Modular Algorithms for Computing Minimal Associated Primes and Radicals of Polynomial Ideals

Toru Aoyama

Kobe University
Department of Mathematics
Graduate school of Science
Rikkyo University
Department of Mathematics

Masayuki Noro

Rikkyo University
Department of Mathematics

ISSAC 2018, July 18, 2018 in New York, USA

Notations

- R : ring
- $\mathbb{K}$: field
- $X = \{x_1, \ldots, x_n\}$
- $R[X]$: polynomial ring over R

Abstract

- Modular algorithms avoid the swell of coefficients which makes ideal computations slow-down.
- For computational targets in R, modular algorithms choose projection maps R to R', take projected images of targets and compute in R' then reconstruct the real computed results in R.
- We apply the Chinese Remainder Theorem (CRT) for Laplagne's algorithm.
- Most basically, CRT utilizes mappings: $\mathbb{Z} \to \mathbb{F}_p$ (p : prime number).
- We utilize mappings: $\mathbb{K}[u] \to \mathbb{K}$, substituting maps for u.
- In order for this method to work correctly, the shape of each modular component must coincide with that of the corresponding component of the ideal.

Contents

Basic facts

Laplagne's Algorithm (Laplagne. S (2006))

Laplagne proposes algorithms for computing minAss(I) and $\sqrt{I}$.

LminAss(I) and Lradical(I)

$Int \leftarrow \langle 1 \rangle, MA \leftarrow \emptyset, Rad \leftarrow \langle 1 \rangle$
while $Int \setminus \sqrt{I} \neq \emptyset$ **do**
  choose $g \in Int \setminus \sqrt{I}$
  $J \leftarrow I : g^{\infty}$
  $U \leftarrow$ a maximal independent set of J.
  $J \leftarrow J\mathbb{K}(U)[X \setminus U]$
  $\{P_1, \ldots, P_n\} \leftarrow$zeroMinAss$(J)$
  $PJ \leftarrow \{P_1 \cap \mathbb{K}[X], \ldots, P_n \cap \mathbb{K}[X]\}$
  $MA \leftarrow MA \cup PJ$
  $Int \leftarrow Int \cap \bigcap_{P \in PJ} P$
  $Rad \leftarrow Rad \cap$ (zeroRadical$(J) \cap \mathbb{K}[X]$)
end while
return MA, Rad

zeroMinAss

zeroMinAss(I)

Input: a zero-dimensional ideal $I = \langle f_1, \ldots, f_k \rangle \subset \mathbb{K}[X]$ $(char(\mathbb{K}) = 0)$
Output: $\mathrm{minAss}(I)$
result $\leftarrow \emptyset$
choose a random $\underline{a} \in \mathbb{K}^{n-1}$ and $I' \leftarrow \varphi_{\underline{a}}(I)$ $(\varphi_{\underline{a}}(x_i) = x_i$ for $i < n$,
$\varphi_{\underline{a}}(x_n) = x_n + \sum_{i=1}^{n-1} a_i x_i)$
compute the reduced Gröbner basis G of I' w.r.t. $<_{lex}$
factorize $g = g_1^{m_1} \ldots g_s^{m_s} \in G \cap \mathbb{K}[x_n]$
For $i = 1$ to s
  $P_i' \leftarrow$ primaryTest$(\langle I', g_i \rangle)$
  If $P_i' \neq \langle 0 \rangle$
    $P_i \leftarrow \varphi_{\underline{a}}^{-1}(P_i')$
    result $\leftarrow$ result $\cup \{P_i\}$
  Else
    result $\leftarrow$ result $\cup$ zeroMinAss$(\langle I, \varphi_{\underline{a}}^{-1}(g_i) \rangle)$
  EndIf
EndFor Return result

- Coordinate changes are performed to make ideals in general position.
- zeroMinAss contains factorizations of polynomials.

CRT for Laplagne's Algorithm

- Laplagne's algorithm contains zeroMinAss.
- zeroMinAss contains factorizations of polynomials.
- In many cases, a factorization over $\mathbb{F}_p$ produces more factors than over $\mathbb{Q}$.
- Laplagne's algorithm regards some variables $U \subset X$ as parameters.
- We utilize mappings: $\mathbb{K}[u] \to \mathbb{K}$ $(u \in U)$ recursively.
- These mappings reduce the number of parameters and keep the characteristic of coefficient fields 0.

