Chapter 1

Algebraic Factorization and GCD Computation

Lihong Zhi

This chapter describes several algorithms for factorization and GCD computation of polynomials over algebraic extension fields. These algorithms are common in using the characteristic set method introduced in the previous chapters. Some performance comparisons between these algorithms are reported. Applications include geometry theorem proving, irreducible decomposition of algebraic variaities, implicitization of parametric equations and verification of geometric conditions.

1.1 Introduction

Factoring polynomials over algebraic extension fields can be traced back to Kronecker (1882). A similar algorithm can also be found in van der Waerden (1953), which was adopted and improved by Trager (1976). Further improvements are given by Encarnación (1997) and Noro and Yokoyama (1997). By using the Chinese remainder theorem, Hensel lemma and lattice techniques, several different approaches were given in Wang (1976), Weinberger and Rothschild (1976), Lenstra (1982, 1987), Landau (1985) and Abbott (1989).

The study of algebraic factorization in Wu's research group started in 1984, motivated by the need for it in the method of Wu (1984, 1987) for geometry theorem proving (GTP). Two different methods were proposed in

Hu and Wang (1986), Wang (1992a) and Wu (1994), and applied to GTP and irreducible decomposition of algebraic varieties (see Wang 1992b, 1994). Investigations along this line have been furthered by Zhi (1996) who has been trying to work out an optimized algorithm by incorporating and improving different techniques.

Let $\boldsymbol{Z}$ denote the integers, $\boldsymbol{Q}$ be the field of rational numbers, $u_1, u_2, \ldots, u_d$, be a set of transcendental elements, abbreviated as $\boldsymbol{u}$. The transcendental extension field obtained from $\boldsymbol{Q}$ by adjoining $\boldsymbol{u}$ is denoted by $\boldsymbol{K}_0$, i.e., $\boldsymbol{K}_0 = \boldsymbol{Q}(\boldsymbol{u})$. The algebraic elements $\eta_1, \eta_2, \ldots, \eta_r$, abbreviated as $\boldsymbol{\eta}$, are defined by an *irreducible ascending set AS*

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

with $A_i \in \boldsymbol{Q}[\boldsymbol{u}, y_1, \ldots, y_i]$, $\deg(A_i, y_i) = m_i > 0$ 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. 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} the minimal polynomial of η_{i-1} for each $i \geq 2$. The field $\boldsymbol{K}_r$ is called an *algebraic extension field* of $\boldsymbol{K}_0$ defined by *AS* (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 *AS* is specified as above, we simply write $\boldsymbol{K}_{i-1}(y_i)$ for $\boldsymbol{K}_i$ without explicitly introducing the algebraic element η_i.

The problem amounts to factorizing a polynomial

$$F(\boldsymbol{u}, \boldsymbol{\eta}, x_1, \ldots, x_t) \in \boldsymbol{K}_r[x_1, \ldots, x_t]$$

over $\boldsymbol{K}_r$.

By choosing a main variable x, suppose x_1 without loss of generality, one can write F in the form

$$F = f_0 x^n + f_1 x^{n-1} + \cdots + f_n$$

with $f_i \in \boldsymbol{K}_r[x_2, \ldots, x_t]$, for $i = 0, 1, \ldots, n$. $f_0 = \mathrm{lc}(F, x)$ is the leading coefficient of F in x. The *content* of F with respect to x is the greatest common divisor of $f_0, \ldots, f_n$; F is *primitive* if its content is 1. F is said to be *squarefree* if it has no repeated factors. In what follows, F is assumed to be squarefree and primitive with respect to its main variable. In the first two methods to be presented, $x_2, x_3, \ldots, x_t$ are treated as transcendental elements and are absorbed in $\boldsymbol{K}_r$, while in the third method, we distinguish the x's from the u's. For nonzero polynomials A, B over $\boldsymbol{K}_r$ with $\deg(A, x) = m \geq \deg(B, x) = n \geq 0$, one defines the pseudo-division by the formula:

$$\mathrm{lc}(B, x)^{[m-n+1]} A = QB + R, \quad \text{and} \quad \deg(R, x) < n,$$

where Q, R are polynomials over $\boldsymbol{K}_r$. We call Q and R the pseudo-quotient and pseudo-remainder of A and B, denoted by $\mathrm{pquo}(A, B, x)$ and $\mathrm{prem}(A, B, x)$, respectively. Similarly, one can defines the pseudo-remainer of A with respect to the ascending set AS as:

$$\mathrm{prem}(A, AS) = \mathrm{prem}(\cdots(\mathrm{prem}(A, A_r, y_r), \cdots), A_1, y_1).$$

1.2 Method of Undetermined Coefficients

Suppose that $F(x)$ can be factorized over $\boldsymbol{K}_r$ as

$$F(x) \equiv f_0 \cdot G(x) \cdot H(x) \mod AS,$$

where

$$\begin{array}{rcl} G(x) & = & x^s + g_1 x^{s-1} + \cdots + g_s, \\ H(x) & = & x^t + h_1 x^{t-1} + \cdots + h_t \end{array} \quad s + t = n, 1 \leq s, t \leq n - 1,$$

and $\equiv$ means that $\mathrm{prem}(F - f_0 GH, AS) = 0$. The above g_i and h_j can be written as

$$\begin{array}{ll} g_i = \sum_{\substack{0 \leq k_l \leq m_l - 1 \\ 1 \leq l \leq r}} g_{ik_1 \cdots k_r} {y_1}^{k_1} \cdots {y_r}^{k_r}, & g_{ik_1 \cdots k_r}, h_{jk_1 \cdots k_r} \in \boldsymbol{K}_0, \\ h_j = \sum_{\substack{0 \leq k_l \leq m_l - 1 \\ 1 \leq l \leq r}} h_{jk_1 \cdots k_r} {y_1}^{k_1} \cdots {y_r}^{k_r}, & i = 1, \ldots, s, j = 1, \ldots, t. \end{array} \tag{1.1}$$

