

判断推理の多項式モデルによる計算アルゴリズム

高橋 拓也

早稲田大学数学応用数理専攻2年 楫研究室所属

2018年2月8日

- 概要
- 判断推理とは
- グレブナー基底と消去理論
- 限量記号消去
- 有限体上の Nullstellensatz
- 推論の多項式モデル
- 判断推理の自動計算

- 計算代数学において多項式計算を始めとした数式処理の発展は著しく、多項式の計算はグレブナー基底や終結式の理論を活用することで計算機に実装することができる。
- 有限個の値を取る論理に対して「与えられた仮定から結論を導くことができるかどうか」という問題は、論理構造を代数的に表現し有限体上の多項式環として取り扱うことで、**多項式のイデアル従属問題**に帰着できることが知られている。[5]

しかし、その理論を具体的な問題に活用する事例はあまり知られていない。

しかし、その理論を具体的な問題に活用する事例はあまり知られていない。

⇒ そこで我々は入社試験や公務員試験で頻出する判断推理の問題を、有限体上の多項式計算によって解くことを試みた。
結果、いくつかの問題（後述）について自動的に解くアルゴリズムを構成することができた。

判断推理とは

順序関係

P、Q、R、S、Tの5人で徒競走をした。

5人の順位について次のことが分かっている。

- i) Rの順位は、Sより上である
- ii) Tの順位は、Rよりも上だが、1着ではなかった
- iii) Qの順位は、Pより上である
- iv) 同着の順位の者はいない

次のア、イ、ウの推論のうち、必ず正しいものはどれか。

ア Qは1着である

イ Sは5着である

ウ 2着はPまたはTである

命題論理

ある集団に、海外旅行の経験をアンケートしたところ、次のア～エのことがわかった。

ア オーストラリアに行ったことがある人は、中国に行ったことがある。

イ メキシコに行ったことがある人は、フランスとベルギーの両方へ行ったことがある。

ウ 中国に行ったことがある人は、ベルギーまたはオーストラリアへ行ったことがある。

エ ドイツに行ったことがない人は、ベルギーに行ったことがない。

このとき確実にいえることはどれか。

1. 中国に行ったことがない人は、メキシコに行ったことがない。
2. ドイツに行ったことがある人は、中国に行ったことがある。
3. フランスに行ったことがない人は、ベルギーに行ったことがない。
4. メキシコに行ったことがある人は、ドイツに行ったことがある。
5. オーストラリアに行ったことがない人は、ベルギーに行ったことがある。

判断推理とは

判断推理

与えられた条件から、必ず推論される命題や推論される可能性がある命題を追求するジャンルである。

大枠としては論理, 関係, 推量推理, 試合等、11の分野から出題される。

我々は、このうち [論理 (命題)], [論理 (真偽)], [位置関係], [順序関係] に関してアルゴリズム的に解く方法を考案できた。

本発表では、命題と真偽の絡んだ論理問題の例について計算機代数ソフト singular を用いた解答法を提唱する。

グレブナー基底と消去理論

Def (グレブナー基底)

k を体とする。多項式環 $k[x_1, \dots, x_n]$ と単項式順序 $>$ に対して、多項式の集合 $G = \{g_1, \dots, g_s\}$ がイデアル $J \subset k[x_1, \dots, x_n]$ のグレブナー基底であるとは、

$$\langle LT(J) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$$

が成立することをいう。

Def (消去イデアル)

$J = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$ に対して、 J の l 次消去イデアル J_l とは、

$$J_l = J \cap k[x_{l+1}, \dots, x_n]$$

で定義された $k[x_{l+1}, \dots, x_n]$ のイデアルである。

グレブナー基底と消去理論

Thm (消去定理)

$J = \langle f_1, \dots, f_s \rangle \subset k[x_1, \dots, x_n]$ に対して G を $x_1, \dots, x_l > x_{l+1}, \dots, x_n$ となる消去順序に関する J のグレブナー基底とする。この時、すべての $0 \leq l \leq n$ に対して、 $G_l = G \cap k[x_{l+1}, \dots, x_n]$ は J の l 次消去イデアル J_l のグレブナー基底である。

e.g) $I = \langle x^3 - yz, yz^2 - z, xz - y^2 \rangle$ に対して、 I の辞書式順序に対するグレブナー基底 $G = \{g_1, \dots, g_5\}$ はそれぞれ、

$$g_1 = x^3 - yz$$

$$g_2 = xz - y^2$$

$$g_3 = y^2 - yz^6$$

$$g_4 = yz - z^7$$

$$g_5 = z^{14} - z$$

$$\therefore G \cap k[y, z] = \{g_3, g_4, g_5\} = \{y^2 - yz^6, yz - z^7, z^{14} - z\}$$

