アフィン半正則な多項式列に付随する Hilbert 級数と関連する Gröbner 基底

Hilbert series associated to affine semi-regular polynomial sequences and related Gröbner bases

福岡工業大学・情報工学部情報通信工学科　　工藤 桃成 [*1]
Momonari Kudo
Department of Information and Communication Engineering, Faculty of Information Enginerring, Fukuoka Institute of Technology

立教大学・理学部数学科　　横山 和弘 [*2]
Kazuhiro Yokoyama
Department of Mathematics, Faculty of Science, Rikkyo University

Abstract

In this article, we introduce some properties of Hilbert series associated to affine semi-regular sequences and related Gröbner bases, which are very useful to analyze the Gröbner basis computation. This article is a resume summarising the authors' recent papers [26] and [27].

1　序

本稿を通して, K を体, $\overline{K}$ をその代数閉包, $R = K[x_1, \ldots, x_n]$ を K 上の n 変数多項式環とし, 計算量は K における四則演算の回数で評価する. また, $R \setminus \{0\}$ の非空な部分集合 F が斉次元のみから成るとき F は斉次であるといい, そうでないとき F は非斉次または**アフィン (affine)** であるという. R の非空な部分集合 F が生成する R のイデアルを $\langle F \rangle_R$, または単に $\langle F \rangle$ と表す. $R \setminus \{0\}$ の非空な有限部分集合 F と R の項順序 $\prec$ が与えられたときに, $\prec$ に関する F の Gröbner 基底の計算量を精密に評価することは, 一般には非常に難しい問題だと考えられている. 実際, F と $\prec$ が一般の場合, 最悪の場合の計算量評価しか知られておらず, それは変数の個数に関して二重指数時間である (cf. [10], [30], [33]). ただし, F が非斉次であって, かつ $\langle F \rangle_R$ が零次元 (すなわち $D_F := \dim_K R/\langle F \rangle_R < \infty$) の場合は FGLM 基底変換 [18] を適用できて, ある項順序 $\prec_1$ に関する $\langle F \rangle_R$ の Gröbner 基底 G_1 がひとたび求まれば, G_1 を入力として別の任意の項順序 $\prec_2$ に関する $\langle F \rangle_R$ の Gröbner 基底 G_2 を $O(nD_F^\omega)$ の計算量で計算可能となる. ここで $2 \leq \omega < 3$ は行列積の指数である. F が斉次の場合も, 上記の G_1 がひとたび求まれば, Gröbner walk アルゴリズム [12] ($\prec_1, \prec_2$ ともに次数付きの場合は Hilbert driven アルゴリズム [37]) によって G_2 を効率的に計算できると期待される. 従って, 特定の項順序 (上記でいうところの $\prec_1$) に対して計算量を精密に評価できるかが問題である. 特に, 次数付き項順序 (特に次数付き逆辞書式順序) に関する Gröbner 基底は他の項順序の場合よりも高速に計算できることが経験則的に知られているため, 次数付き項順序の場合の計算量評価が重要となる.

[*1] 〒 811-0295 福岡県福岡市東区和白東 3-30-1　E-mail: m-kudo@fit.ac.jp
[*2] 〒 171-8501 東京都豊島区西池袋 3-34-1　E-mail: kazuhiro@rikkyo.ac.jp

現在, Gröbner 基底を効率的に計算する方法としては, F_4 [16], F_5 [17], XL [11], およびそれらの改良にあたるアルゴリズムを用いるのが標準的である. 特に F_4 や F_5 等の, Buchberger アルゴリズム [6] を基にしたアルゴリズムでは, (簡約すべき) S 多項式に対応する多項式のペア (**S ペア**と呼ぶ) を選択・収集する方法が, アルゴリズム全体の効率性に大きく影響する. 我々がいま対象としている次数付き項順序においては, そのような方法として, (非斉次かつ零次元の場合に限った話ではないが) **正規戦略 (normal strategy)** を採用し, S ペアの収集と S 多項式の簡約を繰り返すのが最も効率的だと考えられている. 具体的には, その時点で保持している中間基底 (入力 F およびそれまでの計算により F に追加された元全体) H について, 未処理の S ペア $(f,g) \in H^2$ $(f \neq g)$ のうち $\deg \mathrm{LCM}(\mathrm{LM}_\prec(f), \mathrm{LM}_\prec(g))$ の値が最小となるものを複数収集し, それらに対応する S 多項式 $S_\prec(f,g)$ を H で簡約する, というステップを繰り返す. ここで deg は総次数を表し, $\mathrm{LM}_\prec$ は (次数付き) 項順序 $\prec$ に関する先頭単項式を表す. このようなアルゴリズムでは, 各ステップにおいて収集する S ペア (f,g) の次数 $\deg \mathrm{LCM}(\mathrm{LM}_\prec(f), \mathrm{LM}_\prec(g))$ (または対応する $S_\prec(f,g)$ の総次数) の値はそのステップの **step degree** と呼ばれ, アルゴリズムの実行全体における step degree の最大値をそのアルゴリズムの**求解次数 (solving degree)** という (cf. [14], [27]). 求解次数の定義には Macaulay 行列を用いた別の定義もあり, 詳細は 3 節で述べる. いずれにしても, 求解次数を評価することで, 対象とするアルゴリズム全体の計算量評価が可能となる. 入力 F が斉次の場合は, 適切な設定の下, 正規戦略による Gröbner 基底計算において step degree を狭義単調に増加させることができて, 実質的に d-Gröbner 基底 (定義は [4, Section 10.2] を参照) を $d = 1, 2, \ldots$ と順に計算することに等価となる. この場合の求解次数は, 次数付き項順序 $\prec$ に関する F の簡約 Gröbner 基底を G_{red} としたとき, $\mathrm{max.GB.deg}_\prec(F) := \max\{\deg(g) : g \in G_{\mathrm{red}}\}$ に等しい. さらに $\prec$ が次数付き逆辞書式順序であれば, Lazard [28] による $\mathrm{max.GB.deg}_\prec(F)$ の上界 (**Lazard 上界**) を用いることで求解次数を上から評価できる. 一方で F がアフィン (非斉次) の場合, 求解次数は一般に $\mathrm{max.GB.deg}_\prec(F)$ 以上になり得るため, その評価は一般には難しい. ただし, $\prec$ に関する F の Gröbner 基底 G 自体は**斉次化** $F^h := \{f^h := y^{\deg(f)} f(x_1/y, \ldots, x_n/y) \in R[y] : f \in F\}$ の斉次化項順序 $\prec^h$ に関する Gröbner 基底から容易に復元できるため, Lazard 上界を F^h に適用することで, G の計算量を上から評価できる. ここで $\prec^h$ は y が変数の中で最下位となるよう $\prec$ を拡張した $R[y]$ の次数付き項順序である.

