数理解析研究所講究録
第1843巻 2013年 38-50

グレブナー基底候補の正当性検証について

野呂正行
神戸大学大学院理学研究科
noro@math.kobe-u.ac.jp
横山 和弘
立教大学理学部
kazuhiro@math.kyushu-u.ac.jp

1 はじめに

グレブナー基底計算の効率化技法として, モジュラー計算法がある. これは, 中間計算における係数膨張を押える効果をねらったもので, 近年では, 並列計算と組み合わせることで, 大幅な計算効率が期待されている.

本論文では, モジュラー計算法における重要な要素である, lucky prime とモジュラー計算から正しい基底を求める際の計算の正当性について以下の3点について報告する.

1. 現在知られている方法を統一的に分類し, 計算の正当性がどのように保証されているかを明確にする.
2. 一般の設定では, 効率的な正当性の検証法が確立されていないが, それを構成するためのいくつかの試みを報告する.
3. モジュラー計算の連鎖として, 正当性を効率良く検証できるイデアルの操作を提案する.

ここでは, まずいくつかの概念 (lucky prime) を統一し, それらに対応する正当性検証法を紹介することからはじめていく.

2 問題設定と lucky prime の定義

$\mathbb{Q}$ を有理数体, $\mathbb{Z}$ を整数環とし, $\mathbb{F}_p$ を位数 p の有限体とする. 変数の集合を $X=\{x_1,\ldots,x_n\}$ とし, F を $\mathbb{Q}[X]$ の有限部分集合とする. F で生成される $\mathbb{Q}[X]$ のイデアルを I とする. 素数 p に対して, $\{\frac{a}{b} \mid a,b\in\mathbb{Z}, p\nmid b\}$ を $\mathbb{Z}_p^0$ で表す. $\mathbb{Z}$ から $\mathbb{F}_p$ の canonical projection を ϕ_p であらわす. さらに, ϕ_p を $\mathbb{Z}_p^0$ から $\mathbb{F}_p$ への写像に拡張する. すなわち, $\phi_p(\frac{a}{b})=\phi_p(a)\times\phi_p(b)^{-1}$ となる. 同じ記号で, $\mathbb{Z}_p^0[X]$ から $\mathbb{F}_p[X]$ への projection で多項式の係数に ϕ_p を施す写像を表す. また, $\mathbb{Z}_p^0[X]$ の部分集合 S に対して, $\phi_p(S)$ で $\{\phi_p(f) \mid f\in S\}$ を表す.

以下では, I を F で生成される $\mathbb{Q}[X]$ のイデアルとする. F が $\mathbb{Z}_p^0[X]$ の部分集合となるとき, $I_p(F)$ で $\phi_p(F)$ で生成される $\mathbb{F}_p[X]$ のイデアルを表す. F を固定して考え, 混乱がない場合には, F を略して I_p とも書く. さらに, $I_p^0=\phi_p(I\cap\mathbb{Z}_p^0[X])$ とする. p と互いに素な整数は mod$p$ で可逆であるので, $I_p^0=\phi_p(I\cap\mathbb{Z}[X])$ でもあることに注意する. 一般に

$$I_p(F)\subset I_p^0$$

であり, $I_p(F)$ と I_p^0 が等しくなるとは限らない. G を 順序 $\prec$ に関する I の 簡約グレブナー基底, G_p を 順序 $\prec$ に関する $I_p(F)$ の 簡約グレブナー基底とする.

記号について：環 R でのイデアル生成に関しては, $\langle\rangle_R$ の記号を用いる. 混乱がなければ, 添字の R を略す. ここでは, R として $K[X]$, K は係数体であり $K=\mathbb{Q}$ または $\mathbb{F}_p$, を考える. また, X で生成される係数 1 の単項式全体を T とし, 項順序 $\prec$ に関して, 多項式 $f \in R$ の leading power product (係数 1) を $lp_\prec(f)$, 係数付き先頭項を $ht_\prec(f)$, 先頭係数を $hc_\prec(f)$ とおく. 混乱がなければ, 順序 $\prec$ を略す.

多項式の集合 S に対しては $lp_\prec(S)=\{lp_\prec(f) \mid f \in S\}$, $ht_\prec(S)=\{ht_\prec(f) \mid f \in S\}$, $hc_\prec(S)=\{hc_\prec(f) \mid f \in S\}$ とし, イデアル J の 先頭項より生成されるイデアルを J のイニシャルと呼び, $Init_\prec(J)=\langle ht_\prec(f) \mid f \in J\rangle$ で表す. また, 集合 H に対して, $lp_\prec(H)$ で生成されるイデアルも $Init_\prec(H)$ で表す. 混乱がなければ, 順序 $\prec$ を略す.

I が R の斉次イデアルのとき, Hilbert function を HF_I で表す. (通常は $HF_{R/I}$ と書くが, ここでは [1] の記号を用いる.) 本論文で利用する Hilbert function の性質を以下に上げておく.

Lemma 1 (1) I を斉次イデアルとし, G を I のグレブナー基底とする. このとき, 以下が成り立つ.

$$HF_I = HF_{Init(I)} = HF_{Init(G)}$$

(2) I を斉次イデアルとし, F を I の生成集合とする. また, p を素数とする. このとき, 以下が成り立つ.

$$HF_I \leq HF_{I_p(F)}$$

さらに, 以下が成り立つ.

$$HF_I \leq HF_{I_p^0} \leq HF_{I_p(F)}$$

(3) I, J を斉次イデアルとし, $I \subset J$ とする. このとき, 以下が成り立つ.

$$HF_I \geq HF_J$$

等号が成り立つときは, $I=J$ である.

(1) は Theorem 5.2.6 in [3] である. (2) の前半は Theorem 5.3 in [1] であり, 後半は Exercise 5.1.5 in [3] である. (3) は定義より直接示される.

