代数制約の構造情報を用いた幾何定理証明の効率化手法の検討
- グレブナ基底による方法への適用 -

永井 保夫

（株）東芝 情報通信システム技術研究所

1 はじめに

本稿では，代数的手法の一種であるグレブナ基底法を用いた幾何定理証明に対する，代数制約評価の効率化手法の適用について報告する．幾何定理の証明問題を代数制約を用いた制約論理型言語 [5,6] のひとつの応用問題とみなし，代数制約評価系の効率化手法の検討をおこなった．また，いくつかの幾何定理の証明に対して本手法の適用実験をおこなった．

2 代数的手法を用いた幾何定理証明

幾何学的定理の証明問題では，座標系を設定し，その座標系に基づいて仮説と結論からなる幾何定理を代数多項式に変換し，このような領域において代数的手法を用いて証明をおこなう．幾何定理証明の手法にはいくつかの方法があるが，われわれはグレブナ基底の方法を採用する．以下ではまず，グレブナ基底について簡単に説明し，次にグレブナ基底による方法を用いた定式化について述べる．

2.1 グレブナ基底

グレブナ基底は多項式イデアルの計算をするために，B. Buchberger によって提案された概念であり，その計算アルゴリズムは Buchberger アルゴリズムとして知られている [4]．多項式イデアルのグレブナ基底は，イデアルのメンバシップ決定問題を解くために利用される．Buchberger アルゴリズムは数式処理の分野においては有効な手法にひとつであるが，実際の基底計算には非常に時間がかかり，制約の評価順序および単項 (変数) の優先順位が非常に影響を及ぼすことが多い [2,4]．

2.2 グレブナ基底による方法を用いた幾何定理証明

グレブナ基底による定理証明は，結論を示す代数多項式が，仮説を示す代数多項式から生成されるイデアルに属するかどうかを決定するイデアルのメンバシップ問題とみなし，定理が成立するかどうかを決定する．つまり，仮説から結論が導けるかどうかを決定する．

グレブナ基底による方法では，幾何学的な概念の記述によって，直接的なアプローチと反駁的なアプローチに分けることができる．直接的なアプローチは，1) 仮説のグレブナ基底 (標準形) を求め，2) 求められた基底を用いて結論が正しいかどうかを判定する [1,3]．一方，反駁的なアプローチでは，仮説の否定形を求め，仮説に対してこの否定形を加えた多項式集合の充足不能性 (矛盾) を判定する．充足不能性は多項式集合のグレブナ基底を求め，基底の要素に 1 を含んでいるかどうかにより判定できる [2]．

3 代数制約の構造情報を用いた効率化手法の適用

グレブナ基底による方法を用いた幾何の定理証明手続きを効率的におこなうためには，グレブナ基底をいかに効率的に求めるかが重要である．

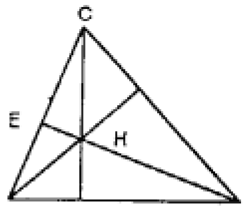
そこで，幾何定理証明において取り扱う多項式集合 (仮説集合と結論) のグレブナ基底を効率的に求めるために，これらの集合を代数制約集合とみなす．グラフ論的手法を用いて代数制約の構造情報を抽出し，抽出された情報を用いて制約論理型言語の代数制約評価を効率化する [7]．

3.1 代数制約の構造情報

代数制約の構造情報は，制約グラフの構造分解によって求められる．スパース構造を有している場合，ブロック三角化行列が生成され，グラフにより表現された問題はブロック三角化行列の順序関係に基づき部分問題 (部分グラフ) に分割され，制約間の依存関係情報が生成される．制約グラフがスパース構造を有していれば，制約間の依存関係情報を，Buchberger アルゴリズムの制御情報とみなして，グレブナ基底を効率的に求めることができる [7]．

3.2 例題による説明

図 1 のような「三角形 ABC においてその高さ BE と CF の交点を H としたとき，直線 AH は直線 BC と直交する」という定理 (3 垂線定理) の証明を考える．座標系として，$A = (0,0)$, $B = (u_1, 0)$, $C = (x_1, x_2)$, $E = (u_2, u_3)$, $H = (x_1, x_3)$ とする．



A=(0,0), B=(u1, 0), C=(x1, x2), E=(u2, u3), H=(x1, x3)

図 1

仮説を示す多項式制約は次のようになる．

$$x_2 u_3 + (u_2 - u_1) x_1 = 0 \;;\; BE \text{ は } AC \text{ と直交する} \quad (1)$$
$$-u_2 x_2 + u_3 x_1 = 0 \;;\; A, E, C \text{ は一直線上にある} \quad (2)$$
$$(u_1 - u_2) x_3 + u_3 x_1 - u_1 u_3 = 0 \;;\; B, E, H \text{ は一直線上にある} \quad (3)$$