Here, the number of $g_{ik_1 \cdots k_r}$ and $h_{jk_1 \cdots k_r}$ is $(s+t) m_1 \cdots m_r = M$. We rename these indeterminate coefficients with a fixed order as $z_1 \prec z_2 \prec \cdots \prec z_M$. Now expand $F - f_0 GH$, compute its pseudo-remainder R with respect to AS, and equate the coefficients of all the power products of R in $y_1, \ldots, y_r, x$ to 0, we shall obtain a system of M polynomial equations

$$\begin{array}{c} V_1(\boldsymbol{u}, z_1, \ldots, z_M) = 0 \\ V_2(\boldsymbol{u}, z_1, \ldots, z_M) = 0 \\ \cdots\cdots \\ V_M(\boldsymbol{u}, z_1, \ldots, z_M) = 0 \end{array} \tag{1.2}$$

with coefficients in $\boldsymbol{K}_0$. Thus, whether the polynomial F can be factorized over $\boldsymbol{K}_r$ is equivalent to whether the above system of polynomial equations has a solution for $z_1, \ldots, z_M$ in the field $\boldsymbol{K}_0$, which can be determined by using the characteristic set method.

Algorithm FactorA. Given an irreducible ascending set $\mathit{AS} = [A_1, \ldots, A_r]$ that defines the field $\boldsymbol{K}_r$ and a polynomial $F \in \boldsymbol{K}_r[x]$ of degree $m > 1$ which is irreducible over $\boldsymbol{K}_0$ and reduced with respect to AS. This algorithm calculates the irreducible factorization of F over $\boldsymbol{K}_r$.

S1. If m is even then set $\overline{m} \leftarrow m/2$, else set $\overline{m} \leftarrow (m-1)/2$.

S2. For $s = 1, \cdots, \overline{m}$ do:

S2.1. Set $t \leftarrow m - s$, and

$$G \leftarrow x^s + g_1 x^{s-1} + \cdots + g_s, \quad H \leftarrow x^t + h_1 x^{t-1} + \cdots + h_t,$$

where g_i, h_j are defined by (1.1).

S2.2. Expand $R \leftarrow \mathrm{prem}(F - f_0 GH, \mathit{AS})$, equate the coefficients of R of all power products in $y_1, \ldots, y_r, x$ to 0 and obtain a system (1.2) of polynomial equations.

S2.3. Solve (1.2) for $x_1, \cdots, x_M$ in $\boldsymbol{Q}(\boldsymbol{u})$ by the characteristic set method. If there is no solution then go back to **S2** for the next s. Otherwise, let $x_1 = \overline{x}_1, \ldots, x_M = \overline{x}_M$ be any solution of (1.2), set

$$G \leftarrow G|_{x_1=\overline{x}_1,\ldots,x_M=\overline{x}_M}, \quad H \leftarrow H|_{x_1=\overline{x}_1,\ldots,x_M=\overline{x}_M},$$

and go to **S4**.

S3. Return "F is irreducible over $\boldsymbol{K}_r$".

S4. Factorize G and H in $\boldsymbol{K}_r[x]$ and return

$$F \leftarrow f_0 \cdot \mathsf{FactorA}(G, \mathit{AS}) \cdot \mathsf{FactorA}(H, \mathit{AS}).$$

Example 1 *Factorize the polynomial* $F = x^3 + 3yx^2 - x + 6y$ *over* $\boldsymbol{K}$*, where* $\boldsymbol{K} = \boldsymbol{Q}(y)$ *is the algebraic extension field defined by* $A = y^2 + 2$.

Suppose that F has a factorization of the form

$$F = [x + (x_1 y + x_2)][x^2 + (x_3 y + x_4)x + (x_5 y + x_6)], i = 1, \ldots, 6, \quad (1.3)$$

where the x_i are unknowns to be determined in $\boldsymbol{Q}$. Comparing the coefficients of x on the two sides of (1.3), we obtain

$$\begin{aligned} x_1y + x_2 + x_3y + x_4 &= 3y, \\ (x_1y + x_2)(x_3y + x_4) + x_5y + x_6 &= -1, \\ (x_1y + x_2)(x_5y + x_6) &= 6y. \end{aligned}$$

Expanding the above equalities, reducing them by A and then comparing the coefficients of y on the two sides of the obtained equalities, we get a set of polynomial equations

$$\begin{aligned} x_1 + x_3 &= 3, \\ x_2 + x_4 &= 0, \\ x_2x_3 + x_1x_4 + x_5 &= 0, \\ x_2x_4 - 2x_1x_3 + x_6 &= -1, \\ x_2x_5 + x_1x_6 &= 6, \\ x_2x_6 - 2x_1x_5 &= 0. \end{aligned} \tag{1.4}$$

By the characteristic set method, we find a rational solution:

$$(x_1, x_2, x_3, x_4, x_5, x_6) = (2, 0, 1, 0, 0, 3).$$

Therefore, F can be factorized as

$$F = (x + 2y)(x^2 + xy + 3)$$

over $\boldsymbol{Q}$. Factorizing $x^2 + xy + 3$ by using the same method, we shall find that it is irreducible.

The above method was proposed by Hu and Wang (1986). It has been improved in Wu (1994) by introducing only one polynomial H and performing $R = \mathrm{prem}(\mathrm{prem}(F, H, x), \mathit{AS})$. For H to be a factor of F it is necessary and sufficient that $R = 0$.

Algorithm FactorA*. Given an irreducible ascending set $\mathit{AS} = [A_1, \ldots, A_r]$ that defines the field $\boldsymbol{K}_r$ and a polynomial $F \in \boldsymbol{K}_r[x]$ of degree $m > 1$, irreducible over $\boldsymbol{K}_0$ and reduced with respect to AS. This algorithm calculates the irreducible factorization of F over $\boldsymbol{K}_r$.

