New algorithms for computing primary decomposition of polynomial ideals

Masayuki Noro

Kobe University/JST CREST

Primary decomposition : the GTZ algorithm

Gianni-Trager-Zacharias (GTZ) algorithm [GTZ]

1. Reduction to zero-dimensional cases
   Extract some of maximal dimensional primary components $Q_1, \ldots, Q_k$
2. Computation of a remaining ideal
   Compute $f^s \notin I$ s.t.
   $I = (I : f^s) \cap (I + \langle f^s \rangle), \quad I : f^s = I : f^\infty = Q_1 \cap \cdots \cap Q_k.$
3. Decomposition of the remaining ideal
   Decompose $I + \langle f^s \rangle$.

Primary decomposition : the SY algorithm

Shimoyama-Yokoyama (SY) algorithm[SY]

1. Computation of minimal associated primes
   Compute minimal associated primes $\{P_1, \ldots, P_l\}$ of I.
2. Computation of pseudo primary component and a remaining ideal
   Compute ideals $\tilde{Q}_1, \ldots, \tilde{Q}_l$ and $f_1^{s_1}, \ldots, f_l^{s_l}$ s.t. $\sqrt{\tilde{Q}_i} = P_i$, $I = (\tilde{Q}_1 \cap \cdots \cap \tilde{Q}_l) \cap (I + \langle f_1^{s_1}, \ldots, f_l^{s_l} \rangle)$.
3. Decomposition of pseudo primary components.
   Compute a primary component Q_i and a remaining ideal I'_i s.t. $\tilde{Q}_i = Q_i \cap I'_i$.
4. Decomposition of remaining ideals.
   Decompose I'_i, $I + \langle f_1^{s_1}, \ldots, f_l^{s_l} \rangle$.

Primary decomposition : the EHV algorithm

Eisenbud-Huneke-Vasconcelos (EHV) algorithm [EHV]

1. Computation of all associated primes
   Compute all associated primes of I via Homological algebra.
2. Computation of primary components
   Compute primary components corresponding to the associated primes via localization.

Existing implementations

- Risa/Asir (in `primdec`)

  `primadec(I,V)` : SY

- Macaulay2

  `primaryDecomposition(i)` : SY

  `primaryDecomposition(i,`

  `Strategy => EisenbudHunekeVasconcelos)` : EHV

- Singular (in `primdec.lib`)

  `primdecGTZ(i)` : GTZ

  `primdecSY(i)` : SY

Motivation to develop a new algorithm

We found examples which are hard to be decomposed by existing implementations.

A simple example(SY fails to decompose it.)

$$I = \langle h_1, sh_2, \ldots, sh_9, s^2\rangle = Q \cap R,$$
$$Q = \langle h_1, s\rangle,\ R = \langle h_2, \ldots, h_9, s^2\rangle,\ h_1, \ldots, h_9 \in \mathbb{Q}[u_1, u_2, u_3, u_4].$$

We can confirm that

$$R = I + J \text{ for } J = \langle h_2, \ldots, h_9\rangle$$
$$I : Q = \langle S\rangle,\ S = \{h_2, \ldots, h_9, s\}.$$

We observed that $J = \langle S \setminus Q\rangle$

$\Rightarrow$ The first step toward our new algorithm

Outline of the new method

A modification of the SY algorithm

1. The isolated primary components are first computed.
   We only keep Q_i extracted from $\tilde{Q}_i$. (We do not use I'.)
   Let $Q_1, \ldots, Q_l$ be the isolated primary components of I.
2. Computation of a large separating ideal
   Separating ideal : an ideal J s.t. $I = Q \cap (I + J)$ for
   $Q = Q_1 \cap \cdots \cap Q_l$
   We find J as a subset of $I : Q$.
3. Decompose $I + J$.

The reason why J should be large

- A small J tends to introduce unnecessary components.
  $J = \langle f^s \rangle$ in GTZ and in SY for I'.
- A successful case
  We succeeded in decomposing an ideal I by enlarging J, keeping $I = Q \cap (I + J)$.
- The reason why $J \subset I : Q$
  $I = Q \cap (I + J)$ implies $J \subset I : Q$.

Separating ideal

Separating ideal

For $I \subset Q$ we call an ideal J a separating ideal for (I, Q) if $J \not\subset I, I + J \neq k[X]$ and $I = Q \cap (I + J)$.

Lemma

For ideals I, J, Q in $k[X]$, $I \subset Q$ implies $I = Q \cap (I + J) \Leftrightarrow Q \cap J \subset I$.

Proposition

There exists m s.t. $(I : Q)^m \cap Q \subset I$.

Corollary

For any $f \in I : Q$, there exists $m > 0$ s.t. $I = Q \cap (I + \langle f^m \rangle)$.