限量記号消去

Def (限量記号消去)

存在記号 $\exists$ や全称記号 $\forall$ といった限量記号が付随している一階述語論理式を考える。与えられた論理式に対して、限量記号を外した等価な論理式を導出することを、限量記号消去という。

実数上の限量記号消去は、柱状代数分解といった概念を用いることで実現できる。

$$\text{e.g) } \exists x(x^2 + ax + b \leq 0) \iff a^2 - 4b \geq 0$$

無限体上の基本理論については盛んに研究が進んでいて、工学における応用もよく知られている。

実は有限体において、ある制限を課すことにより限量記号消去を考えることができる。[3]

有限体上の Nullstellensatz

Thm (フェルマーの小定理)

$\mathbb{F}_p$ を標数 p (p : 素数) の有限体とする。この時、任意の元 $a \in \mathbb{F}_p$ に対して、 $a^p - a = 0$ が成立する。更に、 $V(x^p - x) = \mathbb{F}_p$ が成立する。

Thm (Nullstellensatz)

$J \subset \mathbb{F}_p[x_1, \dots, x_n]$ に対して、

$$I(V(J)) = J + \langle x_1^p - x_1, \dots, x_n^p - x_n \rangle$$

が成立する。

これらの事実を用いることにより、有限体上の方程式において「存在記号を消去すること」と「変数を消去すること」が同値であることが次の定理で示される。

有限体上の Nullstellensatz

Thm (限量記号消去と消去イデアルの関係)

$J \subset \mathbb{F}_p[\mathbf{x}, \mathbf{y}]$ を $\langle x_1^p - x_1, \dots, x_n^p - x_n, y_1^p - y_1, \dots, y_m^p - y_m \rangle$ を含むイデアルとする。

(ただし、 $\mathbf{x} = (x_1, \dots, x_n)$, $\mathbf{y} = (y_1, \dots, y_m)$ とする。)

この時、 $\pi_n : \mathbb{F}_p^{n+m} \rightarrow \mathbb{F}_p^m$ を射影とすると、

$$\pi_n(V(J)) = V(J_n)$$

が成立する。

この定理から、有限体上の多項式の零点は消去イデアルを計算することにより、およそその振る舞いを確認することが可能なことがわかる。

(特に、 $J \neq \langle 1 \rangle \Rightarrow V(J) \neq \emptyset$ である。)

[4] では、有限体上で全称記号や否定を含めて述語論理式を限量記号消去するアルゴリズムが挙げられている。

有限体上の多項式を考察する例として、多値論理の多項式モデルが挙げられる。

多値論理の構造は代数的に表現できることが知られていて、与えられた論理上の推論を多項式のイデアル従属問題に帰着できることが [5] で述べられている。

e.g)

$$X \wedge Y \longleftrightarrow xy + x + y$$

x, y が共に 0 の場合に限り、右辺の多項式は値 0 を取る。

Thm (演繹判定定理)

$V : \mathbb{F}_p[x_1, \dots, x_n] / \langle x_1^p - x_1, \dots, x_n^p - x_n \rangle \rightarrow \mathbb{F}_p$ 、

$V^* : (\text{命題論理式の集合}) \rightarrow \mathbb{F}_p$ をそれぞれ $\mathbb{F}_p$ に値を取る付値とし、

$T : (\text{命題論理式の集合}) \rightarrow \mathbb{F}_p[x_1, \dots, x_n] / \langle x_1^p - x_1, \dots, x_n^p - x_n \rangle$ を

$V^* \circ T = V$ を満たす写像とする。

True に対応する値を $a \in \mathbb{F}_p$ ($a = 0$ または $a = 1$ と考えるとよい) とすると、仮定 $\Phi_1, \dots, \Phi_m$ から結論 Ψ が導かれることと以下は同値である。

$$T(\Psi) - a \in \langle T(\Phi_1) - a, \dots, T(\Phi_m) - a, x_1^p - x_1, \dots, x_n^p - x_n \rangle$$