素数 p の luckyness に関しては, 以下のような定義が提案されている. ([1, 2, 8, 9, 14] を参照)

Definition 1 (lucky prime) F を $\mathbb{Z}_p^0[X]$ の部分集合とする.

(1) 素数 p が F に対して compatible とは, $I_p^0 = I_p(F)$ のときにいう.

(2) 素数 p が F と項順序 $\prec$ に対して lucky とは, I の 簡約グレブナー基底 G と I_p の 簡約グレブナー基底 G_p に対して, $G \subset \mathbb{Z}_p^0[X]$ であって, $\phi_p(G)=G_p$ のときにいう. (簡約を外して, G の各元の 先頭係数が p で割れないとしてもよい)

(3) 素数 p が F と項順序 $\prec$ に対して strongly compatible とは, p が F に対して compatible であり, $\phi_p(Init_\prec(I) \cap \mathbb{Z}_p^0[X]) = Init_\prec(I_p(F))$ のときにいう.

(4) 斉次イデアルの場合に, 素数 p が F に対して Hilbert lucky とは, $HF_I = HF_{I_p(F)}$ のときにいう.

2.1 種々の luckyness の間の関係

これらの "lucky" に関する定義に関して, 次の関係がある.

Lemma 2 以下では F を $\mathbb{Z}_p^0[X]$ の部分集合とする.

(1) F が I のある順序に関するグレブナー基底で, F の元の 先頭係数が p で割れなければ, p は F に対して compatible である.

(2) 素数 p が F と項順序 $\prec$ に対して lucky であれば, 素数 p は F に対して compatible である. すなわち, $I_p(F) = I_p^0$ である.

(3) 素数 p が F と項順序 $\prec$ に対して lucky であることと, strongly compatible であることは同値である.

(4) 斉次イデアルの場合では, 素数 p が F に対して Hilbert lucky であれば, p は F に関して compatible である. (すなわち, $I_p(F) = I_p^0$ である.)

(5) 斉次イデアルの場合では, 素数 p が F と項順序 $\prec$ に対して lucky であれば, 素数 p は F に対して Hilbert lucky である.

定義より, 生成集合 F と項順序 $\prec$ に対して lucky でない素数 (unlucky ともいう) は 簡約グレブナー基底の先頭係数の約数となるため, 有限個である. Lemma 2 より, 斉次多項式の生成集合 F に対して Hilbert lucky でない素数は lucky でない素数となるため, その個数も有限個となる. また, 一般の生成集合 F と項順序 $\prec$ に対して, strong compatible でない素数は lucky でない素数であるので, これも有限個となる. さらに, F に対して compatible でない素数も有限個であることがわかる.

Lemma 3 (lucky prime の個数の有限性) 生成集合 F と項順序 $\prec$ に対して lucky でない素数の個数は有限個である. また, strong compatible でない素数も有限個であり, F に対して compatible でない素数も有限個である. 斉次多項式の生成集合 F に対して Hilbert lucky でない素数も有限個である.

3 種々の正当性判定法

本節では, グレブナー基底候補の正当性判定について, Arnold [1] の結果や Noro-Yokoyama [8] の結果などを合わせて得られる方法, およびそれらが使えない状況での方法について述べる.

グレブナー基底の候補についていくつか定義を与える.

Definition 2 以下では, G_{can} を $I \cap \mathbb{Z}_p^0[X]$ の部分集合とし, $\prec$ を順序とする.

(1) G_{can} が F と項順序 $\prec$ に対する p-Gröbner basis candidate とは G_{can} の各元の $\prec$ に関する先頭係数 p で割れず, $\phi_p(G_{can})$ が $I_p(F)$ の $\prec$ に関するグレブナー基底であるときにいう.

(2) G_{can} がイデアル I と項順序 $\prec$ に対する p-compatible Gröbner basis candidate とは G_{can} の各元の $\prec$ に関する先頭係数は p で割れず, $\phi_p(G_{can})$ が $\phi_p(I \cap \mathbb{Z}_p^0[X])$ の $\prec$ に関するグレブナー基底であるときにいう.

一般には, $I_p(F)$ と I_p^0 は等しくないので, 上の 2 つの定義は異なるものを与える. p-Gröbner basis candidate G_{can} が I のグレブナー基底のときは, p は F と $\prec$ に対して lucky であり, $I_p(F) = I_p^0$ である. (Lemma 2)

modular 計算法で結果を保証するアプローチとして, 大きく以下の 2 つに分類できる.

(1) compatibility と $G_{can} \subset I$ を利用するアプローチ

(2) Hilbert luckyness と $\langle G_{can} \rangle \supset I$ を利用するアプローチ

3.1 compatible 型の結果

Proposition 4 (Theorem 2.6 in [8]) G_{can} が I と $\prec$ に対する p-compatible グレブナー基底であって, $G_{can} \subset I$ ならば, G_{can} は I のグレブナー基底である.

p-compatible Gröbner basis candidate の重要な部分は compatiblity にある. また, これより, G_{can} が自分自身が生成するイデアル $\langle G_{can} \rangle$ のグレブナー基底であることをチェックする必要がない.

Corollary 1 G_{can} が I と $\prec$ に対する p-Gröbner basis candidate であって, $G_{can} \subset I$ とする. このとき, p が comptatible であれば, G_{can} は I のグレブナー基底である.

G_{can} が I の別の順序のグレブナー基底であって, その元の 先頭係数が p で割れなれば, p は compatible であるので, 以下を得る.

Corollary 2 I の別の順序 $\prec'$ に関するグレブナー基底 G' が $\mathbb{Z}_p^0[X]$ の部分集合であり, G' の元の 先頭係数は p で割れないとする. (つまり, p が $\prec'$ と G' に対して lucky とする.) このとき, G_{can} が I と $\prec$ に対する p-Gröbner basis candidate であって, $G_{can} \subset I$ ならば, G_{can} は I のグレブナー基底である.