また，本定理では，($x_2 \neq 0$ かつ $u_1 \neq 0$)，または $u_3 \neq 0$ という補助条件が必要となり，そのために新しい変数 z_1, z_2 を導入し，次のように表現する．

$$(z_1 x_2 u_1 - 1)(z_2 u_3 - 1) = 0 \;; \quad (4)$$

定理の結論をあらわす多項式制約は

$$x_2 x_3 = -x_1(x_1 - u_1) \;;\; AH \text{ は } BC \text{ と直交する} \quad (5)$$

のようになる．

直接的なアプローチでは，仮説集合 $H = \{x_2 u_3 + (u_2 - u_1) x_1 = 0, -u_2 x_2 + u_3 x_1 = 0, (u_1 - u_2) x_3 + u_3 x_1 - u_1 u_3 = 0$, ならびに補助条件 (または非退化条件) $S = \{(z_1 x_2 u_1 - 1)(z_2 u_3 - 1) = 0\}$ のグレブナ基底を計算し，次に，結論 $c = (x_2 x_3 = -x_1(x_1 - u_1))$ が正しいかどうかを，求められたグレブナ基底を用いて判定する．すなわち，基底の要素である多項式を用いて結論 c を書き換えていき，既約になるまで簡約化をおこない，その正規形がゼロになるかどうかを判定する．

次に，反駁によるアプローチでは，まず，結論 c の否定形を新たな変数 z_3 の導入により求める．

$$z_3(x_2 x_3 + x_1(x_1 - u_1)) - 1 = 0 \;;\; \text{結論 } c \text{ の否定形} \quad (6)$$

そして，上記の仮説集合 H ならびに補助条件 S に結論 c の否定形を加えた多項式制約のグレブナ基底を求める．求められた基底の要素に 1 が存在するかどうかを判定する．

グレブナ基底法を用いた幾何定理証明では，変数の優先順位が処理時間に非常に影響を与えるため，その設定をいかにおこなうかが非常に問題となる．Wu の方法においては，変数を独立変数と従属変数に

Improvement of Geometric Theorem Proving Using Dependency Analysis of Algebraic Constraint
Yasuo NAGAI
TOSHIBA, Corp.

分類し，分類された変数の依存関係情報に基づいて三角化形式を生成することにより，処理性能を改善できる．つまり，変数において，独立変数をどのように選択するかが処理性能に非常に影響を及ぼすことになる．グレブナ基底法を用いた定理証明においても，Wu の方法ほど敏感には処理性能に影響を与えないが，変数の独立変数ならびに従属変数への分類が処理性能に影響を与えることが実験的に示されている [2]．

われわれが提案した効率化手法では，変数の独立変数ならびに従属変数への分類は代数制約の構造情報を解析し，得られた構造情報から制約が不足 (不十分) である状態や制約が矛盾または競合した状態を判定することによりおこなうことができる [3]．なお，$u_k \ldots u_1$ は独立変数をあらわし，$x_l \ldots x_1$ は従属変数をあらわす．

$$x_l \succ \cdots \succ x_1 \succ u_k \cdots \succ u_1$$

さらに，変数の優先順位付け，特に従属変数間の順位付けも，代数制約の構造情報の解析により求められる制約間の依存関係 (変数の共有関係) 情報から決定する．

図 2 は，図 1 の例題の代数制約の構造情報をあらわす．

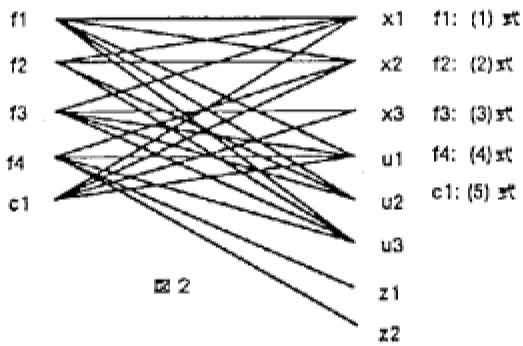


図 2

図 2 の構造情報の解析結果にしたがい，x_1, x_2, x_3，u_1, u_2 を従属変数，u_3, z_1, z_2 を独立変数とみなし，以下のような変数の順位を決定する (本実験では前者を採用した)．

$$[x_1, x_2, x_3, u_1, u_2] \gg [z_1, z_2] \gg u_3$$
または
$$[x_1, x_2, x_3, u_1, u_2] \gg [u_3, z_1, z_2]$$

3.3 制約論理型言語を用いた実験

まず，制約論理型言語 CAL[6] による定理証明問題の記述例を説明し，次に，効率化手法の適用実験結果について示す．

3.3.1 CAL による例題の記述

グレブナ基底を求める代数制約評価系が提供された制約論理型言語 CAL を用いて，3.2 で説明した 3 垂線定理を記述すると次のようになる．図 3 には，直接的なアプローチにより記述したプログラムを，さらに図 4 には構造解析の結果を反映してゴールを並べ換えたプログラムを，図 5 には反駁的なアプローチにより記述したプログラムを示す．

