Factorizing $C_1$ over $\boldsymbol{Q}(y)$ defined by $y^2+3$, one may get two linear factors. $C_1$ has real zeros if and only if the imaginary part $I = u(y_1 - y_2)y_1y_2$ of the two linear factors is zero.

An irreducible decomposition of the polynomial set $\{H_1, \ldots, H_7, I\}$ consists of sixteen components. One component is $[y_1, y_2, y_3, y_4, y_5]$ and the others are all composed of linear polynomials: it is clear that these components represent the two degenerate cases we have discussed above. Therefore, the theorem is true only for one component and false for the other degenerate cases over the reals.

## 4. Decomposition and Implicitization of Curves and Surfaces

Algebraic curves and surfaces are geometric objects defined by zeros of systems of algebraic equations in 2- or 3-dimensional space. In modern geometry engineering like computer-aided geometric design and geometric modeling, it is desirable to decompose such objects into *simpler* and *smaller* subobjects. In the language of algebraic geometry, the problem is to decompose arbitrary algebraic curves and surfaces into irreducible components. In fact, there are several algorithmic methods based on characteristic sets [11, 20] and Gröbner bases [2] for carrying out such decomposition (see [14] for instance). In these methods, algebraic factorization is indispensable.

Let $\mathfrak{V}$ be an algebraic curve or surface in 3-dimensional affine space defined by the common zeros of a set $\mathbb{P}$ of polynomials. While speaking about the *irreducibility* of $\mathfrak{V}$, we mean that $\mathfrak{V}$ cannot be expressed as the union of two or more non-trivial subcurves or subsurfaces of $\mathfrak{V}$. The problem of decomposing $\mathfrak{V}$ into irreducible components is equivalent to computing from $\mathbb{P}$ a sequence of polynomial sets $\mathbb{P}_i$, each of which defines an irreducible subcurve or subsurface $\mathfrak{V}_i$ of $\mathfrak{V}$.

A simple example is to decompose the intersection of two cylinders $x^2 + y^2 = 1$ and $x^2 + z^2 = 1$ in 3-dimensional space [14]. With respect to the variable ordering $x \prec y \prec z$,

$$[x^2 + y^2 - 1, x^2 + z^2 - 1]$$

is a *reducible* ascending set. Decomposing it into irreducible ones requires factoring $x^2+z^2-1$ over the extension field $\boldsymbol{Q}(x, y)$ defined by $x^2 + y^2 - 1$. The intersection is an algebraic curve comprising two irreducible curves defined respectively by

$$x^2 + y^2 - 1 = 0,\ y - z = 0 \ \text{ and } \ x^2 + y^2 - 1 = 0,\ y + z = 0.$$

They are two circles obtained as the sections of the first cylinder by the planes $y - z = 0$ and $y + z = 0$. What follows is a more complicated example.

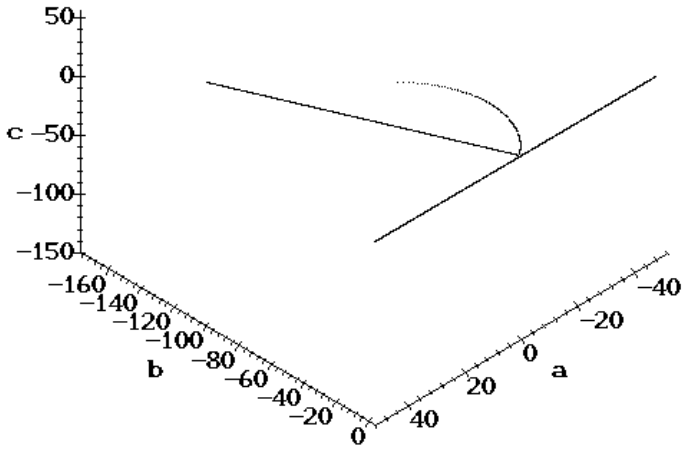
**Example 5**. Let $\mathbb{P} = \{P_1, P_2\}$ with

$$\begin{aligned} P_1 &= -27c^2 + 18abc - 4a^3c - 4b^3 + a^2b^2, \\ P_2 &= 256c^3 - 128a^2c^2 + 144ab^2c + 16a^4c - 27b^4 - 4a^3b^2. \end{aligned}$$