I の グレブナー基底 G' が分かっているので, $G_{can} \subset I$ の検証は, G_{can} の各元の G' に関する正規形計算で確かめることができる.

3.1.1 応用例

compatibility の応用による syzygy 計算アルゴリズムを示す.

Algorithm 1 (Algorithm 15 in [7])
入力 : $F = (f_1, \ldots, f_s)$, $f_1, \ldots, f_s \in \mathbb{Z}[X]^l$; R^l の項順序 $\prec$
出力 : syz(F) の $(POT, \prec)$ に関するグレブナー基底 S
　　$\langle F \rangle$ の $\prec$ に関するグレブナー基底 $G = (g_1, \ldots, g_t)$
　　${}^tG = C \cdot {}^tF$ を満たす (t, s)-行列 C
$m_i \leftarrow (f_i, e_i) \in R^l \oplus R^s = R^{l+s}$; $M \leftarrow \langle m_1, \ldots, m_s \rangle$
restart:
　　$p \leftarrow m_1, \ldots, m_s$ の $(POT, \prec)$ に関する先頭係数を割らない素数
　　$G_{can} \leftarrow M$ の, $\langle G_{can} \rangle \subset M$ をみたす *p-Gröbner candidate*
　　if G_{can} が存在しない *then goto restart*
$S \leftarrow \{h \in R^s \mid (0, h) \in G_{can}\}$
$G \leftarrow \{g \in R^l \mid g \neq 0$ *and* $(g, h) \in G_{can}$ *for some* $h \in R^s\}$
$C \leftarrow$ 第 i 行が $(g_i, h_i) \in G_{can}$ に対する h_i である (t, s)-行列
return (S, G, C)

このアルゴリズムは, (f_i, e_i) で生成される加群 M のグレブナー基底を, f_i 部分より e_i 部分が順序が下の POT 順序で計算することで, syz(F) のグレブナー基底, $\langle F \rangle$ のグレブナー基底および F からグレブナー基底を生成する関係式をまとめて計算するアルゴリズムに基づく. ここで, $(m_1, \ldots, m_s)$ が, e_i 部分が f_i より順序が上の POT 順序に関して既にグレブナー基底になっていて, しかも e_i の先頭係数が 1 であることから, $(POT, \prec)$ に対する p-Gröbner candidate で $G_{can} \subset M$ をみたすものがあれば compatibility により M のグレブナー基底となる.

3.2 Hilbert lucky 型の結果

まず, 斉次多項式の場合に Hilbert lucky を考える. F が始めから斉次である場合には, 以下の Arnold の結果がある.

Proposition 5 (Arnold の主定理: Theorem 7.1 in [1]) G_{can} を F と順序 $\prec$ に対する p-Gröbner candidate であって, $\langle G_{can} \rangle \supset I$ かつ G_{can} は $\langle G_{can} \rangle$ のグレブナー基底とする. このとき, G は I のグレブナー基底である.

p が F に関して Hilbert lucky であることが分かっている場合には, Lemma 2 (4) より p は F に関して compatible になるので, Corollary 1 より, 以下の形のものが得られる.

Lemma 6 p が F に関して Hilbert lucky であるとし, G_{can} を F と順序 $\prec$ に対する p-Gröbner candidate であって, $\langle G_{can} \rangle \subset I$ とする. このとき, G は I のグレブナー基底である.

Remark 1 Complete intersection の場合のように, 予め Hilbert function の値が分かっている場合には, 計算した G_p により, p が Hilbert lucky であるかどうかが判定できる. また, G_p の計算が degree の低い順に計算されるため, Hilbert lucky でない場合には, その計算途中で判定ができる.

3.2.1 非斉次の場合

次に, F が斉次でない場合に Arnold の結果をどのように適応できるかを考える. そのために, いくつかの概念を用意する.

Definition 3 K を係数体とする多項式環 $K[X]$ を考え、 $K[X]$ の元 f に対して, 変数 t を新たに導入して, 斉次化 (homogenization) したものを f^h とする. f が $K[X]$ の元であれば, f^h は $K[X,t]$ の元となる. 逆に斉次多項式 h に対して t に 1 を代入したものを非斉次化 (dehomogenization) といい, $h(X,1)$ を $h|_{t=1}$ または h^d と書く. $K[X,t]$ の部分集合 T に対しても, $T|_{t=1}$ または T^d が同様に定義される.

$K[X]$ のイデアル L に対して, L で生成される $K[X,t]$ のイデアル $\langle f^h \mid f \in L \rangle_{K[X,t]}$ を L の斉次化イデアルと呼び L^h で表す. イデアル L の生成元 S に対して, $\langle S^h \rangle = L^h$ のとき, S を L に対して, ここでは homo-compatible と呼ぶことにする. (このような生成集合を Macauley base と呼ぶ. [6] を参照)

X で生成される項全体 T_x の上の項順序 $\prec$ に対して, $X^h = X \cup \{t\}$ で生成される項全体 T^h の上の項順序 $\prec_h$ を次のように定義する.

T^h の2元 $X^\alpha t^a$, $X^\beta t^b$ に対して, $X^\alpha t^a \prec_h X^\beta t^b$ であるとは, 次のいずれかを満たすときにいう.

(1) $a + |\alpha| > b + |\beta|$ または, (2) $a + |\alpha| = b + |\beta|$ かつ, $X^\alpha \prec X^\beta$ である.

ここで, $\alpha=(\alpha_1,\ldots,\alpha_n)\in\mathbb{Z}_{\geq 0}{}^n$ であって, X^α は $x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ を表し, $|\alpha|=\alpha_1+\alpha_2+\cdots+\alpha_n$ とする. (ここで $\mathbb{Z}_{\geq 0}=\{n\in\mathbb{Z}\mid n\geq 0\}$ である.) $\prec$ が degree compatible な順序であれば, $\prec_h$ の $\mathcal{T}$ への制限 $\prec_h|_{\mathcal{T}}$ は $\prec$ に一致する.

