Risa/Asir における signature based algorithm の実装について

Implementation of a signature based algorithm in Risa/Asir

立教大学理学部　野呂 正行 [*1]
Masayuki Noro
Faculty of Science
Rikkyo University

立教大学理学部　横山 和弘 [*2]
Kazuhiro Yokoyama
Faculty of Science
Rikkyo University

Abstract

Faugère [1] presented the F_5 algorithm for efficiently computing Gröbner bases but the proof of its termination and correctness was incomplete and since then many efforts have been devoted to verify them. As a result many variants of the F_5 algorithm have been proposed by various researchers and they are called signature based algorithms. A Survey by Eder and Faugère [4] gives a summary of signagure based algorithms. In this article we explain the basics of signature based algorithms and reports the computational results by our implementation of a simple signature based algorithm in Risa/Asir.

1　概要

Faugère [1] が F_5 を発表したが, そこで述べられているアルゴリズムの停止性, 正当性に不備があり, 以来, その正当化のための研究が数多く行われてきた. その過程で F_5 アルゴリズムの多数の変種が考案された. これらはまとめて signature-based algorithm (以下, SBA) とよばれている. Eder-Faugère によるサーベイ [4] は 2014 年にプレプリントが arXiv に載り, そこでは 2014 年ごろまでに行われた SBA に関する研究のほとんどが解説されていた. 我々は 2014 年からこのサーベイを元に勉強会を開き, SBA を理解しようと努めたが, 依然として理解困難な点があり, 計算機上への実装はなかなか実現できなかった. 2016 年からは T. Vaccon 氏も交えて議論した結果, Arri-Perry [3] で示された枠組みをもとに理論を構成することで, 理解および実装可能なアルゴリズムを構成することができた. このアルゴリズムは Vaccon-横山 [5], Vaccon-Verron-横山 [6][10] が tropical version の SBA として発表しているが, 通常の多項式環上のアルゴリズムとしてよりわかりやすく解説したものが [7][8] である. 本稿では, [8] に基づいてこのアルゴリズムの原理を解説し, Risa/Asir への実装とその現時点での性能について報告する.

[*1] E-mail: noro@rikkyo.ac.jp
[*2] E-mail: kazuhiro@rikkyo.ac.jp

謝　辞

この研究は JSPS 科研費基盤研究 (C)18K03432 の助成をうけています。

2 Signature

K を体, $R = K[x_1, \ldots, x_n]$ とする. $I = \langle f_1, \ldots, f_\ell \rangle$ を R のイデアルとする. $<$ を R の項順序, $\prec$ を $R^\ell = R\boldsymbol{e}_1 \oplus \cdots \oplus R\boldsymbol{e}_\ell$ の加群項順序 [1] とする. $f \in R$ ($h \in R^\ell$) に対し, $<$ ($\prec$) に関する係数 1 の先頭単項式を $\mathrm{LM}(f)$ ($\mathrm{LM}(h)$) と書く.

定義 1 (signature)
$f \in I$, $f \neq 0$ に対し, $S(f) = \min_\prec \{\mathrm{LM}(h) \mid h = \sum_{i=1}^{\ell} h_i \boldsymbol{e}_i \in R^m, \sum_{i=1}^{\ell} h_i f_i = f\}$ を f の signature と呼ぶ.

注意 1
$f = \sum_{i=1}^{\ell} h_i f_i$ なる任意の表示に対し $\mathrm{LM}(\sum_{i=1}^{\ell} h_i \boldsymbol{e}_i)$ を f の signature と呼んでいる文献もある. 紛らわしい場合には, ここで定義した signature を minimal signature と呼ぶ.

定義 2
M を R の係数 1 の単項式全体, $\mathbb{M}$ を R^ℓ の係数 1 の加群単項式全体とするとき, Syz, NS を次で定義する.

$$\mathrm{Syz} = \mathrm{syz}(f_1, \ldots, f_\ell) = \{\sum_{i=1}^{\ell} h_i \boldsymbol{e}_i \mid \sum_{i=1}^{\ell} h_i f_i = 0\} \subset R^\ell, \quad \mathrm{NS} = \{m\boldsymbol{e}_i \mid m \in M, m\boldsymbol{e}_i \notin \mathrm{LM}(\mathrm{Syz}))\} \subset \mathbb{M}$$

定理 3 (sygyzy のグレブナー基底と signaure)
G を $\mathrm{syz}(f_1, \ldots, f_\ell)$ の $\prec$ に関するグレブナー基底とし, $\mathrm{NF}_G(h)$ を $h \in R^\ell$ の G による剰余とする.

1. $f = \sum_{i=1}^{\ell} h_i f_i \in I$, $f \neq 0$ に対し, $S(f) = \mathrm{LM}(\mathrm{NF}_G(\sum_{i=1}^{\ell} h_i \boldsymbol{e}_i))$.
2. $\{S(f) \mid f \in I, f \neq 0\} = \mathrm{NS}$.
3. $m \in M$ とすると $S(mf) \preceq mS(f)$ で, $S(mf) = mS(f) \Leftrightarrow mS(f) \in \mathrm{NS}$.

