数理解析研究所講究録
920巻 1995年 25-30

3.

Some Computations over Successive Algebraic Extension Fields

小林 英恒 (日大理工)
Dongdai Lin(〃)

Abstract:

In this paper, we first give a brief introduction to Ritt-Wu Method, then show the posibility of doing some computations over successive algebraic extension field by Ritt-Wu method. At the end of this paper, the relation between factorization of polynomials and the computation of primitive element is also discussed.

3.1 Introduction to Ritt-Wu's method

Let K be a field of characteristic zero, $y_1, y_2, \cdots, y_n$ a set of n variables with a fixed ordering $y_1 < \cdots < y_n$. The class $\mathbf{cls}(f)$ of a non-zero polynomial f in the ring $K[y_1, y_2, \cdots, y_n]$ is defined to be the largest subscript of $y_i's$ indeed occurring in f if any, otherwise 0, and y_c is called the main varable of f if $c = cls(f) \neq 0$. The coefficient of the term of highest degree of the main variable is called the **initial** of f, denoted by $\mathbf{Init}(f)$.

Let f and g be two polynomials in the ring $K[y_1, y_2, \cdots, y_n]$, $c = cls(f) \neq 0$. We say that g is reduced with respect to f if $cls(g) < cls(f)$ or $cls(g) \geq cls(f)$ but $deg_{y_c} g < deg_{y_c} f$.

Apparently, if g is not reduced with respect to f, we can find $I, Q, R \in K[y_1, y_2, \cdots, y_n]$ such that

$$I \cdot g = Q \cdot f + R$$

with $cls(I) < cls(f)$ and R reduced with respect to f.

The polynomial R above is called the **pseudo-remainder** of g with respect to f, denoted by $\mathbf{prem}(f, g)$, and the procedure to get R from f and g is called **pseudo-division**.

Remark: In practice, in order to control the growth of the degree and the number of terms of polynomials, we should choose the polynomial I in pseudo-division carefully.

A finite set $\mathcal{A}$ of polynomials $A_1, A_2, \cdots, A_r$ is called an **ascending set** if $r = 1$ and $A_1 \neq 0$ or $r > 1$, $0 < cls(A_1) < \cdots < cls(A_r)$ and A_j is reduced with respect to A_i for all $j > i$. Furthermore, if all the polynomials of $\mathcal{A}$ except A_1 are linear with respect to their own main variables, then it is called **quasi-linear** ascending set.

If a polynomial f is reduced with respect to any polynomial of an asending set $\mathcal{A}$, then we say it is reduced with respect to $\mathcal{A}$, otherwise, we can define the pseudo-remainder $\mathbf{prem}(f, \mathcal{A})$ of f with respect to $\mathcal{A}$ inductively as

$$prem(f, A_1, \cdots, A_s) = prem(prem(f, A_1, \cdots, A_{s-1}), A_s)$$

For any polynomial set $\mathcal{F}$, we denote the set of common zeros of polynomials in $\mathcal{F}$ by $Zero(\mathcal{F})$. If G is another (non-zero) polynomial, we write $Zero(\mathcal{F}/G)$ for $Zero(\mathcal{F}) \backslash Zero(G)$.

For any polynomial set $\mathcal{F}$, we can find an ascending set $\mathcal{C}$ from the ideal $Ideal(\mathcal{F})$ generated by the polynomials in $\mathcal{F}$ such that any polynomial of $\mathcal{F}$

has pseudo-remainder 0 with respect to $\mathcal{C}$, and so

$$Zero(\mathcal{C}/J) \subset Zero(PS) \subset Zero(\mathcal{C})$$

where J is the product of initials of plolynomials in $\mathcal{C}$. The ascending set having such properties is called **characteristic set** of $\mathcal{F}$.

Let $\mathcal{A}$: $A_1(y_1), A_2(y_1, y_2), \cdots, A_r(y_1, \cdots, y_r)$ be an ascending set. $\mathcal{A}$ is said to be irreducible if A_{i+1}, as a polynomial in $K_i[y_{i+1}]$, is irreducible, where $K_0 = K$, K_i is the field $K_{i-1}(\alpha_i)$ obtained from the field K_{i-1} by the adjunction of a root α_i of A_i. The field K_r is called **successive algebraic extension** field of K with adjoining polynomials $A_1, \cdots, A_r$ or simply $\mathcal{A}$.