以上の理論は非常に強力なツールであるが、実際にこれを利用した問題解決の例はあまり知られていない。

そこで我々は有限体上の Nullstellensatz と演繹判定定理を活用し、判断推理の問題をグレブナー基底計算を用いて自動的に解く方法をいくつか考案した。その一例を紹介する。

真偽判定

ある幼稚園で、砂場で遊んでいた A、B、C、D、部屋で遊んでいた E、F、G の 7 人の中に、逆上がりができる子が 2 人いることが分かっている。そこで、A～G に尋ねたところ、それぞれ以下の発言をした。ただし、7 人のうち、本当のことを言っているのは 2 人だけで、あとの 5 人は間違ったことを言っている。

A : B は逆上がりできるよ。

B : A は間違ったことを言っているよ。

C : A も B も 2 人とも間違っていることを言っているよ。

D : 砂場で遊んでいた子の中には逆上がりできる子はいないよ。

E : 私は逆上がりができない。

F : 逆上がりができるのは 2 人とも砂場で遊んでいた子だよ。

G : E と F の少なくともどちらかは本当のことを言っているよ。

このとき確実にいえることはどれか。

1. 本当のことを言っているのは、1 人が砂場で遊んでいた子であり、1 人は部屋で遊んでいた子である。
2. D は本当のことを言っており、E は間違ったことを言っている。
3. B は逆上がりができ、間違ったことは言っていない。
4. F が逆上がりできるならば、G は逆上がりできない

Main Result

仮定に対応するイデアルと結論に対応するイデアルを用意する。結論イデアルに対して演繹判定定理を適用することにより推論が正しいか否かを判断することができる。

そこでまず仮定に対応するイデアルを構成しよう。

idea

- A～G に対応する変数を用意する。
- 逆上がりの可能不可能と主張の真偽にそれぞれ 0, 1 を対応させる。
- 主張を多項式表現する。
- 結論が仮定から導かれるかをイデアル従属判定により確認する。

判断推理の自動証明

ここで、7人のうち2人が逆上がりできるということを多項式表現するために、次の補題を用意する。

lemma

$\mathbb{F}_2[x_1, \dots, x_n]$ において、 $x_1 \sim x_n$ はそれぞれ0か1のいずれか一方の値を取るとする。また、 $x_1 \sim x_n$ に対して i 次の対称式を $S_i(x_1, \dots, x_n)$ とする。このとき、

$x_1 \sim x_n$ に1がちょうど i 個ある

$$\iff S_i(x_1, \dots, x_n) = 1 \text{ かつ } S_{n-i}(x_1 - 1, \dots, x_n - 1) = 1$$

e.g) $x_1 \sim x_5$ に1が3つ

$$\iff 1 \text{ が3つ以上かつ } 0 \text{ が2つ以上}$$

$$\iff$$

$$x_1x_2x_3 + x_1x_2x_4 + \dots + x_3x_4x_5 = 1,$$

$$(x_1 - 1)(x_2 - 1) + (x_1 - 1)(x_3 - 1) + \dots + (x_4 - 1)(x_5 - 1) = 1$$

判断推理の自動証明

計算機代数ソフト singular を用いてグレブナー基底を生成する

```
ring r=2,x(1..7),lp;  
//x(1)~x(7): A~G  
//逆上がりができる: 1、できない: 0  
//0:true 1:false  
poly p1=x(2)-1;  
poly p2=p1-1;  
poly p3=(p1-1)*(p2-1)+(p1-1)+(p2-1);  
//p1=1 かつ p2=1  
poly  
p4=(x(1)-1)*(x(2)-1)*(x(3)-1)*(x(4)-1)-1;  
poly p5=x(5);  
poly p61=  
x(1)*(x(2)+x(3)+x(4))+x(2)*(x(3)+x(4))  
+x(3)*x(4)-1;  
poly p62=(x(1)-1)*((x(2)-1)+(x(3)-1)+(x(4)-  
1))+(x(2)-1)*((x(3)-1)+(x(4)-1))+(x(3)-  
1)*(x(4)-1)-1;  
poly p6=p61*p62+p61+p62;  
//x(1)~x(4) の間に 1 が 2 つ以上 2 つ以下  
poly p7=p5*p6;
```

```
list l11=(p1,p2,p3,p4,p5,p6,p7);  
list l12=(p1-1,p2-1,p3-1,p4-1,p5-1,p6-1,p7-1);  
poly s5=symm(l11)[5]-1;  
// 5 次の対称式  
poly sn2=symm(l12)[2]-1;  
// 2 次の対称式  
//p1~p7 の間に 1 が 5 つ以上、0 が 2 つ以上  
list l21=(x(1),x(2),x(3),x(4),x(5),x(6),x(7));  
list l22=(x(1)-1,x(2)-1,x(3)-1,x(4)-1,x(5)-  
1,x(6)-1,x(7)-1);  
poly s2=symm(l21)[2]-1;  
poly sn5=symm(l22)[5]-1;  
//x(1)~x(7) の間に 1 が 2 つ以上、0 が 5 つ  
以上  
ideal i=sn2,s5,s2,sn5,x(1)^2-x(1),x(2)^2-  
x(2),x(3)^2-x(3),x(4)^2-x(4),x(5)^2-  
x(5),x(6)^2-x(6),x(7)^2-x(7);  
//仮定に対応するイデアル  
ideal g=groebner(i,"fglm");  
//そのグレブナー基底
```


