グレブナ基底求解法のＳＡＴへの適用

2P－4

吉田清明　朱雀保正　元石浩二
（久留米工業大学）

１．はじめに

命題論理の充足可能性問題（以下，ＳＡＴという）は代表的なＮＰ完全問題であり，情報処理分野の基本的かつ重要な問題の１つでもある．この問題に対して従来，Davis-Putnamに代表される記号的方法や，Branch and Bound，切除平面法，内点法，陰的列挙法に基づく定量的方法が提案されてきた[1]．また包除原理に基づく計数法[2]も提案されている．

ＳＡＴは代数化することにより，等価な非線形多元連立代数方程式に変換することができる．これらの方程式はその多峰性のために，解くのが難しいが，これに対しては，すでにグレブナ基底の求解法（完備化アルゴリズム）が提案されている．本稿では，多項式イデアルを対象とした完備化アルゴリズム（ここでBuchbergerアルゴリズム）をＳＡＴに適用する手法（以下，本手法）を提案する．また，本手法を幾つかの規模の小さな例題に対して適用した結果を示す．

２．グレブナ（Gröbner）基底

グレブナ（Gröbner）基底[3]～[6]は連立代数方程式に付随する多項式イデアルである．その特徴は決定論的な簡約操作（M-reduction)が存在し，連立代数方程式の束縛条件の下で，任意の多項式の一意表現がその簡約操作により計算できることである．グレブナ基底を求めるための代表的アルゴリズムとしてはBuchbergerアルゴリズムやその改良版がよく知られている．

３．Buchbergerアルゴリズム

次にBuchbergerアルゴリズムを示す．以下の内容は文献[5]から借用した．

Eを与えられた方程式（等式）の集合，Rを書き換え規則の集合とする．次のアルゴリズムにより，Eのグレブナ基底が，規則の形でRに求まる．

1. $R \leftarrow \varnothing$
2. E中の等式$1 = r$のすべてについて，$1 - r$をR中の書換え規則と算術演算とによって，単純化し，式eを得る．$e \equiv 0$であれば，その等式を捨てる．そうでなければ，E中の等式$1 = r$を$e = 0$で置き換える．
3. $E = \varnothing$であれば，終了．
4. E中から等式$e = 0$を選ぶ．
5. e中の，ある順序による最大の単項を$1'$として，$e = 0$を変形して式$1' = r'$を得る．
6. 規則$1' \rightarrow r'$をRに加える．
7. R中の規則の要対を等式としてEに付け加える．
8. 2へ行く．

４．本手法

本手法の概要は以下の通りである．

Step1:与えられた命題論理を代数化し，非線形多元連立代数方程式に変換する．

Step2:Step1で得られた連立方程式に，Buchbergerアルゴリズム等を適用する．

Step3:グレブナ基底が求まれば，与えられた命題論理は充足可能である．そうでなければ充足不能である．

なお代数化は表１の変換規則に基づき行う．

表１　演算系での等価な表現

	ブール　代数化表現
論理積	$x \cap y \Rightarrow x \cdot y$
論理和	$x \cup y \Rightarrow x + y + x \cdot y$
補元	$\bar{x} \Rightarrow 1 - x$

また各々の変数には，１あるいは０のみが代入されることを仮定しているので，次の定理１が成り立つ．

[定理１]　xを任意の変数として，

$x^n \equiv x$　（ただし，nは自然数）

５．例題

次の論理式fに本手法を適用してみる．

$$f = (\bar{a} \cup c \cup d) \cap (\bar{a} \cup \bar{b} \cup \bar{d}) \cap (\bar{a} \cup b \cup \bar{c}) \cap (a \cup \bar{c} \cup \bar{d}) \cap (\bar{b} \cup \bar{c} \cup d) \cap (a \cup c \cup d) \quad (1)$$

式(1)が充足可能であると仮定すると，次式が得られる．

$$f = 1 \quad (2)$$

ドモルガンの定理より式(2)は次式のように変形可能である．

$$(a \cap \bar{c} \cap \bar{d}) \cup (a \cap b \cap d) \cup (a \cap \bar{b} \cap c) \cup (\bar{a} \cap c \cap d) \cup (b \cap c \cap \bar{d}) \cup (\bar{a} \cap \bar{c} \cap \bar{d}) = 0 \quad (3)$$

式(3)は次の６式と等価である．

Application of the Gröbner Bases Algorithm to the SAT Problem. Kiyoaki YOSHIDA, Yasumasa SUJAKU and Kohji MOTOISHI. *Kurume Institute of Technology, 2228 Kamitsu-machi, Fukuoka 830, JAPAN*