一方で, 入力のアフィン多項式集合 $F = \{f_1, \ldots, f_m\}$ が**過剰決定 (overdetermined)** (式の本数 $>$ 変数の個数), かつ最大斉次部分 $F^{\mathrm{top}} := \{f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}\}$ の生成する R のイデアル $\langle F^{\mathrm{top}} \rangle$ が **Artin 的 (Artinian)** である場合には, Lazard 上界よりもタイトな求解次数の上界が得られることがある. ここで $f \in R \setminus \{0\}$ に対して $f^{\mathrm{top}} := (f^h)|_{y=0}$ である. また, $\langle F^{\mathrm{top}} \rangle$ が Artin 的とはある非負整数 d_0 が存在して任意の $d \geq d_0$ に対し $\langle F^{\mathrm{top}} \rangle_d = R_d$ となるときをいい, そのような d_0 のうち最小のものを**正則性次数 (degree of regularity)** と呼び $D := d_{\mathrm{reg}}(F^{\mathrm{top}})$ と表す. 近年 Tenti [36] は, 有限体 $K = \mathbb{F}_q$ 上, かつ F が $\{x_i^q - x_i : 1 \leq i \leq n\}$ を含むなどの条件を満たす場合に, 求解次数が $2D-2$ 以下となるアルゴリズムの存在を構成的に示した. また, $\langle F^{\mathrm{top}} \rangle$ の Artin 性よりも強い条件として, $\boldsymbol{F} = (f_1, \ldots, f_m)$ が**半正則 (semi-regular)** である場合には, Bardet, Faugère らによって Gröbner 基底計算の解析がなされてきた. 詳細は 2 節で述べるが, 半正則な斉次多項式列とは, 正則な斉次多項式列の過剰決定な場合への拡張であり, アフィン多項式列 $\boldsymbol{F}$ の半正則性は $\boldsymbol{F}^{\mathrm{top}} := (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ のそれで定義される. アフィン半正則かつ共通解を少なくとも 1 つもつような $\boldsymbol{F}$ は多変数多項式暗号の構成において屡々現れるなど, アフィン半正則列は重要なクラスといえる. Bardet, Faugère らの既存研究では, F_5 アルゴリズム [17] において, D 未満の step degree では 0-reduction が起こりえないことや, 総計算量が $O(\binom{n+D}{D}^\omega)$ で上から評価できること, などの主張がある. しかしながら, 彼らの主張や証明は, 必要な仮定が抜けているなど数学的厳密性に欠けており, 正当性が保証されていない.

本稿では, アフィン半正則列に関連する Hilbert 級数と Gröbner 基底の性質に関して, 最近著者によって示された結果 (cf. [26], [27]) の一部を報告する. 特に, F^{top} と F^h に付随する Hilbert 級数の間の関係式を導出したが, これを利用することで Bardet, Faugère らの主張の補正や厳密な証明が可能となる. また, Tenti [36] の上記結果の, 一般のアフィン多項式集合 F への拡張となる結果を紹介する.

記号　次数付き加群 M および $d \in \mathbb{Z}$ に対し, M の d 次斉次部分を M_d と表す. つまり, $M = \bigoplus_{d\in\mathbb{Z}} M_d$ である. さらに, 整数 $\ell \in \mathbb{Z}$ に対して, $M(\ell)_d = M_{\ell+d}$ で定まる次数付き加群 $M(\ell)$ を M の ℓ-th twist と呼ぶ. また, M が有限生成次数付き R-加群のとき, R の Noether 性などから各 M_d は有限次元 K-線形空間であり, M の Hilbert 関数 HF_M, Hilbert 級数 $\mathrm{HS}_M(z)$ をそれぞれ $\mathrm{HF}_M(d) := \dim_K M_d$ $(d \in \mathbb{Z})$, $\mathrm{HS}_M(z) := \sum_{d\in\mathbb{Z}} \mathrm{HF}_M(d) z^d$ で定義する. R の項順序 $\prec$ に関する $f \in R \setminus \{0\}$ の先頭単項式を $\mathrm{LM}_\prec(f)$ と表し, 非空な部分集合 $F \subset R \setminus \{0\}$ に対し $\mathrm{LM}_\prec(F) := \{\mathrm{LM}_\prec(f) : f \in F\}$ とおく (文脈から $\prec$ が明白な場合は単に $\mathrm{LM}(f)$, $\mathrm{LM}(F)$ と表す). また, $f \in R$ の次数 $\deg(f)$ は総次数を意味し, $d \in \mathbb{Z}_{\geq 0}$ に対し $F_d := \{f \in F : \deg(f) = d\}$ と定め, $F_{\leq d} := \bigcup_{i=0}^{d} F_i$ とおく. $f \in R \setminus \{0\}$ の斉次化を $f^h := y^{\deg(f)} f(x_1/y, \ldots, x_n/y) \in R[y]$ と定める.

2　準備

以下では特に断らない限り $f_1, \ldots, f_m \in R = K[x_1, \ldots, x_n]$ を 1 次以上の斉次多項式とし, それらの総次数をそれぞれ $d_1, \ldots, d_m$ とする. つまり, 各 $1 \leq i \leq m$ に対して $d_i := \deg(f_i) \geq 1$ である. また, $1 \leq j_1 < \cdots < j_i \leq m$ を満たす i 個の自然数 $j_1, \ldots, j_i$ に対して $d_{j_1\cdots j_i} := \sum_{k=1}^{i} d_{j_k}$ とおく. このとき, 各 $0 \leq i \leq m$ に対して, 階数 $\binom{m}{i}$ の次数付き自由 R-加群 $K_i(f_1, \ldots, f_m)$ を次で定義する :

$$K_i(f_1, \ldots, f_m) := \begin{cases} \displaystyle\bigoplus_{1\leq j_1<\cdots<j_i\leq m} R(-d_{j_1\cdots j_i})\mathbf{e}_{j_1\cdots j_i} & (i \geq 1), \\ R & (i = 0). \end{cases}$$

ここで $\mathbf{e}_{j_1\cdots j_i}$ は標準基底の元である. 次数 0 の次数付き準同型

$$\varphi_i : K_i(f_1, \ldots, f_m) \longrightarrow K_{i-1}(f_1, \ldots, f_m)$$

を, 標準基底の像を

$$\varphi_i(\mathbf{e}_{j_1\cdots j_i}) := \sum_{k=1}^{i} (-1)^{k-1} f_{j_k} \mathbf{e}_{j_1\cdots \hat{j_k} \cdots j_i}.$$

と定めることで定義する. ここで $\hat{j_k}$ は j_k を省略することを意味し, 例えば, $\mathbf{e}_{1\hat{2}3} = \mathbf{e}_{13}$ である. 記号を簡略化するため, $K_i := K_i(f_1, \ldots, f_m)$ とおく. このとき, 写像列

$$K_\bullet : 0 \xrightarrow{\varphi_{m+1}} K_m \xrightarrow{\varphi_m} \cdots \xrightarrow{\varphi_3} K_2 \xrightarrow{\varphi_2} K_1 \xrightarrow{\varphi_1} K_0 \xrightarrow{\varphi_0} 0 \tag{2.1}$$

は次数付き R-加群の複体である.

定義 1
上の記号の下で, 複体 $K_\bullet$ を斉次多項式列 $(f_1, \ldots, f_m)$ 上の **Koszul 複体 (Koszul complex)** という.

一般に次数付き準同型の核と像は次数付き加群であるため, 各 $0 \leq i \leq m$ に対して $\mathrm{Ker}(\varphi_i)$ と $\mathrm{Im}(\varphi_{i+1})$ は次数付き R-加群であり, Koszul 複体 $K_\bullet$ の i 次ホモロジー群 $H_i(K_\bullet) := \mathrm{Ker}(\varphi_i)/\mathrm{Im}(\varphi_{i+1})$ もそうである (さらには各斉次部分が有限次元 K-線形空間となるような有限生成次数付き R-加群である). 特に $H_0(K_\bullet) = R/\langle f_1, \ldots, f_m\rangle_R$, $H_m(K_\bullet) = 0$ であることに注意する. 1 次ホモロジー群については $(f_1, \ldots, f_m)$ のシジジーを用いて以下のように書き下すことができる. まず, $\mathrm{Ker}(\varphi_1) = \mathrm{syz}(f_1, \ldots, f_m)$ (右辺はシジジー加群 $\{\sum_{j=1}^m h_j \mathbf{e}_j \in \bigoplus_{j=1}^m R(-d_j)\mathbf{e}_j : \sum_{j=1}^m h_j f_j = 0\}$) である. また, $\mathrm{Im}(\varphi_2) \subset K_1 = \bigoplus_{j=1}^m R(-d_j)\mathbf{e}_j$ は $\{\mathbf{t}_{i,j} := f_i\mathbf{e}_j - f_j\mathbf{e}_i : 1 \leq i < j \leq m\}$ によって生成される. 従って,

$$\mathrm{tsyz}(f_1, \ldots, f_m) := \langle \mathbf{t}_{i,j} : 1 \leq i < j \leq m\rangle_R$$

とおけば, 次が成り立つ :

$$H_1(K_\bullet) = \mathrm{syz}(f_1, \ldots, f_m)/\mathrm{tsyz}(f_1, \ldots, f_m). \tag{2.2}$$

定義 2
上の記号の下で, $\mathrm{tsyz}(f_1,\dots,f_m)$ を**自明なシジジーの加群 (module of trivial syzygies)** といい, 各生成元 $\mathbf{t}_{i,j}$ (あるいは $\mathrm{tsyz}(f_1,\dots,f_m)$ の各元) を $(f_1,\dots,f_m)$ の**自明なシジジー (trivial syzygy)** という.

