イデアルの素分解におけるモジュラーアルゴリズムの応用

青山　暢

神戸大学理学研究科数学専攻

1　モジュラーアルゴリズム

代数計算の係数爆発を避けるために，係数を有限体に制限して計算した後に Hensel 構成や中国剰余定理を利用して正しい計算結果を復元するモジュラーアルゴリズムが用いられる．

定理 1. *(Hensel 構成)*
$f \in \mathbb{Z}[X]$，$p : f$ の先頭係数を割らない素数に対して

$$f \equiv g_1 h_1 \pmod{p}$$

と，互いに素な $g, h \in \mathbb{Z}_p$ が存在するとき，任意の $k \in \mathbb{N}$ に対して

$$f \equiv g_k h_k \pmod{p^k}$$

$$g_k \equiv g_1, h_k \equiv h_1 \pmod{p}$$

を満たす $g_k, h_k \in \mathbb{Z}_{p^k}[X]$ が存在する．

定理 2. *(*中国剰余定理*)*
$p_1, p_2 \in \mathbb{N}$ が互いに素であり，それぞれに対し $n_1, n_2 \in \mathbb{Z}$ が与えられているとき

$$n \equiv n_1 \pmod{p_1}, n \equiv n_2 \pmod{p_2}$$

を満たす n が　$\bmod p_1 p_2$ において唯一存在する．

2　Laplagne アルゴリズム

Laplagne アルゴリズムは, 冗長成分を生じないイデアルの根基の素分解アルゴリズムである．このアルゴリズムは 0 次元イデアルの根基計算, 準素分解が比較的容易であることや, radical membership は根基を計算しなくても判定できることを利用している．

補題 3. $I = \bigcap_{i=1}^{m} Q_i$ と準素分解が与えられているとき, イデアル J に対して準素成分から適当に選択することで $I : J^\infty = \bigcap_{J \not\subset \sqrt{Q_i}} Q_i$ と準素分解することができる．特に $I : g^\infty = \bigcap_{g \notin \sqrt{Q_i}} Q_i$ である．

命題 4. $MA \subset minAss(I)$, $Int = \bigcap_{P \in MA} P$ とおく．$g \in Int \setminus \sqrt{I}$ が存在するときに, $I : g^\infty = \bigcap_{i=1}^{m} Q_i$ と, 極小準素分解が与えられていて, u を $I : g^\infty$ の極大独立集合とすれば, $Q_i \cap \mathbb{K}[u] = \{0\}$ を満たす準素成分について $\sqrt{Q_i} \in minAss(I)$ かつ $\sqrt{Q_i} \notin MA$ である．

命題 5. u を $I:g^\infty$ の極大独立集合として, 極小準素分解 $I=\bigcap_{i=1}^{m} Q_i$ が

$$Q_i\cap\mathbb{K}[u]=\{0\}\ \ (1\le i\le l),\quad Q_i\cap\mathbb{K}[u]\neq\{0\}\ \ (l+1\le i\le m)$$

であるとする. このとき

$$I\mathbb{K}(u)[x\setminus u]\cap\mathbb{K}[x]=\bigcap_{i=1}^{l} Q_i$$

と, 極小準素分解できる.

以上の命題により次の Laplagne アルゴリズムが得られる.

アルゴリズム 6. *(Laplagne アルゴリズム)*
Input: I
Output: I の 極小付属素イデアル全体 MA
$Int\leftarrow\langle 1\rangle$
$MA\leftarrow\{\}$
while $Int\setminus\sqrt{I}\neq\{\}$ ***do***
  choose $g\in Int\setminus\sqrt{I}$
  $J\leftarrow I:g^\infty$
  $u\leftarrow J$ の極大独立集合
  $J\leftarrow\sqrt{J\mathbb{K}(u)[x\setminus u]}$
  $PJ=\{P_1,\dots,P_n\}\leftarrow J$ の最小素分解
  $PJ\leftarrow\{P_1\cap\mathbb{K}[x],\dots,P_n\cap\mathbb{K}[x]\}$
  $MA\leftarrow MA\cup PJ$
  $Int\leftarrow Int\cap\bigcap_{P\in PJ} P$
end while
return MA

定理 7. アルゴリズム *6* は冗長成分を生じずに正しく動作する.

3 Padé 近似

モジュラーアルゴリズムによって求められた多項式 h を $\frac{a}{b}\equiv h\pmod I$ を満たす (a,b) で表すために Padé 近似という手法が用いられる.

定義 8. $a,b\in\mathbb{Q}[X],I:\mathbb{Q}[X]$ 上のイデアルが，単項式 φ,ψ に対して *weak term order condition(wtoc)* を満たすとは，$LT(a)\le\varphi, LT(b)\le\psi$ かつ，任意の $\rho\le\varphi,\sigma\le\psi$ であり $\rho,\sigma\notin LT(I)$ なる単項式 ρ,σ に対して $\rho\sigma\notin LT(I)$ が成り立つときを言い，(a,b,I) が $wtoc(\rho,\sigma)$ を満足する，という.

定理 9. (a,b) が $\frac{a}{b}\equiv h\pmod I$ を満たす，既約で互いに素な解であり (a,b,I) が $wtoc(\rho,\sigma)$ を満足するとする．このとき順序に対するシフト $\omega=(\sigma,\rho)$ を与えると，(a,b) は $<_\omega$ について極小な解となる.

この定理を元に，$(h,1)$ という自明な解から出発し，得たい (a,b) についての条件を (ρ,σ) で与えることによって (a,b) を探していく.

参考文献

[1] 佐々木建昭, 今井浩, 浅野孝夫, 杉原厚吉, 計算代数と計算幾何, 岩波書店, (1993).

[2] S. Laplagne, *An algorithm for the computation of the radical of an ideal* , in Proc. ISSAC '06, (2006).

[3] P. Fitzpatrick, J. Flynn, *A Gröbner Basis Technique for Padé Approximation*, J. Symb. Comp. **13**, 133-138, (1992).