$(a \cap \bar{c} \cap \bar{d}) = 0$ (4a)
$(a \cap b \cap d) = 0$ (4b)
$(a \cap \bar{b} \cap c) = 0$ (4c)
$(\bar{a} \cap \cup c \cap d) = 0$ (4d)
$(b \cap c \cap \bar{d}) = 0$ (4e)
$(\bar{a} \cap \bar{c} \cap \bar{d}) = 0$ (4f)

上式に表１の数式化を施すと，各々次のようになる．

$a \cdot (1-c) \cdot (1-d) = 0$ (5a)
$a \cdot b \cdot d = 0$ (5b)
$a \cdot (1-b) \cdot c = 0$ (5c)
$(1-a) \cdot c \cdot d = 0$ (5d)
$b \cdot c \cdot (1-d) = 0$ (5e)
$(1-a) \cdot (1-c) \cdot (1-d) = 0$ (5f)

以上の処理により，式(2)のブール方程式が式（５a)-(5f)の非線形多元連立方程式に変換された．次にこれらの連立方程式にBuchbergerアルゴリズムを適用すると，定理１の条件下で次のようなグレブナ基底が得られる．

$-1+c+d = 0$ (6)
$-b+b \cdot d = 0$ (7)
$-a+a \cdot d = 0$ (8)
$a \cdot b = 0$ (9)

従って，式(1)の命題論理 f は充足可能であると判定できる．

６．実験結果

ＳＡＴと３ＳＡＴの計算量的複雑度は等価である．本手法を比較的小さな規模の３ＳＡＴの例題に適用した結果を表２に示す．実験に使用した計算機はSUN-4/IPX（実装主記憶32MB, 28.5MIPS）である．各々の例題は#1から#5までは5変数，#6から#17までは10変数であり，「無し」，「１」は例題の性質であり，それぞれ充足不能問題，ただ一つの解を持つ充足可能問題であることを表す．「Solve」，「Gröbner」は各々Mathematicaの組み込み関数SolveとGroebnerBasisを用いて実験した場合の各々のCPU時間である．Solveは通常の連立方程式の解を求め，GroebnerBasisはBuchbergerアルゴリズムによりグレブナ基底を求める．CPU時間の測定にもMathematicaの組み込み関数を利用した．充足可能な例題に対しては，ある一組のグレブナ基底を，充足不能な例題に対しては解が無いことを出力した．例題#8，#17の例題に対しては，長時間実行した後，Mathematicaが「Out of memory」のメッセージを返して処理を中断した．これらについては現在，原因を調査中である．

表２　実行結果

例題	節数	実行時間（sec）		解の個数
		Solve	Gröbner	
#1	11	0.700	0.317	無し
#2	12	0.917	0.383	1
#3	12	1.717	0.300	無し
#4	14	2.017	0.147	1
#5	12	1.733	0.317	無し
#6	22	69.30	1.050	無し
#7	19	4.900	1.383	1
#8	24	31.87	――	無し
#9	22	33.98	3.267	1
#10	24	2.417	1.600	無し
#11	28	110.3	3.533	1
#12	24	37.46	2.167	無し
#13	20	14.30	1.600	1
#14	16	8.733	1.083	無し
#15	25	22.58	3.833	無し
#16	20	5.000	2.683	無し
#17	19	11.68	――	1

７．おわりに

ＳＡＴに完備化アルゴリズムを適用することを提案した．表２の実験結果は本手法のＳＡＴへの適用の可能性を示唆しているものと思われる．本稿では適用限界，条件等については明らかにしていない．これらは今後の課題としたい．

文献

[1] 大柳俊夫，山本雅人，大内東：陰的列挙法に基づくＳＡＴアルゴリズム，情報処理学会論文誌，Vol.33, No.12, pp.2464-2473(1993).
[2] K. Iwama: CNF satisfiability test by counting and polynomial average time, SIAM J. Comput. Vol.18, No.2, pp.385-391(1989).
[3] 小林英恒：多変数連立代数方程式の解法，情報処理，Vol.27, No.4, pp.414-421(1986).
[4] 外山芳人：最大公約数-普遍代数多項式イデアル，自動証明におけるユークリッドの互除法，bit, Vol.21, No.5, pp.96-109(1989).
[5] 相場 亮：ブフバーガアルゴリズム，bit, Vol.19, No.10, pp.1384-1385(1986).
[6] Buchberger,B.: Applications of Grobner Bases in Non-Linear Computational Geometry, rends in Computer Algebra, Lecture Notes in Computer Science, No.296, Springer-Verlag, pp.52-80(1987).
[7] 坂井 公：Knuth-Bendix の完備手続きとその応用，コンピュータソフトウェア，Vol.4, No.1, pp.2-22(1987).