New method for the change-of-ordering in Gröbner basis computation

Masayuki Noro

and

Kazuhiro Yokoyama

Institute for Social Information Science

FUJITSU LABORATORIES LTD.

140 Miyamoto, Numazu-shi, Shizuoka, 410-03
JAPAN

(e-mail:{noro,momoko}@iias.flab.fujitsu.co.jp)

Difficulties in Gröbner basis computation

- Explosion of the number of basis elements
- Explosion of terms in basis elements
- Increase of useless pairs
- Coefficient growth of basis elements

New method

Framework — inverse image of a modular Gröbner basis (general trace-lifting) without Gröbner basis check and ideal inclusion check

+

Candidate computation by using modular Gröbner basis elements as templates with Hensel lifting

Compatibility

Definition

p is compatible w.r.t. $F \Leftrightarrow$

$$\phi_p(Id(F) \cap \mathbf{Z}_p[X]) = Id(\phi_p(F))$$

p is permissible for $(F, <) \Leftrightarrow \forall f \in F,\ p \nmid hc_<(f)$

$G \subset Id(F)$ is a p-compatible Gröbner basis candidate of F w.r.t $< \Leftrightarrow p$ is permissible for $(G, <)$ and $\phi_p(G)$ is a Gröbner basis of $Id(\phi_p(F))$ w.r.t. $<$.

- Compatibility $\cdots$ order-independent.
- Checked by two Gröbner basis computation (over $\mathbf{Q}$ and $GF(p)$) w.r.t. any order.
- F is already a Gröbner basis $\Rightarrow$ permissibility implies compatibility.

Main Theorem

p is compatible w.r.t. F and G is a p-compatible candidate $\Rightarrow G$ is a Gröbner basis of F.

Gröbner basis computation with a compatible p

Guess
+
Check (ideal inclusion, Gröbner basis check)

Ordinary trace-lifting

⇓

Finding a compatible p
+
Guess of a p-compatible candidate
Existence ⇒ Correctness

New method

If "Finding a compatible p " is easier than "check"

⇓

Improvement

Candidate computation by Linear Algebra and Hensel Lifting

Direct computation of a Gröbner basis element as an inverse image of the corresponding modular Gröbner basis element.

F : already a Gröbner basis w.r.t. $<_1$

p : a permissible prime for $(F, <_1)$

$\Downarrow$

$\overline{G} \Leftarrow GB_<(\phi_p(F))$

$\Downarrow$

$\overline{G} \ni h \Rightarrow \overline{h}$ (Replace coefficients with undetermined coefficients)

$\Downarrow$

Solve $NF_{<_1}(\overline{h}, F) = 0$ w.r.t. the undetermined coefficients

$\Downarrow$

If the solvings succeed for all the elements of $\overline{G}$, then the obtained polynomials form a p-compatible Gröbner basis candidate.

Solving linear equations

E_h : the linear eqation made from $h \ni \overline{G}$

Properties of E_h

1. E_h is stable w.r.t. p.
2. $\phi_p(E_h)$ has the unique solution h.
3. A subsystem E'_h exists s.t.
   - The number of undetermined coefficients = the number of equations in E'_h
   - E'_h has the unique solution over $\mathbf{Q}$ and $GF(p)$.
   - The solution is stable w.r.t. p.
   - A solution of E_h is a solution of E'_h.

Solving E_h

1. Choose E'_h.
2. $S \leftarrow$ the unique solution of E'_h.
3. If S satisfies E_h then S is the unique solution of E_h, else E_h has no solution.

Solving linear equations by Hensel lifting

Problem 1 *M, B : $n \times n$, $n \times 1$ integer matrix. X : $n \times 1$ matrix with unknown entries. Assuming $det(\phi_p(M)) \neq 0$, solve $MX = B$ over $\mathbf{Q}$.*

Algorithm 2

solve_linear_equation_by_hensel(M, B, p)

$R \leftarrow \phi_p(M)^{-1}$; $c \leftarrow B$; $x \leftarrow 0$; $q \leftarrow 1$; $count \leftarrow 0$

do {

  $t \leftarrow \phi_p^{-1}(R\phi_p(c))$; $x \leftarrow x + qt$; $c \leftarrow (c - Mt)/p$;

  $q \leftarrow qp$; $count \leftarrow count + 1$

  if $count =$ **Predetermined_Constant** *then* {

    $count \leftarrow 0$; $X \leftarrow$ *inttorat*(x, q)

    if $X \neq$ **nil** *then return* X

  }

}

Experiments

Machine ··· Sparc20/61 (89 SPECInt92; 160MB of memory)

Orderings

D the degree reverse lexicographic order

L the lexicographic order

E **D** for the first $n-1$ variables, **L** for the last variable.