Chinese Remainder Theorem

Let R be a commutative ring and $I_1, \ldots, I_s$ pairwise comaximal ideals in R. For $r_1, \ldots, r_s \in R$, there exists $y \in R$ satisfying

$$\begin{aligned} y &\equiv r_1 \bmod I_1 \\ &\vdots \\ y &\equiv r_s \bmod I_s. \end{aligned}$$

y is unique modulo $\cap_{i=1}^{s} I_i$.

CRT can be applied in two typical situations: $R = \mathbb{Z}$ or $R = \mathbb{K}[u]$.

Lagrange's Interpolation in $\mathbb{Z}$

Let $p_1, \ldots, p_s$ be distinct prime numbers from each other, $p = p_1 \cdots p_s$ and $I_1 = \langle p_1 \rangle, \ldots, I_s = \langle p_s \rangle$. Then for $1 \leq i \leq s$, $a_i, b_i \in \mathbb{Z}$ such that

$$a_i(p/p_i) + b_i p_i = 1$$

can be computed by the extended Euclidean algorithm. For any $r_1, \ldots, r_s \in \mathbb{Z}$, the unique y satisfying conditions in CRT is given by

$$y = r_1 L_1 + \cdots + r_s L_s (\text{where } L_i = a_i(p/p_i)).$$

Lagrange's Interpolation in $\mathbb{K}[u]$

Let $k_1, \ldots, k_s \in \mathbb{K}$ be distinct elements from each other, $I_1 = \langle u - k_1 \rangle, \ldots, I_s = \langle u - k_s \rangle$ and

$$L_i = \frac{(u - k_1) \cdots (u - k_{i-1})(u - k_{i+1}) \cdots (u - k_s)}{(k_i - k_1) \cdots (k_i - k_{i-1})(k_i - k_{i+1}) \cdots (k_i - k_s)}.$$

Then the unique y satisfying conditions in CRT is given by

$$y = r_1 L_1 + \cdots + r_s L_s.$$

CRT

Let $r_1, r_2 \in \mathbb{K}[u]$, I_1, I_2 comaximal ideals $\in \mathbb{K}[u]$.

- We name the interpolation $r_1 \pmod{I_1}$ and $r_2 \pmod{I_2}$ $\mathrm{CRT}(r_1, r_2, I_1, I_2)$.
- For $f = \sum_\alpha c_\alpha x^\alpha, g = \sum_\alpha d_\alpha x^\alpha \in \mathbb{K}[u][X]$, we define $\mathrm{CRT}(f, g, I_1, I_2) = \sum_\alpha \mathrm{CRT}(c_\alpha, d_\alpha, I_1, I_2) x^\alpha$.
- For $F = \{ f_1, \ldots, f_s \}$, $G = \{ g_1, \ldots, g_s \} \subset \mathbb{K}[u][X]$ where $LM(f_i)$'s and $LM(g_i)$'s are distinct respectively and $LM(f_i) = LM(g_i)$, we define $\mathrm{CRT}(F, G, I_1, I_2) = \{ \mathrm{CRT}(f_i, g_i, I_1, I_2) \mid 1 \leq i \leq s \}$.
- For $\mathcal{F} = \{ F_1, \ldots, F_t \}$ and $\mathcal{G} = \{ G_1, \ldots, G_t \}$ where $\mathrm{CRT}(F_i, G_i, I_1, I_2)$'s are defined, we define $\mathrm{CRT}(\mathcal{F}, \mathcal{G}, I_1, I_2) = \{ \mathrm{CRT}(F_i, G_i, I_1, I_2) \mid 1 \leq i \leq t \}$.

Rational function reconstruction

Our target is the reduced Gröbner basis G of a minimal associated prime of an ideal I over $\mathbb{K}(u)$. If we apply CRT for the modular images computed over $\mathbb{K}$, what we obtain is an object G' over $\mathbb{K}[u]$. If a coefficient $c(u)$ appearing in G is not a polynomial we have to recover $c(u)$ from the corresponding polynomial coefficient in G'.