In the present paper, we will discuss some computations over such successive algebraic extension field.

3.2 Some Computations over Successive Algebraic Extension Field

In this section, we first discuss the computations of miminal polynomial and primitive element based on Ritt-Wu method, then discuss the relation between the polynomial factorization and the compuation of primitive elements.

Let $A_1(y_1), A_2(y_2), \cdots, A_r(y_r)$ be an irrducible ascending set. As discussed in last section, we can get a successively algebraic extension field E by adjoining the polynomials $A_1(y_1), A_2(y_2), \cdots, A_r(y_r)$ to the ground field K. In fact, we have

Proposition: $E \simeq K[y_1, y_2, \cdots, y_r]/ < A_1, \cdots, A_r >$, where $< A_1, \cdots, A_r >$ is the ideal generated by $A_1, \cdots, A_r$.

So each element of E can be treated as a multivariate polynimial $e(y_1, \cdots, y_r)$ with $deg_{y_i} e < deg_{y_i} A_i$. And the computations in E can be considered as those of polynomials modulo $< A_1, \cdots, A_r >$.

Proposition: Let $\mathcal{A}$: $A_1(y_1), A_2(y_2), \cdots, A_r(y_r)$ be an irreducible ascending set, then the set of all the polynomials which have pseudo-remainder

0 with respect to $\mathcal{A}$ is a prime ideal of polynomial ring $K[y_1, \cdots, y_n]$ under the ordinary polynomial addition and multiplication. Furthermore, it is also a maximal ideal if $r = n$.

In fact,

Proposition Let $\mathcal{A}$ be an irreducible ascending set. Then the ideal of all the polynomials which have pseudo-remainder 0 with respect to $\mathcal{A}$ is the same with the ideal generated by the polynomials of $\mathcal{A}$.

The above proposition tell us that it is possible to carry out the computations in E by Ritt-Wu method.

Proposition Let $f(y_1, \cdots, y_r, y)$ and $g(y_1, \cdots, y_r, y)$ be two polynomial over E, C be the characteristic set of $\{A_1, \cdots, A_r, f(y_1, \cdots, y_r, y), g(y_1, \cdots, y_r, y)\}$ under order $y_1 < \cdots < y_r < y$. Then the polynomial of C which containing only the variable y is the greatest common divisor of $f(y_1, \cdots, y_r, y)$ and $g(y_1, \cdots, y_r, y)$ over E.

Proposition Let $f(y_1, \cdots, y_r, y)$ be a non-zero polynomial of y over E, then the characteristic set of $\{f(y_1, \cdots, y_r, y), A_1, \cdots, A_r\}$ under order $y < y_1 < \cdots < y_r$ must contains a polynomial with only y as its variable.

Let $e(y_1, \cdots, y_r)$ be an element in E and let $g(y_1, \cdots, y_r, y) = y - e(y_1, \cdots, y_r)$, then

Proposition Let $m(y)$ be the polynomial of y in the characteristic set of $\{g(y_1, \cdots, y_r, y), A_1, \cdots, A_r\}$ under ordering $y < y_1 < \cdots < y_r$. If $m(y) = m_1(z) \cdots m_t(z)$, then there is one and only one $m_i(z)$ having pseudo-remainder 0 with respect to the ascending set $\{A_1, \cdots, A_r, g(y_1, \cdots, y_r, y)\}$. In fact, this $m_i(z)$ is the minimal polynomial of the elment $e(y_1, \cdots, y_r)$.

As we know, any seperable finite extension is a simple extension, so

Proposition E is a simple extension of K.

The following proof to this proposition is belong to Van de Waerdan. Since some facts from this proof will fit our purpose, we repeat it here.

Proof: First we prove the proposition for two elments α, β. Let $f(x)$ and $g(x)$ be the minimal polynomials of α and β respectively. We take a field in which $f(x), g(x)$ split. Let the distinct zeros of $f(x)$ be $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_r$ and let those of $g(x)$ be $\beta_1 = \beta, \beta_2, \cdots, \beta_s$.