S1. If m is even then set $\overline{m} \leftarrow m/2$, else set $\overline{m} \leftarrow (m-1)/2$.

S2. For $t = 1, \cdots, \overline{m}$ do:

S2.1. Set $H \leftarrow x^t + h_1x^{t-1} + \cdots + h_t$, where h_j defined by (1.1).

S2.2. Expand $R \leftarrow \text{prem}(\text{prem}(F, H, x), AS)$, equate the coefficients of R of all the power products in $y_1, \ldots, y_r, x$ to 0, and obtain a system of polynomial equations as in (1.2) with $M = tm_1 \cdots m_r$.

S2.3. Solve the system for $x_1, \cdots, x_M$ in $\boldsymbol{Q}(\boldsymbol{u})$ by the characteristic set method. If there is no solution then go back to **S2** for the next t. Otherwise, let $x_1 = \overline{x}_1, \ldots, x_M = \overline{x}_M$ be any solution, set

$$H \leftarrow H|_{x_1=\overline{x}_1,\ldots,x_M=\overline{x}_M}, \quad G \leftarrow \text{pquo}(F, H, x),$$

and go to **S4**.

S3. Return "F is irreducible over $\boldsymbol{K}_r$".

S4. Factorize G and H in $\boldsymbol{K}_r[x]$ and return

$$F \leftarrow f_0 \cdot \mathsf{FactorA}^*(G, AS) \cdot \mathsf{FactorA}^*(H, AS).$$

Now we apply this improved method to Example 1 again. Suppose that F has a factor $H = x + (x_1 y + x_2)$ of degree 1; then

$$\begin{aligned} R &= \text{prem}(\text{prem}(F, H, x), A, y) \\ &= 6y + x_1 y - 3x_1 x_2^2 y + x_2 + 3x_2^2 y - x_2^3 - 6yx_1^2 + 2yx_1^3 + 6x_1^2 x_2 - 12x_1 x_2. \end{aligned}$$

Let $R = 0$, i.e., let the coefficients of y in R be all zero; we obtain

$$\begin{aligned} 6x_1^2 x_2 - x_2^3 + x_2 - 12x_1 x_2 = 0, \\ -3x_1 x_2^2 + 6 - 6x_1^2 + 2x_1^3 + 3x_2^2 + x_1 = 0. \end{aligned} \tag{1.5}$$

Solving this system of equations by the characteristic set method, we find a unique rational solution $(x_1, x_2) = (2, 0)$. Therefore, F can be factorized as

$$F = (x + 2y)(x^2 + xy + 3).$$

From this example one can see that the number of equations in (1.4) is 6 and in (1.5) is 2 but the equations in (1.4) are all simpler than those in (1.5).

1.3 Method via Transformation and Triangularization

This method was discovered by Wang (1992a,1995) during his implementation of the CharSets package. The basic idea underlying the method is the reduction of polynomial factorization over algebraic extension fields to that over the rational number field via linear transformation and the computation of characteristic sets with respect to a proper variable ordering. The factors over the algebraic extension fields are finally determined via algebraic GCD computation. The following lemma (see Wang 1999) guarantees the correctness of the factoring algorithm described below.

Lemma 1 *Let AS and F be as in the preceding section, $c_1, \ldots, c_r$ be r integers,*

$$\overline{F} \leftarrow F|_{x=x-c_1y_1-\cdots-c_ry_r},$$

and $\overline{CS}$ be an characteristic set of $\overline{AS} = AS \cup \{\overline{F}\}$ over $\boldsymbol{K}_0$ with respect to $x \prec y_1 \prec y_2 \cdots \prec y_r$. Let $\overline{C}$ be the first polynomial in $\overline{CS}$ and

$$C \leftarrow \overline{C}|_{x=x+c_1y_1+\cdots+c_ry_r}.$$

If $\overline{CS}$ is irreducible and contains exactly $r+1$ polynomials, then the GCD of F and C is irreducible over $\boldsymbol{K}_r$.

We continue using the above notations and let $\overline{CS} = [\overline{C}_0, \overline{C}_1, \ldots, \overline{C}_r]$ be a characteristic set of $\overline{AS}$. It happens in general that all the polynomials other than $\overline{C}_0$ in $\overline{CS}$ are linear in their leading variables, while $\overline{C}_0$ involves the variables $\boldsymbol{u}$ and x only. If this is the case, $\overline{CS}$ is said to be *quasilinear*. If $\overline{CS}$ is not quasilinear, we make a linear transformation by substituting $x - c_1y_1 - \cdots - c_ry_r$ for x, where $c_1, \ldots, c_r$ are randomly chosen integers. The probability of obtaining a quasilinear characteristic set with such a linear transformation is one (see Wang 1992).

If $\overline{CS}$ is quasilinear and $\overline{C}_0$ is irreducible over $\boldsymbol{K}_0$, then the GCD of F and $C_0 = \overline{C}_0|_{x=x+c_1y_1+\cdots+c_ry_r}$ over $\boldsymbol{K}_r$ must be a true irreducible factor of F over $\boldsymbol{K}_r$ according to Lemma 1. If $\overline{C}_0$ is reducible over $\boldsymbol{K}_0$, we try to determine possible factors of F over $\boldsymbol{K}_r$ by computing the GCD of F with each $\boldsymbol{K}_0$-factor of C_0 over the algebraic extension field $\boldsymbol{K}_r$. Practically, we can start this determination as soon as $\overline{CS}$ is triangularized, without need to arrive at an exact characteristic set. Note that during the computation one should try to remove some factors (over $\boldsymbol{K}_0$) if possible. Some factors of F over $\boldsymbol{K}_r$ may also be determined from those $\boldsymbol{K}_0$-factors and the initials of the polynomials in $CS = \overline{CS}|_{x=x+c_1y_1+\cdots+c_ry_r}$.