Theorem (Gathen-Gerhard (2003))

Let $f, M \in \mathbb{K}[x]$, $\deg(f) < \deg(M) = n > 0$ and $r_i, s_i, t_i \in \mathbb{K}[x]$ be the j-th row in extended Euclidean Algorithm for M, f ,where j is minimal such that $\deg(r_j) < k$. There exist polynomials $r, t \in \mathbb{K}[x]$ satisfying

$$r \equiv tf \pmod{M},\ \deg(r) < k,\ \deg(t) \leq n - k,$$

namely $r = r_j$, $t = t_j$. If in addition $\gcd(r_j, t_j) = 1$, then r, t also satisfy

$$\gcd(t, M) = 1, rt^{-1} \equiv f \pmod{M},\ \deg(r) < k,\ \deg(t) \leq n - k$$

Algorithm for rational function reconstruction

$\mathrm{RFR}(f, M)$

Input: polynomials $f, M \in \mathbb{K}[x]$

Output: $g, h \in \mathbb{K}[x]$ s.t. $f \equiv g/h \pmod{M}$,
h is monic and $\gcd(g, h) = 1$

$r_0 \leftarrow M$, $r_1 \leftarrow f$

$t_0 \leftarrow 0$, $t_1 \leftarrow 1$

$i \leftarrow 1$

While $2\deg(r_i) > \deg(M)$

  $R_i \leftarrow \mathrm{NF} r_{i-1}, \{r_i\}$

  $Q \leftarrow (r_{i-1} - R_i)/r_i$

  $r_{i+1} \leftarrow R_i$, $t_{i+1} \leftarrow t_{i-1} - Qt_i$

  $i \leftarrow i + 1$

EndWhile

Return (r_i, t_i)

RFR

We also utilize the algorithm RFR for reconstructing coefficients of polynomials, ideals and a set of ideals.
Let $\langle M \rangle = \cap_i \langle u - k_i \rangle (k_i \in \mathbb{K}) \in \mathbb{K}[u]$.

- For $f = \sum_\alpha c_\alpha x^\alpha \in \mathbb{K}[u][X]$, we denote $\mathrm{RFR}(f, M)$ $= \sum_\alpha \mathrm{RFR}(c_\alpha, M) x^\alpha$.
- For $F \subset \mathbb{K}[u][X]$, we define $\mathrm{RFR}(F, M)$ $= \{ \mathrm{RFR}(f, M) \mid f \in F \}$.
- For $\mathcal{F} = \{ F_1, \ldots, F_s \}$ where $\mathrm{RFR}(F_i, M)$'s are defined, we define $\mathrm{RFR}(\mathcal{F}, M) = \{ \mathrm{RFR}(F, M) \mid F \in \mathcal{F} \}$.

Remark

- When we reconstruct $\frac{g(u)}{h(u)} \in \mathbb{K}(u)$ $(\gcd(g,h)=1)$ from $f(u) \in \mathbb{K}[u]$ by RFR, we need more than $\deg(g)+\deg(h)$ ideals $\langle u-k_i \rangle$ $(k_i \in \mathbb{K}$ and $h(k_i) \neq 0)$.
- We say that the output of RFR is **stable** if we have more than $\deg(g)+\deg(h)$ ideals.
- We say that the output is **pseudo stable** if $\mathrm{RFR}(f(u),M) = \mathrm{RFR}(f(u),M')$,where $M = \cap_{i=1}^{r} \langle u-k_i \rangle$, $M' = \cap_{i=1}^{s} \langle u-k_i \rangle$ $(r<s)$.
- We regard the pseudo stable output as a candidate of the unique rational function.

New Algorithm

Luckiness (extensions of Noro-Yokoyama (2016))

Let $u \notin X$ be a variable, F a subset of $\mathbb{K}(u)[X]$, G the reduced Gröbner basis of $\langle F \rangle$ and $k \in \mathbb{K}$, then $\langle u-k \rangle$ is a prime ideal in $\mathbb{K}[u]$.

