人工知能　85－5
(1992.11.19)

従属変数の順序変換に基づく三角化手続きの効率化

岡本 青史
(株) 富士通研究所
〒211 川崎市中原区上小田中 1015

あらまし　Wuの手法は，幾何学的概念の定理自動証明における代数学的推論方式として提案され，従来法では解けなかった数々の定理の自動証明を可能にした．本稿では代数学的手法として，簡略なWuの手法をとりあげる．簡略なWuの手法は擬除算に用いて多項式の集合を三角化形式に変換する三角化手続きに基づいている．簡略なWuの手法は三角化手続きにおける擬除算が多項式の項数膨張を引き起こすといった問題点を抱えている．この項数膨張の問題を解決するため，従属変数の順序変換に基づく効率的な三角化手続きを提案する．

和文キーワード　幾何推論，Wuの手法，三角化手続き，擬除算

Efficient Triangulation Procedure by Changing Dependent Variable Ordering

Seishi OKAMOTO
FUJITSU LABORATRIES LTD.
1015, Kamikodanaka Nakahara-ku, Kawasaki 211, Japan
E-mail:seishi@flab.fujitsu.co.jp

Abstract

Wu's method was proposed as an algebraic reasoning method for mechanical geometry theorem proving, and could prove many geometry theorems which could not be proven by traditional methods. In this paper, I deal with simplified Wu's method as an algebraic mathod. Simplified Wu's method is based on the triangulation procedure which transform a polynomial set into a triangular form using pseudo division. Simplified Wu's method has a difficulty that pseudo division causes the term growth of polynomial in the triangulation procedure. To solve this difficulty, I propose an efficient triangulation procedure by changing dependent variable ordering.

英文 key words　Geometry reasoning, Wu's method, triangulation procedure, pseudo division

1. はじめに

幾何学の定理自動証明における推論手法は，論理学的推論手法と代数学的推論手法の二つに大別できる．

論理学的推論手法を用いた幾何学の定理自動証明では，幾何学的概念を述語論理で表現し，導出や簡約を推論原理として証明を行なう．論理学的手法を用いた幾何学の定理証明システムとしては，Nevins による証明システム [13] 等が有名である．Nevins による証明システムは前向き推論に基づいた定理証明を実現するが，証明できる幾何学の問題は単純なものに限られていた．論理学的推論手法の抱える本質的な問題として，幾何学的概念を述語論理で記述することの困難さや，証明を実現するために必要となる変形規則の導入の困難さが挙げられる．

一方，代数学的手法を用いた幾何学の定理自動証明においては，幾何学的概念は代数方程式で表現され，その代数式に代数演算を施すことにより，幾何学の定理自動証明を実現する．代数学的手法を用いた幾何学の定理証明手法として，限定子除去法，Wu の手法，Gröbner 基底法が提案されている．これらの手法は，従来の論理学的手法では解くことの出来なかった多くの複雑な問題の証明に成功している．

限定子除去法 [1] は代数方程式の実数体上の解集合に関する推論手法である．この手法の代数演算は Collins[6] によって提案された CAD (Cylindrical Algebraic Decomposition) アルゴリズムに基づいている．この手法の問題点としては，計算量の大きさや完全な自動化の困難さ等が挙げられる．

Wu の手法 [15] は，多項式の代数多様体に関する推論手法で，Ritt の原理と分解アルゴリズム [14] に基づいている．幾何学の定理自動証明の研究分野に対して，Wu の手法が与えた大きな貢献の一つに，幾何学的図形が退化しないための代数学的条件である非退化条件を考慮した点である．幾何学的図形が退化しないための全ての非退化条件を導出することは難しいとされているが，Wu の手法によって導出される非退化条件によって定理が弱められたり，仮定が矛盾したりしないことは保証されている [4]．Chou は Wu の手法を用いて，500 以上もの幾何学的概念の定理自動証明を成功させている [3]．

Gröbner 基底法 [5, 9, 11] は多項式のイデアルに関する推論手法である．この手法の代数演算は Gröbner 基底を導出する Buchberger アルゴリズム [2] に基づいている．

Wu の手法と Gröbner 基底法による幾何学の定理自動証明は，複雑な問題の証明に成功しており，その健全性も保証されている．しかしながら，完全性や独立変数の選定問題等の本質的な課題も残している．さらに効率の面で，Wu の手法は三角化手続きにおける多項式の項数の膨張が，Gröbner 基底法では Buchberger アルゴリズムにおける多項式の組み合わせ爆発等が問題となっている．この二つの手法の比較は文献 [5, 12] で詳細に行なわれている．

Wu の手法における三角化手続きでの多項式の項数膨張は，擬除算における係数の掛け合わせが伝搬して発生する．この多項式の項数膨張は独立変数の選定，従属変数の順序と密接に関係している [7, 8]．本稿では，従属変数の順序に着目し，擬除算が同伴多項式で定義できることを用いて，各従属変数を採用した際の三角化手続きにおける項数膨張を評価することで，従属変数の順序を変換し，多項式の項数膨張を抑える手法を提案する．

