

代数学的手法に基づく幾何学的推論システム(1)

3F-8

東京大学工学部

伊庭 斉志 井上 博允

1. はじめに

幾何学的概念に関する推論は、ロボティクス・CADなどの広範な応用分野がある。しかしながら、表現及び推論能力の点で、述語論理に基づく多くの推論システムは幾何学的対象を扱うのに適していない。

例えば(Nevins75)に代表される従来の推論システムでは、幾何学的拘束は形式的な記号で表現されており、ヒューリスティクスを伴う変形と記号レベルのマッチングが推論の基本原理であった。その結果、幾何学的概念の本来の特徴である変換不変の性質を的確に表現することができず、補助線を伴う複雑な推論も極めて困難であった。

本稿では、この問題を解決するために代数学的手法を用いて幾何学的推論システムを構築することを試みる。さらに、実験結果をもとにシステムの有効性を示し、効果的な推論手法について述べる。

2. 幾何学的推論と Wu の定理

一般に幾何学の証明問題の仮定は、三角形式と呼ばれる代数幾何学の式として次のように表現される。

$$\begin{aligned} \text{hyp}_1(u_1, \dots, u_d, x_1) &= 0 \\ \text{hyp}_2(u_1, \dots, u_d, x_1, x_2) &= 0 \\ &\dots \\ \text{hyp}_r(u_1, \dots, u_d, x_1, x_2, \dots, x_r) &= 0 \end{aligned} \quad (1)$$

ここで u_1, \dots, u_d は独立変数、 x_1, x_2, \dots, x_r は従属変数である。この時証明すべき命題を記述した式、

$$\text{Conc}(u_1, \dots, u_d, x_1, x_2, \dots, x_r) \quad (2)$$

が(1)の条件の下で恒等的に0となるかを調べることが証明に他ならない。Wuの定理(Wu78)は代数多様体上の解釈として、次のことを主張する。

(2) が (1) の下で恒等的に0となる
即ち定理が成立する
 $\Leftrightarrow \text{Con}_r = 0$

但し Con_r (剰余項) は次のように計算する。これを以下では「Wuの手続き」と呼ぶ。

$$\begin{aligned} \text{Con}_0 &:= \text{Conc} \\ \text{Con}_{i+1} &:= (\text{Con}_i \text{ を } \text{hyp}_{r-i+1} \text{ で変数 } x_{r-i+1} \\ &\quad \text{をもとに割った余り}) \end{aligned}$$

(Chou84)はこの定理を用いて初等幾何学の証明の実験を行った。(Swain86)は証明プログラム(Algeprover)を作成し、証明のための補助条件(自明解を省くための

条件)を計算した。しかしながら、それらの計算手続きの詳細は明らかではない。

我々はこれらの成果をふまえて、効率的なプログラムをMACSYMA上で記述した。一般に多項式 $f(x, y, \dots, z)$ を別の多項式 x, y, \dots, z とは異なる変数をもとに割っても余りは f のままである。従って、結論式 Conc に現れる変数と、式間の変数の依存関係を考慮して、Wuの手続きに効果的な順序で除法を行うための三角形式の導出手法を実現した。次節ではその概略について述べる。

なお代数学的手法を用いる幾何学的推論システムとしては、イデアル理論に基づいたGröbner基底(Buchberger85)によるものもある。しかしながら幾何学上の推論の際には、(1)効率上及び(2)退化の除去条件($A \cdot B - 1 = 0$ for $A \neq 0$)が不要な点で、Wuの定理を用いる方が有効であることが指摘されている(Chou86)。従って本システムでは、Wuの定理を推論の基礎理論として採用した。

3. 三角形式導出のアルゴリズム

Wuの定理に基づいて幾何学的推論システムを実現する場合、その計算の中心は三角化にある。本節では、三角化の単純なアルゴリズムについて述べる。効率化については、次稿で考察する。

入力として与えられた式、

$$\begin{aligned} f_1(u_1, \dots, u_d, x_1, \dots, x_r) \\ f_2(u_1, \dots, u_d, x_1, \dots, x_r) \\ \dots \\ f_r(u_1, \dots, u_d, x_1, \dots, x_r) \end{aligned}$$

を(1)の形に変形することを考える。このための単純なアルゴリズムは、次のようになる。

STEP1: $n := r$

STEP2: $n = 0$ なら終り

STEP3: $f_1 \sim f_n$ を x_n の次数でソートし次列を得る

$$\begin{aligned} f_1, \dots, f_k \quad x_n \text{ を含まない} \\ f_{k+1}, \dots, f_n \quad x_n \text{ の次数の少ない順にソート} \end{aligned}$$

STEP4: $k = n - 1$ のとき (即ち x_n を含むのは唯一)

$$\begin{aligned} \text{hyp}_n &:= f_n \\ f_j &:= f_j \quad (j=1, \dots, n-1) \\ n &:= n - 1 \end{aligned}$$