Trace-lifting

ItDc **Input** ⇒ **D** by [*tl_guess*() + *tl_check*()]

DtLc **D** ⇒ **L** by [*tl_guess*() + *tl_check*()]

Change-of-ordering by new algorithms

Dt$_h$L **D** ⇒ **L** by *tl_h_guess_dh*()

Dt$_h$EtL [**D** ⇒ **E** by *tl_h_guess_dh*()] + [**E** ⇒ **L** by *tl_guess*()]

DlL **D** ⇒ **L** by *candidate_by_linear_algebra*()

Others

FGLM `totolex()` on `GB (Version 3.940)`.

∞ memory exhaustion, or production of a base with very large coefficients, compared with a successful computation

Comparison of various change-of-ordering algorithms

Eqn	Dt_hL	Dt_hEtL	DIL	FGLM
C_6	24	9	10	24
C_7	1.6days	∞	3137	1.3days†
Mod	291	87	83	731
MK_5	130	50	174	696
K_5	78	27	45	210
K_6	7201	1553	1571	> 11280
K_7	12days‡	1.7days	1.0day	—
$RoseO_1$	16	16	14	647
$RoseO_2$	213	29	61	4711

Parallel execution time in **DIL**

Eqn	C_6	C_7	Mod	MK_5	K_5
DIL	10	3137	83	174	45
DIL-parallel	4.4	688	16	32	10

Eqn	K_6	K_7	$RoseO_1$	$RoseO_2$
DIL	1571	1.0day	15	68
DIL-parallel	286	13939	13	45

†On Sparc10/40 (53 SPECint92)
‡On Sony NEWS5000 (53 SPECint92)

Further applications of Hensel Lifting

- Computation of Generalized Shape Lemma (GSL
  $I \subset \mathbf{Q}[x_1, \cdots, x_n]$ is zero-dimensional and in normal position with respect to x_n
  $\Rightarrow$ Zeros of I are represented in the following form:
  $\{(x_1, \cdots, x_n) | x_i = g_i(x_n)/g_n'(x_n)(i = 1, \cdots, n-1); g_n(x_n) = 0\}$
  $g_i(x_n)(i = 1, \cdots, n)$ can be computed by Hensel construction.
- Computation of minimal polynomials in zero-dimensional ideals.
  For zero-dimensional ideal I, univariate polynomials with respect to each variable with the lowest degree in I (=minimal polynomial) can be computed from the corresponding modular template polynomial.

Conclusion

Omission of Gröbner basis check

- Efficient when results have large integer coefficients.

Candidate computation by linear algebra

- Existence of problems which are hard by Buchberger algorithm
  $\Rightarrow$ [Linear algebra + Hensel lifting] is efficient if modular Gröbner basis and normal forms of terms can be easily computed.
- Parallelization is very easy.
- All the methods, including parallel computation have been implemented on Risa/Asir.

An example : cyclic-5 roots

modulus = 99999989

$c_4^{15} + u_1c_4^{10} + u_2c_4^5 + u_3$
$\Rightarrow$
$21u_1 - u_3 - 2563 = 0 \quad 198u_1 - u_2 - 24278 = 0$
$165u_1 - 20130 = 0 \quad -110u_1 + 13420 = 0$
$55u_1 - 6710 = 0 \quad -55u_1 + 6710 = 0$
$-55u_1 + 6710 = 0 \quad -55u_1 + 6710 = 0 \quad -165u_1 + 20130 = 0$

$(c_4^5 + u_1)c_3^2 + (u_2c_4^{11} + u_3c_4^6 + u_4c_4)c_3 + u_5c_4^{12} + u_6c_4^7 + u_7c_4^2$
$\Rightarrow$
$165u_2 - 288u_5 - 2u_7 = 0$
$-233u_2 - 2u_4 = 0$
$440u_2 - 110u_5 = 0$
$-2u_1 + 55u_2 = 0$
$-165u_2 + 286u_5 - 2u_6 = 0$
$231u_2 - 2u_3 = 0$
$-440u_2 + 110u_5 = 0$
$-55u_2 - 2 = 0$

$c_3^7 + u_1c_4c_3^6 + u_2c_4^2c_3^5 + u_3c_3^2 + (u_4c_4^{11} + u_5c_4^6 + u_6c_4)c_3 + u_7c_4^{12} + u_8c_4^7 + u_9c_4^2$
$\Rightarrow$
$737u_1 - 468u_2 - 1650u_4 + 2880u_7 + 20u_9 - 5703 = 0$
$-193u_1 + 32u_2 + 2330u_4 + 20u_6 - 333 = 0$
$-192u_1 - 492u_2 - 4400u_4 + 1100u_7 - 9932 = 0$
$-110u_1 + 40u_2 + 290 = 0$
$63u_1 - 232u_2 + 20u_3 - 550u_4 - 3917 = 0$
$110u_1 - 40u_2 - 290 = 0$
$580u_1 - 220u_2 - 1520 = 0$
$-580u_1 + 220u_2 + 1520 = 0$
$-470u_1 + 180u_2 + 1230 = 0$
$-377u_1 + 348u_2 + 1650u_4 - 2860u_7 + 20u_8 + 4763 = 0$
$213u_1 - 32u_2 - 2310u_4 + 20u_5 + 333 = 0$
$-858u_1 + 892u_2 + 4400u_4 - 1100u_7 + 12682 = 0$
$987u_1 - 168u_2 + 550u_4 + 1187 = 0$
$110u_1 - 40u_2 - 290 = 0$

