Implementation of Prime Decomposition of Polynomial Ideals over Small Finite Fields

Masayuki Noro
Department of Mathematics, Kobe University, Japan

Kazuhiro Yokoyama
Graduate School of Mathematics, Kyushu University, Japan

1 Outline of the procedure

1.1 Main tools

I : an ideal of $K[X]$, $K = \mathbf{F}_q$, $q < 2^{32}$.

(A) Decomposition by factorization

$\sqrt{\langle I, fg\rangle} = \sqrt{\langle I, f\rangle} \cap \sqrt{\langle I, g\rangle}$

(B) Decomposition by saturation

saturation $I : f^\infty = IR_f \cap R$

$\sqrt{I} = \sqrt{I : f^\infty} \cap \sqrt{\langle I, f\rangle}$.

(C) Extension and contraction

$Y \subset X$, $Z = X \setminus Y$

extension: $I^e = K(Y)[Z]I$

contraction: $J^c = J \cap K[X]$

$I^{ec} = I : f^\infty$ for some $f \in K[X]$

(D) Stability under contraction

J is radical (resp. prime, primary)

$\Rightarrow J^c$ is radical (resp. prime, primary).

(E) Decomposition of 0-dimensional ideals

- Frobenius map ϕ
- Separable closure $\mathrm{sc}(H) = \phi^{-1}(H)$

1.2 Pre-decomposition

$\sqrt{I} = \cap_{i=1}^s \sqrt{I_i}$, where I_i is generated by irreducible polynomials by using (A).

1.3 Reduction to 0-dim. ideals

1. Y = a maximal independent set mod I. $Z = X \setminus Y$, $L = K(Y)$.
2. Compute prime divisors of a 0-dim. ideal I^e by using (E) : $\sqrt{I^e} = \cap_{i=1}^r P_i$.
3. Find f s.t. $I^{ec} = I : f^\infty$, then

$$\sqrt{I} = (\cap_{i=1}^r P_i^c) \cap \sqrt{\langle I, f\rangle}$$

holds by (B) and (C). P_i^c is prime by (D).

4. Decompose $\sqrt{\langle I, f\rangle}$.

I is a proper subset of $\langle I, f\rangle$

$\Rightarrow$ termination is guaranteed.

2 Decomposition of 0-dim. ideals

2.1 Intermediate decomposition

J : a 0-dimensional ideal of $L[Z]$

1. $m_{x_i}(t)$ = the minimal polynomial of $x_i \in Z$ w.r.t. J.
2. Factorize $m_{x_i}(t)$ into irreducible factors over $K(Y)$: $m_{x_i}(t) = \prod_j m_{i,j}(t)^{e_{i,j}}$
3. Compute $J_k = \langle J, m_{1,j_1}, m_{2,j_2}, \ldots, m_{s,j_s}\rangle$ Then $\sqrt{J} = \cap_{k=1}^r \sqrt{J_k}$. The minimal polynomial of x_i w.r.t. J_k is irreducible.

J_k is called an intermediate ideal.

2.2 Prime decomposition of intermediate ideals

H : an intermediate ideal.

1. Separable case

Each minimal polynomial is separable.

$\Rightarrow$ Find a polynomial in generic position and apply (A).

2. Inseparable case

Compute the separable closure $\mathrm{sc}(H)$.

Decomposition of $\sqrt{\mathrm{sc}(H)}$ gives prime divisors of H.

2.3 Separable closure $\mathrm{sc}(H)$

H : inseparable intermediate ideal.

1. $m_{x_i}(t)$: the minimal polynomial of x_i.
2. Find a separable polynomial $\mathrm{sc}(m_{x_i})$ s.t. $m_{x_i}(t) = \mathrm{sc}(m_{x_i})(t^{p^{e_i}})$.

$$\phi : f(x_1, \ldots, x_s) \mapsto f(x_1^{p^{e_1}}, \ldots, x_s^{p^{e_s}})$$

3. $\mathrm{sc}(H) = \phi^{-1}(H)$.
4. $\{P_1, \ldots, P_u\}$: prime divisors of $\mathrm{sc}(H)$ $\Rightarrow \{\sqrt{Q_1}, \ldots, \sqrt{Q_u}\}, Q_k = \sqrt{\phi(P_k)}$ are prime divisors of H.

3 Implementation

3.1 Polynomial factorization

Field extension is often necessary for sufficient evaluation points.

$\Rightarrow$ Primitive root representation for efficient computation over extension fields

3.2 Incremental decomposition

J : a 0-dimensional ideal.

1. $m(x_i)$: the minimal polynomial of x_i.
2. Decompose $\langle J, m_k\rangle$ for each factor m_k of m. $\Rightarrow$ early detection of trivial ones.

3.3 Minimal polynomials

$J \subset L[Z]$: a 0-dimensional ideal.

1. $L = K$ or $L = K(y_1)$

The minimal polynomial is computed via FGLM-type algorithm.

$L = K(y_1) \Rightarrow$ Evaluation, Hensel lifting and Padé approximation.

2. $L = K(y_1, y_2, \ldots)$

Elimination by the Buchberger alg.