The algebraic curve defined by $\mathbb{P}$ is the intersection of two discriminant surfaces in 3-dimensional space. It may be decomposed into two irreducible curves: one of them is a line defined by $b = 0$ and $c = 0$. The other component is quite complex. It may be defined by the following total degree Gröbner basis

$$\begin{aligned} \mathbb{G} = [&P_1, \\ &512ac^2 + 4104c^2 - 1024b^2c + 352a^3c + 256a^2bc - 1764abc - 121b^3 + 16a^4b - 108a^3b + 32a^5, \\ &- 2048bc^2 + 512a^2c^2 + 1432ac^2 - 4104c^2 - 434b^2c - 528a^2bc + 1764abc + 32a^4c - 568a^3c \\ &+ 108ab^3 + 121b^3 + 108a^3b - 32a^5, \\ &- 256c^3 + 128a^2c^2 + 108ac^2 - 144ab^2c - 72a^2bc + 27b^4 + 16ab^3]. \end{aligned}$$

The two components of the curve are plotted for $-50 \leq a \leq 50$ in the figure below.




In decomposing $\mathbb{P}$ into irreducible ascending sets under $a \prec b \prec c$, we have to factorize a bivariate polynomial of 12 terms with largest coefficient of 89 digits over $\boldsymbol{Q}(a)$ defined by the following minimal polynomial

$$A = 134217728a^4 + 2820096000a^3 + 17689155840a^2 + 42431509152a + 31381059609.$$

Our algorithm examines that the polynomial is irreducible.

Geometric objects such as curves and surfaces may be algebraically represented by implicit or parametric equations. The advantage of each representation depends upon the type of problems to be solved. In geometric modeling, one often needs to convert one representation into the other. The implicitization of parametric objects can be carried out by using Gröbner bases, characteristic sets and other elimination techniques. Here, two examples are presented to show how algebraic factorization may be used to reduce the complexity of the implicitization problem.

**Example 6**. Determine the implicit form (in the variables $x$ and $y$) of the curve given by the following system of equations

$$\begin{aligned}
&(x-u)^2 + (y-v)^2 - 1 = 0,\\
&v^2 - u^3 = 0,\\
&2v(x-u) + 3u^2(y-v) = 0,\\
&(3wu^2 - 1)(2wv - 1) = 0.
\end{aligned}$$

These equations come from a formulation of an offset to the curve $y^2 - x^3 = 0$. The example was communicated by P. Vermeer from the Department of Computer Science, Purdue University. We were told that it ran out of swap space (280 MB) before obtaining the solution by using the Gröbner basis implementation in Macsyma on a Symbolic machine. We have tried to determine the implicit equations using the characteristic set method with Wu's projection theorem. For the first trial, we do not decompose the polynomial set according to the given factorization of the last polynomial. The computation of a characteristic set (with respect to $x \prec y \prec u \prec v \prec w$) is very easy (10.1 seconds in Maple 4.3 on an Apollo DN10000), but the zero decomposition is rather difficult. We tried to compute it with six variants, of which four did not succeed within 2000 CPU seconds. For the two successful variants, 11 quasi-irreducible ascending sets were produced in 937.3 and 1003.88 seconds, respectively. The biggest integer coefficient of the occurring polynomials has more than 800 digits (while the biggest coefficient of the input polynomials is 6). The projection of these ascending sets using our implementation of Wu's algorithm took more than 2000 seconds.

To make the projection possible, we tried to decompose the ascending sets into irreducible ones (which are hoped to be simpler). The irreducibility test for the 11 ascending sets all requires polynomial factorization over algebraic extension fields. If we decompose the input set into two sets of polynomials, then the quasi-irreducible

zero decomposition can be computed in about 740 seconds, yielding 18 ascending sets, where the occurring polynomials have big integer coefficients too.