1. $\mathbb{K}[u]_{(u-k)} := \{\frac{f}{g} | f, g \in \mathbb{K}[u], g(k) \neq 0\}$.
2. $\phi_{(u-k)} : \mathbb{K}(u) \to \mathbb{K}; f \mapsto f(k)$. We denote projection maps $\mathbb{K}[u]_{(u-k)} \to \mathbb{K}$ and $\mathbb{K}[u]_{(u-k)}[X] \to \mathbb{K}[X]$ by the same symbol $\phi_{(u-k)}$ such that $\frac{f}{g} \mapsto \frac{f(k)}{g(k)}$ and $\sum_\alpha c_\alpha x^\alpha \mapsto \sum_\alpha \phi_{(u-k)}(c_\alpha) x^\alpha$ (c_α is the coefficient of $c_\alpha x^\alpha$).
3. $I_{(u-k)}(F) := \langle \phi_{(u-k)}(f) | f \in F \rangle$.
4. $\langle u-k \rangle$ is said to be **weak permissible** for F if $F \subset \mathbb{K}[u]_{(u-k)}$. $\langle u-k \rangle$ is said to be **permissible** for F if $\langle u-k \rangle$ is weak permissible for F and $\phi_{(u-k)}(LC(f)) \neq 0$ for all $f \in F$
5. Let $\sqrt{\langle G \rangle} = \cap_{i=1}^m P_i$ be the prime decomposition and G_i the reduced Gröbner basis of P_i. $\langle u-k \rangle$ is said to be **effectively minass lucky** for G if $\langle u-k \rangle$ is permissible for G and G_i ($i = 1, \ldots, m$), $\sqrt{I_{(u-k)}(G)} = \cap_{i=1}^m Q_i$ is the prime decomposition and $\phi_{(u-k)}(G_i)$ is the reduced Gröbner basis of Q_i.

Fundamental lemmas

Lemma

Let G be a Gröbner basis (respectively the reduced Gröbner basis) of $I \subset \mathbb{K}(u)[X]$ $(u \notin X)$. If an ideal $\langle u-k \rangle$ is permissible for G, then $\phi_{(u-k)}(G)$ is a Gröbner basis (respectively the reduced Gröbner basis) of $I_{(u-k)}(G)$.

Lemma

Let $u \notin X$ be a parameter, $I \subset \mathbb{K}(u)[X]$ an ideal and $G = \{g_1, \ldots, g_m\}$ the reduced Gröbner basis of I. If $k \in \mathbb{K}$, $\langle u-k \rangle$ is permissible for G and $I_{(u-k)}(G)$ is a prime ideal in $\mathbb{K}[X]$, then I is a prime ideal in $\mathbb{K}(u)[X]$.

Lemma

Let P, Q be ideals in $\mathbb{K}(u)[X]$, $G = \{g_1, \ldots, g_s\}$ the reduced Gröbner basis of P, $H = \{h_1, \ldots, h_r\}$ the reduced Gröbner basis of Q. If $k \in \mathbb{K}$ and $\langle u-k \rangle$ is permissible for G, H and $\langle \phi_{(u-k)}(G) \rangle \not\subset \langle \phi_{(u-k)}(H) \rangle$, then $P \not\subset Q$.

New algorithm

modZeroMinAss(G, U)

Input: G a Gröbner basis of a zero-dimensional ideal in $\mathbb{Q}(U)[X]$,
U a set of parameters

Output: a subset P of $\mathrm{minAss}(\langle G \rangle) = \{P_1, \ldots, P_m\}$ such that
$P = \{\, P_i \mid j \neq i \Rightarrow LM(P_j) \neq LM(P_i) \,\}$

If $U = \emptyset$
  $MA \leftarrow$ zeroMinAss$(\langle G \rangle)$
  $GB' \leftarrow \{$ the reduced Gröbner basis of $I \mid I \in MA \,\}$
  $GB \leftarrow GB' \setminus \{\, G_i \in GB' \mid j(\neq i)$ exists s.t. $LM(G_i) = LM(G_j) \,\}$
  Return $\{\, \langle G_i \rangle \mid G_i \in GB \,\}$
EndIf
$M \leftarrow 1$, $Z \leftarrow \emptyset$, $GB \leftarrow \emptyset$, $GB_R \leftarrow \emptyset$
$u \leftarrow$ an element of U

Continued on next page.