としてSTEP2へ

STEP5: $f_j := \text{Rem}(f_j, f_{k+1}, x_n)$ (但し $j=k+2, \dots, n$)

としてSTEP2へ

ここで $\text{Rem}(f, g, x)$ は、式 f を式 g で変数 x をもとに割った余りを示す。

STEP3において、 $f_1 \sim f_n$ は $x_1 \sim x_n$ までの従属変数のみを含む。STEP5により、 $f_{k+2} \sim f_n$ の x_n の次数は f_{k+1} の次数より小さくなるので、このアルゴリズムの停止性は保証される。

このアルゴリズムの計算量は次のように評価される。STEP3に来たときの f_1, \dots, f_n の x_n の次数を各々 d_1, \dots, d_n とする。このとき x_n を消去し終わるまでに必要な割り算の回数 $D(n)$ は、

$$D(n) = \{(d_i > 0 \text{ となる個数}) - 1\} * \text{Min}((d_1, \dots, d_n))_{d_j > 0}$$

となる。今 $\{(d_i > 0 \text{ となる個数}) - 1\} \leq n \leq r$ であるから、STEP3~5の割り算の繰り返しは、 $O(r^2)$ でおさえられる。

$D(n)$ を用いて、各変数で除算の回数を推定し、必要なら $x_1 \sim x_n$ を並べかえて、三角化の際の計算量を減らすことができる。

次節では、以上の原理に基づいて実現したシステムでの幾何学的推論の実行例を示す。

4. 推論の実行例

本節では、他の手法との比較としてしばしば用いられるHilbertの9点定理の証明を例にとりて、推論の過程を説明する。

9点定理は、次のような命題である。

三角形ABCの三頂点から対辺に下ろした垂線の足をD, E, F, 垂心をHとして、AH, BH, CHの中点を各々P, Q, R, 三辺の中点をL, M, Nとすれば、9点D, E, F, L, M, N, P, Q, Rは同一円周上にある(図1)

ここでE, D, F, M (ABの中点)が同一円周上にあることを証明しよう。この時、適当な座標系(A(0,0), B(a,0), C(b,c), D(d,e), E(f,g), F(h,0), M(h,0), S(i,j))。但しSは円DEFの中心)をとることで、命題の仮定($f_1 \sim f_7$)と結論(Conc)は以下ようになる。

$f_1 = -c \cdot e + (-b+a) \cdot (d-a)$	DがBC上
$f_2 = (-b+a) \cdot d - c \cdot e$	AD⊥BC
$f_3 = c \cdot g + b \cdot (f-a)$	AC⊥BE
$f_4 = -b \cdot g + c \cdot f$	EがAC上
$f_5 = -2 \cdot h + a$	MがABの中点
$f_6 = 2 \cdot g \cdot j + (2 \cdot f - 2 \cdot b) \cdot i - g^2 - f^2 + b^2$	SE=SF
$f_7 = 2 \cdot e \cdot j + (2 \cdot d - 2 \cdot b) \cdot i - e^2 - d^2 + b^2$	SD=SF
Conc = $(2 \cdot h - 2 \cdot b) \cdot i - h^2 + b^2$	SF=SM

ここで三角形式を導出し、次式を得る。

$$\text{hyp}_1(d, j, f, g, i, a, h) = a - 2 \cdot h$$

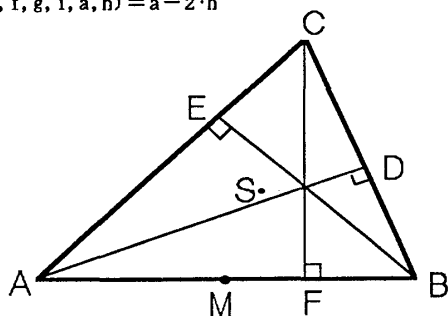


図1. Hilbertの9点定理

$$\text{hyp}_2(d, j, f, g, i, a) = c \cdot g + b \cdot (f-a)$$

$$\text{hyp}_3(d, j, f, g, i) = 2 \cdot g \cdot j + (2 \cdot f - 2 \cdot b) \cdot i - g^2 - f^2 + b^2$$

$$\text{hyp}_4(d, j, f, g) = c \cdot d \cdot g + b \cdot d \cdot f - b \cdot c \cdot e - b^2 \cdot d$$

$$\text{hyp}_5(d, j, f) = (c^2 + b^2) \cdot d \cdot f - b^2 \cdot c \cdot e - b^3 \cdot d$$