Below we give in table form the timing statistics on the non-trivial irreducibility tests for the above-mentioned ascending sets with three factoring functions. The timings are provided in CPU seconds and include the time for garbage collection, in Maple V.2 running on a Sun SPARC 2 station. The computation was interrupted manually after 3600 CPU seconds, which is indicated by $> 3600$. The meanings of the headings of the table are explained as follows: Ex – the example number; $d$ – the number of transcendental elements for the extension field; $\deg(\mathbb{A})$ – the degrees of the polynomials in the defining ascending set, separated by the slant; $\deg(F)$ – the degree of the polynomial to be factorized; zfactor – our implementation of the algorithm FactorA in Maple V.2; cfactor – the function in CharSets 1.2 [17]; factor – Maple's built-in function.

Timing Statistics in Maple V.2

| Ex | $d$ | $\deg(\mathbb{A})$ | $\deg(F)$ | zfactor | cfactor | factor |
|---|---|---|---|---|---|---|
| 1 | 0 | 4/2 | 2 | 1.26 | 301.5 | 3 |
| 2 | 0 | 4/2 | 2 | 65.76 | 22.96 | 42.46 |
| 3 | 0 | 2/2/2 | 2 | 103.2 | >3600 | 2759.58 |
| 4 | 0 | 4 | 2 | 0.83 | 1.43 | 1.76 |
| 5 | 0 | 2/6 | 2 | 1273.02 | 809.8 | 2925.03 |
| 6 | 0 | 4 | 2 | 3.33 | 9.95 | 8.05 |
| 7 | 1 | 8 | 2 | 893.6 | >3600 | >3600 |
| 8 | 0 | 4/2 | 2 | 1.31 | >3600 | 2.8 |
| 9 | 0 | 2/2 | 2 | 0.43 | 20 | 3.16 |
| 10 | 0 | 4/2 | 2 | 1.2 | 246.1 | 3.03 |
| 11 | 0 | 2/2 | 2 | 6.48 | 882.2 | 20.13 |

**Example 7** [12]. Consider the following set of four polynomials

$$\begin{aligned} P_1 &= v - u^2, \\ P_2 &= (x-u)^2 + (y-v)^2 + z^2 - r^2, \\ P_3 &= 2su - x + u, \\ P_4 &= y - v + s, \end{aligned}$$

which arise from a formulation in computing the $r$-offset of the parabola given by $v = u^2$ and $w = 0$ in 3-dimensional Euclidean space. To determine the $r$-offset, one has to get the implicit equations and inequations in $x, y, z, r$ by eliminating the variables $u, v, s$ with projection. We have no difficulty to compute the $r$-offset using projection methods without factorization. However, if we want to compute an irreducible zero or variety decomposition of the polynomial set $\mathbb{P} = \{P_1, \ldots, P_4\}$, then algebraic factorization will occur. When the variable ordering $r \prec x \prec y \prec z \prec u \prec v \prec s$ is used, several non-trivial polynomials have to be factorized over algebraic extension fields. Here are some examples:

- $2u^2 - 2y + 1$ over the extension field $\boldsymbol{Q}(r, y, z)$ defined by the minimal polynomial $4z^2 + 4y - 4r^2 - 1$;
- $8yz^2 - 4z^2 + 8y^2 + 8x^2y - 8r^2y - 6y + 14x^2 + 4r^2 + 1$ over $\boldsymbol{Q}(r, x, y)$ defined by the minimal polynomial

$$A = 16y^3 - 24y^2 + 12y - 27x^2 - 2;$$

- $12yu^2 - 6u^2 + 18xu + 4y^2 - 4y + 1$ over $\boldsymbol{Q}(r, x, y, z)$ defined by the irreducible ascending set

$$[A, 12z^2 + 16y^2 - 4y + 12x^2 - 12r^2 + 1].$$

The test of irreducibility and factorization for the above three polynomials took only 0.08, 0.25 and 0.31 CPU seconds respectively using FactorA in Maple V.3 running on an Alpha station 600.

## 5. Verification of Geometric Conditions

In the way of studying geometric spaces (non-commutative geometries), the general problem of automated verification of geometric conditions was addressed in [10]. Some examples on the verification of the Tam configuration for the circle space using algebraic methods were discussed. We take one of them which was considered as a benchmark example. It is actually a quantifier elimination problem over the reals. J. Pfalzgraf [10] tried to solve the problem using the CAD method without success. We explain how this problem can be solved by making use of algebraic factorization.