New algorithm

modZeroMinAss(G, U)

Loop
  choose $z \in \mathbb{Z} \setminus Z$ s.t. $\langle u - z \rangle$ is effectively minass lucky for G
  $Z \leftarrow Z \cup \{z\}$, $m \leftarrow u - z$
  $MA \leftarrow \text{modZeroMinAss}(\phi_{(u-z)}(G), U \setminus \{u\})$
  If $MA = \emptyset$
    Return $\emptyset$
  EndIf
  $GB' \leftarrow \{$ the reduced Gröbner basis of $I \mid I \in MA \}$
  If $GB \neq \emptyset$
    $GB' \leftarrow \mathrm{CRT}(GB, GB', \langle M \rangle, \langle m \rangle)$
  EndIf
  $GB'_R \leftarrow \mathrm{RFR}(GB', mM)$
  If $GB_R = GB'_R$
    If for all $G_i \in GB_R$, $\langle G_i \rangle \supset \langle G \rangle$
      Return $P = \{ \langle G_i \rangle \mid G_i \in GB_R \}$
    EndIf
  EndIf
  $M \leftarrow mM$, $GB \leftarrow GB'$, $GB_R \leftarrow GB'_R$
EndLoop

Correctness and Termination of modZeroMinAss

- If $U = \emptyset$ then the algorithm simply calls zeroMinAss.
- Assume that the algorithm terminates and outputs a correct result in the case $\#U = s$. Suppose $\#U = s + 1$.
- Let $G_1, \ldots, G_m$ be the reduced Gröbner bases of $\mathrm{minAss}(\langle G \rangle)$ and $\{ G_{i_1}, \ldots, G_{i_k} \} = \{ G_i \mid j \neq i \Rightarrow LM(G_j) \neq LM(G_i) \}$.
- $\mathrm{minAss}(\langle \phi_{(u-z)}(G) \rangle) = \{ \langle \phi_{(u-z)}(G_1) \rangle, \ldots, \langle \phi_{(u-z)}(G_m) \rangle \}$ and $LM(G_i) = LM(\phi_{(u-z)}(G_i))$.
- $GB' = \{ \phi_{(u-z)}(G_{i_1}), \ldots, \phi_{(u-z)}(G_{i_k}) \}$ and for each $H \in GB'$ there exists the unique element G_i such that $LM(H) = LM(G_i)$.
- GB_R will be eventually the set $\{ \langle G_{i_1} \rangle, \ldots, \langle G_{i_k} \rangle \}$ after sufficient interpolations.
- In this case, for all $G_i \in GB_R$, $\langle G_i \rangle \supset \langle G \rangle$. (termination)
- When the algorithm terminates, $P_i \in P$ is a prime ideal in $\mathbb{Q}(U)[X]$ and $P_i \supset \langle G \rangle$. $\sqrt{P_i} = P_i \supset \sqrt{\langle G \rangle} = \cap_{i=1}^{m} \langle G_i \rangle$, which implies that $P_i \supset \langle G_j \rangle$ for some j.
- Since $\langle G \rangle$ is zero-dimensional $\langle G_j \rangle$ is maximal and $P_i = \langle G_j \rangle$. (correctness)

Remark

- The output P has no redundant components.
- Depending on the input, some components of GB' can have the same leading monomial set. In such a case, we can not determine which pair of ideals we should interpolate. Therefore we do not perform interpolations for such components.
- In practical use, we cannot decide whether a moduli $\langle u - z \rangle$ is effectively minass lucky during the computation. Therefore the result can be a noise for our modular algorithm. However, even if we do not assume the effective minass luckiness of moduli, if the algorithm terminates then the result is a subset of $\mathrm{minAss}(\langle G \rangle)$.

Modular Algorithm for Laplagne's Algorithm

Utilizing modZeroMinAss instead of zeroMinAss, we can compute $\mathrm{minAss}(I)$ for $I \subset \mathbb{Q}[X]$.

modLMinAss(I)

Input: an ideal $I \subset \mathbb{Q}[X]$
Output: $\mathrm{minAss}(I)$
Int $\leftarrow \langle 1 \rangle$, MA $\leftarrow \emptyset$
While Int $\setminus \sqrt{I} \neq \emptyset$
  choose $g \in$ Int $\setminus \sqrt{I}$
  $U \leftarrow$ a maximal independent set of $I : g^\infty$
  $G \leftarrow$ a Gröbner basis of $I : g^\infty$ in $\mathbb{Q}(U)[X \setminus U]$
  $P \leftarrow$ modZeroMinAss(G, U)
  If $P = \emptyset$
    $P \leftarrow$ zeroMinAss$(\langle G \rangle)$
  EndIf
  $PG \leftarrow \{P_i \cap \mathbb{Q}[X] \mid P_i \in P\}$
  MA $\leftarrow$ MA$\cup PG$, Int $\leftarrow$ Int $\cap \bigcap_{P \in PG} P$
EndWhile
Return MA

Existance of minass lucky moduli

- We suppose all $\langle u - z \rangle$ are effectively minass lucky. In general, we can not decide whether an ideal is effectively minass lucky or not while the computation.
- We show that there are sufficiently many effectively minass lucky ideals.