証明

1. $h = \sum_{i=1}^{\ell} h_i \boldsymbol{e}_i$, $r = \sum_{i=1}^{\ell} r_i \boldsymbol{e}_i = \mathrm{NF}_G(h)$ とすると, $f = \sum_{i=1}^{\ell} h_i f_i = \sum_{i=1}^{\ell} r_i f_i$ である. もし $S(f) \prec \mathrm{LM}(r)$ ならば, $h' = \sum_{i=1}^{\ell} h'_i \boldsymbol{e}_i$ が存在して $f = \sum_{i=1} h'_i f_i$ かつ $\mathrm{LM}(h') \prec \mathrm{LM}(r)$ となるが, このとき $r - h' \in \mathrm{Syz}$ となるので $\mathrm{LM}(r - h') = \mathrm{LM}(r) \in \mathrm{LM}(\mathrm{Syz})$ となり矛盾である. よって $S(f) = \mathrm{LM}(r)$.
2. 明らか.
3. $f = \sum_{i=1}^{\ell} h_i f_i$, $\mathrm{LM}(\sum_{i=1}^{\ell} h_i \boldsymbol{e}_i) = S(f)$ とする. $h' = \sum_{i=1}^{\ell} mh_i \boldsymbol{e}_i$ とおくと $mf = \sum_{i=1}^{\ell} mh_i f_i$, $\mathrm{LM}(h') = mS(f)$ より $S(mf) \preceq mS(f)$. $mS(f) = S(mf)$ なら 2. より $mS(f) \in \mathrm{NS}$. $mS(f) \in \mathrm{NS}$ ならば, $\mathrm{LM}(h') \in \mathrm{NS}$ より $\mathrm{LM}(h') = \mathrm{LM}(\mathrm{NF}_G(h')) = S(mf)$

∎

$mS(f)$ を mf の guessed signature と呼ぶ場合がある.

[1] 加群項順序については, 例えば [2]5 章 2 節を参照.

定義 4 (𝔖(シグマ)-簡約, 𝔖-既約)

1. $f \in I$ の先頭項を $g \in I$ で簡約する際, $S(f) \succ S(mg) \quad (m = \frac{\mathrm{LM}(f)}{\mathrm{LM}(g)})$ が成り立つとき, (regular) 𝔖-top-簡約 (略して 𝔖-簡約) と呼ぶ.

2. 1. で $S(f) \succeq S(mg)$ としたとき singular 𝔖-(top-) 簡約と呼ぶ.

3. f を regular 𝔖-簡約する $g \in I$ が存在しないとき f は 𝔖-既約という.

f を g で 𝔖-簡約して r となるとき $S(r) = S(f)$ となることに注意する.

定理 5 (𝔖-既約元に関する一意性, 最小性)

1. $s \in \mathrm{NS}$ とするとき, $p \in I$, $S(p) = s$ が 𝔖-既約 $\Leftrightarrow \mathrm{LM}(p) = \min_{<}\{\mathrm{LM}(q) \mid S(q) = s\}$

2. $m \in M$ とするとき, $p \in I$, $\mathrm{LM}(p) = m$ が 𝔖-既約 $\Leftrightarrow S(p) = \min_{\prec}\{S(q) \mid \mathrm{LM}(q) = m\}$

3. $p, p' \in I$ が 𝔖-既約のとき $S(p) = S(p') \Leftrightarrow \mathrm{LM}(p) = \mathrm{LM}(p')$

証明

1. $p, q \in I$, $S(p) = S(q) = s$ とする. $\mathrm{LM}(q) < \mathrm{LM}(p)$ ならば, ある $c \in K$ に対し $r = p - cq$ が $S(r) \prec s$ かつ $\mathrm{LM}(r) = \mathrm{LM}(p)$ を満たす. この時 p は r により 𝔖-簡約されるので, p は 𝔖-既約でない. よって p が 𝔖-既約ならば $\mathrm{LM}(p) \leq \mathrm{LM}(q)$ となる. p が 𝔖-既約でないなら, ある $q \in I$ が存在して $\mathrm{LM}(q) = \mathrm{LM}(p)$ かつ $S(q) \prec S(p)$. このときある $c \in K$ に対し $r = p - cq$ が $S(r) = s$ かつ $\mathrm{LM}(r) < \mathrm{LM}(p)$. すなわち $\mathrm{LM}(p) \neq \min_{<}\{\mathrm{LM}(q) \mid S(q) = s\}$.

2. $p, q \in I$, $\mathrm{LM}(p) = \mathrm{LM}(q)$ とする. $S(q) \prec S(p)$ ならば, p は q により regular 𝔖-簡約されるので p は 𝔖-既約でない. よって p が 𝔖-既約ならば $S(p) \preceq S(q)$. p が 𝔖-既約でないなら, ある $q \in I$ が存在して $\mathrm{LM}(q) = \mathrm{LM}(p)$ かつ $S(q) \prec S(p)$. このとき $S(p) \neq \min_{\prec}\{S(q) \mid \mathrm{LM}(q) = m\}$

3. 1., 2. より成り立つ.

∎

3 𝔖-グレブナー基底

定義 6 (𝔖-グレブナー基底)

$G \subset I$ が次を満たすとき G を I の 𝔖-グレブナー基底と呼ぶ.

任意の 𝔖-既約な $p \in I$ に対し $g \in G$, $m \in M$ が存在して $\mathrm{LM}(p) = m\mathrm{LM}(g)$, $S(p) = mS(g)$.