本稿の構成は以下の通りである．2 節では Wu の手法に必要な代数学的準備を行なう．3 節では Wu の手法を紹介し，完全性，独立変数の選定問題，非退化条件に関する問題点を挙げる．4 節では独立変数の順序変換法を提案し，5 節で例題を通してその有効性を検証する．

2. 代数学的準備

K を標数 0 の基礎体とするとき，多項式とは多項式環 $K(u_1,\ldots,u_d)[x_1,\ldots,x_r]$ 中の元であり，特に断らない限り 0 でないとする．このとき $u_1,\ldots,u_d$ を独立変数 (*independent variable*)，$x_1,\ldots,x_r$ を従属変数 (*dependent variable*) という．特に断らない限り，これらの変数には

$$u_1 \prec \cdots \prec u_d \prec x_1 \prec \cdots \prec x_r$$

なる順序が与えられているとする．また $u = u_1,\ldots,u_d$ なる略記を断りなく使う．

定義 1. $f \in A[x_1,\ldots,x_p]$ なる最小の自然数 $p \leq r$ を f のクラス (*class*) といい，$class(f)$ で表す．また $f \in A$ のとき，f のクラスを 0 とする．

$class(f) = p > 0$，f における x_p の最大次数 $deg(f, x_p) = k$ なる多項式 f は

$$f = a_0 x_p^k + a_1 x_p^{k-1} + \cdots + a_k$$

と表現できる．このとき $a_i \in A[x_1, \ldots, x_{p-1}]$ $(i = 0, \ldots, k)$ であり，特に $a_0 \neq 0$ である．

上述の f の表記において，a_0 を f の主係数 (*leading coefficient*) といい，$lc(f)$ で表す．また，x_p を f の主変数 (*leading variable*) といい，$lv(f)$ で表す．さらに，$deg(g, x_p) < deg(f, x_p)$ をみたす多項式 g は f に帰着される (*g is reduced with respect to f*) という．

f を上述の多項式，g を任意の多項式とする．このとき，擬除算 (*pseudo division*) は次のアルゴリズムで定義され，出力される R を f による g の擬剰余 (*pseudo remainder*) といい，$prem(g, f)$ で表す．

Step1 $r := g$.
Step2 $m := deg(r, x_p), c_m := lc(r)$.
Step3 $m < k$ ならば，$R := r$ を出力して終了．
$m \geq k$ ならば，Step4 へ．
Step4 $r := a_0 r - c_m x_p^{m-k} f$ とし，Step2 へ．

定義 2. 多項式の列 $\mathcal{F} = f_1, \ldots, f_r$ が次の (1) または (2) をみたすとき，$\mathcal{F}$ を擬昇鎖 (*quasi ascending chain*) または三角化形式 (*triangular form*) という．

(1) $r = 1$，かつ $f_1 \neq 0$.
(2) $r > 1$，$0 < class(f_1) < \cdots < class(f_r)$.

定義2において，$\mathcal{F} = \{f_1\}$ が $f_1 \neq 0$，$class(f_1) = 0$ をみたすとき，擬昇鎖 $\mathcal{F}$ は矛盾している (*contradictory*) という．

定義 3. $\mathcal{F} = f_1, \ldots, f_r$ を擬昇鎖とする．このとき f_i が $K(u)[x_1, \ldots, x_i]/(f_1, \ldots, f_{i-1})$ $(i = 1, \ldots, m)$ 上で既約であれば，$\mathcal{F}$ は既約 (*irreducible*) であるといい，そうでなければ，$\mathcal{F}$ は可約 (*reducible*) であるという．ただし，$(f_1, \ldots, f_i)$ は $f_1, \ldots, f_i$ によって生成される $K(u)[x_1, \ldots, x_i]$ の多項式イデアルを表す．

$\mathcal{F} = f_1, f_2, \ldots, f_r$ を擬昇鎖とし，各 $i = 1, \ldots, r$ に対し $p_i = class(f_i), I_i = lv(f_i)$ とおき，$p_1 > 0$ とする．このとき，G を任意の多項式とし，$R_r = G$ とおいて次のように擬除算を逐次的に行う．

$$\begin{aligned} I_r^{s_r} R_r &= Q_r f_r + R_{r-1}, \\ I_{r-1}^{s_{r-1}} R_{r-1} &= Q_{r-1} f_{r-1} + R_{r-2}, \\ &\cdots, \\ I_1^{s_1} R_1 &= Q_1 f_1 + R_0. \end{aligned}$$