CAL ではインクリメンタルに代数制約を評価していき，基底を求める．したがって，本実験では基底の効率的な求解のために，図 4 のように制約の評価順序を変更し，さらに，変数の順序付けを CAL の組み込み述語 pre をもちいておこなった．

```
:- public tp_orthocenter/0.
%% Theorem of Orthocenter  %%
tp_orthocenter  :-
        x2*u3+(u2-u1)*x1=0,
        -u2*x2+u3*x1=0,
        (u1-u2)*x3+u3*x1-u1*u3=0,
        (z1*x2*u1-1)*(z2*u3-1)=0,
        evalwrite(x2*x3+x1*(x1-u1)).
```

図 3: 直接的なアプローチにより記述したプログラム

```
:- public tp_orthocenter1/0.
%% Theorem of Orthocenter  %%
tp_orthocenter1  :-
        x2*u3+(u2-u1)*x1=0,
        -u2*x2+u3*x1=0,
        (z1*x2*u1-1)*(z2*u3-1)=0,
        (u1-u2)*x3+u3*x1-u1*u3=0,
        evalwrite(x2*x3+x1*(x1-u1)).
```

図 4: ゴールを並べ換えたプログラム

```
:- public tp_orthocenter_rf/0.
%% Theorem of Orthocenter (Refutational) %%
tp_orthocenter_rf  :-
        x2*u3+(u2-u1)*x1=0,
        -u2*x2+u3*x1=0,
        (u1-u2)*x3+u3*x1-u1*u3=0,
        (z1*x2*u1-1)*(z2*u3-1)=0,
        z3*(x2*x3+x1*(x1-u1))-1=0.
```

図 5: 反駁的なアプローチにより記述したプログラム

3.3.2 実験結果

直接的アプローチを用いた定理証明手続きに対して，効率化手法を適用しない場合と適用した場合について実験をおこなった．実験対象とした定理は 3.2 節の 3 垂線定理ならびに 9 点円定理 [1] である．なお，これらの定理は補助条件や非退化条件がすべて与えられていると仮定する．結果として，表 1 のように，3 垂線定理では処理時間が約 1/3 に短縮された．さらに，問題がより複雑な 9 点円定理では処理時間が約 1/300 にも短縮することができた．

対象とした幾何定理	適用前	適用後
3 垂線定理 (5 仮説，8 変数)	7565	2371
9 点円定理 (9 仮説，12 変数)	3524098	12753

表 1: 幾何定理証明の実験結果 (単位:msec)

4 まとめ

まず，代数的手法を用いた幾何定理証明，特にグレブナ基底法を用いた幾何定理証明について述べた．次に，代数制約の構造情報を用いてグレブナ基底を求める効率化手法について，例題を示して説明をおこなった．そして，本効率化手法をいくつかの幾何定理の証明問題に対して適用した．具体的にはグレブナ基底を求める代数制約評価系が提供されている制約論理型言語 CAL を用いて実験をおこない，本手法の有効性を示した．

謝辞

本研究は第 5 世代コンピュータプロジェクトの一環として行なわれた．本研究の機会を与えてくださり，常にご指導いただいた ICOT の淵一博所長，古川康一研究次長，生駒憲治部長代理，新田克己第 7 研究室室長ならびに，有益なコメントをいただいた長谷川隆三部長代理に深く感謝いたします．また，CAL を利用するにあたり，いろいろ教えて頂いた相場亮第 4 研究室室長代理をはじめとした第 4 研究室の皆様に感謝いたします．

参考文献

[1] B. Kutzler, Algebraic Approaches to Automated Geometry Theorem Proving, PhD Thesis, Johannes Kepler Unversity, RISC-LINZ Series no. 88-74.0, (1988)
[2] D. Kapur, A Refutational Approach to Geometry Theorem Proving, Artificial Intelligence 37, (1988)
[3] D. Kapur and J.L. Mundy, Wu.s Method and Its Application to Perspective Viewing, Artificial Intelligence 37, (1988)
[4] B. Buchberger, Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory, Publications/Reports, RISC-Linz Series no. 83-29.0, (1983)
[5] 渕一博監修，溝口文雄他編，制約論理プログラミング，知識情報処理シリーズ 別巻 2，共立出版，(1989)
[6] K. Sakai and A. Aiba, CAL: A Theoretical Background of Constraint Logic Programming and its Applications, J. of Symbolic Computation 8, (1989)
[7] 永井保夫，制約グラフの構造分解および整合性解析による代数制約評価系の効率化についての検討，人工知能学会合同研究会「AI シンポジウム '90」，人工知能学会研究会資料 SIG-FAI-HICG-KBS-9001-12, (1990)