Primary decomposition : SYC

SYC : Shimoyama-Yokoyama with Colon ideal

Input : an ideal $I \subset k[X]$

Output : an irredundant primary decomposition of I

$L \leftarrow \emptyset$; $Q \leftarrow k[X]$; $I_t \leftarrow I$

while$I_t \neq k[X]$ do ($I = Q \cap I_t$ at this point)

$P_t \leftarrow MinimalAssociatedPrimes(I_t)$

$L_t \leftarrow IsolatedPrimaryComponents(I_t, P_t)$

$Q_t \leftarrow \bigcap_{J \in L_t} J$

if $Q \not\subset Q_t$ then $\{Q \leftarrow Q \cap Q_t; L \leftarrow L \cup L_t\}$

if $Q = I$ break

$J_t = SeparatingIdeal(I_t, Q_t, (I_t : Q_t))$ $(I_t = Q_t \cap (I_t + J_t))$

$I_t \leftarrow I_t + J_t$

end do

return $RemoveRedundancy(L)$

Primary decomposition : SYCA

SYCA : Shimoyama-Yokoyama with Colon ideal (Absolute)

Input : an ideal $I_{in} \subset k[X]$

Output : an irredundant primary decomposition of I_{in}

$L_{all} \leftarrow \emptyset$; $Q_{all} \leftarrow k[X]$; $I_t \leftarrow I_{in}$

RESTART: $L \leftarrow \emptyset$; $Q \leftarrow k[X]$; $I \leftarrow I_t$; $C = \{0\}$

while $I_t \neq k[X]$ do ($I_{in} = Q_{all} \cap I$, $I = Q \cap I_t$ at this point)

$P_t \leftarrow MinimalAssociatedPrimes(I_t)$

$L_t \leftarrow IsolatedPrimaryComponents(I_t, P_t)$; $Q_t \leftarrow \bigcap_{J \in L_t} J$

if $Q \subset Q_t$ goto RESTART else $Q \leftarrow Q \cap Q_t$

if $Q_{all} \not\subset Q_t$ then $\{ L \leftarrow L \cup L_t;\ Q_{all} \leftarrow Q_{all} \cap Q_t;\ L_{all} \leftarrow L_{all} \cup L_t \}$

if $Q_t = I_t$ or $Q = I$ or $Q_{all} = I_{in}$ break

if $I : Q = C$ goto RESTART

else $\{J \leftarrow SeparatingIdeal(I, Q, (I : Q));\ I_t \leftarrow I + J;\ C \leftarrow I : Q\}$

end do

return $RemoveRedundancy(L_{all})$

$SeparatingIdeal(I, Q, C)$

$SeparatingIdeal(I, Q, C)$

Input : $I \subset k[X]$, $Q = \cap_{i=1}^{r} Q_i$, $C = I : Q$

(all isolated components appear in $\{Q_1, \ldots, Q_r\}$)

Output : a separating ideal J for (I, Q)

$G \leftarrow$ a Gröbner basis of $I : Q$

$H = \{h_1, \ldots, h_k\} \leftarrow G \setminus \sqrt{I}$

$S_0 \leftarrow$a generating set of a separating ideal for (I, Q)

(computed from H)

return $\langle S_0 \rangle$

Computation of S_0

Partial search (search the first largest contiguous block)

$S_0 \leftarrow \emptyset$

for $i = 1$ to k do

  $m \leftarrow$ the smallest integer s.t. $Q \cap (I + \langle h_i^m \rangle) = I$

  if $(I + \langle S_0 \cup \{h_i^m\} \rangle) \cap Q \neq I$ break

  $S_0 \leftarrow S_0 \cup \{h_i^m\}$

end do

Full search

$S \leftarrow \{h_i^{m_i} \mid m_i$ is the smallest integer s.t. $Q \cap (I + \langle h_i^{m_i} \rangle) = I\ \}$

$l \leftarrow$the largest index l s.t. $Q \cap (I + \{h_1^{m_1}, \ldots, h_l^{m_l}\}) = I$ (binary search)

$S_0 \leftarrow \{h_1^{m_1}, \ldots, h_l^{m_l}\})$

for $i = l + 1$ to k do

  if $(I + \langle S_0 \cup \{h_i^{m_i}\} \rangle) \cap Q = I$

  $S_0 \leftarrow S_0 \cup \{h_i^{m_i}\}$

end do

Experiments

Primary decomposition of ideals with many embedded components

- Ideals related to computation of local b-functions [NN]
- Ideals generated by adjacent minors [DES]
  For an $m \times n$ matrix $X = (x_{ij})$, primary decomposition of the ideal $A_{k,m,n}$ generated by adjacent $k \times k$-minors of X has been investigated by several authors.

These are examples which are hard to decompose by existing algorithms.