よく知られた事実として以下がある. (Proposition 4.3.18, 4.3.21, Corollary 4.3.8, Tutorial 53 in [6] などを参照)

Lemma 7 以下では, L を $\mathbb{Q}[X]$ のイデアルとし, $\prec$ を degree compatible な順序とする.

(1) G が L の $\prec$ に関するグレブナー基底であれば, G は L に対して homo-compatible である. さらに, G^h は L^h の $\prec_h$ に関するグレブナー基底となる. G が 簡約であれば, G^h も 簡約である.

(2) G' を L^h の $\prec_h$ に対するグレブナー基底とする. このとき, $G'|_{t=1}$ は L の $\prec$ に対するグレブナー基底である. G' が 簡約であれば, $G'|_{t=1}$ も 簡約である.

(3) F を L の生成集合とする. $L^h=(\langle F^h\rangle : t^\infty)$ である. F が homo-compatible であるための必要十分条件は $(\langle F^h\rangle : t^\infty)=\langle F^h\rangle$

Lemma 8 $\prec$ が degree compatible な順序であって, $F\subset\mathbb{Z}_p^0[X]$ が I のある別の degree compatible な順序 $\prec'$ に関するグレブナー基底であり, さらに, F の各元の 先頭係数は p で割れないとする. このとき, F は I に対して homo-compatible であり, $\phi_p(F)$ は $I_p(F)$ に対しても homo-compatible である.

Lemma 9 (Theorem 2.4 in [4] の修正版その1) G_{can} を F と degree compatible な項順序 $\prec$ に対する p-Gröbner candidate であって, $\langle G_{can}\rangle\supset I$ かつ G_{can} は $\langle G_{can}\rangle$ のグレブナー基底とする. このとき, $\phi_p(F)$ が $I_p(F)$ に対して homo-compatible ならば G は I のグレブナー基底である. 実際に, homo-compatible であるかどうかは,

$$(\langle\phi_p(F)^h\rangle : t^\infty)=\langle\phi_p(F)^h\rangle$$

であるかどうかで判定できる.

Lemma 9 より, **change of order** 型のものとして以下が成り立つ.

Corollary 3 (Theorem 2.4 in [4] の修正版その2) $\prec$ が degree compatible な順序であって, F は I のある別の degree compatible な順序 $\prec'$ に関するグレブナー基底であり, F は $\mathbb{Z}_p^0[X]$ の部分集合で, F の各元の $\prec'$ に対する先頭係数は p で割れないとする. G_{can} を F と degree compatible な順序 $\prec$ に対する p-Gröbner candidate であって, $\langle G_{can}\rangle\supset I$ かつ G_{can} は $\langle G_{can}\rangle$ のグレブナー基底とする. このとき G は I のグレブナー基底である.

次に, $\phi_p(F)$ が $I_p(F)$ に対して homo-compatible でない場合を考える. 順序 $\prec$ は degree-compatible としておく. このとき, 次の分解を考える.

$$\langle\phi_p(F^h)\rangle=(\langle\phi_p(F^h)\rangle : t^\infty)\cap\langle\phi_p(F^h)\cup\{t^k\}\rangle,$$

ここで k は $(\langle\phi_p(F^h)\rangle : t^k)=(\langle\phi_p(F^h)\rangle : t^\infty)$ となる正整数とする. $(\langle\phi_p(F^h)\rangle : t^\infty)=I_p(F)^h$ であり, G_p を $I_p(F)$ のグレブナー基底とすると, G_p^h は $I_p(F)^h$ のグレブナー基底である.

ここで, 次の補題を用意する. (証明は Lemma 5.3.11 と Exercise 5.3.3 in [3] による.)

Lemma 10 K を体とし, X を変数の集合とする. A, B を $K[X]$ の斉次イデアルとする. このとき, $HF_{A\cap B} + HF_{A+B} = HF_A + HF_B$ となる.

以下, G_{can} を p-Gröbner candidate とする. すなわち, $G_{can} \subset \mathbb{Z}_p^0[X]$ であって, $\phi_p(G_{can}) = G_p$ とする. さらに, $\langle F^h \cup \{t^k\}\rangle$ の $\prec_h$ に対する 簡約グレブナー基底を計算し, それを H とする. このとき, $\langle F^h \cup \{t^k\}\rangle$ は斉次イデアルであるので, Proposition 5 が使えて, t^k の効果で $\langle F^h\rangle$ のグレブナー基底計算より効率がよいと予想される. 特に, $k = 1$ のように k が非常に小さいときには, $\langle F^h \cup \{t^k\}\rangle$ のグレブナー基底計算が効率的であることが期待される. $k = 1$ であれば, $\langle F^h \cup \{t\}\rangle$ は実質 F の各元の次数最大部分だけからなるイデアルであり, $\mathbb{Q}[X]$ の斉次イデアルのグレブナー基底計算になる. Lemma 10 により, 以下の定理が得られる.

Theorem 1 (Theorem 2.4 in [4] の修正版その4) G_{can} を p-Gröbner candidate とし, G_{can} は $\langle G_{can}\rangle$ のグレブナー基底であり, $I \subset \langle G_{can}\rangle$ とする. さらに, p は H に対して lucky とする. (すなわち, $H \subset \mathbb{Z}_p^0[X]$ であって, $\phi_p(H)$ は $\langle \phi_p(H)\rangle$ のグレブナー基底である.) このとき, G_{can} は I のグレブナー基底である.