注意 2

1. G として無限集合を許していることに注意する. 例えば, $G = \{g \mid g \in I, g \text{ は 𝔖-既約 }\}$ は 𝔖-グレブナー基底である.

2. 上の条件は次と同値:

   任意の $p \in I$ に対し $g \in G$, $m \in M$ が存在して $\mathrm{LM}(p) = m\mathrm{LM}(g)$, $S(p) \succeq mS(g)$.

命題 7

G が 𝔖-グレブナー基底とするとき, f が 𝔖-既約 $\Leftrightarrow \mathrm{LM}(f) = m\mathrm{LM}(g)$, $S(f) \succ mS(g)$ を満たす $g \in G$, $m \in M$ が存在しない.

証明 f が $\mathfrak{S}$-既約でないならば, ある $p \in I$ が存在して $S(p) \prec S(f)$, $\mathrm{LM}(p) = \mathrm{LM}(f)$. このような p のうち $S(p)$ を最小のものをとれば p は $\mathfrak{S}$-既約となるので, $\mathfrak{S}$-グレブナー基底の定義より $g \in G$, $m \in M$ が存在して $\mathrm{LM}(f) = \mathrm{LM}(p) = m\mathrm{LM}(g)$, $mS(g) = S(p) \prec S(f)$. 逆に, $\mathrm{LM}(f) = m\mathrm{LM}(g)$, $S(f) \succ mS(g)$ を満たす $g \in G$, $m \in G$ が存在するならば, $p = mg$ とおけば $\mathrm{LM}(f) = \mathrm{LM}(p)$, $S(p) \preceq mS(g) \prec S(f)$ より f は p により regular $\mathfrak{S}$-簡約されるので f は $\mathfrak{S}$-既約でない. ∎

定義 8
単項式順序 $<$, 加群単項式順序 $\prec$ が次を満たすとき, $\prec$ は $<$ と compatible であるという:
$t, s \in M$ が $t < s$ を満たすならば, $i = 1, \ldots, \ell$ に対し $t\boldsymbol{e}_i \prec s\boldsymbol{e}_i$.

命題 9
加群項順序 $\prec$ は項順序 $<$ と compatible とする. $f, g \in I$ とし, f が $\mathfrak{S}$-既約とする. このとき $u, v \in M$ に対し $\mathrm{LM}(f) = u\mathrm{LM}(g)$, $S(f) = vS(g)$ ならば $u = v$.

証明 $u > v$ とすると, $\mathrm{LM}(vg) < \mathrm{LM}(ug) = \mathrm{LM}(f)$. $S(f) \in \mathrm{NS}$ で $S(f) = vS(g)$ より $vS(g) \in \mathrm{NS}$ なので $S(vg) = vS(g) = S(f)$. これは $\mathfrak{S}$-既約な f に対する $\mathrm{LM}(f)$ の最小性に反する.
$u < v$ とすると, compatibility より $S(ug) \preceq uS(g) \prec vS(g) = S(f)$ かつ $\mathrm{LM}(ug) = \mathrm{LM}(f)$ より f は ug により regular $\mathfrak{S}$-可約となり, f の $\mathfrak{S}$-既約性に反する. ∎

定理 10 (有限 $\mathfrak{S}$-グレブナー基底)
加群単項式順序 $\prec$ が単項式順序 $<$ と compatible のときイデアル I の任意の $\mathfrak{S}$-グレブナー基底 G に対し, その有限部分集合で, $\mathfrak{S}$-グレブナー基底となるものがとれる.

証明 $L = \{(\mathrm{LM}(g), S(g)) \mid f \in G\}$ で生成される $M \oplus \mathbb{M}$ のモノイデアルの有限生成系 $L_0 = \{(\mathrm{LM}(g_1), S(g_1)), \ldots, (\mathrm{LM}(g_k), S(g_k))\}$ $(g_1, \ldots, g_k \in G)$ をとり, $G_0 = \{g_1, \ldots, g_k\}$ とおく. 任意の $p \in I$ に対し, $g \in G$, $m \in M$ が存在して $\mathrm{LM}(p) = m\mathrm{LM}(g)$ かつ $S(p) = mS(g)$. この g に対し $g_i \in G_0$, $u, v \in M$ が存在して $\mathrm{LM}(g) = u\mathrm{LM}(g_i)$ かつ $S(p) = vS(g_i)$. このとき命題 9 より $u = v$ が成り立つから, $\mathrm{LM}(p) = mu\mathrm{LM}(g_i)$ かつ $S(p) = muS(g_i)$. よって G_0 は I の $\mathfrak{S}$-グレブナー基底である. ∎

系 11
加群単項式順序 $\prec$ が単項式順序 $<$ と *compatible* のとき $\mathfrak{S}$-既約な有限個の元からなる $\mathfrak{S}$-グレブナー基底が存在する.

証明 $G = \{g \mid g \in I, g$ は $\mathfrak{S}$-既約 $\}$ の有限部分集合で $\mathfrak{S}$-グレブナー基底となるものをとればよい. ∎

定義 12
$p \in I$ は $\mathfrak{S}$-既約とするとき, $m \in M$ $(m \neq 1)$, $\mathfrak{S}$-既約な $p' \in I$ で $\mathrm{LM}(p) = \mathrm{LM}(mp')$ かつ $S(p) = mS(p') = S(mp')$ を満たすものが存在しないとき, p は原始的であるという. 原始的な元のみからなり, 各元の signature が全て相異なるグレブナー基底を極小 $\mathfrak{S}$-グレブナー基底とよぶ.