Algorithm FactorB. Given an irreducible ascending set $AS = [A_1, \ldots, A_r]$ that defines the field $\boldsymbol{K}_r$ and a polynomial $F \in \boldsymbol{K}_r[x]$ that is reduced with respect to AS and irreducible over $\boldsymbol{Q}$, this algorithm gives the irreducible factorization of F over $\boldsymbol{K}_r$.

S1. Set $AS^* \leftarrow [A_i : \deg(A_i, y_i) > 1, A_i \in AS]$. If AS^* is empty, then the procedure terminates and return F. Otherwise, let $y_{p_1} \prec y_{p_2} \cdots \prec y_{p_s}$ be the leading variables of the polynomials in AS^*. Choose a set of integers $[c_1, \ldots, c_s]$.

S2. Set $\overline{F} \leftarrow F|_{x=x-c_1y_1-\cdots-c_sy_s}$. Compute a characteristic set $\overline{CS}$ of $AS^* \cup \overline{F}$ with respect to the variable ordering $x \prec y_{p_1} \cdots \prec y_{p_s}$. Let Δ be the set of the irreducible factors (over $\boldsymbol{K}_0$) of the initials of the polynomials in $\overline{CS}$ and Ω the set of the irreducible factors (over $\boldsymbol{K}_0$) of the first polynomial in $\overline{CS}$ which is not included in Δ.

S3. If $\overline{CS}$ is quasilinear, then go to **S4**. If Ω is empty, then choose a new set of integers $c_1, \ldots, c_s$ and go to **S2**. Otherwise, set $\Delta \leftarrow \Delta \cup \Omega$, $\Omega \leftarrow \emptyset$.

S4. Set $G \leftarrow F, \Omega \leftarrow \Omega|_{x=x+c_1y_1+\cdots+c_sy_s}$ and $\Delta \leftarrow \Delta|_{x=x+c_1y_1+\cdots+c_sy_s}$. For each $P \in \Omega \cup \Delta$, compute the GCD F_P of G and P over $\boldsymbol{K}_r$ with heuristic normalization, and set $G \leftarrow G/F_P$ over $\boldsymbol{K}_r$. If some true factors of F are found, then apply FactorB to F_P and obtain an irreducible factorization F_P^* for each $P \in \Delta \cup \{G\}$, then return

$$F^* = \prod_{P \in \Omega} F_P \prod_{P \in \Delta \cup \{G\}} F_P^*.$$

Otherwise, if $\overline{CS}$ is quasilinear, then return F; otherwise try new $c_1, \ldots, c_s$ and go to **S2**.

Normalizing a polynomial G by AS amounts to finding a polynomial G^* that differs from G only by a factor in $\boldsymbol{K}_r$, and $\mathrm{lc}(G^*, x) \in \boldsymbol{Q}[\boldsymbol{u}]$. In many cases, G^* is much simpler than G, but the opposite is also true in many other cases. Heuristic use of normalization may improve the efficiency of FactorB considerably (see Wang 1992a, 1999). An immediate variation of the above algorithm is to compute not only the characteristic set but also the characteristic series in **S2**. The irreducible factors of F are determined from those ascending sets in the series whose irreducibility can be easily verified.

Example 2 *Factorize the polynomial*

$$\begin{aligned} F &= 2x^3 - 2x^2y_2 + 2x^2y_1 + 4x^2y_1y_2 - 2xy_1y_2^2 + 2x^2y_2^2 + y_1x \\ &\quad -6y_1y_2 - xy_1y_2 - 4x^2 - 4xy_2 - 12 \end{aligned}$$

over $\boldsymbol{K}$, where $\boldsymbol{K} = \boldsymbol{Q}(y_1, y_2)$ is the algebraic extension field defined by the irreducible ascending set

$$AS = [y_1^2 + 2, 2y_2^3 - y_1y_2 - y_1].$$

We begin by choosing $c_1 = 0, c_2 = 0$; $\overline{F} = F$. A characteristic set of $\{\overline{F}\} \cup AS$ with respect to the ordering $x \prec y_1 \prec y_2$ is quasilinear and the first polynomial can be factorized over $\boldsymbol{Q}$ into $2G_1G_2$:

$$\begin{aligned} G_1 &= 2x^6 + 12x^4 - 8x^3 + 13x^2 - 14x + 27, \\ G_2 &= 4x^12 - 48x^11 + 292x^10 - 820x^9 + 1561x^8 - 3490x^7 + 7657x^6 \\ &\quad -14400x^5 + 23778x^4 - 28080x^3 + 3888x^2 + 15552x + 23328 \end{aligned}$$

One may find that the GCD of F and G_1 over $\boldsymbol{K}$ is

$$F_1 = x + y_1 - y_2,$$

and the GCD of F and G_2 over $\boldsymbol{K}$ is

$$F_2 = x^2 - 2x + xy_2^2 + 2xy_1y_2 + 3y_1.$$

Therefore, F is factorized into $2F_1F_2$ over $\boldsymbol{K}$.

1.4 Hybrid Method with Modular Techniques

The methods described previously are both of sufficient generality. But in the presence of having trancendentals, the algorithms are quite slow. This is mainly because the complexity of computation in $\boldsymbol{Q}(\boldsymbol{u})$ is high. It turns out that in this case the modular techniques of using integer substitution and Hensel lifting can be adapted to improve the methods.

Following standard modular approach to the factorization of a multivariate polynomial over an algebraic function field, we have the following steps:

- Ensure that the polynomial is squarefree.
- Find "lucky" integer substitutions to reduce the multivariate polynomial to a univariate polynomial, and the algebraic function field to an algebraic number field.
- Factorize the univariate polynomial over the algebraic number field.
- Lift the univariate factors as well as the ascending set.
- Check the true factors.