次に, Castelnuovo-Mumford 正則量, 正則性次数, 半正則性の定義を復習する. M を有限生成次数付き R-加群とするとき, Hilbert の syzygy 定理により, M は長さ $\ell \leq n$ の極小自由分解

$$\mathbf{F}_\bullet \ : \ 0 \longrightarrow \bigoplus_{j=1}^{b_\ell} R(-a_{\ell,j}) \xrightarrow{\varphi_\ell} \cdots \xrightarrow{\varphi_2} \bigoplus_{j=1}^{b_1} R(-a_{1,j}) \xrightarrow{\varphi_1} \bigoplus_{j=1}^{b_0} R(-a_{0,j}) \xrightarrow{\varphi_0} M \longrightarrow 0$$

をもつ. ここで各 φ_i は次数 0 の次数付き準同型であり, 斉次多項式を成分にもつ行列で表現される.

定義 3
上記の記号の下で,

$$\mathrm{reg}(M) := \max\{a_{i,j} - i : 0 \leq i \leq \ell,\ 1 \leq j \leq b_i\} < \infty$$

と定義し, これを M の **Castelnuovo-Mumford 正則量 (Castelnuovo-Mumford regularity)** という.

定義 4
M が **Artin 的 (Artinian)** であるとは, ある整数 d_0 が存在して, $d \geq d_0$ を満たす任意の整数 d に対して $M_d = 0$ となるときをいう.

M が Artin 的であれば $\mathrm{reg}(M) = \max\{d : M_d \neq 0\}$ となる (cf. [15, Corollary 4.4]). いま, 斉次多項式集合の正則性次数を定義する.

定義 5 ([2, Definition 4], [3, Definition 4])
斉次多項式集合 $F = \{f_1,\dots,f_m\}$ の**正則性次数 (degree of regularity)** を, $R/\langle F\rangle_R$ が Artin 的の場合は

$$d_{\mathrm{reg}}(F) := \min\{d \in \mathbb{Z}_{\geq 0} : R_d = \langle F\rangle_d\} = \deg(\mathrm{HS}_{R/\langle F\rangle_R}) + 1$$

と定義し, $R/\langle F\rangle_R$ が Artin 的でない場合は $d_{\mathrm{reg}}(F) := \infty$ で定義する.

注意 1
定義 5 において, $R/\langle F\rangle_R$ が Artin 的ならば, $d_{\mathrm{reg}}(F) = \mathrm{reg}(R/\langle F\rangle_R) + 1 = \mathrm{reg}(\langle F\rangle_R)$ が成り立つ. 一方, $R/\langle F\rangle_R$ が Artin 的でないならば, $\mathrm{reg}(\langle F\rangle_R) < \infty = d_{\mathrm{reg}}(F)$ である.

斉次多項式列が半正則であることの定義を復習する. よく知られているように, 斉次多項式列の半正則性には以下に述べる 2 種類の定義があり, 一方は他方より強い条件で定義される. 本稿では, 弱い条件である, Bardet らによる半正則性の定義を採用する. 以下, 斉次多項式列の d-正則性, 半正則性を定義する.

定義 6 ([2, Definition 3], [13, Definition 1 and Theorem 1])
記号は上の通りとし, d を自然数で $d \geq \max\{d_i : 1 \leq i \leq m\}$ を満たすものとする. このとき, 斉次多項式列 $\boldsymbol{F} = (f_1,\dots,f_m) \in R^m$ が **d-正則 (d-regular)** であるとは, 次の同値条件を満たすときをいう :

1. 任意の $i \in \{1,\dots,m\}$, および $d_i \leq t < d$ を満たす任意の自然数 t に対して, $t - d_i$ 次斉次多項式 $g \in R_{t-d_i}$ が $gf_i \in \langle f_1,\dots,f_{i-1}\rangle_R$ を満たすならば $g \in \langle f_1,\dots,f_{i-1}\rangle_R$ である.
2. 等式 $\mathrm{HS}_{R/\langle f_1,\dots,f_m\rangle_R}(z) \equiv \frac{\prod_{j=1}^m (1-z^{d_j})}{(1-z)^n} \pmod{z^d}$ が成り立つ.
3. $\boldsymbol{F}$ 上の Koszul 複体を $K_\bullet$ とするとき, その 1 次ホモロジー群 (2.2) に関して $H_1(K_\bullet)_{\leq d-1} = 0$ が成り立つ. ここで $H_1(K_\bullet)_{\leq d-1}$ は次数付き R-加群 $H_1(K_\bullet)$ の次数 $d-1$ 以下の斉次部分全ての直和である.

定義 7 ([2, Definition 5], [3, Definition 5 and Proposition 6], [13, Proposition 1 (d)])
(1 次以上の) 斉次多項式のなす列 $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ が**半正則 (semi-regular)** であるとは, 次の同値条件を満たすときをいう.

1. $F = \{f_1, \ldots, f_m\}$ の正則性次数 $D := d_{\mathrm{reg}}(F)$ に対して, $\boldsymbol{F}$ は D-正則である (すなわち $d = D$ に対し定義 6 に述べた同値条件が満たされる).
2. 等式 $\mathrm{HS}_{R/\langle f_1,\ldots,f_m\rangle_R}(z) = \left[\frac{\prod_{j=1}^m (1-z^{d_j})}{(1-z)^n}\right]$ が成り立つ. ここで $[\cdot]$ は非正係数をもつ最小次数項での打ち切り (そのような項の次数以上の項は 0 とみなす) を表す.

定義 6, 定義 7 の同値性の証明については, [13] の Theorem 1, Proposition 1 をそれぞれ参照せよ. 定義 6 の条件 2 から, 斉次多項式列の d-正則性, 半正則性は実際には多項式の順序によらない. また, 斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m)$ について, $\boldsymbol{F}$ が d-正則であればその任意の部分列 $\boldsymbol{F}_i := (f_1, \ldots, f_i)$ も d-正則となるが (cf. [13, Proposition 2 (a)]), $\boldsymbol{F}$ が半正則であっても $\boldsymbol{F}_i$ が半正則になるとは限らないことに注意する.