命題 13
$\mathfrak{S}$-グレブナー基底は極小 $\mathfrak{S}$-グレブナー基底を含む. G, G' が極小 $\mathfrak{S}$-グレブナー基底 のとき $\{(\mathrm{LM}(g), S(g)) \mid g \in G\} = \{(\mathrm{LM}(g), S(g)) \mid g \in G'\}$.

証明 $\mathfrak{S}$-グレブナー基底から原始的な元を, signature ごとに 1 つずつ選べば極小 $\mathfrak{S}$-グレブナー基底となる. 一意性は通常の極小グレブナー基底の先頭項集合の一意性と同様に示せる. ∎

系 14
加群単項式順序 $\prec$ が単項式順序 $<$ と *compatible* のとき, $P = \{S(p) \mid p$ は原始的 $\}$ は有限集合である.

証明 G を, 各 $s \in P$ に対し原始的な元を 1 つずつ選んで作った集合とすると, G は極小 $\mathfrak{S}$-グレブナー基底となる. 一方で, 系 11 より有限 $\mathfrak{S}$-グレブナー基底が存在するので, その部分集合として有限な極小 $\mathfrak{S}$-グレブナー基底が存在する. よって一意性より G は有限集合であり, P も有限集合となる. ∎

4 $\mathfrak{S}$-グレブナー基底を計算するアルゴリズム

定義 15 (s 以下 (未満) $\mathfrak{S}$-グレブナー基底)
$s \in \mathbb{M}$ に対し, $G \subset I$ ($\{f_1, \ldots, f_\ell\} \subset G$) が次を満たすとき G を I の s 以下 (未満) $\mathfrak{S}$-グレブナー基底と呼ぶ.

$\mathfrak{S}$-既約で $S(p) \preceq s$ ($S(p) \prec s$) を満たす $p \in I$ に対し $g \in G$, $m \in M$ が存在して $\mathrm{LM}(p) = m\mathrm{LM}(g)$, $S(p) = mS(g)$

注意 3
$\boldsymbol{e}_{i_0} = \min_{\prec} \mathbb{M}$ とすれば, $\{f_1, \ldots, f_\ell\}$ は $\boldsymbol{e}_{i_0}$ 以下 $\mathfrak{S}$-グレブナー基底である.

定義 16 (必要な signature)
s 未満 $\mathfrak{S}$-グレブナー基底 G が s 以下 $\mathfrak{S}$-グレブナー基底となるとき, s を不必要な signature, そうでないとき s を必要な signature と呼ぶ.

定義 17 (擬正則な S ペア)
1. $g, g' \in I$ の S 多項式が $cmg - c'm'g'$ ($c, c' \in K, m, m' \in M$ のとき, $mS(g) \neq m'S(g)$ なら $p = (g, g')$ を 擬正則な S ペアと呼ぶ.
2. $mS(g) \succ m'S(g')$ なら mg を, $mS(g) \prec m'S(g')$ なら $m'g'$ を主成分とよぶ.
3. 擬正則な S ペア p の主成分 mg に対する guessed signature $mS(g)$ を 擬正則な S ペアの guessed signature と呼び, $\hat{S}(p)$ と書く.

注意 4
以下で行われる G による $\mathfrak{S}$-簡約は, 擬正則な S ペアの guessed signature s を, その S 多項式の signature とみなして $mS(g) \prec s$ なる $m \in M$, $g \in G$ により簡約を行うことを意味する. G が s 未満 $\mathfrak{S}$-グレブナー基底のとき, $g, g' \in G$ で, mg が $mS(g) = s$ なる主成分でも, $S(mg) < s$ となる場合には, g, g' の S 多項式が G による $\mathfrak{S}$-簡約で 0 になる.

補題 18
$s \in \mathrm{NS}(Syz)$ とし, G を s 未満 $\mathfrak{S}$-グレブナー基底とする. $Z = \{(m, g) \mid g \in G, m \in M, s = mS(g)\}$ とし, Z の元で $\mathrm{LM}(mg)$ が最小なものを $m_0 g_0$ とする. $\mathrm{LM}(m_0 g_0) = \mathrm{LM}(m_1 g_1)$ となる $m_1 \in M$, $g_1 \in G$ で $m_1 S(g_1) \prec s$ を満たすものが存在するとき, (g_0, g_1) は guessed signature が s の擬正則な S ペアで, ある $c_0, c_1 \in K$ に対し $\mathrm{Spoly}(g_0, g_1) = c_0 m_0 g_0 - c_1 m_1 g_1$.