3.3 グレブナー基底候補に対する生成関係式による検証

$F = \{f_1, \ldots, f_m\} \subset \mathbb{Q}[X]$, G_{can} を $I = \langle F\rangle$ のグレブナー基底候補で, $I \subset \langle G_{can}\rangle$ を満たすものとする. $\langle \phi_p(F)^h\rangle$ のグレブナー基底が計算できる場合には, 前節の方法により $G_{can} \subset I$ のチェックが可能であるが, この計算ができない場合には, 各 $g \in G_{can}$ に対する生成関係式, すなわち $g = h_1 f_1 + \cdots + h_m f_m$ $(F = \{f_1, \ldots, f_m\})$ なる表示を作るという方法が考えられる.

生成関係式をつくる方法としては, 有限体上の生成関係式から CRT あるいは Hensel で構成する方法が提案されている. この方法で必要となる有限体上の生成関係式は, Buchberger アルゴリズムを実行中に剰余だけでなく商も記録しておくことにより得られるが, 一般に h_i は冗長な項を多数含み, 項数が巨大になるため, そのまま CRT, Hensel 構成を適用するのは効率がよくない. よって, 次の方法により項数を減らすことが考えられる.

1. $g \in G_{can}$ に対し, 生成関係式 $\phi_p(g) = h_1\phi_p(f_1) + \cdots + h_m\phi_p(f_m)$ を作る.
2. h_i の係数を未定係数に置き換えた H_i に対し $g = H_1 f_1 + \cdots + H_m f_m$ を満たす未定係数の値が存在することを示す.
3. 一旦有限体上で解いて, 0 にしてよい係数を 0 にしてから有理数体上で解く.

この方法により有限体上の生成関係式の項数を減らすことができるが, 0 にできる係数の選び方に任意性があるため, 残った未定係数に対する方程式を実際に $\mathbb{Q}$ 上で解く際に, 不必要な係数膨張を招く懸念もある. もし, $syz(\phi_p(F))$ のグレブナー基底 S が分かっていれば, $(h_1, \ldots, h_m)$ の代わりにこれを S で割った剰余 $(r_1, \ldots, r_m)$ を使うことができる. S に関して 簡約な $(r_1, \ldots, r_m)$ で $\phi_p(g) = r_1\phi_p(f_1) + \cdots + r_m\phi_p(f_m)$ を満たすものは一意的である. よって $(r_1, \ldots, r_m)$ を使うことは, 上で述べた, 方程式を解いて冗長係数を 0 にするのと同じ効果をもつ.

3.3.1 計算例 1 : cyclic-7 の場合

g を, C_7 (cyclic-7) の全次数逆辞書式順序グレブナー基底の中のある元とする. $p = 31991$ に対し, $\phi_p(g) = h_1\phi_p(f_1) + \cdots + h_7\phi_p(f_7)$ を満たす $h_1, \ldots, h_7$ を, 計算履歴から求める. $(r_1, \ldots, r_7)$ を,

$(h_1,\ldots,h_7)$ を $syz(C_7)$ のグレブナー基底で割った剰余とする. このとき, それぞれから未定係数の値を求める過程の内訳は次の通りとなる.

	$(h_1,\ldots,h_7)$	$(r_1,\ldots,r_7)$
未定係数の方程式 $Ac=b$ の生成	470sec	20sec
A のサイズ	29572×39591	6647×6250
有限体上での $Ac=b$ の求解	12000sec	(100sec)
パラメタを 0 にして $\mathbb{Q}$ 上で求解	330sec	350sec
得られた係数の最大サイズ	98 桁	98 桁

表が示すように, この例では, syzygy は方程式のサイズ縮小にのみ有効であった.

3.3.2 計算例 2 : Romanovski の例

V. G. Romanovski et al. [10] で扱われているイデアル I は, 8 変数で 10 桁程度の係数の非斉次な生成を持つ. この例については $I\subset\langle G_{can}\rangle$ なるグレブナー基底候補 G_{can} の計算は modular 計算により容易にできる. 実際, 数個程度の素数で CRT での結果が stable になる. また, 得られた $J=\langle G_{can}\rangle$ に対し, $\sqrt{J}$ はきれいな形の素分解を持つので, $\sqrt{I}$ も同様であると期待できる. しかし, I の $\mathbb{Q}$ 上のグレブナー基底計算は, どのような方法でも容易ではない. さらに, 斉次化すると, 有限体でもグレブナー基底が終わらない.

実験の結果, 候補 G_{can} の元のうち二つ (g_1, g_2) を I に添加すれば Buchberger アルゴリズムによりグレブナー基底 G_{can} を得ることが分かった. g_1, g_2 はほとんど support が同じなので, 取りあえず一つ選んで生成関係式を作る実験を行っている. 有限体上での syzygy 計算が困難のため, 先に述べた, 計算履歴から作った未定係数の方程式を有限体上で解いて, 0 にできそうな係数を 0 にしてから改めて方程式を解く, という方法を適用した. 最初に得られる線形方程式を表す行列のサイズは $(1.6\times 10^5)\times(3.5\times 10^5)$ 程度で, 未定係数のうち 2.2×10^5 個を 0 とした残りの変数 $(1.3\times 10^5$ 個) に関する線形方程式を得た. これを 2012 年 9 月から $\mathbb{Q}$ 上でのガウス消去により計算している. 2013 年 3 月現在まだ終了していないが, CRT および並列計算による計算が有効であろう. これは今後の課題である.

4 実際の構成法について

modular 法を利用したグレブナー基底計算は以下の 3 通りが考えられている. これらは, グレブナー基底計算途中の係数膨張や項の膨張, 余計な計算 (簡約操作など) を押えることをねらいとしている.