このとき，$R_0 = R$ とおいて次式が成り立つ．

$$I_1^{s_1} \cdots I_r^{s_r} G = Q_1' f_1 + \cdots + Q_r' f_r + R$$

ここで $1 \leq i \leq r$ に対し，Q_i' は多項式，s_i は非負整数である．また任意の $j (1 \leq j \leq r)$ に対し，R は f_j に帰着される．

定義 4. 上述において，R を $\mathcal{F}$ による G の終剰余 (*final remainder*) といい，$prem(G, f_1, \ldots, f_r)$ で表す．また，終剰余 R を求める手続きを逐次擬除算 (*successive pseudo division*) という．

定義 5. $\mathcal{F} = f_1, \ldots, f_r$ を擬昇鎖とし，$I_i = lc(f_i) (i = 1, \ldots, r)$ とする．

(1) 任意の対 $i < j$ に対し，f_j が f_i に帰着されるとき，$\mathcal{F}$ を昇鎖 (*ascending chain*) という．
(2) 任意 $i (1 \leq i \leq r)$ に対し，$prem(I_i, f_1, \ldots, f_r) \neq 0$ が成り立つとき，$\mathcal{F}$ を弱い昇鎖 (*weak ascending chain*) という．

定義5において，(1)⇒(2) が成り立つ．

定理 1. $\mathcal{F} = f_1, \ldots, f_r$ を既約な弱い昇鎖，$g \in K(u)[x_1, \ldots, x_r]$ を多項式とする．このとき，次の (1),(2) は同値である．

(1) $prem(g, f_1, \ldots, f_r) = 0$.
(2) E を基礎体 K の拡大体とし，$\mu = (\tilde{u}_1, \ldots, \tilde{u}_d, \tilde{x}_1, \ldots, \tilde{x}_r) \in E^{d+r}$ とする．このとき μ が $f_1, \ldots, f_r$ の共通の零点ならば，$g(\mu) = 0$．ここで各 $i = 1, \ldots, d$ に対し，$\tilde{u}_i$ は K 上で超越的とする．

3. Wu の手法

3.1. 幾何学的概念の代数表現への変換

Wu の手法の代数的定式化のために，幾何学的概念は記述される体 K が代数的に閉じている計量幾何学の公理で表現されていると仮定する．ここで計量幾何学とは，Affine 幾何学に垂直の公理と線分一致の公理を加えた幾何学である．また，計量幾何学においては無限の公理が成り立つことより，K の標数は 0 である．

この仮定に基づいて，ある座標系の導入することで幾何学的概念 (S) の仮定は

$$\begin{aligned} h_1(u_1, \ldots, u_d, x_1, \ldots, x_r) &= 0 \\ &\cdots \\ h_n(u_1, \ldots, u_d, x_1, \ldots, x_r) &= 0 \end{aligned}$$

と表現でき，(S) の結果は

$$g(u_1,\ldots,u_d,x_1,\ldots,x_r)=0$$

と表現できる．ここで，各 $i=1,\ldots,n$ に対し，$h_i,\ g\in K(u_1,\ldots,u_d)[x_1,\ldots,x_r]$ である．各 h_i $(1\leq i\leq n)$ を (S) の仮定多項式 (*hypothesis poly nomial*) といい，g を (S) の結果多項式 (*conclusion polynomial*) という．

上述の代数表現への変換において，$u_1,\ldots,u_d$ は独立変数，$x_1,\ldots,x_r$ は従属変数として座標系が導入されている．ここで，$u_1,\ldots,u_d$ が独立でない場合，Wu の手法の健全性は保証されなくなる．このように，独立変数の選定問題は代数学的手法を用いた幾何学の定理自動証明において本質的な問題である．この問題は幾何学の意味論に深く関与する問題で，[3, 7, 8, 12] 等でその選定手法が提案されている．

3.2. 代数演算

Wu の手法の代数演算は，Ritt の原理と分解手続き [14] からなる．Ritt の原理は仮定多項式の集合を特徴集合と呼ばれる昇鎖に変換する手続きであり，Ritt の分解手続きは Ritt の原理で得られた特徴集合が可約な場合，既約な特徴集合に分解する手続きである [16].

しかし本稿では Ritt の原理と分解手続きに基づく Wu の手法の詳細については触れず，Ritt の原理の代わりに代数演算として多項式集合の三角化手続きを用いる簡略な Wu の手法について考察する．

多項式集合の三角化手続きとは，多項式の集合 $H=\{h_1,\ldots,h_r\}$ を入力して，次の三角形式 $\mathcal{F}=f_1,\ldots,f_s$ を出力する手続きをいう．ここで，$h_i\in K(u_1,\ldots,u_d)[x_1,\ldots,x_r]$ $(1\leq i\leq r)$ である．

$$\begin{aligned} &f_1(u_1,\ldots,u_d,x_1)\\ &\quad\cdots\\ &f_s(u_1,\ldots,u_d,x_1,\ldots,x_s)\end{aligned}$$

