数理解析研究所講究録
986巻 1997年 78-82

逐次代数拡大体の簡約表現

電子技術総合研究所 元吉文男 (Fumio Motoyoshi)

1. はじめに

数式処理システムで代数的数を扱う場合に、原始元を用いて単一拡大として1つの定義多項式で代数的数を表現する方法が一般的である。しかし、この方法では$\sqrt[3]{2}$というような根号を多数扱う場合には、局所的な計算には出現しない数までも含めた拡大体として処理するために効率が低下すると考えられる。また、穴井等によって拡大体を逐次拡大として表現すると計算の効率が上がることが示されている。

ただ、逐次拡大で表現したときに、拡大の順番によって以下に示すような不便が生じることがある： 最初の拡大として$Q(\sqrt{3})$があり、ここで$a^2-2-\sqrt{3}=0$としてaを導入すると、拡大体は$Q(\sqrt{2})(\sqrt{2+\sqrt{3}})$となるが、この体は$Q(\sqrt{2})(\sqrt{3})$と同じものであり、表現上では後者をとった方が見易いし、拡大の次数も小さいので計算の効率もよいと考えられる。

ここでは、逐次拡大による表現を、上記のような場合にも適切に表現されるように、簡約化する方法について述べる。

2. 拡大体の簡約化表現

基礎体K上の拡大体$K(\alpha)$が与えられたときに、これを簡約表現にする方法の概略を以下に示す。

1. $K(\alpha)$の自明でない極大部分体$K(\beta)$を求める
2. その極大部分体の数により次の操作を行なう。

部分体の数	操作
なし	αの定義多項式の最小化
1個	この簡約化手続きを再帰的に適用して極大部分体$K(\beta)$を簡約化
	αの$K(\beta)$での定義多項式の最小化
2個以上	それぞれの極大部分体$K(\beta_i)$を簡約化
	表現が最小となる2つの極大部分体の合成

以上の方法で定義多項式の最小化が一意的に可能であれば、$K(\alpha)$の表現が一意的に決定できることになる。これが、ある意味で可能であることを以下に示す。

定義多項式の最小化は、αが定義多項式$f(x)\in K[x]$で与えられたときに、$K(\alpha)$と同じ体を表現する定義多項式のうち、最小のものを探索する問題になる。2つの多項式$f(x)$と

$g(x)$ が同じ体を表す関係~は次のように定義できる。

$$f(x) \sim g(x) \stackrel{\text{def}}{=} f(x) \subset g(x) \wedge g(x) \subset f(x) \tag{1}$$

$$f(x) \subset g(x) \stackrel{\text{def}}{=} \forall\alpha(f(\alpha) = 0 \rightarrow \exists\beta g(\beta) = 0 \wedge P(\alpha) = P(\beta)) \tag{2}$$

すなわち、$f(x) \sim g(x)$ とは、$f(x) = 0$ の任意の根αについて、$g(x) = 0$ が $K(\alpha)$ 中に根を持ち、かつ、$g(x) = 0$ の任意の根βについて、$f(x) = 0$ が $K(\beta)$ 中に根を持つことである。

問題は、$f(x)$ に対して $g(x) \sim f(x)$ となる最小の多項式が求まるかということになるが、少なくとも次のようにすれば可能である。

- $K = Q$ のとき
  最小多項式の係数は整数としても一般性を失わない。このとき、$f(x)$ の大きさを係数の絶対値の最大なもので定義する。その値が同じときには、次数の大きい係数を優先する辞書式順序とすれば、任意の多項式の大きさが比較できる。
  このような順序付けをすれば、$f(x)$ よりも小さい多項式の数は有限であるので、最小の多項式は探索できる。
- $K = Q(\beta_1, \beta_2, \ldots, \beta_m)$ のとき
  このときの定義多項式の係数は $Q(\beta_1, \beta_2, \ldots, \beta_m)$ の要素であるが、この場合も各係数を $\beta_1, \beta_2, \ldots, \beta_m$ に関する多項式として表現でき、その係数を整数にすることができる。したがって、上と同じように順序付けをすることによって、$f(x)$ より小さい多項式の数が有限になるので最小の多項式は決定できる。

以上の方法により、実用的に計算可能かどうかはともかくとして、拡大体の最小表現多項式は一意的に決定できることがわかった。

しかし、上での順序付けでは $x^2 + 3x - 1$ の方が $x^2 - 13$ よりも小さいことになってしまい、計算機あるいはユーザにとって望ましい順序とはいえないので、実際に実現するには別の考察が必要になろう。すぐにでも実現できることは、その体が2項拡大体になっていることは検出可能であるので、2項拡大体の定義多項式の順序を特に小さくするような順序付けをとることである。

3. 簡約化の実現

$f(x)$ を定義多項式とする体の極大部分体を表す定義多項式を以下の手続きで計算する。

1. $f(x)$ の根を分解体を求めながら計算し、それを$\alpha_1, \alpha_2, \ldots, \alpha_n$とする。
2. 上の結果をもとに $f(x)$ の Galois 群 G を$\alpha_1, \alpha_2, \ldots, \alpha_n$に関する置換群として表現する。
3. G からα_1を含む極小ブロック $S = \{\alpha_{k_1} = \alpha_1, \alpha_{k_2}, \ldots, \alpha_{k_m}\}$ を求める
4. S の安定化群を G_Sとし、$G = G_S + g_2 G_S + \cdots + g_{n/m} G_S$ と分解する。
5. 次に示す z に関する多項式 $h(z)$ が重根を持たないように整数 s を決める。

$$h(z) = \prod_{i=1}^{n/m} (z - g_i a), \quad (g_1 = e) \tag{3}$$

ただし

$$a = \prod_{i=1}^{m}(s - \alpha_{k_i}) \tag{4}$$

である。

この手続きで得られる多項式 $h(z)$ が極大部分体の定義多項式である。現在のところでは、$h(z)$ が3次以下の場合で2項拡大になる場合のみ最小化の手続きを実現している。