注意 2
$m \leq n$ ならば, 斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ が半正則であることは, $\boldsymbol{F}$ が**正則 (regular)** であることに同値である. ここで $\boldsymbol{F}$ が正則であるとは, $\mathrm{HS}_{R/\langle f_1,\ldots,f_m\rangle_R}(z) = \frac{\prod_{j=1}^m (1-z^{d_j})}{(1-z)^n}$ を満たすときをいい (同値な, そして定義 6 の条件 1 に類似の定義として [22, Definition 7.6.1] を参照), このとき $\boldsymbol{F}$ の任意の部分列 $(f_1, \ldots, f_i)$ も正則である. $\boldsymbol{F}$ が正則であれば $\boldsymbol{F}$ 上の Koszul 複体 (2.1) のホモロジーは $H_i(K_\bullet) = 0$ $(i \geq 1)$ を満たす. また, $R = K[x_1, \ldots, x_n]$ の斉次元からなる正則列の長さは n 以下であることが証明できる (cf. [22, Section 7.6]). 以上を踏まえると, 半正則列は正則列の過剰決定 $(m > n)$ な場合への拡張とみなせる.

注意 3
Fröberg [19] により, 無限体上において斉次多項式列 $\boldsymbol{F}$ は generic に半正則であることが予想されている. 正確にいえば, K を無限体とし, 各 d に対し $N_d := \binom{n+d-1}{d}$ とおいて d 次斉次部分 R_d をアフィン空間 $\mathbb{A}^{N_d}(K)$ と自然に同一視するとき, 任意の自然数 n, m, $d_1, \ldots, d_m$ に対し,

$$V := \left\{\boldsymbol{F} = (f_1, \ldots, f_m) \in \mathbb{A}^{N_{d_1}}(K) \times \cdots \times \mathbb{A}^{N_{d_m}}(K) : \boldsymbol{F} \text{ は半正則}\right\}$$

は Zariski 位相に関して非空な開集合である, と予想される. よく知られているように, この予想は少なくとも $m \leq n$ であれば正しい.

注意 4
Pardue [32] は斉次多項式列の半正則性を, Bardet らの定義より強い条件で定義している. 具体的には, 斉次多項式列 $\boldsymbol{F} = (f_1, \ldots, f_m) \in R^m$ が Pardue の意味で半正則 (または**強半正則**) であるとは, $1 \leq i \leq m$ を満たす任意の自然数 i に対して等式 $\mathrm{HS}_{R/\langle f_1,\ldots,f_i\rangle_R}(z) = \left[\frac{\prod_{j=1}^i (1-z^{d_j})}{(1-z)^n}\right]$ が成り立つときをいう. 定義から明らかに強半正則列は半正則列であり, $m \leq n$ であれば正則, 半正則, 強半正則は全て同値となる. $m > n$ の場合に半正則列が強半正則列となるか否かは不明だが, Pardue は無限体上における「斉次多項式列が generic に半正則であること」と「斉次多項式列が generic に強半正則であること」の同値性, および Moreno-Socías 予想 [31] の主張はこれらよりも強い条件であることを示している (cf. [32, Theorem 2]).

アフィン多項式列 (斉次とは限らない多項式列) については, その最大斉次部分により半正則性を定義する.

定義 8
アフィン多項式列 $\boldsymbol{F} := (f_1, \ldots, f_m) \in R^m$ が**半正則 (semi-regular)** であるとは, その最大斉次部分 $\boldsymbol{F}^{\mathrm{top}} := (f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}})$ が半正則であるときをいう. ここで $f \in R \setminus \{0\}$ に対し $f^{\mathrm{top}} := (f^h)|_{y=0}$ である.

注意 5
十分大きい体上で, $m > n$ の条件下で n 変数 m 本の非斉次多項式 $f_1, \ldots, f_m$ をランダム生成する場合, Fröberg 予想 [19] を仮定しても, 「$\boldsymbol{F} = (f_1, \ldots, f_m)$ が半正則であり, 同時に $F = \{f_1, \ldots, f_m\}$ が $\overline{K}$ 上で共通零点をもつこと」は起こりにくいと考えられる. 実際, 係数を独立一様ランダムに選ぶことで上記の $f_1, \ldots, f_m$ が生成されたとき, Fröberg 予想が正しければ, 高確率で $\boldsymbol{F}^{\mathrm{top}}$ は半正則となることが期待できる. 一方, 斉次化 $\boldsymbol{F}^h = (f_1^h, \ldots, f_m^h)$ についても同様のことがいえて $\mathrm{HS}_{R[y]/\langle F^h \rangle}(z) = \left[\frac{\prod_{j=1}^{m}(1-z^{d_j})}{(1-z)^{n+1}} \right]$ となるので, $m > n$ であれば $\mathrm{HS}_{R[y]/\langle F^h \rangle}(z)$ は多項式となり, 従って $F^h = \{f_1^h, \ldots, f_m^h\}$ は $(0, \ldots, 0)$ 以外に $\overline{K}^{n+1}$ 内で共通零点をもたない. よって特に, F も $\overline{K}^n$ 内に共通零点をもたない. ここで, 一般に R の斉次イデアル I に対して, I の $\overline{K}$ 上の射影的零点 (すなわち $(x_1, \ldots, x_n) = (0, \ldots, 0)$ 以外の $\overline{K}$ 上の共通解を定数倍で同一視したもの) が存在しないことは, $\mathrm{HS}_{R/I}(z)$ が多項式となることに同値である (この同値性が明文化されている文献はあまり見当たらないが既知の事実であり, 例えば [10, Proposition 3.3.7] を参照).

$\boldsymbol{F} = (f_1, \ldots, f_m)$ がアフィン半正則であり, 同時に F が $\overline{K}$ 上で共通零点をもつようになるのは, 例えば, 最大斉次部分 $f_1^{\mathrm{top}}, \ldots, f_m^{\mathrm{top}}$ がランダムに生成され, 一方で低次の項には '従属性' がもたされるような場合である. 例えば, 係数を独立一様ランダムに選ぶことで n 変数 m 本の斉次多項式 $g_1, \ldots, g_m$ を生成し, 点 $(a_1, \ldots, a_n) \in K^n$ を任意に選んだ後, 各 $i \in \{1, \ldots, m\}$ に対して $f_i := g_i(x_1, \ldots, x_n) - g_i(a_1, \ldots, a_n)$ と定めれば, F は $\overline{K}$ 上で共通零点 $(a_1, \ldots, a_n)$ をもち, かつ高確率で $\boldsymbol{F}^{\mathrm{top}}$ は半正則になると期待できる.

Bardet, Faugère らは, アフィン半正則列 $\boldsymbol{F} := (f_1, \ldots, f_m) \in R^m$ について, 入力 $F = \{f_1, \ldots, f_m\}$ に対する Gröbner 基底計算の解析を行い, ある種の heuristic の下で次の定理 9 が成り立つと主張している.

定理 9 ([1], [3, Proposition 6 (iv)])
$\boldsymbol{F} := (f_1, \ldots, f_m) \in R^m$ をアフィン半正則列とする. このとき, 入力 $F = \{f_1, \ldots, f_m\}$ に対して F_5 アルゴリズム [17] を実行した場合, $d < d_{\mathrm{reg}}(F^{\mathrm{top}})$ なる各 step degree d で 0-reduction は起こらない. また, $D := d_{\mathrm{reg}}(F^{\mathrm{top}})$ とおくとき, F_5 アルゴリズムの総計算量は $O(\binom{n+D}{D}^{\omega})$ で上から評価される.

3 求解次数 (solving degree)

本節では, 求解次数の定義を復習した後, その性質および評価に関する既存結果の一部を紹介する. 求解次数は Gröbner 基底の計算量を評価する上で重要な役割を果たす特徴量であって, Ding-Schmidt の論文 [14] で初めてその名称が登場し, 近年特に Gorla ら (cf. [5], [8], [9], [20], [21]) によって研究されてきた. ただし, 求解次数には複数の定義があって, 著者の知る限り, 以下に述べる 3 種類の定義が存在する.