We assumed that x_1 is the main variable and the polynomial F is squarefree and primitive with respect to x_1 in the algebraic extension field $\boldsymbol{Q}(\boldsymbol{u}, \boldsymbol{\eta})$. The set of integers $\boldsymbol{b}, \boldsymbol{a}$, with $\boldsymbol{b} = (b_1, \ldots, b_d)$ and $\boldsymbol{a} = (a_2, \ldots, a_t)$, is said to be *lucky* if it satisfies 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. $AS^{(0)} = [A_1(\boldsymbol{b}, y_1), \ldots, A_r(\boldsymbol{b}, y_1, \ldots, y_r)]$ is still an irreducible ascending set.

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

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

Here, and later on, $\operatorname{res}(F, G, x)$ denotes the resultant of the polynomials F, G with respect to the variable x; F' is the partial differential of F with respect to x_1. 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 (see Abbott 1989) and the primitive element theory.

Proposition 1 *(Hilbert Irreducibility Theorem) Let P be irreducible in $\boldsymbol{Z}$ 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 $1 \leq i \leq s$. Let $\overline{P} = P(b_1, \ldots, b_s, x_1, \ldots, x_t)$ be 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 $0 < a < 1$.*

For the Hensel lemma, we refer to Zassenhaus (1969) for details. Now the most important thing is to determine when to stop the lifting and check the true factors. Let us look at two examples.

Example 3 *Factorize $F = ux^2 - 2yx - u + 1 \in \boldsymbol{Q}[u, y, x]$ with y defined by the polynomial $A = y^2 - u$.*

The solution is given by

$$F \equiv u\left(x + \frac{u-y}{u}\right)\left(x - \frac{u+y}{u}\right) \mod A.$$

The factors have u appearing in the denominators.

Example 4 *Factorize $F = x^2 - u \in \boldsymbol{Q}[u, y, x]$ with y defined by $A = u^3y^2 - 1$.*

The solution is given by

$$F = (x + u^2 y)(x - u^2 y) \mod A.$$

The factors have powers of u higher than that in the original F.

The above two simple examples show that it is necessary to distinguish the transcendental elements $\boldsymbol{u}$ from the variables $x_1, \ldots, x_t$ because the total degree in $x_1, \ldots, x_t$ is bounded by that of the original F, but this is not true for the total degree in $\boldsymbol{u}$ and much worse, $\boldsymbol{u}$ can appear in the denominators of the factors. In Abbott (1989) a possible upper bound for the total degree in $\boldsymbol{u}$ was given, but unfortunately the bound is often too large and his proof, based on Trager (1976), is not complete. We adopt an optimal bound; after arriving at that bound, we multiply every factor by a common polynomial and check whether it is a true factor of F over the field $\boldsymbol{K}_r$. This common polynomial can be obtained according to the following discussion taken from Abbott (1989).

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

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

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 $\mathrm{dis}(A_i) = \mathrm{res}(A_i, {A_i}', y_i)$.

Proposition 2 *The square of the defect of the basis for $\boldsymbol{K}_r$ divides its discriminant.*

The following algorithms can be considered as variants of the method of P. S. Wang (1976); the algorithm SFactorC improves the method of Trager (1976) by using non-squarefree norms of polynomials.

Algorithm FactorC. Given an irreducible ascending set $AS = [A_1, \ldots, A_r]$ that defines the algebraic function field $\boldsymbol{K}_r$ and a squarefree polynomial $F \in \boldsymbol{K}_r[x_1, \ldots, x_t]$, the algorithm determines the irreducible factorization of F over $\boldsymbol{K}_r$.

S1. Choose lucky integers $\boldsymbol{b} \leftarrow (b_1, \ldots, b_d)$ and $\boldsymbol{a} \leftarrow (a_2, \ldots, a_t)$. Set

$$\begin{aligned} F^{(0)} &\leftarrow F(\boldsymbol{b}, \boldsymbol{\eta}, x_1, \boldsymbol{a}), \\ AS^{(0)} &\leftarrow [A_1(\boldsymbol{b}, y_1), \ldots, A_r(\boldsymbol{b}, y_1, \ldots, y_r)]. \end{aligned}$$

S2. Use $\mathsf{UFactorC}$ to factorize $F^{(0)}(\boldsymbol{\eta}, x_1)$ over $\boldsymbol{Q}(\boldsymbol{\eta})$ defined by $AS^{(0)}$:

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

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

S3. Apply Hensel lifting to the factors $G_i^{(0)}$ and $AS^{(0)}$ such that

$$\begin{aligned} &F \equiv G_1^{(\delta)}(\boldsymbol{u}, \boldsymbol{\eta}, x_1, \ldots, x_t) \cdots G_m^{(\delta)}(\boldsymbol{u}, \boldsymbol{\eta}, x_1, \ldots, x_t) \mod (U^{\delta+1}, AS^{(\delta)}), \\ &AS \equiv AS^{(\delta)} \mod (U^{\delta+1}). \end{aligned}$$

S4. When $\delta > \deg(F, \boldsymbol{u}) + \sum_{i=2}^{t} \deg(F, x_i) + \sum_{i=1}^{r} \deg(A_i, \boldsymbol{u})$ (the degree in $\boldsymbol{u}$ means the *total degree*), try the true factor test to obtain

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

Algorithm UFactorC. Given an irreducible ascending set $AS = [A_1, \ldots, A_r]$ that defines $\boldsymbol{Q}(\boldsymbol{\eta})$ and a squarefree polynomial $F \in \boldsymbol{Q}(\boldsymbol{\eta})[x]$. The algorithm calculate the irreducible factorization of F over $\boldsymbol{Q}(\boldsymbol{\eta})$.