証明 $h = \mathrm{Spoly}(g_0, g_1) = c_0 u_0 g_0 - c_1 u_1 g_1$ ($c_0, c_1 \in K$) とする. $u_i = \frac{\mathrm{LCM}(\mathrm{LM}(g_0), \mathrm{LM}(g_1))}{\mathrm{LM}(g_i)}$ ($i = 0, 1$) とおけば, $u_0 \mid m_0$, $u_1 \mid m_1$ で $\frac{m_0}{u_0} = \frac{m_1}{u_1}$. $\frac{m_0}{u_0} = t$ とおくと $c_0 m_0 g_0 - c_1 m_1 g_1 = th$. $s \in \mathrm{NS}(Syz)$ より $s = m_0 S(g_0) = S(m_0 g_0)$ で,

$$s = S(m_0 g_0) = S(c_0 m_0 g_0 - c_1 m_1 g_1) = S(th) \preceq tS(h),$$

$$tS(h) \preceq \max(tS(u_0 g_0), tS(u_1 g_1)) \preceq \max(tu_0 S(g_0), tu_1 S(g_1)) = \max(m_0 S(g_0), m_1 S(g_1)) = s$$

より $S(th) = tS(h) = s$. もし $t \neq 1$ ならば $S(h) \prec s$ より, ある $g \in G$, $m \in M$ が存在して mg は $\mathfrak{S}$-既約かつ $S(mg) = mS(g) = S(h)$. このとき $tmS(g) = tS(h) = s$ より $(tm, g) \in Z$ である. ここで, mg は $\mathfrak{S}$-既約より, $\mathrm{LM}(mg) \leq \mathrm{LM}(h) < \mathrm{LM}(u_0 g_0)$ だから $\mathrm{LM}(tmg) < \mathrm{LM}(tu_0 g_0) = \mathrm{LM}(m_0 g_0)$ となり, $m_0 g_0$ のとり方に反する. よって $t = 1$ で, $h = c_0 m_0 g_0 - c_1 m_1 g_1$, すなわち (g_0, g_1) は guessed signature s の 擬正則な S ペアである. ∎

定理 19 (s 未満 $\mathfrak{S}$-グレブナー基底からの s 以下 $\mathfrak{S}$-グレブナー基底の構成)
G を s 未満 $\mathfrak{S}$-グレブナー基底とする. $Z = \{(m, g) \mid g \in G, m \in M, s = mS(g)\}$ とし, Z の元で $\mathrm{LM}(mg)$ が最小なものを $m_0 g_0$ とする.

1. $\mathrm{LM}(m_0 g_0) = \mathrm{LM}(m_1 g_1)$ となる $m_1 \in M$, $g_1 \in G$ で $m_1 S(g_1) \prec s$ を満たすものが存在しないとき $m_0 g_0$ は $\mathfrak{S}$-既約で G は s 以下 $\mathfrak{S}$-グレブナー基底. このとき $S(m_0 g_0) = s$.
2. $\mathrm{LM}(m_0 g_0) = \mathrm{LM}(m_1 g_1)$ となる $m_1 \in M$, $g_1 \in G$ で $m_1 S(g_1) \prec s$ を満たすものが存在するとき, $m_0 g_0$ を, $mS(g) \prec s$, $m \in M$, $g \in G$ なる mg でできるだけ簡約したものを r とする.
   (a) $r = 0$ なら G は s 以下 $\mathfrak{S}$-グレブナー基底で, $s \in \mathrm{LM}(Syz)$.
   (b) $r \neq 0$ なら (g_0, g_1) は guessed signagure が s の 擬正則な S ペアで, $G \cup \{r\}$ が $\mathfrak{S}$-グレブナー基底で $S(r) = s$.

証明 1. を示す. もし $S(m_0 g_0) \prec s$ なら, G が s 未満 $\mathfrak{S}$-グレブナー基底であることから $\mathrm{LM}(m_0 g_0) = \mathrm{LM}(mg)$, $mS(g) \preceq S(m_0 g_0)$ を満たす $g \in G$, $m \in M$ が存在する. これは仮定に反するので, $S(m_0 g_0) = s$. $m_0 g_0$ が $\mathfrak{S}$-既約でないとすれば, $\mathfrak{S}$-既約な $p \in I$ が存在して $\mathrm{LM}(p) = \mathrm{LM}(m_0 g_0)$ かつ $S(p) \prec s$. G は s 未満 $\mathfrak{S}$-グレブナー基底より, $m \in M$, $g \in G$ が存在して $\mathrm{LM}(p) = \mathrm{LM}(mg)$ かつ $mS(g) = S(p)$. これは仮定に反する. よって $m_0 g_0$ は $\mathfrak{S}$-既約かつ $S(m_0 g_0) = s$ となるので, 定義により G は s 以下 $\mathfrak{S}$-グレブナー基底となる. 2. を示す. (a) の場合, 簡約に用いる mg はすべて $mS(g) \prec s$ を満たし、$m_0 S(g_0) = s$ であることから, $\mathrm{LM}(h) = s$ であるような $h \in \mathrm{Syz}$ が存在する. よって $s \in \mathrm{LM}(Syz)$ であり, $S(p) = s$ を満たす $p \in I$ は存在しないので, G は s 以下 $\mathfrak{S}$-グレブナー基底である. (b) の場合, もし $S(m_0 g_0) \prec s$ ならば G が s 未満 $\mathfrak{S}$-グレブナー基底であることから $r = 0$ となるので, $S(m_0 g_0) = s$ である. このとき, $s \in \mathrm{NS}(Syz)$ より, 補題 18 より (g_0, g_1) は擬正則な S ペアで, それを $\mathfrak{S}$-簡約して得られた $r \neq 0$ は $S(r) = s$ なる $\mathfrak{S}$-既約元である. ∎

系 20
$s \in \mathrm{NS}(Syz)$ で, G が s 未満 $\mathfrak{S}$-グレブナー基底とするとき, *guessed signature* s の擬正則 S ペアが存在しないならば G は s 以下 $\mathfrak{S}$-グレブナー基底である.