このとき，$s=r$ を仮定する．この仮定は次数の制限 (*dimensionality restriction*) と呼ばれ，幾何学的概念の代数表現に冗長なものが含まれていないことや，三角化手続きの出力が矛盾した三角形式でないことに対応する．

三角化手続きのアルゴリズムは文献 [3, 7] 等で提案されているが，ここでは次のアルゴリズムを採用する．

Step1 $n:=r, A:=H, B:=\emptyset, C:=\emptyset, F:=\emptyset$.
Step2 $n:=0$ ならば F を出力して終了.
Step3 $B:=\{h_i|deg(h_i,x_n)=0, h_i\in A\}$
$C:=A-B$
Step4 C 中で x_n に関する次数最小の多項式を h として，$C:=C-\{h\}$
Step5 $C=\emptyset$ ならば $A:=B, n:=n-1$ として Step2 へ.
$C\neq\emptyset$ ならば $A:=B\cup\{h\}\cup\{h_j|h_j=prem(h_i,h), h_i\in C\}$ として Step3 へ.

Step4 において，次数が最小の多項式が C 中に複数個存在する場合は，それらの多項式で項数最小の多項式を h として選ぶ．

3.3. 代数学的定式化

多項式の集合 H を三角化形式 $\mathcal{F}=f_1,\ldots,f_r$ に変換する前述の三角化手続きにおいて，任意の j $(1<j\leq r)$ に対して，

$$prem(I_j,f_1,\ldots,f_{j-1})\neq 0$$

が成立することを仮定する．ここで $I_j=lc(f_j)(1\leq j\leq r)$ である．このとき，三角形式 $f_1,\ \ldots,f_r$ は弱い昇鎖となる．そこで，定理 1に基づいて，簡略な Wu の手法における代数学的定式化を以下で与える．

仮定多項式の集合から三角化手続きによって得られた三角化形式を $\mathcal{F}=f_1,\ldots,f_r$ とする．ここで，$I_j=lc(f_j)$ $(1\leq j\leq r)$ として，$I_1\neq 0,\ldots,I_r\neq 0$ を非退化条件という．また，結果多項式 g の F による終剰余 $R=prem(g,f_1,\ldots,f_r)$ を逐次擬除算によって計算する．このとき，簡略な Wu の手法における代数学的定式化を次のように与える．

(1) $R=0$ の場合，三角形式 $\mathcal{F}$ が既約であるか可約であるかにかかわらず，幾何学的陳述は非退化条件のもとで一般に真となる．

(2) $R\neq 0$ の場合，三角形式 $f_1,\ldots,f_r$ が既約分解し，各既約成分に対し逐次擬除算を実行し，終剰余を計算する．このとき，全ての既約成分に対して終剰余が 0 になれば，幾何学的陳述は一般に偽となる．そうでなければ，幾何学的陳述は一般には真ではない．

ユークリッド幾何学では作図可能性より解の存在が保証されていることから，この定式化はユークリッド幾何学の定理証明でも有効である [4].

Wu の手法では，Ritt の原理によって得られる非退化条件が定理を弱めたり，仮定の矛盾を引き起こしたりしないことは保証されている [3]. 簡略

なWuの手法においては，次の例1のように三角化手続きによって得られる非退化条件を加えることで，上の保証が成り立たなくなる場合がある．

例 1. [3] $h_1 = x^2, h_2 = xy, g = x + y$ とする．このとき $f_1 = h_1, f_2 = h_2$ で，$prem(g, x1, x2) = 0$ となる．よって，上の定式化によると $(f_1 = 0, f_2 = 0, x_1 \neq 0) \Rightarrow g = 0$ となるが，非退化条件 $x_1 \neq 0$ を加えることで，仮定の矛盾を引き起こす．

ただし幾何の定理証明において，この例やTarski幾何学における特殊な不完全性 [10] はほとんど起こらないことが主張されている [7].

前述の代数学的定式化に基づいて，簡略なWuの手法による幾何学の定理自動証明の例を挙げる．

例 2. $ABCD$ を平行四辺形とし，E を2つの対角線 AC と BD との交点とする．このとき，$AE \equiv CE$ が成り立つ．

この陳述に対し，$A = (0,0), B = (u_1, 0), C = (u_2, u_3), D = (x_2, x_1), E = (x_4, x_3)$ なる座標系を導入する．このとき，陳述の仮定と結果は

$$
\begin{aligned}
h_1 &= u_1x_1 - u_1u_3 = 0\\
h_2 &= u_3x_2 - (u_2 - u_1)x_1 = 0\\
h_3 &= x_1x_4 - (x_2 - u_1)x_3 - u_1x_1 = 0\\
h_4 &= u_3x_4 - u_2x_3 = 0\\
g_1 &= 2u_2x_4 + 2u_3x_3 - u_3^2 - u_2^2 = 0
\end{aligned}
$$