S1. Select a set of integers $\boldsymbol{c} \leftarrow (c_1, \ldots, c_r)$ such that the characteristic set CS of $AS \cup \{w - c_1 y_1 - \cdots - c_r y_r\}$ under the variable ordering $w \prec y_1 \prec \cdots \prec y_r$ is irreducible and quasilinear.

S2. Normalize $CS \leftarrow [C_0(w), y_1 - C_1(w), \ldots, y_r - C_r(w)]$.

S3. Set $F^*(w, x) \leftarrow F(C_1(w), \ldots, C_r(w), x)$ and apply $\mathsf{SFactorC}$ to $F^*(\xi, x)$ over $\boldsymbol{Q}(\xi)$:

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

where ξ has minimal polynomial $C_0(w)$.

S4. Substitute $\xi = \sum_{i=1}^{r} c_i \eta_i$ for ξ in each F_i.

S5. Return $F \leftarrow F_1(\boldsymbol{\eta}, x) \cdots F_s(\boldsymbol{\eta}, x)$.

Algorithm SFactorC. Given a monic minimal polynomial $m(y)$ of α and a squarefree polynomial $F \in \boldsymbol{Q}(\alpha)[x]$, the algorithm compute the irreducible factorization of F over $\boldsymbol{Q}(\alpha)$.

S1. Choose a positive integer s and set

$$\begin{aligned} G(\alpha, x) &\leftarrow F(\alpha, x - s\alpha), \\ R(x) &\leftarrow \operatorname{res}(G(y, x), m(y), y). \end{aligned}$$

S2. If $R(x)$ is squarefree, then go to **S3**. Otherwise, compute over $\boldsymbol{Q}$ an irreducible factorization

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

If $k = 1$ then go to **S1**, else set

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

and apply $\mathsf{SFactorC}$ to $F/(G_1 \cdots G_k)$ and $G_i's$:

$$\begin{aligned} &G_i \leftarrow G_{i1}(\alpha, x) \cdots G_{im_i}(\alpha, x), \quad 1 \leq i \leq k, \\ &F/(G_1 \cdots G_k) \leftarrow G_{01}(\alpha, x) \cdots G_{0m_0}(\alpha, x); \end{aligned}$$

then return

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

and the algorithm terminates.

S3. Factorize R over $\boldsymbol{Q}$:

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

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

S4. For $i = 1, \ldots, l$ do:

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

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

S5. Return $F \leftarrow H_1(\alpha, x) \cdots H_l(\alpha, x)$.

Example 5 *Factorize* $F = x^2 - y + 1$ *over* $\boldsymbol{K} = \boldsymbol{Q}(y, a)$ *defined by* $\mathit{AS} = [a^2 - (y-1)^3]$.

Pick the substitution value 0 for y; then F and AS are mapped to

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

respectively. The ascending set $\mathit{AS}^{(0)}$ is still irreducible. Applying UFactorA to $F^{(0)}$, one gets

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

Hensel lifting $\mathit{AS}^{(0)}$ and the two factors of $F^{(0)}$ proceeds as follows:

$$\begin{array}{rcl}
F & \equiv & (x - a - ay)(x + a + ay) \mod (y^2, \mathit{AS}), \\
\mathit{AS} & \equiv & [a^2 - 3y + 1] \mod (y^2), \\
F & \equiv & (x - a - ay - ay^2)(x + a + ay + ay^2) \mod (y^3, \mathit{AS}), \\
\mathit{AS} & \equiv & [a^2 + 3y^2 - 3y + 1] \mod (y^3), \\
F & \equiv & (x - a - ay - ay^2 - ay^3)(x + a + ay + ay^2 + ay^3) \mod (y^4, \mathit{AS}), \\
\mathit{AS} & \equiv & [a^2 - y^3 + 3y^2 - 3y + 1] \mod (y^4).
\end{array}$$

Now begin the true factor test. The discriminant of $\boldsymbol{K}$ is $\mathrm{dis}(a^2 - (y-1)^3) = -4(y-1)^3$. Let D be the greatest factor whose square divides the discriminant; clearly $D = y - 1$. Take one of the above two factors, e.g.,

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

Then, we have

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

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 $\boldsymbol{K}$.

1.5 GCD Computation over Algebraic Fields

Using the same notations, we consider the problem of finding the greatest common divisor (GCD) of two polynomials F and G over the algebraic extension field $\boldsymbol{K}_r = \boldsymbol{Q}(\boldsymbol{u}, \boldsymbol{\eta})$. Corresponding to the above three algebraic factorization algorithms, there are three methods for determining the GCD of multivariate polynomials over algebraic extension fields. For the modular method of computing the GCD over an algebraic number field, we refer to Langemyr and McCallum (1989).

1.5.1 Method A

For the undetermined coefficients method, Wu (1994) supposed that

$$\begin{aligned} F(x) &= f_0 x^n + f_1 x^{n-1} + \cdots + f_n, \\ G(x) &= g_0 x^m + g_1 x^{m-1} + \cdots + g_m \end{aligned}$$

with $f_i, g_j \in \boldsymbol{K}_r$ already known. Let

$$\begin{aligned} C_{n-e}(x) &= c_0 x^{n-e} + c_1 x^{n-e-1} + \cdots + c_{n-e}, \\ D_{m-e}(x) &= d_0 x^{m-e} + d_1 x^{m-e-1} + \cdots + d_{m-e} \end{aligned}$$

be two polynomials satisfying $\mathrm{prem}(D_{m-e}F - C_{n-e}G, AS) = 0$ and

$$\begin{aligned} c_i &= \textstyle\sum_{\substack{0 \le k_l \le m_l - 1 \\ 1 \le l \le r}} c_{ik_1 \cdots k_r} {y_1}^{k_1} \cdots {y_r}^{k_r}, \\ d_j &= \textstyle\sum_{\substack{0 \le k_l \le m_l - 1 \\ 1 \le l \le r}} d_{jk_1 \cdots k_r} {y_1}^{k_1} \cdots {y_r}^{k_r}. \end{aligned}$$