証明 もし定理 19 の 2. の条件が成立するならば, $s \in \mathrm{NS}(Syz)$ より, 補題 18 により (g_0, g_1) は 擬正則な S ペアでなければならない. 擬正則な S ペアは存在しないので, 定理 19 の 1. より G は s 以下 $\mathfrak{S}$-グレブナー基底となる. ∎

定理 21 (s 以下 $\mathfrak{S}$-グレブナー基底からの s_1 未満 $\mathfrak{S}$-グレブナー基底 ($s \prec s_1$) の構成)
G を s 以下 $\mathfrak{S}$-グレブナー基底とし, $s_1 = \min_{\prec}\{\hat{S}(p) \mid p$ は G から作った 擬正則 S ペア $, s \prec \hat{S}(p)\}$ とすると, G は少なくとも s_1 未満 $\mathfrak{S}$-グレブナー基底となる.

証明 $N = \{s' \mid s' \succ s, G$ が s' 以下 $\mathfrak{S}$-グレブナー基底にならない $\}$ とおく. もし $N = \emptyset$ ならば, 任意の $s_1 \succ s$ に対し G は s_1 以下 $\mathfrak{S}$-グレブナー基底である. $N \neq \emptyset$ のとき, $s_0 = \min_{\prec} N$ とすると, $s' \prec s_0$

に対し G は s' 以下 $\mathfrak{S}$-グレブナー基底より, G は s_0 未満 $\mathfrak{S}$-グレブナー基底である. 仮定により G は s_0 以下 $\mathfrak{S}$-グレブナー基底にならないので, $s_0 \in \mathrm{NS}(Syz)$ である. 系 20 より guessed signature s_0 の 擬正則 S ペアが存在する. よって $s_1 \preceq s_0$ で, G は s_1 未満 $\mathfrak{S}$-グレブナー基底でもある. ∎

以下で示すアルゴリズム 1 は, 定理 19, 定理 21 を交互に適用して s 以下 $\mathfrak{S}$-グレブナー基底を帰納的に構成していく. その際, 定理 21 により, 擬正則な S ペアが作れない s は不要な signature である. すなわち, 擬正則 S ペアは必要な signature を見つけるツールとして用いられる. 必要な signature s に対し, $\mathfrak{S}$-既約な元を一つ見つければ十分なので, 処理する必要がある S ペアは s に対し一つでよい. ここで, 不要な signature を判定するための重要な性質を紹介する.

命題 22 (syzygy criterion)
擬正則 S ペアの guessed signature s が, 既に知られている syzygy h に対する $\mathrm{LM}(h)$ で割り切れるなら, その S ペアは捨ててよい.

証明 $\mathrm{LM}(h) \mid s$ のとき, $s \in \mathrm{LM}(\mathrm{Syz})$ だから s は不要な signature でありその S ペアを処理する必要はない. 実際, その S ペアから作られる S 多項式の signature は s 未満であり, s 未満 $\mathfrak{S}$-グレブナー基底による $\mathfrak{S}$-簡約で 0 になる. ∎

Algorithm 1 signature based algorithm

Input : $f_1, \ldots, f_\ell \in R$
Output : $I = \langle f_1, \ldots, f_\ell \rangle$ の $\mathfrak{S}$-グレブナー基底

1: $G \leftarrow \{f_1, \ldots, f_\ell\}$; $S(f_i) \leftarrow \boldsymbol{e}_i$ $(i = 1, \ldots, \ell)$; $S \leftarrow \emptyset$; $s_{prev} \leftarrow = \min_{\prec}\{\boldsymbol{e}_1, \ldots, \boldsymbol{e}_\ell\}$
2: $D \leftarrow G$ から作った 擬正則 S ペア全体
3: **while** $D \neq \emptyset$ **do**
4: $s \leftarrow \min_{\prec}\{S(p) \mid p \in D\}$
5: **if** s を割り切る S の元がない **then**
6: $R \leftarrow \{mg \mid g \in G, m \in M, mS(g) = s\}$
7: $mg \leftarrow R$ 中で $\mathrm{LM}(mg)$ が最小の元
8: **if** mg を主成分とする $p \in D$ が存在する **then**
9: $r \leftarrow \mathrm{Spoly}(p)$ を G で regular 簡約した余り
10: **if** $r \neq 0$ **then**
11: $S(r) \leftarrow s$; $D \leftarrow D \cup$ (G と r から作った 擬正則 S ペア); $G \leftarrow G \cup \{r\}$
12: **else**
13: $S \leftarrow S \cup \{s\}$
14: **end if**
15: **end if**
16: **end if**
17: $D \leftarrow D \setminus \{q \in D \mid S(q) = s\}$; $s_{prev} \leftarrow s$
18: **end while**
19: **return** G

命題 23
アルゴリズム 1 の 17 行目において, G は s 以下 $\mathfrak{S}$-グレブナー基底である.