第一の定義として, 1 節で述べたように, 正規戦略により Gröbner 基底を計算するアルゴリズム (**正規戦略アルゴリズム**) を実行した際の step degree の最大値を**求解次数 (solving degree)** と呼ぶ. この定義は Ding-Schmidt によって初めて与えられた (cf. [14, p. 36]). 彼らの論文 [14] では, アルゴリズムの実行中に最も計算時間のかかる step degree を求解次数と呼んでいる箇所もあり, 暗号の分野では屡々こちらの定義が採用されているが, そのように定義すると求解次数はアルゴリズムの実装方法にも依存し得るため, 本稿では考えないものとする. また, step degree を各ステップにおいて (その次数が最小になるよう) 収集する S ペア (f, g) の次数 $\deg \mathrm{LCM}(\mathrm{LM}_{\prec}(f), \mathrm{LM}_{\prec}(g))$ ではなく, 対応する S 多項式の次数 $\deg S_{\prec}(f, g)$ と定義する場合は, 求解次数はアルゴリズムの実行全体において実際に生成された S 多項式の次数の最大値に他ならない (この定義は [36] や, [35] などで採用されている). 求解次数は, 実行する正規戦略アルゴリズムを $\mathcal{A}$ としたとき, その入力多項式集合 F と項順序 $\prec$ にも依存するので, 本稿では $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ と表すことにする.

第二の定義として, **Macaulay 行列 (Macaulay matrix)** を用いるものがあり, この定義による求解次数は採用するアルゴリズムには依存せず入力多項式集合 F と次数付き項順序 $\prec$ にのみ依存する. ここで

Macaulay 行列とは, 係数体 K 上の行列であって, 非空かつ有限な多項式集合 $S \subset R$ と次数付き項順序 $\prec$ に対して以下のように定義される：$d = \max\{\deg(f) : f \in S\}$ とおき, R における d 次以下の単項式全体のなす集合を $\mathcal{T}_{\leq d}$ とおいて, その元を $\prec$ に関して降順に並べて $\mathcal{T}_{\leq d} = \{t_1, \ldots, t_{\ell-1}, t_\ell = 1\}$ とする. また, S の元を任意に並べて $S = \{h_1, \ldots, h_k\}$ とし, 各元を $a_{i,j} \in K$ を用いて $h_i = \sum_{j=1}^{\ell} a_{i,j} t_j$ と表す. このとき, $k \times \ell$ 行列 $(a_{i,j})_{i,j}$ を次数付き項順序 $\prec$ に関する S の Macaulay 行列といい, 項順序 $\prec$ を固定したとき $\mathrm{Mac}(S)$ と表す. Lazard [28] は, 十分大きい d に対して $\mathcal{S}_{\leq d}(F) := \{tf : f \in F_{\leq d},\ t \in \mathcal{T}_{\leq d-\deg(f)}\}$ を生成し, $\mathrm{Mac}(\mathcal{S}_{\leq d}(F))$ の行簡約階段形に対応する多項式集合として $\prec$ に関する $\langle F\rangle_R$ の Gröbner 基底を求める方法を示した (その方法を基にしたアルゴリズムとして XL [11] が後に提案され, 現在ではその様々な改良が存在する). Caminata-Gorla は [8] において, $\mathrm{Mac}(\mathcal{S}_{\leq d}(F))$ の行簡約階段形に対応する多項式集合を $B_{\leq d}(F)$ と表すとき, $B_{\leq d}(F)$ が $\prec$ に関する $\langle F\rangle_R$ の Gröbner 基底となるような最小の非負整数 d を, F の求解次数と定義した. 本稿では Caminata-Gorla [8] によって定義されたこの求解次数を $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ と表す.

第三の定義は, 第二の定義の亜種であり, より小さい値になり得るという意味で改良ともいえる. 詳細を述べると, 第二の定義では 1 つの d に対する Macaulay 行列 $\mathrm{Mac}(\mathcal{S}_{\leq d}(F))$ の簡約を考えたが, ここでは $d = 1, 2, \ldots$ と小さい順に $\mathrm{Mac}(\mathcal{S}_{\leq d}(F))$ を簡約し, 各 d における簡約結果として得られる多項式を F に加えていくことで次数付き項順序 $\prec$ に関する Gröbner 基底を求める戦略を考える. ただし, 各 d における簡約では, $M := \mathrm{Mac}(\mathcal{S}_{\leq d}(F))$, $B := B_{\leq d}(F)$ とおいて, $\deg(f) < d$ を満たす多項式 $f \in B$ であって, $\mathrm{LM}_{\prec}(f)$ が M の行に対応する多項式の先頭単項式として現れないようなものが得られた場合, $B' := B \cup \{tf : t \in \mathcal{T}_{\leq d-\deg(f)},\ tf \notin \langle B\rangle_K\}$ に対応する Macaulay 行列 $\mathrm{Mac}(B')$ を改めて M とおき, M を行簡約して得られる多項式集合を改めて B とおく. この操作を, 上記のような f が得られなくなるまで繰り返して $\langle F\rangle_R$ の生成集合を拡張した後, 拡張された生成集合が Gröbner 基底でなければ d を $d+1$ に置き換えて同様の操作を行う (詳細は紙数の都合上 [9, Section 1] または [27, Section 3] を参照). 以上の戦略は Mutant-XL アルゴリズム [7] において既に用いられていたため, [20] や [34] では **mutant 戦略 (mutant strategy)** と名付けられている. 上記の mutant 戦略によって $\prec$ に関する $\langle F\rangle_R$ の Gröbner 基底が得られる最小の d を求解次数と定義し, $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ と表す. 定義から直ちに次の不等式

$$\max.\mathrm{GB.deg}_{\prec}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mac}}(F) \tag{3.1}$$

が得られる. 実際には, $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ は $\max.\mathrm{GB.deg}_{\prec}(F)$ と F の **last fall degree** d_F (定義は [23], [24], または [9] を参照) のうち大きい方に一致する (cf. [9, Theorem 3.1]). 他にも, [9] において $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ に関する諸性質が調べられているので参照されたい. ただし [9] では $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ を表す記号として $\mathrm{sd}_{\prec}(F)$ が用いられているので注意する (第一・二の定義を含め, 我々の記号 $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$, $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$, $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ は [9] の記号 $\mathrm{sd}_{\prec}(F)$ を基にして区別のために新たに導入したものである).

もし F が斉次なら, 正規戦略で Gröbner 基底を計算することは, 斉次イデアル $\langle F\rangle_R$ の d-Gröbner 基底 (定義は紙数の都合で省略するので [4, Section 10.2] を参照) を $d = 1, 2, \ldots$ と順に計算することに他ならず, そのような計算を行う任意の正規戦略アルゴリズム $\mathcal{A}$ に対して $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F) = \mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ が成り立ち, さらに (3.1) において等号が成り立つ. 従って, 求解次数の上界として, $\max.\mathrm{GB.deg}_{\prec}(F)$ の上界を適用できる. 実際, F の $\overline{K}$ 上の射影的零点が高々有限個なら, F に適切な線形変数変換を施した後, 次の定理 10 に述べる **Lazard 上界** (3.2) (**Macaulay 上界**とも呼ばれる) を適用できる.