(1) Chinese Remainder Theorem(CRT) 型

(2) Hensel Lifting 型

(3) 混在型 (主に Buchberger 計算法ベース)

(1) **CRT 型**: この方法の利点は, 並列計算化が可能であり, unlucky prime の処理にも優れている. また, mod$p$ での計算には, F_4 が効率的に使える利点もある. 問題点は, 優れた係数評価法がないため, どこまで modulus(法) を上げれば G_{can} が求まるかが不明であり, modulus の設定 (失敗した場合の次の modulus の取り方も含む) に heuristic が入る. 実際的な実装には, この設定が重要である.

LUCKY, UNLUCKY の判定：複数の素数 $p_1,\ldots,p_k$ に対して G_{p_i} を計算するが, 正しい結果を得るには, すべてが lucky でなくてはならない. change-of-order 型のように, lucky な素数が予め分かっている場合には問題ない.

一方, 一般の場合, すなわち, I の特別な情報を持っていない場合, には計算した中からより分ける必要がある. $\mathcal{G}=\{lp(G_{p_1}),\ldots,lp(G_{p_k})\}$ を計算した結果とするとき, $\mathcal{G}$ を $lp(G_p)$ が一致する部分集合 (同値類) に分ける. すなわち, $G_p, G_q \in \mathcal{G}$ に対して, $G_p \cong G_q \Leftrightarrow lp(G_p)=lp(G_q)$ により定義する関係は同値関係となる. そこで, この同値関係による類別を

$$\mathcal{G}=\mathcal{G}_1 \cup \cdots \cup \mathcal{G}_\ell$$

とする. この中から正しい $\mathcal{G}_i$ を選択する必要がある. Lemma 3 より lucky でない素数は有限個しかないので, heuristic な方法としては, 各 $\mathcal{G}_i$ のうちで一番要素数 (cardinality) が多いものが選択される. (DELETEUNLUCKYPRIMESSB in [4] などを参照)

より精密な評価法として以下をあげておく.

(1) I が斉次イデアルの場合には, Hilbert function を比べ, 他より真に大きいものは unlucky であり, 捨てることになる.

(2) I が一般のイデアルの場合には, 各 $\mathcal{G}_i$ の中から代表をとり, 斉次化イデアル $\langle F^h\rangle$ に対する $lp(F^h)$ のグレブナー基底を計算して, その Hilbert function を求め, 他より大きいものは unlucky と見なす.

(2) **Hensel Lifting 型**：この方法は多項式の因数分解には効果的であったが, グレブナー基底の持ち上げには, グレブナー基底の各元の元の生成集合による表現が必要であり, ここに問題がある. また, CRT 同様に優れた係数評価が重要であり, 特に, 結果の正当性評価をするためには, どこまで lifting するかを決める必要があり, ここには, 精度の高い係数評価が必要になる. この設定にも, heuristic が入ることになるが, unlucky 素数を選んでしまった場合の処理が無駄になる.

(3) 混在型：混在型には, グレブナー trace 法 [12] や Hilbert driven 法 [13] がある. 以下では, イデアル I の生成集合を F とし, 項順序を $\prec$ とする.

グレブナー TRACE 法：グレブナー基底計算において, mod p で 0 に簡約されるものは $\mathbb{Q}$ 上でも 0 に簡約されるものとみなしてグレブナー基底の候補 G_{can} をつくり, $G_{can} \supset I$ と G_{can} が $\langle G_{can}\rangle$ のグレブナー基底であることを確認することで, G_{can} が正しい I のグレブナー基底であることを保証する方法である. これは, $\phi_p(G_{can})$ が $I_p(F)$ のグレブナー基底 G_p に一致することを意味し, 結果として G_{can} は F と $\prec$ に対して p-Gröbner basis candidate であることに注意する.

これに対して compatible 型の方法を適用することで, 以下の改良が可能となる.

(T-1) p が予め compatible であれば, Corollary 1 より, G_{can} が $\langle G_{can}\rangle$ のグレブナー基底である検査を $\phi_p(G_{can})$ が $I_p(F)$ のグレブナー基底であることの検査に置き換えることができる. compatible の条件は, 例えば, Corollary 2 のように, F がある別の項順序での I のグレブナー基底であった場合, つまり change of order 型の場合に適用できる.

HILBERT DRIVEN 法：F を斉次イデアルとし, 項順序 $\prec$ を考える. Hilbert function HF_I が既知の場合に, 各非負整数 s に対する

$$HF_I(s)=\dim_{\mathbb{Q}}(\mathbb{Q}[X][s]/I[s])=\dim_{\mathbb{Q}}\mathbb{Q}[X][s]-\dim_{\mathbb{Q}} I[s]$$

の情報を用いてグレブナー基底を計算する方法である．ここで，$\mathbb{Q}[X][s]$ は $\mathbb{Q}$ 上の次数 s の斉次式全体を表し，$I[s] = I \cap \mathbb{Q}[X][s]$ を表すものとする．([1] の記号を使う．) 想定される場合は change of order 型の場合である．まず比較的計算しやすい順序でグレブナー基底 G を計算しておけば，HF_I が計算でき，(さらに，G に対して lucky な素数 p なら Hilbert lucky である．)

ここでも，trace 法を応用して p を利用することができる．すなわち，p の luckyness を計算途中で判定しながらすすめる．$HF_I \leq HF_{I_p(F)}$，つまり $\dim_{\mathbb{Q}} I[s] \geq \dim_{\mathbb{F}_p} I_p(F)[s]$ であるので，以下を行うことができる．(Traverso [13] とは若干異なる形で書く．)

(H-1) trace 法での計算中の s 次の元の導出において，丁度 $\dim_{\mathbb{Q}} I[s]$ 個現れなければ p は Hilbert unlucky となる．(mod$p$ で 0 に簡約された中に，0 にならないものがある．) この場合に，p を動的に取り換える．p はいままでの計算途中で現れた多項式の 先頭係数を割らないものとする．