Let G be the reduced Gröbner basis of a zero-dimensional ideal $I \subset \mathbb{K}(u)[X]$, $\sqrt{\langle G \rangle} = \cap_{i=1}^{m} P_i$ the prime decomposition, G_i the reduced Gröbner basis of P_i. If $\langle u - k \rangle$ is permissible for G and G_i's, then

- $\phi_{(u-k)}(G)$ and $\phi_{(u-k)}(G_i)$'s are Gröbner basis of $\langle \phi_{(u-k)}(G) \rangle$ and $\langle \phi_{(u-k)}(G_i) \rangle$'s respectively.
- $\langle \phi_{(u-k)}(G) \rangle$ and $\langle \phi_{(u-k)}(G_i) \rangle$'s are zero-dimensional.

For simplicity, we assume that I is in general position with respect to x_n.

Conditions for effectively minass lucky

Set

$$NP = \{k \in \mathbb{K} \mid \langle u-k \rangle \text{ is not permissible for } G \text{ or some } G_i\}.$$

A modulus $\langle u-k \rangle$ is effectively minass lucky for G if the following four conditions hold.

1. $k \notin NP$.
2. $\sqrt{I_{(u-k)}(G)} = I_{(u-k)}(G_1) \cap \cdots \cap I_{(u-k)}(G_m)$.
3. If $i \neq j$, then $I_{(u-k)}(G_i) \neq I_{(u-k)}(G_j)$.
4. Each $I_{(u-k)}(G_i)$ is prime.

$\sqrt{I_{(u-k)}(G)} = I_{(u-k)}(G_1) \cap \cdots \cap I_{(u-k)}(G_m)$

Lemma

Let $G \subset \mathbb{K}(u)[X]$ be the reduced Gröbner basis of a zero-dimensional ideal $\langle G \rangle$ and $H \subset \mathbb{K}(u)[X]$ the reduced Gröbner basis of $\sqrt{\langle G \rangle}$. Except for a finite number of $k \in \mathbb{K} \setminus NP$, $\sqrt{I_{(u-k)}(G)} = I_{(u-k)}(H)$.

- If $\langle u - k \rangle$ is permissible for G, H, then $\sqrt{I_{(u-k)}(H)} = \sqrt{I_{(u-k)}(G)}$..
- For each $x_i \in X$ there exists a univariate square-free polynomial $f_i(x_i) \in \langle H \rangle$ and $r_i(u) = \text{resultant}_{x_i}(f_i, f_i') \neq 0$.
- If $\langle u - k \rangle$ is permissible for $f_i(x_i)$ and $r_i(k) \neq 0$ for all i, then $\phi_{(u-k)}(f_i) \in I_{(u-k)}(H)$ is square-free and $I_{(u-k)}(H)$ is radical.

$\sqrt{I_{(u-k)}(G)} = I_{(u-k)}(G_1) \cap \cdots \cap I_{(u-k)}(G_m)$

Proposition

Except for a finite number of $k \in \mathbb{K} \setminus NP$,
$\sqrt{I_{(u-k)}(G)} = I_{(u-k)}(G_1) \cap \cdots \cap I_{(u-k)}(G_m)$.

- $\tilde{I} = \langle 1 - (t_1 + \cdots + t_m), t_1 G_1, \ldots, t_m G_m \rangle \subset \mathbb{K}(u)[t_1, \ldots, t_m, X]$ $(t_i > X)$.
- Let $\tilde{H}$ be the reduced Gröbner basis of $\tilde{I}$.
- If $\langle u - k \rangle$ is permissible for all intermediate polynomials appearing during the execution of Buchberger's algorithm for computing $\tilde{H}$, then the reduced Gröbner basis of $\langle 1 - (t_1 + \cdots + t_m), t_1 \phi_{(u-k)}(G_1), \ldots, t_m \phi_{(u-k)}(G_m) \rangle$ is $\phi_{(u-k)}(\tilde{H})$.
- $\phi_{(u-k)}(\tilde{H}) \cap \mathbb{K}[X] = \phi_{(u-k)}(H)$ and $\phi_{(u-k)}(H)$ is the reduced Gröbner basis of $I_{(u-k)}(G_1) \cap \cdots \cap I_{(u-k)}(G_m)$.