Proceeding as in Section 1.2, we get a linear system of polynomial equations:

$$\begin{aligned} W_1(u, z_1, \ldots, z_{N_1}) &= 0, \\ W_2(u, z_1, \ldots, z_{N_1}) &= 0, \\ &\cdots\cdots \\ W_N(u, z_1, \ldots, z_{N_1}) &= 0, \end{aligned}$$

where $N = (m+n-e+1)m_1 m_2 \cdots m_r$ and $N_1 = (m+n-2e+1)m_1 m_2 \cdots m_r$. Owing to the linearity in $c_{ik_1 \cdots k_r}$ and $d_{jk_1 \cdots k_r}$, it is easy to see whether or not the system has solutions for $(c_i, d_i) \in \boldsymbol{K}_r$ for any given e. We start now from $e = \min(m, n)$. If there exists no solution, then we proceed to the case of $e - 1$. Proceeding in the same way further and further, we will ultimately get the GCD of F and G as required.

It is very interesting that the above algorithm has been also used for computing the approximate GCD for polynomials whose coefficients have errors (see Corless 1995 and Karmarkar and Lakshma 1996).

Example 6 *Find the GCD in* $\boldsymbol{Q}[u, y]$ *of*

$$F = x^2 - u,\ G = x^2 + 2u^2yx + u$$

with y *defined by* $A = u^3y^2 - 1$.

Suppose

$$\begin{aligned} C_1 &= x + (c_1y + c_2), \quad c_i \in \boldsymbol{Q}(u), \\ D_1 &= x + (d_1y + d_2), \quad d_i \in \boldsymbol{Q}(u) \end{aligned}$$

such that

$$R = \mathrm{prem}(D_1F - C_1G, A) = 0.$$

Expanding R and equating the coefficients to zero, we get

$$\begin{aligned} d_1 - c_1 - 2u^2 &= 0, \\ d_2 - c_2 &= 0, \\ -2u^3c_2 &= 0, \\ -2u^2 - 2c_1 &= 0, \\ d_1 + c_1 &= 0, \\ d_2 + c_2 &= 0. \end{aligned}$$

Computing a characteristic set of the above equation system, one gets a set of solutions $\{c_1 = -u^2, c_2 = 0, d_1 = u^2, d_2 = 0\}$. Hence

$$C_1 = x - u^2y,\ D_1 = x + u^2y,$$

and the GCD is given by

$$H = \frac{F}{C_1} = \frac{G}{D_1} = x + u^2y \in \boldsymbol{Q}[u, y, x].$$

1.5.2 Method B

Generalizing the Euclidean algorithm for computing the GCD of $F(x)$ and $G(x)$ over $\boldsymbol{Q}$ to algebraic extension filed $\boldsymbol{K}_r = \boldsymbol{Q}(\boldsymbol{u}, \boldsymbol{\eta})$, we form a polynomial remainder sequence (prs) $f_1, f_2, \ldots, f_{k+1}$ as follows:

$$\begin{array}{ll} f_1 = F, \quad f_2 = G, & \text{suppose } \deg(F, x) \geq \deg(G, x) \\ f_i = \mathrm{prem}(\mathrm{prem}(f_{i-2}, f_{i-1}, x), AS), & \text{for } 3 \leq i \leq k+1, \\ f_i \neq 0, & \text{for } 1 \leq i \leq k \text{ and } f_{k+1} = 0. \end{array}$$

The above procedure is similar to computing a characteristic set of the polynomial set $AS \cup \{F, G\}$ and the last polynomial in the characteristic set corresponds to the GCD of F and G over $\boldsymbol{K}_r$.

Let us look at Example 2 again. During the execution of algorithm FactorB , we need to compute the GCD of F and G_1 over $\boldsymbol{K}$. Computing a characteristic set of $AS \cup \{F, G\}$ with respect to the ordering $y_1 \prec y_2 \prec x$, we obtain

$$\begin{aligned} CS \;=\; & [y_1^2+2, \ -2y_2^3+y_1y_2+y_1, 139696xy_1y_2^2+144205xy_1y_2 \\ & -87277x+66440y_1x-180960y_1y_2-98706y_1-61437y_2 \\ & -103091xy_2-121347y_1y_2^2-176301y_2^2+22858xy_2^2+6816]. \end{aligned}$$

Normalizing the last polynomial in CS, we get

$$CS_1 = [y_1^2+2, -2y_2^3+y_1y_2+y_1, x+y_1-y_2].$$

The last polynomial in CS_1 is the GCD of F and G_1 over $\boldsymbol{K}_r$.

1.6 Implementations and Applications

The described algorithms FactorA and FactorB for polynomial factorization have been implemented by Wang (1992a,1995) in his charsets package in the Maple system; the algorithm FactorC was implemented by Zhi (1996) also in the Maple system. The algorithms for computing the GCD by methods A and B were implemented by Zhi (1996) and Wang (1992a,1995), respectively, in Maple. A large set of examples is chosen to compare the performances between these different methods as well as the Maple built-in functions. See the timings in Wang (1992a) and Zhi (1996, 1997). According to these experimental results, our three methods seem to be efficient in different cases. If the degrees of the polynomial and the ascending set are less than 4, then FactorA works well; FactorB is relatively faster when the transcendental elements $\boldsymbol{u}$ do not appear in the AS; FactorC is very powerful for factorizing multivariate polynomials over algebraic function fields. Combining these three methods and some criteria for irreducibility test in Wang (1992a), a hybrid factoring algorithm is given by Zhi (1996).