証明 while ループの 4 行目において G が s_{prev} 以下 $\mathfrak{S}$-グレブナー基底ならば, 5 行目において G は定理 21 より s 未満 $\mathfrak{S}$-グレブナー基底である. このとき, 定理 19 より 17 行目における G は s 以下 $\mathfrak{S}$-グレ

ブナー基底である. 注意 3 よりループに最初に入った時点で G は s_{prev} 以下 $\mathfrak{S}$-グレブナー基底だから, 数学的帰納法により定理の主張が成立する. ∎

補題 24
アルゴリズム 1 において, G に追加される r は原始的である.

証明 ある r が原始的でないとすれば, G が s 未満 $\mathfrak{S}$-グレブナー基底であることから $g \in G$, $m \in M$ $(m \neq 1)$ が存在して $\mathrm{LM}(r) = \mathrm{LM}(mg)$, $S(r) = mS(g)$ が成り立つ. r の計算において $mg \in R$ なので, R 中で $\mathrm{LM}(mg)$ が最小で, かつ $\mathrm{LM}(mg)$ を regular $\mathfrak{S}$-簡約する G の元が存在しなかったことになる. これは mg を主成分とするペア p が存在することに反する. ∎

定理 25
加群単項式順序 $\prec$ が単項式順序 $<$ と compatible のときアルゴリズム 1 は停止して $\mathfrak{S}$-グレブナー基底を出力する.

証明 $D = \emptyset$ となったとき, 定理 21 により G は任意の s_1 に対し s_1 以下 $\mathfrak{S}$-グレブナー基底となる. すなわち G は $\mathfrak{S}$-グレブナー基底である. 停止性を示す. 命題 24 より G に追加される元は全て原始的であり, signature は相異なる. compatibility と 系 14 よりこのような元は有限個しか生成されない. よって, 新たに D に追加されるペアは有限個であり, アルゴリズムは停止する. ∎

5 Risa/Asir での実装

アルゴリズム 1 の Risa/Asir 上への実装は, 既存の Buchberger アルゴリズムの実装である `dp` 系, `nd` 系関数の関数を流用した. 具体的には, `nd` の多項式データ型に signature を追加し, signature 自体は実装を簡略化するため `dp` の単項式データ型を用いた. 加群項順序としては Schreyer 順序:

$$te_i \prec se_j \Leftrightarrow tLM(f_i) < sLM(f_j) \text{ または } (tLM(f_i) = sLM(f_k) \text{ かつ } i < j)$$

および POT 順序:

$$te_i \prec se_j \Leftrightarrow i < j \text{ または } (i = j \text{ かつ } t < s)$$

のみを実装した. SBA を実行する関数は `nd_sba(Base,Vars,P,Ord|options)` で, `P`= 0 の場合有理数体上, `P` が 2^{29} 未満の素数の場合有限体 $\mathbb{F}_P$ 上での計算を行う. 計算を制御するオプション `options` としては `top` (1 のとき 先頭項に対してのみ簡約を行い, 0 のとき簡約できる項がなくなるまで簡約する; デフォルトは 0), `sba_pot` (1 のとき POT 順序, 0 のとき Schreyer 順序; デフォルトは 0) などがある. 以下の計算機実験は, Mac mini(2018) 上の `asir 20201215` で行った. 計算時間の単位は秒である. 今回は Buchberger アルゴリズムとの挙動の違いや処理する S ペアの個数や S ペア消去の効き方を見るために, よく知られたベンチマーク問題に対して有限体 $\mathbb{F}_{32003}$ 上でのみ実験を行った.

5.1 計算時間の比較

表 1 で, `full`, `top` は `nd_sba` をそれぞれ `top`= 0, `top`= 1 で実行した結果で, `buch` は Risa/Asir の Buchberger アルゴリズム実装である `nd_gr` を実行した結果である. `Singular` は, Singular [9] の SBA 実装である `sba` を, Schreyer 順序と, ある rewrite order で実行する `sba(i,0,1)` という引数で呼び出した結果である. Singular については, より以前から SBA の一種である rewrite basis アルゴリズム [4] を実装し

	full	top	buch	Singular
f855	3.7	7.2	0.74	7.7
filter9	6.7	9.2	0.08	6.9
hairer2	140	36	0.87	28
cyclic7	0.84	0.50	0.98	0.53
cyclic8	47	25	28	26
extcyc6	4.1	3.2	2.2	2.4
extcyc7	880	640	460	310
noon8	2.0	0.43	4.2	1.2
noon9	31	3.9	57	14

	full	top	buch	Singular
eco11	4.1	6.6	15	9.5
eco12	39	59	130	99
redeco11	1.2	1.8	4.2	1.2
redeco12	8.4	12	36	8.8
reimer6	8.0	9.9	2.5	5.1
reimer7	1900	4400	540	780
katsura10	7.3	19	62	11
katsura11	62	150	610	97
katsura12	550	1400	5900	870

表 1: SBA と Buchberger アルゴリズムの計算時間

ていて効率化の努力も行なっていると考えられるので, 今回の我々の実装での結果と比較して極端な差がないか確認するために結果を追加した.

Risa/Asir における Buchberger アルゴリズム実装との比較は, ここでの例だけでは優劣の判断は難しいが, noon, eco, redeco, katsura のように大きく高速化したものもある. また, Singular の sba との比較を見ると, Asir の SBA における top 簡約の結果と Singular の結果が比較的近いように見える. また, それらの間には大きな差はないようである.