If $i \neq j$, then $I_{(u-k)}(G_i) \neq I_{(u-k)}(G_j)$.

Proposition

Except for a finite number of $k \in \mathbb{K} \setminus NP$, $I_{(u-k)}(G_i)$'s are distinct.

- $1 \in \langle G_i \rangle + \langle G_j \rangle$.
- If $\langle u - k \rangle$ is permissible for G_i, G_j and all the coefficients in the generating relation of 1, then $1 \in I_{(u-k)}(G_i) + I_{(u-k)}(G_j)$,

Each $I_{(u-k)}(G_i)$ is prime.

Proposition (Zippel (1993))

Let $F(X_1, \ldots, X_n, Y_1, \ldots, Y_m)$ be an irreducible polynomial over $\mathbb{Q}$ and let $R(N)$ denote the number of integer x_i with $|x_i| < N$ such that $F(x_1, \ldots, x_n, Y_1, \ldots, Y_m)$ is reducible. Then

$$R(N) < cN^{n-1/2} \log N$$

where c depends only on the degree of F.

Proposition

Set $N_i = \{k \in \mathbb{Z} \mid |k| < N, k \notin NP, I_{(u-k)}(G_i)$ is not prime$\}$. Then $\#N_i \leq cN^{1/2} \log N$ for a constant c.

- $G_i = \langle x_1 - c_1, \ldots, x_{n-1} - c_{n-1}, g_i(x_n) \rangle$, $c_1, \ldots, c_{n-1}, g_i(x_n) \in \mathbb{Q}(u)[x_n]$ and $g_i(x_n)$ is irreducible over $\mathbb{Q}(u)$
- $g_i(x_n)$ can be written as $g_i(x_n) = \tilde{g}(u, u_1, \ldots, u_l, x_n)/d(u, u_1, \ldots, u_l)$
- $\tilde{g}$ is irreducible over $\mathbb{Q}$.
- The irreducibility of $\phi_{(u-k)}(g_i(x_n))$ is equivalent to that of $\tilde{g}(k, u_1, \ldots, u_l, x_n)$

Probability of effectively minass lucky

Theorem

Set $NEML = \{k \in \mathbb{Z} \mid |k| < N, k \notin NP, \langle u-k \rangle$ is not effectively minass lucky for G$\}$. Then there exist constants c_1, c_2 such that $\#(NP \cup NEML) \leq c_1 + c_2 N^{1/2} \log N$.

- $BAD_2 = \{k \in \mathbb{K} \setminus NP \mid \sqrt{I_{(u-k)}(G)} \neq I_{(u-k)}(G_1) \cap \cdots \cap I_{(u-k)}(G_m)\}$
- $BAD_3 = \{k \in \mathbb{K} \setminus NP \mid I_{(u-k)}(G_i) = I_{(u-k)}(G_j)$ for some $i, j (i \neq j)\}$
- $\#(NP \cup NEML) \leq (\#NP + \#BAD_2 + \#BAD_3) + (mc) N^{1/2} \log N.$

Corollary

If k is randomly chosen from $\{k \in \mathbb{Z} \mid |k| < N\}$, then the probability that $\langle u-k \rangle$ is effectively minass lucky tends to 1 as $N \to \infty$.

Strategies and improvements

When we choose an unlucky modulus there is a possibility that our algorithm does not terminate. Therefore we should discard unlucky modular images during computations.

strategy

1. Choose $z \in \mathbb{Z} \setminus Z$ such that $\langle u - z \rangle$ is permissible for G.
2. Compute $\textsc{modZeroMinAss}(I_{(u-z_i)}(G))$, classify them by leading monomial sets of their components and perform CRT for the class of largest cardinality.
3. In $\textsc{modZeroMinAss}$, if GB_R is pseudo stable and there are some $G_i \in GB_R$ such that $\langle G_i \rangle \not\supset \langle G \rangle$, then we discard G_i's and return $\{ \langle G_j \rangle \mid G_j \in GB_R, \langle G_j \rangle \supset \langle G \rangle \}$.