と代数的に表現される．三角化手続きを用いて，仮定多項式を次の三角化形式に変換する．

$$
\begin{aligned}
f_1 &= u_1x_1 - u_1u_3 = 0\\
f_2 &= u_3x_2 - (u_2 - u_1)x_1 = 0\\
f_3 &= (u_3x_2 - u_2x_1 - u_1u_3)x_3 + u_1u_3x_1 = 0\\
f_4 &= u_3x_4 - u_2u_3 = 0
\end{aligned}
$$

このとき，$prem(g, f_1, \ldots, f_4) = 0$ が成立することより，この陳述は次の非退化条件のもとで真となる．

$$
\begin{aligned}
&I_1 = u_1 \neq 0,\ I_2 = I_4 = u_3 \neq 0\\
&I_3 = u_3x_2 - u_2x_1 - u_1u_3 \neq 0
\end{aligned}
$$

ここで，$u_1 \neq 0, u_3 \neq 0$ は A, B, C が同一直線上にないことの代数学的表現であり，$u_3x_2 - u_2x_1 - u_1u_3 \neq 0$ は AC と BD が唯一つの交点をもつことの代数学的表現である．

4. 従属変数の順序変換手法

4.1. 本手法の背景

簡略なWuの手法において，三角化手続きに伴う多項式の項数の膨張は効率上の大きな問題点である．この項数の膨張は，擬除算における係数の掛け合わせが伝搬して起こるものと考えられる．またこの項数の膨張は，従属変数の順序に密接に関係している．次の例を見てみよう．

例 3. 多項式集合を $S = \{-x_1^2 + 2u_1x_1 - u_4^2 + u_3^2 - 2u_1u_2, -x_3^2 + 2u_1x_3 - x_2 + u_3^2 + u_2^2 - 2u_1u_2, -u_4x_3 + x_1x_2 - u_2\}$ とする．このとき，従属変数の順序を $x_3 < x_2 < x_1$ とすると，S の三角形式の元である多項式の項数の総数は154となる．しかしながら，$x_1 < x_2 < x_3$ と順序づけると，項数の総数は18となる．

このように，従属変数の順序変換は三角化手続きの効率に劇的な変化を与える．また，多項式の項数の膨張は，三角化手続き自身の効率に関与するだけではなく，可約の場合の分解アルゴリズムの効率にも大きく影響する．そこで本稿では，多項式の項数膨張を最小限に抑える従属変数の順序変換手法を提案する．

4.2. 評価関数

まず，同伴多項式の定義を与える．A を次の $m \times (m+n)$ 行列とする．

$$
A = \begin{bmatrix}
a_{11} & \cdots & a_{1,m-1} & a_{1m} & \cdots & a_{1,m+n}\\
\vdots & & \vdots & \vdots & & \vdots\\
a_{m1} & \cdots & a_{m,m-1} & a_{mm} & \cdots & a_{m,m+n}
\end{bmatrix}
$$

この行列 A の $m-1$ 列までの行列を B とし，その残りの $m \times (n+1)$ の行列の各列を B の n 列目に付け加えて $n+1$ 個の $m \times m$ 行列を生成する．生成された $n+1$ 個の行列の行列式を係数とする次の n 次の多項式を A の同伴行列 (*associated polymonial*) といい，$\mathcal{P}(A)$ で表す．

$$
\begin{aligned}
\mathcal{P}(A) = &\begin{vmatrix}
a_{11} & \cdots & a_{1,m-1} & a_{1m}\\
\vdots & & \vdots & \vdots\\
a_{m1} & \cdots & a_{m,m-1} & a_{mm}
\end{vmatrix} x^n + \cdots\\
&+ \begin{vmatrix}
a_{11} & \cdots & a_{1,m-1} & a_{1,m+n}\\
\vdots & & \vdots & \vdots\\
a_{m1} & \cdots & a_{m,m-1} & a_{m,m+n}
\end{vmatrix} x^0
\end{aligned}
$$

$m \leq n$，$a_m \neq 0$，$b_n \neq 0$ として，多項式 $f, g \in K(u)[x_1, \ldots, x_r]$ がある従属変数 x_p $(1 \leq p \leq r)$ に関して

$$f = a_0 x_p^m + a_1 x_p^{m-1} + \cdots + a_m$$
$$g = b_0 x_p^n + b_1 x_p^{n-1} + \cdots + b_n$$

と書けたとする．また，x_p に関する f の g による擬剰余を $prem(f,g,x_p)$ と表記する．このとき，次の命題1が成立する．命題1は，擬除算における擬剰余が f,g の x_p に関する係数を要素とする $(m-n+2)\times(m+1)$ 行列の同伴多項式で表記出来ることを示している．