例

上記の逐次代数拡大体の簡約化法を利用して次の根号を簡約化してみる。

$$a = \sqrt[3]{\sqrt[3]{2} - 1} \tag{5}$$

これは、$x^3 - 2 = 0, y^3 - x + 1 = 0$ という逐次拡大体として表現されるがこれを簡約化する。もちろん、a が $Q(\sqrt[3]{2})$ の要素ではないことは事前に確認してあるものとする。以下では理解の容易さのために、わかっている結果を利用するが、実際の計算では分解体の表現は以下のような見易いものではない。

a の Q に関しての定義多項式は

$$y^9 + y^6 + y^3 - 1 \tag{6}$$

であり、これから分解体は (結果から逆算して)

$$P = Q(\sqrt[3]{2}, \sqrt[3]{3}, \omega) \tag{7}$$

となる。ここでωは1の原始3乗根である。この分解体の表現を使用すると、a およびその共役根は

$$y_1 = \sqrt[3]{3}(1 - \sqrt[3]{2} + \sqrt[3]{2^2})/3 \tag{8}$$
$$y_2 = \sqrt[3]{3}\omega(1 - \sqrt[3]{2} + \sqrt[3]{2^2})/3 \tag{9}$$
$$y_3 = \sqrt[3]{3}\omega^2(1 - \sqrt[3]{2} + \sqrt[3]{2^2})/3 \tag{10}$$
$$y_4 = \sqrt[3]{3}(1 - \sqrt[3]{2}\omega + \sqrt[3]{2^2}\omega^2)/3 \tag{11}$$
$$y_5 = \sqrt[3]{3}\omega(1 - \sqrt[3]{2}\omega + \sqrt[3]{2^2}\omega^2)/3 \tag{12}$$
$$y_6 = \sqrt[3]{3}\omega^2(1 - \sqrt[3]{2}\omega + \sqrt[3]{2^2}\omega^2)/3 \tag{13}$$
$$y_7 = \sqrt[3]{3}(1 - \sqrt[3]{2}\omega^2 + \sqrt[3]{2^2}\omega)/3 \tag{14}$$
$$y_8 = \sqrt[3]{3}\omega(1 - \sqrt[3]{2}\omega^2 + \sqrt[3]{2^2}\omega)/3 \tag{15}$$
$$y_9 = \sqrt[3]{3}\omega^2(1 - \sqrt[3]{2}\omega^2 + \sqrt[3]{2^2}\omega)/3 \tag{16}$$

となる。このとき、P 上の自己同型写像で Q を動かさないものは

$$\sqrt[3]{3} \mapsto \sqrt[3]{3}\omega, \tag{17}$$
$$\sqrt[3]{2} \mapsto \sqrt[3]{2}\omega, \tag{18}$$
$$\omega \mapsto \omega^2 \tag{19}$$

から生成されるものである。置換群でy_iをiで書くことにすると、Galois群Gは

$$(1\ 2\ 3)(4\ 5\ 6)(7\ 8\ 9),$$
$$(1\ 4\ 7)(2\ 5\ 8)(3\ 6\ 9),$$
$$(2\ 3)(4\ 7)(5\ 9)(6\ 8)$$

を生成元とする(位数18の)群になる。

Gにおいて1を含む極小ブロックは$\{1,2,3\}$, $\{1,4,7\}$, $\{1,5,9\}$, $\{1,6,8\}$の4つである。それぞれのブロックに対応する極大部分体の定義多項式を求める際に、実際には、適当なsを選んで(3)式を無平方にするが、ここでは説明のために(4)式のaに該当する根の対称式を目の子で以下のものにする。

$\{1,2,3\}$のとき

$$y_1y_2y_3 = \sqrt[3]{2} - 1$$

定義多項式は $x^3 + 3x^2 + 3x - 1 \sim x^3 - 2$ (20)

$\{1,4,7\}$のとき

$$y_1 + y_4 + y_7 = \sqrt[3]{3}$$

定義多項式は $x^3 - 3$ (21)

$\{1,5,9\}$のとき

$$y_1 + y_5 + y_9 = \sqrt[3]{2}^2\sqrt[3]{3}$$

定義多項式は $x^3 - 12$ (22)

$\{1,6,8\}$のとき

$$y_1 + y_6 + y_8 = \sqrt[3]{2}\sqrt[3]{3}$$

定義多項式は $x^3 - 6$ (23)

以上のことを計算機で実現した結果を次に示す。

```
* (time (maximal-subfield '(1 0 0 3 0 0 3 0 0 -1)))
  101.75 seconds of real time
  95.83 seconds of user run time
  5.56 seconds of system run time
  [Run times include 11.39 seconds
   GC run time]
  0 page faults and
  56668608 bytes consed.
((1 0 0 -2) (1 0 0 -6) (1 0 0 -12) (1 0 0 -3))
```

これから、与えられた拡大体は(20)と(21)の合成として表現できることがわかる。

4. まとめ

代数拡大体を一意的に逐次拡大体として表現する手法とその一部分を実現した結果を示したが、実行時間のうちのほとんどが、Galois 群の計算にかかっているため、実用的にするために極大部分体を効率的に計算する手法を取り入れる必要がある。また、定義多項式の最小化についても効率的に処理できる範囲を広げるための手段を開発する必要がある。