$(c_4^5+u_1)c_2+u_2c_4^{11}+u_3c_4^6+u_4c_4$
$\Rightarrow$
$144u_2+u_4=0 \quad u_1+55u_2=0$
$-143u_2+u_3=0 \quad -55u_2+1=0$

$(c_3+u_1c_4)c_2+u_2c_4c_3^6+u_3c_4^2c_3^5+u_4c_4^4c_3^3+u_5c_3^2+(u_6c_4^{11}+u_7c_4^6+u_8c_4)c_3+u_9c_4^{12}+u_{10}c_4^7+u_{11}c_4^2$
$\Rightarrow$
$-737u_2+468u_3+28u_4+1650u_6-2880u_9-20u_{11}=0$
$193u_2-32u_3-8u_4-2330u_6-20u_8=0$
$-20u_1+192u_2+492u_3-96u_4+4400u_6-1100u_9=0$
$110u_2-40u_3=0$
$-63u_2+232u_3+16u_4-20u_5+550u_6=0$
$-110u_2+40u_3-20u_4-20=0$
$-580u_2+220u_3+40u_4=0$
$580u_2-220u_3-40u_4=0$
$470u_2-180u_3-40u_4=0$
$377u_2-348u_3+12u_4-1650u_6+2860u_9-20u_{10}=0$
$-213u_2+32u_3+8u_4+2310u_6-20u_7=0$
$858u_2-892u_3+36u_4-4400u_6+1100u_9=0$
$-987u_2+168u_3+44u_4-550u_6=0$
$-110u_2+40u_3=0$

$c_2^3+u_1c_4c_2^2+u_2c_4^2c_2+u_3c_4^2c_3^6+u_4c_4^3c_3^5+u_5c_4^4c_3^4+u_6c_4c_3^2+(u_7c_4^{12}+u_8c_4^7+u_9c_4^2)c_3+u_{10}c_4^{13}+u_{11}c_4^8+u_{12}c_4^3$
$\Rightarrow$
$-28u_3+14u_4-8u_5-3168u_7+26u_8+26841u_{10}-219u_{11}+u_{12}-2=0$
$18u_3-10u_4+8u_5+13421u_7-109u_8+u_9-5126u_{10}+42u_{11}+2=0$
$u_2-54u_3+27u_4-15u_5-14630u_7+120u_8+2563u_{10}-21u_{11}-3=0$
$-19u_3+9u_4-3u_5+7689u_7-63u_8+22693u_{10}-186u_{11}-3=0$
$54u_3-27u_4+15u_5+u_6+14630u_7-120u_8-2563u_{10}+21u_{11}+3=0$
$11u_3-3u_4-u_5-12441u_7+102u_8-15983u_{10}+131u_{11}+2=0$
$5u_3-3u_4-4147u_7+34u_8+1584u_{10}-13u_{11}+2=0$
$u_1-14u_3+7u_4-3u_5-3168u_7+26u_8-6710u_{10}+55u_{11}-3=0$
$2u_5+3542u_7-29u_8-9273u_{10}+76u_{11}=0$
$8u_3-6u_4+4u_5+4752u_7-39u_8-6710u_{10}+55u_{11}+1=0$
$9u_3-4u_4+4u_5+7315u_7-60u_8+5126u_{10}-42u_{11}+1=0$
$31u_3-16u_4+9u_5+6336u_7-52u_8-20130u_{10}+165u_{11}+2=0$
$-3u_3+3u_4-3u_5-6710u_7+55u_8+2563u_{10}-21u_{11}=0$
$-17u_3+10u_4-8u_5-13420u_7+110u_8+5126u_{10}-42u_{11}-1=0$

$(c_4^5+u_1)c_1+u_2c_4^{11}+u_3c_4^6+u_4c_4$
$\Rightarrow$
$-144u_2-u_4=0 \quad -55u_2+1=0 \quad -u_1-1=0$
$143u_2-u_3=0 \quad 55u_2-1=0$