**Example 8** [10]. Determine whether for any $x_1, x_2, y_1, y_2, z_1, z_2, x_1', x_2', y_1', y_2' \in \boldsymbol{R}$ (the field of reals) satisfying

$$P_1 = (x_1 - y_1)^2 + (x_2 - y_2)^2 - (x_1' - y_1')^2 - (x_2' - y_2')^2 = 0$$

there exist $\zeta_1$ and $\zeta_2$ in $\boldsymbol{R}$ such that

$$P_2 = (x_1' - \zeta_1)^2 + (x_2' - \zeta_2)^2 - (x_1 - z_1)^2 - (x_2 - z_2)^2 = 0,$$
$$P_3 = (y_1' - \zeta_1)^2 + (y_2' - \zeta_2)^2 - (y_1 - z_1)^2 - (y_2 - z_2)^2 = 0.$$

Let $\mathbb{P} = \{P_1, P_2, P_3\}$ and fix the variable ordering as $x_1 \prec x_2 \prec y_1 \prec y_2 \prec z_1 \prec z_2 \prec x_1' \prec x_2' \prec y_1' \prec y_2' \prec \zeta_1 \prec \zeta_2$. Computing a characteristic set $\mathbb{C}$ of $\mathbb{P}$ with respect to this ordering, we get $\mathbb{C} = [P_1, C_2, C_3]$ with

$$\begin{aligned}
C_2 = {} & 2x_1^2y_1'\zeta_1 - 2x_1^2y_2z_2 + 2x_2^2y_1'\zeta_1 - 2x_2^2y_1z_1 + 2y_1z_1x_1'^2 + 2y_2z_2x_1'^2 + 2x_1y_1x_1'y_1' - x_1^2\zeta_1^2 + x_1^2z_2^2 - y_1^2\zeta_1^2 \\
& + x_2^2y_1^2 + y_1^2z_2^2 - x_2^2\zeta_1^2 + x_2^2z_1^2 - y_2^2x_1'^2 - y_2^2\zeta_1^2 + x_1^2y_2^2 + y_2^2z_1^2 - 2x_1y_1y_1'\zeta_1 - 2x_1x_2y_1y_2 + 2x_1y_1y_2z_2 \\
& + 2x_2y_2x_1'y_1' - 2x_1y_1x_1'\zeta_1 + 2x_1x_2y_1z_2 - 2x_2y_2y_1'\zeta_1 - 2x_2y_2x_1'\zeta_1 + 2x_1x_2y_2z_1 + 2x_2y_1y_2z_1 - 2x_1z_1x_1'y_1' \\
& - 2x_2z_2x_1'y_1' - 2y_1z_1x_1'y_1' - 2y_2z_2x_1'y_1' + 2x_1z_1x_1'\zeta_1 + 2x_2z_2x_1'\zeta_1 - 2y_1z_1x_1'\zeta_1 - 2y_2z_2x_1'\zeta_1 - 2x_1z_1y_1'\zeta_1 \\
& - 2x_1x_2z_1z_2 + 2x_1y_2z_1z_2 - 2x_2z_2y_1'\zeta_1 + 2x_2y_1z_1z_2 + 2y_1z_1y_1'\zeta_1 + 2y_2z_2y_1'\zeta_1 - 2y_1y_2z_1z_2 + 2x_1y_1\zeta_1^2 \\
& - 2x_1y_1z_2^2 - 2x_2y_1^2z_2 + 2y_1^2x_1'\zeta_1 + 2x_2y_2\zeta_1^2 - 2x_2y_2z_1^2 - 2x_1y_2^2z_1 + 2y_2^2x_1'\zeta_1 + 2z_1^2x_1'y_1' + 2z_2^2x_1'y_1' \\
& + 2x_1z_1y_1'^2 + 2x_2z_2y_1'^2 - y_1^2x_1'^2 - z_1^2x_1'^2 - z_2^2x_1'^2 - x_1^2y_1'^2 - z_1^2y_1'^2 - x_2^2y_1'^2 - z_2^2y_1'^2, \\
C_3 = {} & x_1^2 - x_1y_1 + x_2^2 - x_2y_2 - x_1'^2 + x_1'y_1' - x_2'^2 + x_2'y_2' + x_1'\zeta_1 + x_2'\zeta_2 - x_1z_1 - x_2z_2 - y_1'\zeta_1 - y_2'\zeta_2 + y_1z_1 + y_2z_2.
\end{aligned}$$