Improvements which are not written in the pseudo code.

- Recording the number of moduli for the reconstruction.
- Utilizing modular computations for RFR.
- Preprocessing by $\textsc{simplification}$.

Expelimentations

Experimentations

- All of our algorithms were implemented in SINGULAR.
- We take timings about three kinds of ideals. Timings were measured on a 64-bit Linux machine with Intel Xeon E5-2650 v2, 2.60GHz and 256GB memory.
- We construct examples of ideals from ideals given by Decker-Greuel-Pfister (1999). For $I_i \in \mathbb{Q}[v_1, \ldots, v_n]$ and $I_j \in \mathbb{Q}[u_1, \ldots u_n]$, we set a map

$$\varphi_{u,v} : \mathbb{Q}[u_1, \ldots u_n] \to \mathbb{Q}[v_1, \ldots, v_n]; u_m \mapsto v_m (1 \leq m \leq n)$$

and denote that $I_{i \cap j} = I_i \cap \varphi_{u,v}(I_j)$

Timing data

Table: Timing data of computing minimal associated primes of examples

	$I_{3\cap 8}$	$I_{18\cap 31}$	$I_{18\cap 33}$	$I_{31\cap 33}$	$I_{7\cap 9}$	$I_{7\cap 12}$	$I_{5\cap 23}$	$I_{1\cap 4}$
Variables	3	4			6		8	9
Ours	1.2	34.4	28.4	34.9	54.9	240	5880	812
Laplagne's	$> 4h$	$> 4h$	$> 4h$	$> 4h$	284	87.1	12100	$> 4h$

Table: Timing data of computing radicals of examples

	$I_{3\cap 8}$	$I_{18\cap 31}$	$I_{18\cap 33}$	$I_{31\cap 33}$	$I_{7\cap 9}$	$I_{7\cap 12}$	$I_{5\cap 23}$	$I_{1\cap 4}$
Variables	3	4			6		8	9
Ours	1.01	32.1	25.5	30.7	53.2	122	269	645
Laplagne's	0.95	608	2580	$> 4h$	398	$> 4h$	80.9	$> 4h$

Concluding Remarks

- Our algorithm is fast for some class of ideals and will be a choice when general-purpose algorithms can not decompose ideals in practical time.
- Our algorithm is suitable for parallelizations.
- We need more researches of luckiness and moduli whose modular images of irreducible polynomials keeps their irreducibility.

Reference

- Arnold, E, A; Modular algorithms for computing Gröbner bases. Journal of Symbolic Computation 35. (2000) 403–419.
- Decker, W., Greuel, G,-M., Pfister.; Primary decomposition: Algorithms and comparisons. Algorithmic algebra and number theory, Springer Berlin, Heidelberg, 187-220, (1999).
- Decker, W., Greuel, G,-M., Pfister, G., Schönemann, H.: SINGULAR 4-1-0 — A computer algebra system for polynomial computations. `http://www.singular.uni-kl.de` (2015)
- Gathen, J, V, Z,. Gerhard, J.: Modern Computer Algebra. Cambridge University Press New York, NY, USA. (2003).
- Greuel, G,-M., Pfister, G.: A singular introduction to commutative algebra. (2008).

Reference2

- Idrees, N., Pfister, G., Steidel, S.; Parallelization of modular algorithms. Journal of Symbolic Computation 46 (2011) 672-684
- Kawazoe, T., Noro, M.: Algorithms for computing a primary ideal decomposition without producing intermediate redundant components. Journal of Symbolic Computation 46.10 (2011) 1158–1172
- Laplagne, S.: An algorithm for the computation of the radical of an ideal. Proceedings of the 2006 international symposium on Symbolic and algebraic computation. ACM, (2006)
- Laplagne, S.: Computation of the minimal associated primes. Challenges in Symbolic Computation Software 06271 (2006)
- Noro, M., Yokoyama K.: Usage of Modular Techniques for Efficient Computation of Ideal Operations. Mathematics in Computer Science (2017)
- R, Zippel.: Effective Polynomial Computation. Springer US.