命題 1. 上述の f,g において，$R = prem(f,g,x_p)$ とするとき，次式が成立する．

$$R = \mathcal{P}\left(\begin{bmatrix} b_n & b_{n-1} & \cdots & b_0 & & & \\ & b_n & b_{n-1} & \cdots & b_0 & & \\ & & \ddots & & & \ddots & \\ & & & b_n & b_{n-1} & \cdots & b_0 \\ a_m & a_{m-1} & \cdots & \cdots & \cdots & \cdots & a_0 \end{bmatrix}\right)$$

2次の正方行列 $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ に対して，関数 $\mathcal{D}$ を $\mathcal{D}(A) = ad + bc$ で定義する．さらに n 次の正方行列 $A = (a_{ij})$ に対して，$\mathcal{D}$ を行列式の定義と同様に以下のように帰納的に定義する．今，$n-1$ 次の関数 $\mathcal{D}$ が定義されているとする．$\tilde{a}_{ij} = \mathcal{D}(A')$ $(1 \le i,j \le n)$ とおく．これは行列式の定義における余因子に相当し，A' は A から i 行と j 列の要素を取り除いた $(n-1)\times(n-1)$ の行列である．このとき $\mathcal{D}(A) = a_{11}\tilde{a}_{11} + a_{22}\tilde{a}_{12} + \cdots + a_{1n}\tilde{a}_{1n}$ で $\mathcal{D}(A)$ を定義する．

$\mathcal{D}$ の定義から明らかなように，符合の付け変え等を除けば行列式における数々の定理は に適用できる．例えば下三角行列 $A = (a_{nn})$ に対して，$\mathcal{D}(A) = a_{11}a_{22}\cdots a_{nn}$ が成立する．このことは，$\mathcal{D}$ が効率良く計算できることを示している．

命題1における行列の各要素 a_i, b_j $(1 \le i \le m, 1 \le j \le n)$ の項の長さをそれぞれ a'_i, b'_j で表す．このとき関数 $\mathcal{M}$ を以下のように定義する．

$$\mathcal{M}(f,g,x_p) = \mathcal{D}\left(\begin{bmatrix} b'_n & b'_{n-1} & \cdots & b'_0 & & & \\ & b'_n & b'_{n-1} & \cdots & b'_0 & & \\ & & \ddots & & & \ddots & \\ & & & b'_n & b'_{n-1} & \cdots & b'_0 \\ a'_m & a'_{m-1} & \cdots & \cdots & \cdots & \cdots & a'_0 \end{bmatrix}\right)$$

以上の定義と命題1から，次の命題が容易に導き出される．

命題 2. 多項式 f,g は命題1と同様とするとき x_p に関する f の g による擬剰余の項数は $\mathcal{M}(f,g,x_p)$ で抑えられる．

3節における三角化手続きのアルゴリズムにおいて，今変数を y とし，y を含む最小次数の多項式を f とする．このとき $deg(f,y) > 1$ ならば，他の任意の y を含む多項式を g とした場合，一般には $prm(g,f)$ は変数 y を含む．よってこの場合は変数 y における項数膨張を $\mathcal{D}$ では評価できないことになる．しかしながら，$\mathcal{D}$ は擬剰余の各次数ごとの係数の項数を評価しているので，次の擬除算における $\mathcal{D}$ へその係数の項数を入力することで，最終的に y を含まない多項式の項数を評価できる．以下の議論では，$\mathcal{D}$ は最終的な項数を評価しているとする．

本稿では，この $\mathcal{M}$ を擬除算における擬剰余の項数を測る評価関数として採用する．$\mathcal{M}$ は擬除算において，項の消去が起こらなかった場合の項数を測っている．以下でこの評価関数を用いて，従属変数の順序を決定する手法を提案する．

4.3. 従属変数の順序変換アルゴリズム

多項式の集合 $H = \{h_1,\ldots,h_r\}$ と従属変数の集合 $X = \{x_1,\ldots,x_r\}$ を入力してある従属変数 x を出力する次の評価アルゴリズム $Ord1(H,X)$ を提案する．

Step1 $i := r, A := \emptyset$
Step2 $i := 0$ ならば x を出力して終了．
Step3 $A := \{h_j | deg(h_j,x_i) = 0, h_j \in H\}$
A 中で x_i に関する次数最小の多項式を h として，$A := A - \{h\}$
Step5 $A = \emptyset$ ならば x_i を出力して終了．
Step6 $e_i = \sum \mathcal{M}(f_j,h)$ $(f_j \in A)$
Step7 $e > e_i$ ならば $e = e_i, x = x_i$
$i := i-1$ をとして Step2 へ

このアルゴリズムの Step7 では，最も評価値の低い変数だけを保持しており，最終的に最も評価値の低い変数 x を出力している．ここで，x_i に関する評価値 e_i の降順でソートされた変数のリストを出力する評価アルゴリズムを $Ord2(H,X)$ で表す．この $Ord2(H,X)$ のアルゴリズムは $Ord1(H,X)$ の Step7 を次の Step7' に変えたものである．