For $k \neq 1$, the equation $\alpha_i + x\beta_k = \alpha_1 + x\beta_1$ has at most one root x in K for every i and every $k \neq 1$. If we take c different from the roots of all these linear equations, we have $\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$ for every i and $k \neq 1$.

Let $\theta = \alpha_1 + c\beta_1 = \alpha + c\beta$, then we can assert that θ would be a primitive element of $K(\alpha, \beta)$. In fact, β satisfies the equations $g(\beta) = 0$ and $f(\theta - c\beta) = f(\alpha) = 0$, with coefficients in $K(\theta)$. The polynomial $g(x)$, $f(\theta - cx)$ have only the root β in common by the choice of c. But β is a simple root of $g(x)$, therefore, $g(x)$ and $f(\theta - cx)$ have but one linear factor $x - \beta$ in common. The coefficients of this greatest common divisor and so β must lie in $K(\theta)$. Thus we have $K(\alpha, \beta) = K(\theta)$.

This completes the proof of theorem for $r = 2$. Once it is proved for $r - 1(\geq 2)$, we have $K(\alpha_1, \cdots, \alpha_{r-1}) = K(\eta)$ and so $K(\alpha_1, \cdots, \alpha_r) = K(\eta, \alpha_r) = K(\theta)$ according to the already proved part of theorem.

¿From the proof, we can see that,

Proposition For almost all vectors $(c_1, \cdots, c_r) \in K^n$, $\sum_i c_i\alpha_i$ would give a primitive element of E

So the task to find a primitive element for E is to choose a vector $(c_1, \cdots, c_r)$ and check if it is a primive element, this is equivalent to check if its miminal polynomial has degree $\Pi deg_{y_i} A_i$.

The above technique for finding the primitive elements is not new, but each author has their own method to check the primitiveness of the element, here we want tell the Ritt-Wu method can also fit this purpose.

¿From now on, we suppose we have found a primitive element θ for the successive algebraic exension field E of K and its minimal polynomial $m(x)$.

Without loss of generality, we can consider E as an extension field of K

by adjoining $m(x)$. Let $f(y_1, \cdots, y_r, y)$ be a squarefree polynomial of variable y over E, then it can be writen into the form $f(x, y)$.

Proposition If $f(x, y)$ is irreducible over E, then for almost all $c \in E$(or in K), the characteristic set of $\{m(x), f(x, y), z - (y + cx)\}$ is quasi-linear.

Proposition Suppose $f(x, y) = f_1(x, y) \cdots f_t(x, y)$, where $f_i(x, y)$ are irreducible polynomials over E. Then for almost all integer $c \in E$, a element of the form $y + cx$ would be a primitive element(over K) of the extension fields of E obtained by adjoining the polynomials $f_i(x, y)$ respectively.

Proposition Let $y+cx$ be the form mentioned in the above proposition, $g_i(z)$ its minimal polynomial(over K) as a primitive element of the extension field of E obtained by adjoining polynomial $f_i(x, y)$. Then if $g(z)$ be the polynomial of z in the characteristic set of $\{m(x), f(x, y), z-(y+cx)\}$ under order $z < x < y$, we have $g_i(z)|g(z)$ for all i.

Proposition Let $g(z)$ as above. Suppose $g(z) = \Pi_i g_i'(z)$, where $g_i'(z)$ are the irreducible factors of $g(z)$ over K, then $gcd(g_i'(y - cx), f(x, y))$ is an irreducible factor of $f(x, y)$ over E if it is not equal to 1. Furthermore, such greatest common divisors can give out all the irreducible factors of $f(x, y)$ over E.

References:

1. B. L. Van der Waerden, Modern Algebra, Revised English Edition(1953),

2. Dongming Wang, A Mehod for Facorizing Multivariate Polynomials over Successive Algebraic Extension Fields

3. Yokoyama, K., Noro, M., and Takeshima, T.(1990). Computing Primitive Elements of Extension Fields. J. Symb. Comp. 8/6, 553-580.