$$\begin{aligned} \text{hyp}_6(d, j) = & c^2 \cdot (2 \cdot b \cdot d \cdot e^2 \cdot j - 4 \cdot c \cdot d^2 \cdot e \cdot j \\ & + 2 \cdot b \cdot c \cdot d \cdot e \cdot j - 2 \cdot b \cdot d^3 \cdot j + 2 \cdot b^2 \cdot d^2 \cdot j - b \cdot d \cdot e^2 \\ & + c \cdot d^2 \cdot e^2 + b \cdot c \cdot d \cdot e^2 - b^2 \cdot c \cdot e^2 - b \cdot d^3 \cdot e \\ & + 2 \cdot b^2 \cdot d^2 \cdot e - b^3 \cdot d \cdot e + c \cdot d^4 - b \cdot c \cdot d^3) \end{aligned}$$

$$\text{hyp}_7(d) = -b \cdot c \cdot e^2 - b^2 \cdot d \cdot e$$

上式で独立変数は省略してある。得られた三角形式に対してWuの手続きを実行すると、以下ようになる。

$$\text{Con}_1 = -(2 \cdot b - a) \cdot (4 \cdot i - 2 \cdot b - a)$$

$$\text{Con}_2 = (c \cdot g + b \cdot f - 2 \cdot b^2) \cdot (4 \cdot b \cdot i - c \cdot g - b \cdot f - 2 \cdot b^2)$$

$$\begin{aligned} \text{Con}_3 = & -(c \cdot g + b \cdot f - 2 \cdot b^2) \cdot (4 \cdot b \cdot g \cdot j - 2 \cdot b \cdot g^2 + c \cdot f \cdot g \\ & - b \cdot c \cdot g - b \cdot f^2 + b^2 \cdot f) \end{aligned}$$

$$\begin{aligned} \text{Con}_4 = & b^2 \cdot (c \cdot e - b \cdot d) \cdot (4 \cdot b \cdot c \cdot d^2 \cdot f \cdot j - 4 \cdot b \cdot c^2 \cdot d \cdot e \cdot j \\ & - 4 \cdot b^2 \cdot c \cdot d^2 \cdot j + 2 \cdot c^2 \cdot d^2 \cdot f^2 + 2 \cdot b^2 \cdot d^2 \cdot f^2 \\ & - c^3 \cdot d \cdot e \cdot f - 4 \cdot b^2 \cdot c \cdot d \cdot e \cdot f - 3 \cdot b \cdot c^2 \cdot d^2 \cdot f \\ & - 4 \cdot b^3 \cdot d^2 \cdot f + 2 \cdot b^2 \cdot c^2 \cdot e^2 + b \cdot c^3 \cdot d \cdot e \\ & + 4 \cdot b^3 \cdot c \cdot d \cdot e + b^2 \cdot c^2 \cdot d^2 + 2 \cdot b^4 \cdot d^2) \end{aligned}$$

$$\text{Con}_5 = -b^3 \cdot c^3 \cdot (c \cdot e - b \cdot d) \cdot (c \cdot e + b \cdot d)$$

$$(4 \cdot d \cdot j - b \cdot e - c \cdot d)$$

$$\text{Con}_6 = -b^3 \cdot c^3 \cdot (2 \cdot d - b) \cdot (b \cdot e - c \cdot d) \cdot (c \cdot e - b \cdot d)$$

$$(c \cdot e + b \cdot d) \cdot (e^2 - c \cdot e + d^2 - b \cdot d)$$

$$\text{Con}_7 = 0$$

$$\text{Subsidiaries} = b \cdot c \cdot (b^2 + c^2) \cdot d$$

$$(b \cdot e^2 - 2 \cdot c \cdot d \cdot e + b \cdot c \cdot e - b \cdot d^2 + b^2 \cdot d) \cdot (f - b)$$

従って定理は成立する。つまり円DEF上にMがあることが証明された。但しSubsidiariesは、前述の補助条件を示す。

本例は、VAX8600のMACSYMA上でCPUtimeが195秒(その内GCtimeが39秒)で証明が終了した。このことは、明らかに補助線の必要な問題に対して、従来のようなアド・ホックなヒューリスティックスを必要としない代数学的手法の有効性を示している。なおここでは、座標系の取り方が仮定の式を簡単にしているが、一般の位置に系を設定した場合でも、変数が5つ、式数が2つ増えるのみで、効率は急激には悪化しない。

さらにいくつかの定理の証明の他、画像理解で用いられる推論に対しても実験を行い、本手法の有効性を確認した(伊庭88)。

5. おわりに

本稿では、代数幾何学的表現を用いて幾何学的推論システムを実現する方法について説明した。

代数的手法は、述語論理による従来の幾何学的推論システムの持つ不完全さを補い、幾何学的概念の適切な扱いを可能にする。本例が示すように、幾何学的概念に本質的な補助線やヒューリスティックスを伴う推論・証明において、この手法は特に有効であると思われる。

参考文献は、次稿"代数学的手法に基づく幾何学的推論システム(2)"において一括して表記する。