The initials of $C_2$ and $C_3$ are

$$I_2 = (x_2 - y_2)^2 + (x_1 - y_1)^2,$$
$$I_3 = x_2' - y_2',$$

respectively. According to Ritt-Wu's characteristic set method [11, 20], we have

$$\mathrm{Zero}(\mathbb{P}) = \mathrm{Zero}(\mathbb{C}/I_2I_3) \cup \mathrm{Zero}(\mathbb{P} \cup \{I_2\}) \cup \mathrm{Zero}(\mathbb{P} \cup \{I_3\}),$$

where $\mathrm{Zero}(\mathbb{C}/I)$ denotes the set of all common zeros of $\mathbb{C}$ for which $I \neq 0$. If $I_2 = 0$, then $x_1 = y_1, x_2 = y_2$ and thus $x_1' = y_1', x_2' = y_2'$ (as $P_1 = 0$). In this case, $P_2 = P_3$ and the existence of $\zeta_1$ and $\zeta_2$ is obvious. Therefore, $\mathrm{Zero}(\mathbb{P} \cup \{I_2\})$ does not have to be further considered.

Computing a characteristic set of $\mathbb{P} \cup \{I_3\}$ yields $\mathbb{C}' = [C_1', I_3, C_3', C_4']$, where

$$\begin{aligned}
C_1' = {} & x_1^2 - 2x_1y_1 + y_1^2 + x_2^2 - 2x_2y_2 + y_2^2 - x_1'^2 + 2x_1'y_1' - y_1'^2, \\
C_3' = {} & -y_1'\zeta_1 + y_1z_1 + y_2z_2 - x_1'^2 + x_1'\zeta_1 + x_1^2 - x_1z_1 + x_2^2 - x_2z_2 - x_1y_1 - x_2y_2 + x_1'y_1', \\
C_4' = {} & -2x_1^2y_2z_2 + 2x_1y_1x_2'^2 - 2x_2^2y_1z_1 + 2x_2y_2x_2'^2 - x_1^2x_2'^2 - x_2^2x_2'^2 + x_1^2z_2^2 + x_2^2y_1^2 + y_1^2z_2^2 + x_2^2z_1^2 + x_1^2y_2^2 + y_2^2z_1^2 \\
& - 2x_1x_2y_1y_2 + 2x_1y_1y_2z_2 + 2x_1x_2y_1z_2 + 2x_1x_2y_2z_1 + 2x_2y_1y_2z_1 - 2x_1x_2z_1z_2 + 2x_1y_2z_1z_2 + 2x_2y_1z_1z_2 \\
& - 2y_1y_2z_1z_2 - 2x_1y_1z_2^2 - 2x_2y_1^2z_2 - 2x_2y_2z_1^2 - 2x_1y_2^2z_1 - y_1^2x_2'^2 - y_2^2x_2'^2 + 2x_1^2x_2'\zeta_2 + 2x_1y_1\zeta_2^2 - x_1^2\zeta_2^2 \\
& - y_1^2\zeta_2^2 - x_2^2\zeta_2^2 - 4x_1y_1x_2'\zeta_2 + 2y_1^2x_2'\zeta_2 + 2x_2^2x_2'\zeta_2 + 2x_2y_2\zeta_2^2 + 2y_2^2x_2'\zeta_2 - 4x_2y_2x_2'\zeta_2 - y_2^2\zeta_2^2.
\end{aligned}$$

The initials of $C_3'$ and $C_4'$ are $I_3' = x_1' - y_1'$ and $I_4' = I_2$, respectively. Now we have

$$\mathrm{Zero}(\mathbb{P} \cup \{I_3\}) = \mathrm{Zero}(\mathbb{C}'/I_2I_3') \cup \mathrm{Zero}(\mathbb{P} \cup \{I_2, I_3\}) \cup \mathrm{Zero}(\mathbb{P} \cup \{I_3, I_3'\}).$$

Since $I_3 = I_3' = 0$ implies that $x_1 = y_1$ and $x_2 = y_2$, both Zero($\mathbb{P} \cup \{I_2, I_3\}$) and Zero($\mathbb{P} \cup \{I_3, I_3'\}$) do not have to be further considered as explained above.