3.4 Early termination

1. $P \subset P' \Rightarrow P'$ is redundant
2. If $J = \cap P \subset \sqrt{I}$ then $J = \sqrt{I}$.

3.5 Competitive computation

Minimal polynomial computation by OpenXM.

1. Requests from a client

server1 : FGLM, server2 : Buchberger

2. The result returned first is used.
3. Remaining server is reset immediately.

4 Timings

Timings of `primedec_mod` (in sec)

Risa/Asir on PC (Athlon MP1900+ $\times$ 2)

T_B, T_F, T_C : Minimal poly. comp. by Buchberger, competitive and FGLM

Sing : `minAssGTZ` in Singular 2-0-4

$*$: $>$ 5 minutes

$\mathbf{F}_2$	Dim	T_C	T_F	T_B	Sing
$Logar$	7	12	12	12	20
8_3	5	8.4	8.6	8.4	0.8
P_{4444}	1	1.9	12	1.4	2
P_{666}	1	2.4	4	$*$	20
P_{765}	1	6	6	$*$	24
$Hcyclic(6)$	3	2	2	2	$*$

$Logar$: $2ahi + bh^2 + 2cdj - cei - cgh - deh, ai^2 + 2bhi + 2cfj - cgi + d^2j - dei - dgh - efh, bi^2 + 2dfj - dgi - efi - fgh, f(fj - gi)$.

8_3: $C + cE - eC - E, F - C, E - G, eF + fH + hE - fE - hF - eH, fG - gF, gH + G - hG - H, cH - hC$.

$Hkatsura(n)$ Homogenized katsura-n system: $u_l u - \sum_{i=-n}^n u_i u_{l-i} (l = 0, \cdots, n-1)$, $\sum_{l=-n}^n u_l - u$.

$Hcyclic(n)$ Homogenized Cyclic-n system: $\sum_{i=1}^n \prod_{j=i}^{k+j-1} c_{j \bmod n}\ (k = 1, \ldots, n-1)$, $\prod_{j=1}^n c_j - c^n$.

P_{4444} : $x^8 + x^2 + t, y^8 + y^2 + t, z^8 + z^2 + t, u^8 + u^2 + t$.

P_{666} : $x^{12} + x^2 + t, y^{12} + y^2 + t, z^{12} + z^2 + t$.

$\mathbf{F}_3$	Dim	T_C	T_F	T_B	Sing
$Logar$	7	32	32	32	$*$
8_3	5	1	1	1	0.5
Q_{765}	1	22	22	$*$	$*$
Q_{4321}	2	1	1	3	$*$
$Hkatsura(6)$	1	5	5	5	26
$Hcyclic(6)$	2	2.5	2.5	2.5	$*$

P_{765} : $z^{14} + z^2 + t, y^{12} + z^2y^{10} + z^4y^8 + z^6y^6 + z^8y^4 + z^{10}y^2 + z^{12} + 1, x^{10} + (y^2 + z^2)x^8 + (y^4 + z^2y^2 + z^4)x^6 + (y^6 + z^2y^4 + z^4y^2 + z^6)x^4 + (y^8 + z^2y^6 + z^4y^4 + z^6y^2 + z^8)x^2 + y^{10} + z^2y^8 + z^4y^6 + z^6y^4 + z^8y^2 + z^{10}$.

$P_{12,12,12}$: $x^{12} + x^{10} + x^8 + x^2 + t, y^{12} + y^{10} + y^8 + y^2 + t, z^{12} + z^{10} + z^8 + z^2 + t$.

Q_{765} : $z^{21} + z^3 + t^2, y^{18} + z^3y^{15} + z^6y^{12} + z^9y^9 + z^{12}y^6 + z^{15}y^3 + z^{18} + 1, x^{15} + (y^3 + z^3)x^{12} + (y^6 + z^3y^3 + z^6)x^9 + (y^9 + z^3y^6 + z^6y^3 + z^9)x^6 + (y^{12} + z^3y^9 + z^6y^6 + z^9y^3 + z^{12})x^3 + y^{15} + z^3y^{12} + z^6y^9 + z^9y^6 + z^{12}y^3 + z^{15}$.

Q_{4321} : $z^9 + z^3 + t^2, y^9 + z^3y^6 + z^6y^3 + z^9 + 1, x^6 + (y^3 + z^3)x^3 + y^6 + z^3y^3 + z^6, y^6 + (z^3 + u^3)y^3 + z^6 + u^3z^3 + u^6$.

R_{543} : $z^{25} + z^5 + t^2, y^{20} + z^5y^{15} + z^{10}y^{10} + z^{15}y^5 + z^{20} + 1, x^{15} + (y^5 + z^5)x^{10} + (y^{10} + z^5y^5 + z^{10})x^5 + y^{15} + z^5y^{10} + z^{10}y^5 + z^{15}$.

$\mathbf{F}_{53}$	Dim	T_C	T_F	T_B	Sing
$Logar$	7	92	95	93	32
8_3	5	14	14	14	2
$Hcyclic(6)$	2	39	39	38	$*$
$Hkatsura(6)$	1	22	22	80	$*$
$Hkatsura(7)$	1	238	229	1190	$>$ 1h