Step7 e_i の降順で変数のリスト x をソートする．
$i := i-1$ をとして Step2 へ．

しかし，上記の評価アルゴリズムを使わずとも，多項式の形だけから従属変数の順序が決定できる場合があり，そのような Criteria を次に提案す

る．この Criteria の導入は従属変数の順序変換手法自体の効率化に大きく貢献する．

Criterion1 1つの多項式にしか現れない従属変数が存在する．

Criterion2 従属変数が1つしか現れない多項式が存在する．

Criterion1 をみたす従属変数は最も順序が高い変数として採用する．また，Criterion2 をみたす従属変数は最も順序が低い従属変数として採用する．Criterion1 は条件を満たす従属変数が他の多項式に伝搬することを防ぎ，Criterion2 は条件を満たす多項式に他の従属変数が伝搬されてくることを防ぐ．

さらに次の Criterion3 を提案する．ここで，x_i に現れる多項式の集合を $T(x_i)$ で表し，その要素数を $|T(x_i)|$ で表す．

Criterion3 $T(x_{i_1}) = \cdots = T(x_{i_n})$かつ $|T(x_{i_j})| = n(j = 1, \ldots, n)$ をみたす $i_1, \ldots, i_n$ が存在する．

Criterion3 をみたす従属変数の集合 X と多項式の集合 H は $Ord2(H, X)$ で X に関する従属変数の順序を決定する．これらの多項式集合に X 以外の変数が伝搬されると，一般に効率の低下を招く．

以上の評価アルゴリズムと Criteria を用いて，従属変数の順序変換を用いた三角化手続きの効率化手法を提案する．

この手法における入力と出力は三角化手続きと同様で，入力は多項式の集合 H と従属変数の集合 X であり，出力は三角化形式である．このアルゴリズムは各 Step において，$T = \emptyset$ が成立すれば停止して，$Append[H1, H2]$ を出力する．アルゴリズム中の $C1, C2, C3$ は Criterion1,Criterion2,Criterion3 を表している．また，$tri(F, V)$ は 3.2 節の三角化手続きに多項式集合 F，変数の集合 V を入力した場合の出力される三角化形式を表している．ここで，Step4 における tri は通常の三角化手続きであるが，Step4 における tri は変数 y だけに関する三角化である．

Step1 $T := H, H1 := \emptyset, H2 := \emptyset, Y := X$

Step2 $C1$ が変数 y，多項式 f で成立すれば，$H1 := Append[\{f\}, H2], T := T' - \{f\}$，$Y := Y - \{y\}$ として Step2 へ．

Step3 $C2$ が変数 y，多項式 f で成立すれば，$H2 := Append[H1, \{f\}], T := T - \{f\}$，$Y := Y - \{y\}$ として Step2 へ．

Step4 $C3$ が変数の集合 U，多項式の集合 F で成立すれば，$V = Ord2(U, F)$ なる変数のリスト V を得て，$H2 := Append[tri(F, V), H2], Y := Y - U$ として Step2 へ．

Step5 $y = Ord1(T, X)$ を得て，$f = tri(T, X, y)$ を得る．$T := T - \{f\}, Y := Y - \{y\}$ $H1 := Append[\{f\}, H2]$ として Step2 へ．

4.4. 実施例

例 4. 次の多項式は Butterfly theorem[3] の仮定多項式である．

$$
\begin{aligned}
h_1 &= -x_1^2 + 2u_1x_1 - u_4^2 + u_3^2 + u_2^2 - 2u_1u_2 \\
h_2 &= -x_3^2 + 2u_1x_3 - x_2^2 + u_3^2 + u_2^2 - 2u_1u_2 \\
h_3 &= -u_3x_3 + u_2x_2 \\
h_4 &= -x_5^2 + 2u_1x_5 - x_4^2 + u_3^2 + u_2^2 - 2u_1u_2 \\
h_5 &= -u_4x_5 + x_1x_4 \\
h_6 &= (-x_5 + u_2)x_6 + u_3x_5 - u_2x_4 \\
h_7 &= (-x_3 + x_1)x_7 + u_4x_3 - x_1x_2
\end{aligned}
$$

ここで例4の三角形式 $\{f_1, \ldots, f_7\}$ を，従属変数の順序変換アルゴリズムで求めると，次のようになる．

$$
\begin{aligned}
f_1 &= h_1 \\
f_2 &= (x_1^2 + u_4^2)x_4^2 - 2u_1u_4x_1x_4 - u_3^2u_4^2 \\
&\quad -u_2^2u_4^2 + 2u_1u_2u_4^2 \\
f_3 &= h_5\ ,\ f_4 = h_2\ ,\ f_5 = h_3 \\
f_6 &= h_6\ ,\ f_7 = h_7
\end{aligned}
$$