表 2 は, SBA と Buchberger アルゴリズムにおける総簡約回数および 0 簡約回数の比較である. NF は総簡約回数, Z はその内の 0 簡約回数で, **冗長** は, Buchberger アルゴリズムでは現れない, 先頭項が生成済みの基底の先頭項で割り切れるような基底の個数を表す. 全般的には, 0 簡約回数が SBA において Buchberger アルゴリズムより減っている. しかし, 総簡約回数が増えている例がいくつかある. これらの例では, Buchberger アルゴリズムでは 0 簡約される, あるいは冗長と判断される基底が生成されていることがわかる. このような例, 特に reimer7 などでは, 冗長基底のために計算時間が多くかかっていると考えられる. 一方で, 総簡約回数も冗長基底も少ない例, 特に katsura12 などでは計算時間が大幅に短縮されている.

5.2 計算の詳細の比較

表 3 は, SBA における, 各 S ペア消去判定基準で消去された S ペアの個数の内訳で, syz は syzygy criterion (命題 22) で, sig は, 処理済み S ペアと同一 signature を捨てる criterion で, lm は, signature s の処理において, $s = mS(g)$ となる mg のうち先頭項が最小の mg が主成分の S ペアが存在しない場合に, signature s の S ペアを捨てる criterion (定理 19) でそれぞれ捨てられた S ペアの個数を表す. 表によれば, syzygy criterion が最も多く S ペア消去に寄与することがわかる. 一方で定理 19 による S ペア消去は, 数は少ないものの重要である. これを外すと, singular 簡約で 0 になるはずの基底が生成され, それから余分な S ペアが多数生成されることになる.

6 おわりに

ここで行った実験は, 有限体上の計算のみであり, SBA と Buchberger アルゴリズム, あるいは F_4 アルゴリズムなどとの計算効率の比較をより深く行うには, 有理数体上での計算も必要である. またここでは加群項順序として Schreyer 順序のみを用いたが, POT 順序を含むより多くの種類の項順序での比較も行う必要がある. 特に, POT 順序での計算は, $\langle f_1 \rangle$, $\langle f_1, f_2 \rangle$ ... に対するグレブナー基底を逐次的に計算すること

	SBA			Buchberger	
	NF	Z	冗長	NF	Z
f855	2429	949	1072	1881	1522
filter9	4792	1385	2767	2518	1863
hairer2	2680	430	2005	986	714
cyclic8	4359	720	2501	5925	4468
extcyc7	12879	1468	8436	17175	14076
noon9	4416	682	61	29182	25509
eco12	3452	1524	895	7199	6320
redeco12	2036	1013	0	8204	7181
reimer7	10468	1299	7160	3266	1907
katsura12	3364	1247	37	21763	19683

表 2: 簡約回数, 0 簡約回数の比較

	syz	sig	lm
f855	1026836	43979	1939
filter9	5596949	104061	7406
hairer2	2447165	55313	9553
cyclic8	6199422	160870	7947
extcyc7	62134296	1052454	18462
noon9	6706533	129642	221
eco12	1428487	229438	3115
redeco12	236162	171048	382
reimer7	38848413	1326332	12659
katsura12	1813535	207680	0

表 3: S ペア消去の内訳

になり, 0 簡約が一つも生じないような例も報告されている. しかし, 残念ながら Risa/Asir 上の実装ではまだそういう例は見つからず, 実装にまだ未熟な点がありそうである. 他に, 予備的実験で, 全次数逆辞書式でない項順序では, アルゴリズムが停止するまで Buchberger アルゴリズムと比べて長時間かかる場合も観測された. 項順序と加群項順序が compatible でない場合のアルゴリズムの停止性も, 全次数逆辞書式でない項順序での $\mathfrak{G}$-グレブナー基底計算を行う上で重要ではないかと考えている.

参 考 文 献

[1] J.-C. Faugère, A new efficient algorithm for computing Gröbner bases without reduction to zero (F_5), in Proc. ISSAC2002, 75-83, 2002.

[2] D. Cox, J. Little, D. O'Shea, Using Algebraic Geometry. GTM Vol. 185, Springer, 2005.

[3] A. Arri, J. Perry, The F5 criterion revised, J. Symb. Comp., 46, 1017-1029,2011. A revised version : https://arxiv.org/abs/1012.3664v6.

[4] C. Eder, J.-C. Faugère, A survey on signature-based algorithms for comptuing Gröbner bases, J. Symb. Comp., 80, 719-784, 2017.

[5] T. Vaccon, K. Yokoyama, A tropical F_5 algorithm, in Proc. ISSAC2017, 429-436, 2017.

[6] T. Vaccon, T. Verron, K. Yokoyama, An affine tropical F_5 algorithm, in Proc. ISSAC2018, 383-390, 2018.

[7] 阿部拓実, F_5 アルゴリズムの正当性と停止性について, 立教大学修士論文, 2019.

[8] 横山和弘, Signature-based アルゴリズムの正当性・停止性について, 計算機代数夏の学校 2019.

[9] W. Decker, G.-M. Greuel, G. Pfister, H. Schönemann, SINGULAR 4-2-0 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de, 2019.

[10] T. Vaccon, T. Verron, K. Yokoyama, An affine tropical F_5 algorithm, J. Symb. Comp., 102, 132-152, 2021.