定理 10 ([28, Theorem 2], [29, Théorèm 3.3])
上記の記号の下で, F の $\overline{K}$ 上の射影的零点は高々有限個 *(*従って $m \geq n-1$*)* であるものとし, $f_1 = \cdots = f_m = 0$ は $\overline{K}$ 上で $x_n = 0$ の非自明解をもたないとする. さらに, $d_1 \geq \cdots \geq d_m$ と仮定すると, x_n が変数の中で最下位となるような任意の次数付き逆辞書式順序 $\prec$ に対して, $\ell := \min\{m, n\}$ とおくとき, 次が成り立つ：

$$\max.\mathrm{GB.deg}_{\prec}(F) \leq d_1 + \cdots + d_\ell - \ell + 1. \tag{3.2}$$

一方で F が非斉次の場合, (3.1) において等号が成立するとは限らない. また, $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ と $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ の大小関係も不明であり, これらを評価するのは一般には難しい. しかし, F を斉次化して考えることで, $\prec$ に関する F の Gröbner 基底の計算量を評価できる場合がある (特に $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ を上から評価できる). $\prec$ を R における次数付き項順序とする. y を斉次化に用いる新たな変数として, $x_1, \ldots, x_n, y$ の中で y が最下位となるように $\prec$ を拡張して得られる $R[y]$ 上の次数付き項順序を $\prec^h$ と表し, これを項順序 $\prec$ の y による**斉次化項順序** (あるいは単に**斉次化**) という. $\prec$ が次数付き逆辞書式順序であれば $\prec^h$ もそうであることに注意する.

補題 11 ([25, Proposition 4.3.18])
記号は上の通りとするとき, もし $\tilde{G}$ が $\prec^h$ に関する $\langle F^h \rangle_{R[y]}$ の Gröbner 基底であれば, $\tilde{G}$ の非斉次化 $G := \tilde{G}|_{y=1} = \{g(x_1, \ldots, x_n, 1) : g \in \tilde{G}\}$ は次数付き項順序 $\prec$ に関する $\langle F \rangle_R$ の Gröbner 基底である.

従って, F^h が定理 10 と同様の仮定を満たし, かつ $\prec$ が次数付き逆辞書式順序であれば, $\prec$ に関する $\langle F \rangle_R$ の Gröbner 基底を計算するコストは, $\prec^h$ に関する $\langle F^h \rangle_{R[y]}$ の Gröbner 基底を計算するコストで上から評価できる. 実際, $d_1 \geq \cdots \geq d_m$ と仮定した上で, F が零次元 (すなわち $\dim_K R/\langle F \rangle_R < \infty$) で, かつ F^{top} が $\overline{K}$ 上で $(0, \ldots, 0)$ 以外に共通零点をもたなければ, 定理 10 を適用できて, $\ell := \min\{m, n+1\}$ に対して

$$\mathrm{max.GB.deg}_{\prec^h}(F^h) \leq d_1 + \cdots + d_\ell - \ell + 1 \tag{3.3}$$

となる. ここで, F^{top} が $\overline{K}$ 上で $(0, \ldots, 0)$ 以外に共通零点をもたないことは, $R/\langle F^{\mathrm{top}} \rangle$ が Artin 的であることに同値である (cf. [10, Proposition 3.3.7]). また, 一般の次数付き項順序 $\prec$ に対して

$$\mathrm{max.GB.deg}_{\prec}(F) \leq \mathrm{sd}_{\prec}^{\mathrm{mac}}(F) \leq \mathrm{sd}_{\prec^h}^{\mathrm{mac}}(F^h) = \mathrm{max.GB.deg}_{\prec^h}(F^h)$$

が成り立ち, 特に $\prec$ が次数付き逆辞書式順序であれば中央の求解次数間の不等号は等号となる (証明は [8] を見よ). 従って $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ についても, (3.3) の右辺で上から評価できる.

$\langle F \rangle$ の簡約 Gröbner 基底の最大次数について, もし $R/\langle F^{\mathrm{top}} \rangle$ が Artin 的であれば, R における任意の次数付き項順序 $\prec$ に対して

$$\mathrm{max.GB.deg}_{\prec}(F) \leq d_{\mathrm{reg}}(F^{\mathrm{top}}) \tag{3.4}$$

が成り立つ (cf. 後述の定理 15 (4)). この不等式の証明は [8, Remark 15] にも書かれているが, 定理 15 (4) は別の方法で証明されているので, 原著 [26] を適宜参照されたい. また, 正則性次数 $d_{\mathrm{reg}}(F^{\mathrm{top}})$ と求解次数 $\mathrm{sd}_{\prec}^{\mathrm{mac}}(F)$ はいずれも $\mathrm{max.GB.deg}_{\prec}(F)$ 以上である一方, 前者 2 つの値は (仮に F が半正則であっても) 一致するとは限らないことに注意する. 実際, [5], [8], [9] に具体例が示されている.

一方 Tenti [36] は, K が位数の小さい有限体で, かつ F が field equation と呼ばれる多項式を含む場合に, 求解次数 $\mathrm{sd}_{\prec}^{\mathcal{A}}(F)$ が正則性次数に関して線形となるような Buchberger-like アルゴリズム $\mathcal{A}$ の存在を示した:

定理 12 ([35, Theorem 2.1], [36, Theorem 3.65 & Corollary 3.67])
上記の記号の下で, $K = \mathbb{F}_q$ と仮定し, $\{x_i^q - x_i : 1 \leq i \leq n\} \subset F$ を満たすものとする. $D := d_{\mathrm{reg}}(F^{\mathrm{top}})$ とおくとき, もし $D < \infty$ かつ $D \geq \max\{q, \max\{\deg(f) : f \in F\}\}$ であれば, ある正規戦略アルゴリズム $\mathcal{A}$ が構成的に存在して, 本節 (または 1 節) 2 段落目の step degree を各ステップで収集する S ペアの次数 (resp. 対応する S 多項式の次数) と定めるとき $\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D - 1$ (resp. $\mathrm{sd}_{\prec}^{\mathcal{A}}(F) \leq 2D - 2$) を満たす. さらに $\mathcal{A}$ の計算量は, K における四則演算の回数として

$$O(L_q(n, D)^2 L_q(n, D-1)^2 L_q(n, 2D-2)) \tag{3.5}$$

となる. ここで $L_q(n, d)$ は $\mathbb{F}_q[x_1, \ldots, x_n]/\langle x_1^q, \ldots, x_n^q \rangle$ における次数 d 以下の単項式の総数を表す.

また, $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F)$ に関して, 最近 Salizzoni は $D \geq \max\{\deg(f) : f \in F\}$ であれば $\mathrm{sd}_{\prec}^{\mathrm{mut}}(F) \leq D + 1$ が成り立つことを示した (cf. [34, Theorem 1.1]).

4　主結果

ここでは [26], [27] において得られた結果の一部を報告する．$f_1,\dots,f_m \in R \setminus K$ をそれぞれ総次数 $d_1,\dots,d_m$ の (斉次とは限らない) 多項式とし, $F=\{f_1,\dots,f_m\}$ とおき, その最大斉次部分 F^{top} および斉次化 F^h をそれぞれ $F^{\mathrm{top}}=\{f_1^{\mathrm{top}},\dots,f_m^{\mathrm{top}}\}$, $F^h=\{f_1^h,\dots,f_m^h\}$ とする．多項式列 $\boldsymbol{F}=(f_1,\dots,f_m)$ に対して, $\boldsymbol{F}^{\mathrm{top}}$ および $\boldsymbol{F}^h$ を F の場合と同様に定める．また, $\prec$ を R の次数付き項順序とする．

定理 13 ([26, Theorems 1 & 7, Corolary 1], [27, Theorem 1])
記号は上の通りとし, $D:=d_{\mathrm{reg}}(F^{\mathrm{top}})$ とおく．このとき, もし $\boldsymbol{F}$ が半正則であれば次が成り立つ：

(1) $d<D$ を満たす任意の非負整数 d に対して, $\mathrm{HF}_{R[y]/\langle F^h\rangle}(d)=\mathrm{HF}_{R/\langle F^{\mathrm{top}}\rangle}(d)+\mathrm{HF}_{R[y]/\langle F^h\rangle}(d-1)$ が成り立ち, 従って $\mathrm{HF}_{R[y]/\langle F^h\rangle}(d)=\sum_{i=0}^{d}\mathrm{HF}_{R/\langle F^{\mathrm{top}}\rangle}(i)$ となる．