ここで，従属変数の選定順序は $\{x_1, x_4, x_5, x_2, x_3, x_6, x_7\}$ である．この三角化形式は従属変数の順序に関する項数膨張の点から言えば，最適解である．つまり他のどの従属変数の順序を用いた場合よりも項数膨張が大きくなることはない．この例4においては全ての従属変数が Criterion1 または Criterion3 をみたし，$\mathcal{D}$ が呼ばれたのは，x_4 と x_3 の順序を決める時だけである．このように幾何学の定理自動証明においては，上述した Criteria がみたされる場合がたびたび登場することを確認している．また，$\mathcal{D}$ が呼ばれる場合の対象なる変数の数は一般に少ない．さらに，幾何学の定理自動証明で有名な種々の問題（simson の定理，pascal の定理，九点円定理等々）を本提案手法で解かせてみた結果，最適な三角化形式を導出できている．以上の考察から，幾何学の定理自動証明において，本提案手法は有効であると思われる．

5. おわりに

本稿では，従属変数の順序が三角化手続きの効率に密接に関係することに着眼し，擬除算における多項式の膨張の評価関数を導入し，項数の膨張を抑える従属変数の順序変換法を提案した．また，本提案手法の有効性を実験によって検証した．

また現在，Wuの手法は機械設計用CADの幾何推論手法として注目されてきている．Wuの手法のCADシステムへの応用のためには，効率の問題や誤差をどのように処理するか等の問題を解決しなくてはならない．特に効率の面において，CADシステムでは膨大な数の変数が必要とされる．変数の数の増加は一般に，三角化手続きにおける多項式の項数の膨張を誘発するので，実際のCADシステムの幾何推論手法としてWuの手法を採用する場合，本稿で述べた従属変数の順序変換手法によって多項式の項数の膨張を抑えることは実用化のために非常に有効であると考えられる．

最後に今後の課題を述べると，代数学的手法の抜本的な効率化手法，幾何学的意味論までも表現できる代数式と述語論理を統合した表現手法，代数学的推論手法と論理学的推論手法を統合した幾何推論の実現等は非常に興味ある今後の課題である．

参考文献

[1] D. Arnon. Geometric reasoning with logic and algebra. *Artificial Intelligence*, Vol. 37, pp. 37–60, 1988.

[2] B. Buchberger. *Gröbner bases:An algorithmic method in polynomial ideal theory*, pp. 184–232. D.Reidel Publishing Company, 1985.

[3] S. C. Chou. *Mechanical geometry theorem proving.* D.Reidel Publishing Company, 1988.

[4] S. C. Chou. An introduction to Wu's method for mechanical theorem proving in geometry. *Journal of Automated Reasoning*, Vol. 4, pp. 237–267, 1988.

[5] S. C. Chou and W. F. Schelter. Proving geometry theorems with rewrite rules. *Journal of Automated Reasoning*, Vol. 2, No. 4, pp. 253–273, 1986.

[6] G. E. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In *proceedings Second GI Conference on Automata Theory and Formal Languages*, pp. 134–183. Lecture Notes in Computer Science, 1975.

[7] 伊庭 斉志. 代数学的手法に基づく幾何学的概念の推論 – 第1報：Wuの手法を用いた幾何学的推論 –. 人工知能学会誌, Vol. 5, No. 3, pp. 300–310, 1990.

[8] 伊庭 斉志. 代数学的手法に基づく幾何学的概念の推論 – 第2報：軌跡問題の解法 –. 人工知能学会誌, Vol. 5, No. 3, pp. 311–323, 1990.

[9] D. Kapur. Geometry theorem proving using Hilbert's nullstellensatz. In *Symposium on Symbolic and Algebraic Computation*, pp. 202–208, 1986.

[10] D. Kapur and J. L. Mundy. Wu's method and its application to perspective viewing. *Artificial Intelligence*, Vol. 37, No. 1-3, pp. 15–36, 1988.

[11] B. Kutzler and S. Stifter. On the application of Buchberger's algorithm to automated geometry theorem proving. In *Journal of Symbolic Computation*, pp. 389–397, 1986.

[12] B. A. Kutzler. *Algebraic approaches to automated geometry theorem proving.* PhD thesis, Institut für Mathematik Technisch-Naturwissenschaftliche Fakultät Johannes Kepler Universität Linz, Nov. 1988.

[13] A. J. Nevins. *Plain Geometry Theorem Proving Using Forward Chaining. Artificial Intelligence*, Vol.6, pp. 1–23, 1975.

[14] R. F. Ritt. *Differential Algebra.* AMS Colloquium Publication, 1950.

[15] W. T. Wu. On the decision problem and the mechanization of theorem proving in elementary geometry. *Scientica Sinica*, Vol. 21, pp. 157–179, 1978.

[16] W. T. Wu. Basic principles of mechanical theorem proving in elementary geometries. *Journal of Automated reasoning*, Vol. 2, No. 4, pp. 221–252, 1986.