As we have pointed out at the beginning of this chapter, our motivation for studying algebraic factorization comes from geometry theorem proving. Following Wu (1984), one may express a theorem in elementary (unordered) geometry by means of a set HS 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 HS is a zero of C, and if not, which parts of the zeros of HS are zeros of C. An elementary version of Wu's method proceeds by computing first a characteristic set CS of HS and then the pseudo-remainder R of C with respect to CS. 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 CS. 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 CS and perform further decompositions. See Wu (1984), Chou and Gao (1990) and Wang (1994, 1999). CS is reducible often when some geometric ambiguities such as bisection of angles and contact of circles are involved in the theorem (see Wu 1987). To test the irreducibility of CS or to decompose CS into irreducible ascending sets, it is necessary to factorize polynomials over successive algebraic extension fields. Wang (1994) presented a set of geometric theorems whose automated proofs may require algebraic factorization. For example, when we prove Poncelet's theorem, the following factorization is necessary (see Wang and Zhi 1998):

$$\begin{aligned} f &= (x_4 x_3^2 R^2 - x_3^4 - (x_2^2 + x_1^2)x_3^2 - x_1^2 x_2^2 \\ &= (2x_3 R - 2x_4^2 + 2x_2 x_4 + 2x_1 x_4 + x_3^2 - x_1 x_2) \\ &\quad (2x_3 R + 2x_4^2 - 2x_2 x_4 - 2x_1 x_4 - x_3^2 + x_1 x_2) \end{aligned}$$

over the algebraic field $\boldsymbol{K} = \boldsymbol{Q}(x_1, x_2, x_3, x_4)$ defined by

$$\begin{aligned} A &= 4x_4^4 - 8(x_2 + x_1)x_4^3 - 4(x_3^2 - x_2^2 - 3x_1 x_2 - x_1^2)x_4^2 \\ &\quad + 4(x_2 + x_1)(x_3^2 - x_1 x_2)x_4 - (x_2 + x_1)^2 x_3^2. \end{aligned}$$

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* sub-objects. 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 and Gröbner bases for carrying out such decompositions. See Wang (1992b) for instance. In these methods, algebraic factorization is indispensable. Other applications of algebraic factorization include verification of geometric conditions and implicitizations of curves and surfaces. See Wang and Zhi (1998) for more examples and timings.

Polynomial factorization over algebraic fields is one of the most difficult problems in computer algebra. Until now, we only can factor polynomials of low degree. Further study and improvement are necessary.

Reference

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

Buchberger, B. (1985): Gröbner bases: An algorithmic method in polynomial ideal theory. In: Bose, N. K. (ed.): Multidimensional systems theory. Reidel, Dordrecht, pp. 184–232.

Corless, R. M., Gianni, P. M., B.M.Trager, B. M and Watt, S. M. (1995): The singular value decomposition for polynomial systems. In: Proc. ISSAC'95, Montreal, Canada, pp. 195-207.

Encarnación, M. J. (1997): Factoring polynomials over algebraic number fields via norms. In: Proc. ISSAC'97, Hawaii, ACM Press, New York, pp. 265–270.

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

Karmarkar, N., Lakshman, Y. N. (1996): Approximate polynomial greatest common divisors and nearest singular polynomials. In: Proc. ISSAC'96, Zurich, Switzerland, pp. 35-39.

Kronecker, L. (1882): Grundzüge einer arithmetischen theorie der algebraischen Gröβen. J. f. d. reine u. angew. Math. **92**: 1-122.

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

Langemyr, L., McCallum, S. (1989): The computation of polynomial greatest common divisors over an algebraic number field. J. Symbolic Comput. **8**: 429-444.

Lenstra, A. K. (1982): Lattices and factorization of polynomials over algebraic number fields. In: Proc. EUROCAM'82, Marseilles, France, pp. 32–39.

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

Noro, M., Yokoyama, K. (1997): Factoring polynomials over algebraic extension fields. Preprint. FUJITSU.

Trager, B. M. (1976): Algebraic factoring and rational function integration. In: Proc. SYMSAC'76, Yorktown Heights, ACM Press, New York, pp. 219–226.

van der Waerden, B. L. (1953): Modern algebra. **1**. Engl. transl. by Blum. New York: Frederick Vngar Publ. Co.

Wang, D. (1992a): A method for factorizing multivariate polynomials over successive algebraic extension fields. Preprint. RISC Linz.

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

Wang, D. (1994): Algebraic factoring and geometry theorem proving. In: Proc. CADE-12, Nancy,1994, Springer-Verlag, Berlin Heidelberg New York Tokyo, pp. 386–400 (Lecture notes in artificial intelligence, **814**).

Wang, D. (1995): An implementation of the characteristic set method in Maple. In: Pfalzgraf, J. and Wang, D. (eds.): Automated practical reasoning: Algebraic approaches. Springer-Verlag, Wien New York, pp. 187–201.

Wang, D. (1999): Elimination methods. Springer-Verlag, Wien New York (in press).

Wang, D., Zhi, L. (1998): Algebraic factorization applied to geometric problems. In: Proc. ASCM'98, Lanzhou, China, pp. 23-37.

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

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

Wu, W.-t. (1984): Basic principles of mechanical theorem proving in elementary geometries. J. Syst. Sci. Math. Sci. **4**: 207–235 [also in J. Automat. Reason. **2** (1986): 221–252].

Wu, W.-t. (1987): A zero structure theorem for polynomial equations-solving. Math. Mech. Res. Preprints **1**: 2–12.

Wu, W.-t. (1994): Some remarks on factorization and GCD of multivariate polynomials. Math. Mech. Res. Preprints **3**: 1–14.

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

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

Zhi, L. (1997): An optimal method for algebraic factoring. J. Comput. Sci. Tech. **12**: 1–9.