(2) Hilbert 関数 $\mathrm{HF}_{R[y]/\langle F^h\rangle}$ は単峰的 (unimodal) であり, $d=D-1$ で最大値をとる．より詳しく言えば, $(R[y]/\langle F^h\rangle)_{d-1}$ から $(R[y]/\langle F^h\rangle)_d$ への y 倍写像は, $d<D$ を満たす任意の非負整数 d に対し単射であり, $d\geq D$ を満たす任意の非負整数 d に対し全射となる．

(3) ある非負整数 d_0 が存在して, $d\geq d_0$ を満たす任意の整数 d に対して $\mathrm{HF}_{R[y]/\langle F^h\rangle}(d_0)=\mathrm{HF}_{R[y]/\langle F^h\rangle}(d)$ が成り立つ．すなわち, F^h の代数閉包 $\overline{K}$ 上の射影的零点の個数は高々有限個である．この d_0 は $\langle F^h\rangle$ の $\prec^h$ に関する簡約 Gröbner 基底の最大次数の上界を与えることに注意する (cf. [27, Lemma 2.2.2])．

(4) 等式 $\mathrm{HS}_{R[y]/\langle F^h\rangle}(z)\equiv\frac{\prod_{j=1}^{m}(1-z^{d_j})}{(1-z)^{n+1}}\pmod{z^D}$ が成り立ち, 従って F^h は D-正則である．

定理 13 (2), (3) は同定理 (1) の証明の過程で得られ, また, 定理 13 (4) は同定理 (1) を用いて証明されることに注意する (詳細は [26, Theorem 7, Corollary 1] の証明を参照)．定理 13 (4) より, F^h の次数 D 未満の Gröbner 基底元の計算に F_5 アルゴリズム [17] (or その variant) を用いれば, 0-reduction となる S 多項式ペアを全て容易に回避できることがわかる．従って Bardet, Faugère らの定理 9 前半の主張が成り立つ．

斉次化 F^h の $\prec^h$ に関する簡約 Gröbner 基底の最大次数については, 次の定理 14 が得られた．

定理 14 ([27, Theorem 2])
記号は上の通りとし, $D:=d_{\mathrm{reg}}(F^{\mathrm{top}})$ とおく．このとき, 次が成り立つ：

(1) $m>n$ かつ $d_1\leq d_2\leq\cdots\leq d_m$ を満たすものとし, もし F^{top} が強半正則 (定義は注意 4 を参照) なら,

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h)\leq d_1+d_2+\cdots+d_n+d_m-n \tag{4.1}$$

である．さらに, $d_m\leq D$ であれば, d_m を d_{n+1} に置き換えても (4.1) は成り立つ．

(2) s_0 を saturation $(\langle F^h\rangle:\langle y^\infty\rangle):=\bigcup_{s\in\mathbb{Z}_{\geq 0}}(\langle F^h\rangle:\langle y^s\rangle)$ の saturation exponent, すなわち

$$s_0:=\min\left\{s\in\mathbb{Z}_{\geq 0}\mid(\langle F^h\rangle:\langle y^s\rangle)=(\langle F^h\rangle:\langle y^\infty\rangle)\right\} \tag{4.2}$$

とするとき, 次の不等式が成り立つ：

$$\max.\mathrm{GB.deg}_{\prec^h}(F^h)\leq D+s_0. \tag{4.3}$$

ここで $(\langle F^h\rangle:\langle y^s\rangle):=\{f\in R[y]:fy^s\in\langle F^h\rangle\}$ である．定理 14 (1) の (4.1) 右辺は, $d_1=\cdots=d_m$ のとき Lazard 上界 (3.3) に一致する．ただし, Lazard 上界 (3.3) では $d_1,\dots,d_m$ が降順になるように $f_1,\dots,f_m$ を並べていたが, 定理 14 (1) では $\boldsymbol{F}$ の強半正則性を課すことで $d_1,\dots,d_m$ を昇順にとることができているので, $d_1=\cdots=d_m$ でない場合には (4.1) 右辺は (3.3) のそれよりも小さい値をとり得る．また, 定理 14 (2)

の (4.3) により, (4.2) で定義される s_0 を評価することで $\mathrm{max.GB.deg}_{\prec^h}(F^h)$ を上から評価できる. (4.3) の上界 $D+s_0$ や, 同じく $\mathrm{max.GB.deg}_{\prec^h}(F^h)$ の上界である定理 13 (3) の d_0 の評価は今後の課題である.

最後の結果として, イデアル $\langle F\rangle_R$, $\langle F^{\mathrm{top}}\rangle_R$, $\langle F^h\rangle_{R[y]}$ の $\prec$, $\prec$, $\prec^h$ に関する簡約 Gröbner 基底をそれぞれ G, G_{top}, G_{hom} とおくとき, これらの計算および先頭単項式集合に関して, 次の定理 15 が成り立つ:

定理 15 ([26, Theorem 1 & Section 5], [27, Theorem 3])
記号は上の通りとするとき, 次が成り立つ:

(1) $d<D$ を満たす任意の非負整数 d に対して $\mathrm{LM}_{\prec^h}(G_{\mathrm{hom}})_d=\mathrm{LM}_{\prec}(G_{\mathrm{top}})_d$ が成り立つ.

(2) $\langle \mathrm{LM}_{\prec^h}((G_{\mathrm{hom}})_{\le D})\rangle_{R[y]}\cap R_D=R_D$ が成り立つ. さらに, $g^{\mathrm{top}}:=g(x_1,\dots,x_n,0)\neq 0$ となるような任意の $g\in(G_{\mathrm{hom}})_D$ に対し, g^{top} は単項, すなわち $g^{\mathrm{top}}=\mathrm{LT}_{\prec}(g)$ である ($\mathrm{LT}_{\prec}$ は先頭項を表す).

(3) 正規戦略アルゴリズムを用いて G_{hom}, G を計算する際, 計算の初期段階 (すなわち次数 D の G_{hom} の元が初めて得られるより前) で生成される多項式に関して '強い' 関係が成り立つ (詳細は [27] を参照).

(4) $D\ge\max\{\deg(f):f\in F\}$ なら, $\mathrm{max.GB.deg}_{\prec}(F)\le D$ であり, ある正規戦略アルゴリズム $\mathcal{A}$ が構成的に存在し, 3 節 (または 1 節) 2 段落目の step degree を各ステップで収集する S ペアの次数 (resp. 対応する S 多項式の次数) と定めるとき $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)\le 2D-1$ (resp. $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)\le 2D-2$) を満たす.

定理 15 (3) は同定理 (1) を用いて示され, これにより計算の初期段階 (言い換えれば step degree が初めて D 以上になる前) では G_{hom} と G の計算は対応する. また, G の計算の初期段階では, 'degree fall' と呼ばれる現象が起こらない, すなわち中間基底による S 多項式の簡約結果としてその S 多項式より低次の非零元が得られないこともわかる (実際にはより強く, そのステップの step degree 未満の次数をもつ非零元が S 多項式の簡約結果として得られることはない). 定理 15 (4) は同定理 (1), (2) を用いて示され, アルゴリズム $\mathcal{A}$ は, 定理 12 のそれ (詳細は [36] 参照) と同様に構成される. 一方, $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)$ の評価式を得る上では, 定理 12 の仮定 $K=\mathbb{F}_q$, $\{x_i^q-x_i:1\le i\le n\}\subset F$, $D\ge q$ を必要としないため, 定理 15 (4) は定理 12 前半の拡張である. ただし定理 12 後半の (3.5) のような計算量の評価式は現時点で得られておらず, その導出は今後の課題である (他にも, F が非斉次の場合における $\mathrm{sd}^{\mathrm{mac}}_{\prec}(F)$ と $\mathrm{sd}^{\mathcal{A}}_{\prec}(F)$ の大小関係を調べることも課題である).