$(c_3+u_1c_4)c_1+u_2c_4c_3^6+u_3c_4^2c_3^5+u_4c_4^3c_3^4+u_5c_4^4c_3^3+(u_6c_4^{11}+u_7c_4^6+u_8c_4)c_3+u_9c_4^{12}+u_{10}c_4^7+u_{11}c_4^2$
$\Rightarrow$
$-737u_2+468u_3-242u_4+28u_5+1650u_6-2880u_9-20u_{11}=0$
$193u_2-32u_3+14u_4-8u_5-2330u_6-20u_8=0$
$192u_2+492u_3-360u_4-96u_5+4400u_6-1100u_9=0$
$-20u_1+110u_2-40u_3+40u_4=0$
$-63u_2+232u_3-82u_4+16u_5+550u_6=0$
$-110u_2+40u_3-40u_4-20u_5=0$
$-580u_2+220u_3-100u_4+40u_5-20=0$
$580u_2-220u_3+80u_4-40u_5=0$
$470u_2-180u_3+60u_4-40u_5=0$
$377u_2-348u_3+202u_4+12u_5-1650u_6+2860u_9-20u_{10}=0$
$-213u_2+32u_3-14u_4+8u_5+2310u_6-20u_7=0$
$858u_2-892u_3+520u_4+36u_5-4400u_6+1100u_9=0$
$-987u_2+168u_3-78u_4+44u_5-550u_6=0$
$-110u_2+40u_3-20u_4=0$

$(c_2+u_1c_4)c_1+u_2c_2^2+u_3c_4c_2+u_4c_4c_3^6+u_5c_4^2c_3^5+u_6c_4^3c_3^4+u_7c_4^4c_3^3+u_8c_3^2+(u_9c_4^{11}+u_{10}c_4^6+u_{11}c_4)c_3+u_{12}c_4^{12}+u_{13}c_4^7+u_{14}c_4^2$
$\Rightarrow$
$-737u_4+468u_5-242u_6+28u_7+1650u_9-2880u_{12}-20u_{14}=0$
$193u_4-32u_5+14u_6-8u_7-2330u_9-20u_{11}=0$
$-20u_3+192u_4+492u_5-360u_6-96u_7+4400u_9-1100u_{12}=0$
$-20u_1+110u_4-40u_5+40u_6=0$
$-63u_4+232u_5-82u_6+16u_7-20u_8+550u_9=0$
$-110u_4+40u_5-40u_6-20u_7=0$
$-580u_4+220u_5-100u_6+40u_7=0$
$-20u_2+580u_4-220u_5+80u_6-40u_7=0$
$470u_4-180u_5+60u_6-40u_7-20=0$
$377u_4-348u_5+202u_6+12u_7-1650u_9+2860u_{12}-20u_{13}=0$
$-213u_4+32u_5-14u_6+8u_7+2310u_9-20u_{10}=0$
$858u_4-892u_5+520u_6+36u_7-4400u_9+1100u_{12}=0$
$-987u_4+168u_5-78u_6+44u_7-550u_9=0$
$-110u_4+40u_5-20u_6=0$

$c_1^2+u_1c_4c_1+u_2c_4c_3^6+u_3c_4^2c_3^5+u_4c_4^3c_3^4+u_5c_4^4c_3^3+u_6c_3^2+(u_7c_4^{11}+u_8c_4^6+u_9c_4)c_3+u_{10}c_4^{12}+u_{11}c_4^7+u_{12}c_4^2$
$\Rightarrow$
$737u_2-468u_3+242u_4-28u_5-1650u_7+2880u_{10}+20u_{12}-20=0$
$-193u_2+32u_3-14u_4+8u_5+2330u_7+20u_9=0$
$-192u_2-492u_3+360u_4+96u_5-4400u_7+1100u_{10}-20=0$
$20u_1-110u_2+40u_3-40u_4-40=0$
$63u_2-232u_3+82u_4-16u_5+20u_6-550u_7=0$
$110u_2-40u_3+40u_4+20u_5+20=0$
$580u_2-220u_3+100u_4-40u_5-20=0$
$-580u_2+220u_3-80u_4+40u_5=0$
$-470u_2+180u_3-60u_4+40u_5=0$
$-377u_2+348u_3-202u_4-12u_5+1650u_7-2860u_{10}+20u_{11}=0$
$213u_2-32u_3+14u_4-8u_5-2310u_7+20u_8=0$
$-858u_2+892u_3-520u_4-36u_5+4400u_7-1100u_{10}=0$
$987u_2-168u_3+78u_4-44u_5+550u_7=0$
$110u_2-40u_3+20u_4=0$

$c_0+u_1c_1+u_2c_2+u_3c_3+u_4c_4$
$\Rightarrow$
$u_4-1=0 \quad u_3-1=0$
$u_2-1=0 \quad u_1-1=0$

modulus = 11

$c_4^{15}+u_1$

$\Rightarrow$

$-u1+21=0$

$198=0 \quad 165=0$

$-110=0 \quad 55=0$

$-55=0 \quad -55=0$

$-55=0 \quad -165=0$