(H-2) さらに計算された次数 s の元の個数が $\dim_{\mathbb{Q}} I[s]$ に一致した時点で，今後の次数 s の可能な元を導出する計算を止めることができる．

さらに，Lemma 6 を使うことで以下を使うこともできる．

(H-3) 最後まで計算できた場合に，$\phi_p(G_{can})$ が $I_p(F)$ のグレブナー基底であれば，G_{can} は I のグレブナー基底になる．(つまり，G_{can} が $\langle G_{can} \rangle$ のグレブナー基底であること，$\langle G_{can} \rangle \supset I$ の確認は不要となる．)

Lemma 11 (H-3) が正しいこと．すなわち，最後まで計算できた場合に，$\phi_p(G_{can})$ が $I_p(F)$ のグレブナー基底であれば，G_{can} は I のグレブナー基底になる．

5 さらなる計算における luckyness の応用

重要なイデアルの操作においても modular 計算が有効に適用できることを示す．ここでは，イデアル商売，saturation，根基計算を取り上げる．これらは，イデアル分解に重要な役割を果たすもので，これらを有機的に組み合わせることで，イデアル分解の効率化が期待される．

5.1 イデアル商と saturation への応用

まず最初に，イデアル商計算における luckyness について考える．(Theorem 2.8 in [8] を復習する.) ここで，I の生成集合 F と compatible な素数 p の組が必要になるが，F を 項順序 $\prec$ に対する I の簡約グレブナー基底であって，$F \subset \mathbb{Z}_p^0[X]$ になるような p を取ればよい．

Lemma 12 (Theorem 2.8 in [8]) $F \subset \mathbb{Q}[X]$ をイデアル I の生成集合とし，素数 p は F に対して compatible とする．(項順序を固定して lucky としてもよい．) さらに，多項式 f は $\mathbb{Z}_p^0[X]$ の要素で $\phi_p(f) \neq 0$ とする．多項式集合 $H \subset \mathbb{Z}_p^0[X]$ で H の各元の項順序 $\prec$ に関する主係数が p で割れず，$\phi_p(H)$ が $(I_p^0 : \phi_p(f))$ の $\prec$ に関するグレブナー基底であり，$H \subset (I : f)$ であれば，H は $(I : f)$ のグレブナー基底である．

$(I : f)$ のグレブナー基底の候補 H として，$\phi_p(H)$ が $(\langle \phi_p(F) \rangle : \phi_p(f))$ のグレブナー基底であるものがあったとする．(CRT などで構成すると仮定する) このとき，$H \subset (I : f)$ をチェックし，これが OK であれば H が $(I : f)$ のグレブナー基底であることが保証される．このチェックは，H の各元 h に対して，$NF_F(hf) = 0$ となるかどうかのみを調べればよい．

イデアル商 $(I:f)$ の計算は $I\cap\langle f\rangle$ の計算に帰着されるが, この計算に対して, 同様の方法が適用できる.

Lemma 13 $F\subset\mathbb{Q}[X]$ をイデアル I の生成集合とし, 素数 p は F に対して compatible とする. (はじめから F を I のグレブナー基底としてもよい.) さらに, 多項式 f は $\mathbb{Z}_p^0[X]$ の要素で $\phi_p(f)\neq 0$ とする. 多項式集合 $H\subset\mathbb{Z}_p^0[X]$ で H の各元の主係数が p で割れず, $\phi_p(H)$ が $\langle\phi_p(F)\rangle\cap\langle\phi_p(f)\rangle$ の項順序 $\prec$ に関するグレブナー基底であり, $H\subset I\cap\langle f\rangle$ であれば, H は $I\cap\langle f\rangle$ のグレブナー基底である.

イデアル商を繰り返す操作により saturation が計算できるので, 上の補題は saturation に関して拡張される. (直接証明もできる.)

Lemma 14 $F\subset\mathbb{Q}[X]$ をイデアル I の生成集合とし, 素数 p は F に対して compatible とする. さらに, 多項式 f は $\mathbb{Z}_p^0[X]$ の要素で $\phi_p(f)\neq 0$ とする. 多項式集合 $H\subset\mathbb{Z}_p^0[X]$ で項順序 $\prec$ に関する H の各元の主係数が p で割れず, $\phi_p(H)$ が $(\langle\phi_p(F)\rangle:\phi_p(f)^\infty)$ の $\prec$ に関するグレブナー基底であり, $H\subset(I:f^\infty)$ であれば, H は $(I:f^\infty)$ のグレブナー基底である.

Remark 2 CRT 型の場合には, ここでの modular 計算が有効に働くことが予期される. $(I:f)$ の計算, すなわち $I\cap\langle f\rangle$, や $(I:f^\infty)$ の計算においては, slack variable y を導入して, $\mathbb{Q}[X\cup\{y\}]$ の中で elimination order $X\prec\prec y$ の下で, それぞれ $\langle yF\cup\{(1-y)f\rangle$ や $\langle F\cup\{yf-1\}\rangle$ の elimination ideal のグレブナー基底の計算を行う. (ここで, F を I の生成集合とし, $yF=\{yf\mid f\in F\}$ とする.) Lemma 12, 13, 14 では, $\mathbf{F}_p$ 上での計算では, $\mathbb{F}_p[X\cup\{y\}]$ で計算し, $\mathbb{F}_p[X]$ での elimination ideal のグレブナー基底として H_p を計算するが, $\mathbb{Q}$ 上で構成する H_{can} においては, $\mathbb{Q}[X\cup\{y\}]$ での対応するグレブナー基底を構成するわけではなく, H_p に対応するものだけである. これは, 次に説明するイデアルの和 (Lemma 15) においても同様である.