Results

Q_i : isolated components, R_i : embedded components

- ideals related to b-function

  $\mathrm{disc} f_k$: A_k singularity, g_k : D_k singularity

$$
\begin{aligned}
I_1 &= J_{\mathrm{disc}(f_4)} + \langle s^2 \rangle = Q_1 \cap R_1, \\
I_2 &= J_{\mathrm{disc}(f_5)} + \langle s^3 \rangle = Q_1 \cap R_1 \cap R_2, \\
I_3 &= J_{g_5} + \langle s^4 \rangle = Q_1 \cap R_1 \cap R_2 \cap R_3 \cap R_4,
\end{aligned}
$$

- Adjacent minors

Ideal	# Q_i	# R_i
$A_{2,3,4}$	6	3
$A_{2,3,5}$	10	9
$A_{2,3,6}$	18	23
$A_{2,3,7}$	32	56
$A_{2,3,8}$	57	131

Ideal	# Q_i	# R_i
$A_{2,4,4}$	15	17
$A_{2,4,5}$	35	61

Computation by existing implementations

- I_1
  EHV in Macaulay2 and GTZ in Singular succeed.
  All SY fail to decompose I_1.
- I_2, I_3
  All existing implementations fail to decompose I_2 and I_3.
- $A_{2,3,5}$
  21 hours by SY in Macaulay2
- $A_{2,3,n}$ $(n \geq 6)$, $A_{2,4,4}$, $A_{2,4,5}$
  It seems impossible.
  ($A_{2,4,4}$ and $A_{2,3,5}$: given in [DES] and [HS] via cellular decomposition.)

Timings : SYC

Ideal	Total	Colon	Sep	#Iso	#Emb
I_1	0.05	0	0.01	1	1(1)
I_2	0.6	0.03	0.1	1	2(2)
I_3	17	0.4	1.5	1	4(12)
$Huneke$	470	210	180	1	4(4)
$A_{2,3,4}$	13	5	5	6	3(23)
$A_{2,3,5}$	$>$ 10h	–	–	–	–

#Iso : the number of isolated components.

#Emb : the number of embedded components

(n) : the number of components before removing redundancy

Computation of S_0 : partial search for I_i, full search for $A_{k,m,n}$.

Timings: SYCA

Ideal	Total	Colon	Sep	#Iso	#Emb
I_1	0.08	0.004	0.004	1	1 (1)
I_2	0.9	0.03	0.1	1	2 (2)
I_3	17	0.6	1.7	1	4 (8)
$Huneke$	108	9.8	38	1	4 (4)
$A_{2,3,4}$	0.5	0.03	0.1	6	3(3)
$A_{2,3,5}$	5	0.2	2.3	10	9(9)
$A_{2,3,6}$	133	2.8	48	18	23(23)
$A_{2,3,7}$	3540	25	2090	32	56(56)
$A_{2,3,8}$	146h	284	62h	57	131(131)
$A_{2,4,4}$	31	1.8	15	15	17(21)
$A_{2,4,5}$	12700	102	7800	35	61(68)

Conclusion

- Success for many examples which are hard to decompose

  $I_2, I_3, A_{2,3,6}, A_{2,3,7}, A_{2,3,8}, A_{2,4,5}$

- The number of redundant components are small.

  $A_{2,3,k}$: no redundant components

- Possibility of parallel computation
  - $Q = \langle f_1, \ldots, f_m \rangle \Rightarrow I : Q = \cap_i (I : f_i)$
  - Computation of isolated components
  - Computation of $h_i^{m_i}$ s.t. $(I + \langle h_i^{m_i} \rangle) \cap Q = I$

References

DES P. Diaconis, D. Eisenbud, B. Sturmfels, Lattice walks and primary decomposition. In B. Sagan, R. Stanley eds, Mathematical Essays in Honor of Gian-Carlo Rota, Birkhäuser, 173-194 (1998).

DGP W. Decker, G.-M. Greuel, G. Pfister, Primary decomposition: Algorithms and comparisons. *Algorithmic algebra and number theory*, Springer, 187-220 (1998).

EHV D. Eisenbud, C. Huneke, W. Vasconcelos, Direct methods for primary decomposition. *Invent. Math.* **110**, 207-235 (1992).

GTZ P. Gianni, B. Trager, G. Zacharias, Gröbner basis and primary decomposition of polynomial ideals. *J. Symb. Comp.* **6**, 149-167 (1988).

HS S. Hoşten, J. Shapiro, Primary Decomposition of Lattice Basis Ideals. *J. Symb. Comp.* **29**, 625-639 (2000).

NN K. Nishiyama, M. Noro, Stratification associated with local b-functions. *J. Symb. Comp.* **45**, 462-480 (2010).

O T. Oaku, Algorithms for b-Functions, Restrictions, and Algebraic Local Cohomology Groups of D-Modules. *Advances in Applied Mathematics* **19**, 61-105 (1997).

SY T. Shimoyama, K. Yokoyama, Localization and Primary Decomposition of Polynomial ideals. *J. Symb. Comp.* **22**, 247-277 (1996).