Thus, the problem is reduced to determining (i) whether for any $x_1, x_2, y_1, y_2, z_1, z_2, x_1', x_2', y_1', y_2'$ satisfying $P_1 = 0, I_2 \neq 0, I_3 \neq 0$ there exist $\zeta_1, \zeta_2 \in \boldsymbol{R}$ such that $C_2 = 0$ and $C_3 = 0$, and (ii) whether for any $x_1, x_2, y_1, y_2, z_1, z_2, x_1', x_2', y_1', y_2'$ satisfying $C_1' = 0, I_3 = 0, I_2 \neq 0, I_3' \neq 0$ there exist $\zeta_1, \zeta_2 \in \boldsymbol{R}$ such that $C_3' = 0$ and $C_4' = 0$.

For (i), we found that $C_2$ can be factorized over the extension field $\boldsymbol{Q}(x_1, x_2, y_1, y_2, z_1, z_2, x_1', x_2', y_1', y_2')$ defined by the minimal polynomial $P_1$ as

$$C_2 = (D_2 + D_1)(D_2 - D_1)/I_2,$$

where

$$\begin{aligned} D_1 = &- x_1 z_1 y_1' - x_2 z_2 y_1' - y_2 z_2 x_1' + x_2^2 y_1' - x_2 y_2 x_1' - x_2 y_2 y_1' + y_2^2 x_1' + x_1^2 y_1' - y_1 z_1 x_1' + x_2 z_2 x_1' + y_1 z_1 y_1' \\ &+ y_2 z_2 y_1' - x_2^2 \zeta_1 - y_2^2 \zeta_1 - x_1^2 \zeta_1 - y_1^2 \zeta_1 + 2 x_1 y_1 \zeta_1 + 2 x_2 y_2 \zeta_1 - x_1 y_1 x_1' - x_1 y_1 y_1' + x_1 z_1 x_1' + y_1^2 x_1', \\ D_2 = &- x_2 z_1 y_2' + y_2 z_1 y_2' + x_1 z_2 y_2' - y_1 z_2 y_2' + x_2 y_1 y_2' - x_1 y_2 y_2' + x_1 y_2 x_2' - x_1 z_2 x_2' + y_1 z_2 x_2' + x_2 z_1 x_2' \\ &- y_2 z_1 x_2' - x_2 y_1 x_2'. \end{aligned}$$

With Maple V.2 on a Sun SPARC 2 station, the factorization costs cfactor 14.33 CPU seconds and zfactor 11.11 CPU seconds. The Maple function factor returns "object too large" after 781.06 CPU seconds. The two factors of $C_2$ are linear in $\zeta_1$, while $C_3$ is linear in $\zeta_2$. Hence, the existence of $\zeta_1$ and $\zeta_2$ is guaranteed.

For (ii), $C_4'$ can be factorized over the extension field $\boldsymbol{Q}(x_1, x_2, y_1, y_2, z_1, z_2, x_1', x_2', y_1')$ defined by the minimal polynomial $C_1'$ as

$$C_4' = (D_4 + D_3)(D_4 - D_3)/I_2,$$

where

$$\begin{aligned} D_3 = &- x_2^2 \zeta_2 + 2 x_1 y_1 \zeta_2 - y_2^2 \zeta_2 - x_1^2 \zeta_2 + 2 x_2 y_2 \zeta_2 - y_1^2 \zeta_2 + x_1^2 x_2' - 2 x_1 y_1 x_2' + x_2^2 x_2' - 2 x_2 y_2 x_2' + y_2^2 x_2' + y_1^2 x_2', \\ D_4 = &\, x_1 z_2 x_1' - x_1 y_2 x_1' - y_1 z_2 x_1' - x_2 z_1 x_1' + y_2 z_1 x_1' + x_2 y_1 x_1' + x_2 z_1 y_1' - y_2 z_1 y_1' - x_1 z_2 y_1' + y_1 z_2 y_1' - x_2 y_1 y_1' \\ &+ x_1 y_2 y_1'. \end{aligned}$$

This factorization costs cfactor 8.73 seconds, zfactor 7.9 seconds and factor 147.81 seconds (CPU time in Maple V.2 on the same Sun SPARC 2 station). Now, the two factors of $C_4'$ are linear in $\zeta_2$, while $C_3'$ is linear in $\zeta_1$. Therefore, in this case the existence of $\zeta_1$ and $\zeta_2$ is also guaranteed. This completes our solution to the problem.