5.2 イデアルの交わりへの応用

イデアルの交わりへの 応用を 2 種類与える. つまり,

(1) 2 つのイデアル A,B が与えられたときに $I=A\cap B$ のグレブナー基底を計算する場合

(2) イデアル I が与えられ, $I=A\cap B$ となるとき, A,B のグレブナー基底を計算する場合

を考える. (1) は Lemma 13 の一般形といえるものであり, compatible 型で示される.

Lemma 15 $F_A\subset\mathbb{Q}[X]$ をイデアル A の生成集合とし, $F_B\subset\mathbb{Q}[X]$ をイデアル B の生成集合とする. 素数 p は F_A,F_B に対して compatible とする. (はじめから, F_A,F_B は A,B のある項順序に関するグレブナー基底としておいてもよい.) $\phi_p(H)$ が $\langle\phi_p(F_A)\rangle\cap\langle\phi_p(F_B)\rangle$ の項順序 $\prec$ に関するグレブナー基底であり, $H\subset A\cap B$ であれば, H は $A\cap B$ のグレブナー基底である. (ここで, $H\subset A\cap B$ の判定には, F_A,F_B がそれぞれのグレブナー基底であれば, それらに関する正規形を計算することで判定できる.)

次に (2) の場合を示す. イデアル I が mod$p$ において 2 つのイデアル A_p,B_p の交わりになっている場合に, その成分 A_p,B_p に対応するイデアル A,B が存在した場合に, $I=A\cap B$ となることを保証するものである. 応用として, $I=(I:f^\infty)\cap(I+\langle f^k\rangle)$ の分解が想定される.

Lemma 16 $G \subset \mathbb{Q}[X]$ をイデアル I の項順序 $\prec$ に対するグレブナー基底とし，素数 p として，$G \subset \mathbb{Z}_p^0[X]$ であって，G の $\prec$ に対する先頭係数 p で割れないものとする．2つのイデアル A, B の $\prec$ に関するグレブナー基底を G_A, G_B とし，$G_A, G_B \subset \mathbb{Z}_p^0[X]$ であって，G_A, G_B の各元の $\prec$ に対する 先頭係数 は p で割れないとする．つまり，p は G, G_A, G_B に対して lucky であるとする．さらに，$\langle \phi_p(G) \rangle = \phi_p(I \cap \mathbb{Z}_p^0[X]) = \langle \phi_p(G_A) \rangle \cap \langle \phi_p(G_B) \rangle$ であって，$I \subset A \cap B$ とするとき，$I = A \cap B$ である．(ここで，$\phi_p(G_A)$ は $\phi_p(A \cap \mathbb{Z}_p^0[X])$ のグレブナー基底であり，$\phi_p(G_B)$ は $\phi_p(B \cap \mathbb{Z}_p^0[X])$ のグレブナー基底である．)

5.3 根基計算への応用

F で生成されるイデアル I の根基 $\sqrt{I}$ の計算に modular 法を導入する．一般の方法では，斉次元成分に分割し，0 次元化して各変数の最小多項式を計算し，それを無平方分解することが基本である．

ここでは，このアプローチとは別に，modular での根基計算を利用した方法を I のグレブナー基底 G がすでに求まっている場合に与える．そこで，各素数 p として G と項順序 $\prec$ に対して lucky なものをとり，modular 法により，各有限体 F_p 上で $\sqrt{I_p(G)}$ のグレブナー基底 H_p を計算し，これから $H_{can} \subset \mathbb{Z}_p^0[X]$ を計算する．($\phi_p(H_{can}) = H_p$ となる．)

Lemma 17 (cf. Theorem 5.5 in [5]) $J = \langle H_{can} \rangle$ とおく．さらに，$H_{can} \subset \sqrt{I}$ であるとする．すなわち，H_{can} の各元 h に対して，$NF_G(h^k) = 0$ となる k が存在するとする．このとき，$J = \sqrt{I}$ であり，H_{can} は $\sqrt{I}$ のグレブナー基底となる．

参考文献

[1] E.Arnold, Modular algorithms for computing Gröbner bases, J.Symb.Comp. 35, 403-419, 2003.

[2] H.-G. Gräbe, On lucky primes, J.Symb.Comp. 15, 199-209, 1993.

[3] G.-M.Greuel, G.Pfister, A Singular Introduction to Commutative Algebra, Second Edition, Springer-Verlag, Heidelberg, 2008.

[4] N.Idrees, G.Pfister, S.Steidel, Parallelization of modular algorithms, J.Symb.Comp.46, 672-684, 2011.

[5] 門田めぐみ, modular 計算による多項式イデアルの分解アルゴリズム, 神戸大学大学院理学研究科修士論文, 2009.

[6] M.Kreuzer, L.Robbiano, Computational Commutative Algebra 2, Springer-Verlag, Heidelberg, 2005.

[7] M. Noro, Modular Algorithms for Computing a Generating Set of the Syzygy Module, Proc. CASC2009, LNCS 5743, Springer, 259-268 (2009).

[8] M.Noro, K.Yokoyama, A modular method to compute the rational univariate representation, J.Symb.Comp.28, 243-263, 1999.

[9] F.Pauer, On lucky ideals for Gröbner bases computation, J.Symb.Comp.14, 471-482, 1992.

[10] V. G. Romanovski, X. Chen, Z. Hu, Linearizability of linear systems perturbed by fifth degree homogeneous polynomials, J. Phys A: Math. Theor. 40, 5905-5919, 2007.

[11] V.G.Romanovski, M.Presern, An approach to solving systems of polynomials via modular arithmetics with applications, J. Computational and Applied Mathematics 236, 196-208, 2011.

[12] C.Traverso, Gröbner trace algorithms, ISSAC '88, LNCS 358, 125-138, 1989.

[13] C.Traverso, Hilbert functions and the Buchberger algorithm, J.Symb.Comp.22, 355-376, 1997.

[14] F.Winkler, A p-adic approach to the computation of Gröbner bases, J.Symb.Comp.6, 287-304, 1988.