謝　辞

本研究は科学研究費基金 (20K14301, 21K03377, 23K12949) の助成を受けて行われました.

参 考 文 献

[1] M. Bardet: Étude des systémes algébriques surdéterminés. Applications aux codes correcteurs et á la cryptographie. PhD thesis, Université Paris IV, 2004.

[2] M. Bardet, J.-C. Faugére, and B. Salvy: On the complexity of Gröbner basis computation of semi-regular overdetermined algebraic equations (extended abstract). In: Proceedings of the International Conference on Polynomial System Solving, 71–74, 2004.

[3] M. Bardet, J.-C. Faugére, B. Salvy, and B.-Y. Yang: Asymptotic behaviour of the degree of regularity of semi-regular polynomial systems. In: Proceedings of Eighth International Symposium on Effective Methods in Algebraic Geometry (MEGA 2005), 2005.

[4] T. Becker and V. Weispfenning: Gröbner Bases: A Computational Approach to Commutative Algebra. GTM, **141**, Springer, NY, 1993.

[5] M. Bigdeli, E. De Negri, M. M. Dizdarevic, E. Gorla, R. Minko, and S. Tsakou: Semi-Regular Sequences and Other Random Systems of Equations. In: Women in Numbers Europe III, **24**, pp. 75–114, Springer, 2021.

[6] B. Buchberger: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Innsbruck: Univ. Innsbruck, Mathematisches Institut (Diss.), 1965.

[7] J. A. Buchmann, J. Ding, M. S. E. Mohamed, and W. S. A. E. Mohamed: MutantXL: Solving Multivariate Polynomial Equations for Cryptanalysis. In H. Handschuh, S. Lucks, B. Preneel, and P. Rogaway (eds), Symmetric Cryptography, Dagstuhl Seminar Proceedings, **9031**, pp. 1–7, Dagstuhl, Germany, 2009.

[8] A. Caminata and E. Gorla: Solving Multivariate Polynomial Systems and an Invariant from Commutative Algebra. In: Arithmetic of Finite Fields (Proc. of WAIFI 2020), LNCS, **12542**, pp. 3–36, Springer, 2021.

[9] A. Caminata and E. Gorla: Solving degree, last fall degree, and related invariants. J. Symb. Comp., **114**, 322–335 (2023).

[10] J. G. Capaverde: Gröbner bases: Degree bounds and generic ideals. PhD thesis, Clemson University, 2014.

[11] N. Courtois, A. Klimov, J. Patarin, and A. Shamir: Efficient Algorithms for Solving Overdefined Systems of Multivariate Polynomial Equations. EUROCRYPT 2000, LNCS, **1807**, pp. 392–407, Springer, 2000.

[12] S. Collart, M. Kalkbrener, and D. Mall: Coverting bases with the Groebner walk. J. Symb. Comp., **24**, Issues 3–4, 465–469, 1997.

[13] C. Diem: Bounded regularity. Journal of Algebra, **423**, 1143–1160, 2015.

[14] J. Ding and D. Schmidt: Solving Degree and Degree of Regularity for Polynomial Systems over a Finite Fields. In: M. Fischlin and S. Katzenbeisser (eds), Number Theory and Cryptography, LNCS, **8260**, pp. 34–49, Springer, Berlin, Heidelberg.

[15] D. Eisenbud: The Geometry of Syzygies: A Second Course in Algebraic Geometry and Commutative Algebra. Springer, GTM, **229**, 2005.

[16] J.-C., Faugère: A new efficient algorithm for computing Gröbner bases (F4). Journal of Pure and Applied Algebra, **139** (1999), 61–88.

[17] J.-C., Faugère: A new efficient algorithm for computing Gröbner bases without reduction to zero (F5). In: Proceedings of ISSAC 2002, ACM Press, (2002), pp. 75–82.

[18] J.-C., Faugère, P. Gianni, D. Lazard, and T. Mora: Efficient Computation of Zero-dimensional Gröbner Bases by Change of Ordering. J. Symb. Comp., **16** (4), 329–344, 1993.

[19] R. Fröberg: An inequality for Hilbert series of graded algebras. Math. Scand., **56** (1985), 117–144.

[20] G. Gaggero and E. Gorla: The complexity of solving a random polynomial system. arxiv:2309.03855.

[21] E. Gorla, D. Mueller, and C. Petit: Stronger bounds on the cost of computing Gröbner bases for HFE systems. J. Symb. Comp., **109**, 386–398, 2022.

[22] G.-M. Greuerl and G. Pfister: A Sinular Introduction to Commutative Algebra. 2nd Edition, Springer, 2007.

[23] M.-D. A. Huang, M. Kosters, Y. Yang, and S. L. Yeo: On the last fall degree of zero-dimensional Weil descent systems. J. Symb. Comp., **87** (2018), 207–226.

[24] M.-D. A. Huang, M. Kosters, and S. L. Yeo: Last fall degree, HFE, and Weil descent attacks on ECDLP. In: Advances in Cryptology — CRYPTO 2015, LNCS, **9215**, 581–600, Springer, Berlin, Heidelberg, 2015.

[25] M. Kreuzer and L. Robbiano: Computational Commutative Algebra 2. Springer, 2003.

[26] M. Kudo and K. Yokoyama: On Hilbert-Poincaré series of affine semi-regular polynomial sequences and related Gröbner bases. In: T. Takagi et al. (eds), Mathematical Foundations for Post-Quantum Cryptography, Mathematics for Industry, 26 pages, Springer, to appear (arXiv:2401.07768).

[27] M. Kudo and K. Yokoyama: The solving degree for computing Gröbner bases of affine semi-regular polynomial sequences. in preparation.

[28] D. Lazard: Gröbner bases, Gaussian elimination and resolution of systems of algebraic equations. In: Computer algebra (London, 1983), LNCS, **162**, pp. 146–156, Springer, Berlin, 1983.

[29] D. Lazard: Résolution des systèmes d'équations algébriques. Theoretical Computer Science, **15**, Issue 1, 77–110, 1981.

[30] E. W. Mayr and S. Ritscher: Dimension-dependent bounds for Gröbner bases of polynomial ideals. J. Symb. Comp., **49** (2013), 78–94.

[31] G. Moreno-Socías: Autour de la fonction de Hilbert-Samuel (escaliers d'idéaux polynomiaux), Thèse, École Polytechnique, 1991.

[32] K. Pardue: Generic sequences of polynomials. Journal of Algebra, **324.4**, 579–590, 2010.

[33] S. Ritscher: Degree Bounds and Complexity of Gröbner Bases of Important Classes of Polynomial Ideals. PhD thessis, Technische Universität München Institut für Mathematik, 2012.

[34] F. Salizzoni: An upper bound for the solving degree in terms of the degree of regularity. arXiv:2304.13485.

[35] I. Semaev and A. Tenti: Probabilistic analysis on Macaulay matrices over finite fields and complexity constructing Gröbner bases. Journal of Algebra, **565**, 651–674, 2021.

[36] A. Tenti: Sufficiently overdetermined random polynomial systems behave like semiregular ones. PhD Thesis, University of Bergen, 2019, available at https://hdl.handle.net/1956/21158

[37] C. Traverso: Hilbert functions and the Buchberger algorithm. J. Symb. Comp., **22.4** (1996), 355–376.