**Acknowledgments**. This work was supported by AFCRST under PRA M94-1 and a project of LIAMA.

## References

[1] Abbott, J. A.: On the factorization of polynomials over algebraic fields. Ph.D thesis. School of Math. Sci., Univ. of Bath, England (1989).

[2] Buchberger, B.: Gröbner bases: An algorithmic method in polynomial ideal theory. In: Multidimensional Systems Theory (N. K. Bose, ed.), D. Reidel Publ. Co., Dordrecht Boston (1985) 184–232.

[3] Chou, S.-C., Gao, X.-S.: Ritt-Wu's decomposition algorithm and geometry theorem proving. In: Proc. CADE-10, LNCS **449** (1990) 207–220.

[4] Conti, P., Traverso, C.: A case of automatic theorem proving in Euclidean geometry: The Maclane $8_3$ theorem. In: Proc. AAECC-11, LNCS **948** (1995) 183–193.

[5] Gao, X.-S.: On the theory of resolvents and its applications. MM Res. Preprints **6** (1991) 79–93.

[6] Hu, S., Wang, D.: Fast factorization of polynomials over rational number field or its extension fields. Kexue Tongbao **31** (1986) 150–156.

[7] Landau, S.: Factoring polynomials over algebraic number fields. SIAM J. Comput. **14** (1985) 184–195.

[8] Lenstra, A. K.: Lattices and factorization of polynomials over algebraic number fields. In: Proc. EUROCAM '82, Marseille (1982) 32–39.

[9] Lenstra, A. K.: Factoring multivariate polynomials over algebraic number fields. SIAM J. Comput. **16** (1987) 591–598.

[10] Pfalzgraf, J.: A category of geometric spaces: Some computational aspects. Ann. Math. Artif. Intell. **13** (1995) 173–194.

[11] Ritt, J. F.: Differential algebra. Amer. Math. Soc., New York (1950).

[12] Sturm, T., Weispfenning, V.: Computational geometry problems in REDLOG. In: Automated Deduction in Geometry (D. Wang, ed.), LNAI **1360** (1998) 58–86.

[13] Trager, B. M.: Algebraic factoring and rational function integration. In: Proc. ACM SYMSAC '76, Yorktown Heights (1976) 219–226.

[14] Wang, D.: Irreducible decomposition of algebraic varieties via characteristic sets and Gröbner bases. Comput. Aided Geom. Design **9** (1992) 471–484.

[15] Wang, D.: A method for factorizing multivariate polynomials over successive algebraic extension fields. Preprint. RISC-Linz, Johannes Kepler Univ., Austria (1992).

[16] Wang, D.: Algebraic factoring and geometry theorem proving. In: Proc. CADE-12, LNAI **814** (1994) 386–400.

[17] Wang, D.: An implementation of the characteristic set method in Maple. In: Automated Practical Reasoning: Algebraic Approaches (J. Pfalzgraf and D. Wang, eds.), Springer-Verlag, Wien New York (1995) 187–201.

[18] Wang, P. S.: Factoring multivariate polynomials over algebraic number fields. Math. Comput. **30** (1976) 324–336.

[19] Weinberger, P. J., Rothschild, L. P.: Factoring polynomials over algebraic number fields. ACM Trans. Math. Softw. **2** (1976) 335–350.

[20] Wu, W.-t.: Basic principles of mechanical theorem proving in elementary geometries. J. Syst. Sci. Math. Sci. **4** (1984) 207–235.

[21] Wu, W.-t.: On reducibility problem in mechanical theorem proving of elementary geometries. Chin. Quart. J. Math. **2** (1987) 1–20.

[22] Zassenhaus, H.: On Hensel factorization I. J. Number Theory **1** (1969) 291–311.

[23] Zhi, L.: Polynomial factorization over algebraic fields and its applications. Ph.D thesis, Academia Sinica, China (1996).