高橋 拓也 (楫研究室) 判断推理の多項式モデルによる計算アルゴリズム 2018年2月8日 22 / 30

```
g[1]=x(7)^2+x(7)
g[2]=x(6)+x(7)+1
g[3]=x(5)+1
g[4]=x(4)
g[5]=x(3)
g[6]=x(2)
g[7]=x(1)
```

判断推理の自動証明

次に、

1. 本当のことを言っているのは、1 人が砂場で遊んでいた子であり、1 人は部屋で遊んでいた子である。
2. D は本当のことを言っており、E は間違ったことを言っている。
3. B は逆上がりができ、間違ったことは言っていない。
4. F が逆上がりできるならば、G は逆上がりできない
が「必ず」仮定から導かれるか確認する。

idea

- 与えられた仮定において、ある条件が仮定から導かれる「時がある」か確かめるためには、その条件に対応する多項式に対してイデアル従属判定を行えば良い。
- 与えられた仮定において、ある条件が仮定から「必ず」導かれるか確かめるためには、その条件の「否定」に対応する多項式が与えられた仮定下で零点を持たないことを確かめれば良い。

この場合は、与えられた仮定に対応するイデアルに、結論の否定に対応する多項式を付加させグレブナー基底をとったとき、 $\langle 1 \rangle$ が生成されるかどうか確かめれば良い。

idea

- 「B は逆上がりができる」が必ず導かれる
- $\Leftrightarrow$ 「「B は逆上がりができない」が導かれない」
- $\Leftrightarrow \langle G, x_2 - 1 \rangle = \langle 1 \rangle$
- $\Leftrightarrow x_2 - 1 \notin \langle G \rangle$ ($\langle G \rangle \neq \langle 1 \rangle$ のとき)

判断推理の自動証明

```
list l31=(p1,p2,p3,p4);
list l32=(p1-1,p2-1,p3-1,p4-1);
poly ss1=symm(l31)[1]-1;
poly ssn3=symm(l32)[3]-1;
list l41=(p5,p6,p7);
list l42=(p5-1,p6-1,p7-1);
poly sr1=symm(l41)[1]-1;
poly srn2=symm(l42)[3]-1;
ideal re1=(ss1-1)*(ssn3-1)*(sr1-1)*(srn2-1),g;
//砂場に1人、部屋に1人ずつ本当のことを言っている、の否定
ideal g1=groebner(re1);
g1;
ideal re2=(p4-1)*p5,g;
```

```
//Dは本当のことを言っており、Eは間違ったことを言っている、の否定
ideal g2=groebner(re2);
g2;
ideal re3=x(2)*(p2-1),g;
//Bは逆上がりができ、間違ったことは言っていない、の否定
ideal g3=groebner(re3);
g3;
ideal re4=x(6)-1,x(7)-1,g;
//Fが逆上がりできるならば、Gは逆上がりできない、の否定
ideal g4=groebner(re4);
g4;
```

判断推理の自動証明

```
g1[1]=x(7)^2+x(7)
g1[2]=x(6)+x(7)+1
g1[3]=x(5)+1
g1[4]=x(4)
g1[5]=x(3)
g1[6]=x(2)
g1[7]=x(1)
g2[1]=1
g3[1]=x(7)^2+x(7)
g3[2]=x(6)+x(7)+1
g3[3]=x(5)+1
g3[4]=x(4)
g3[5]=x(3)
g3[6]=x(2)
g3[7]=x(1)
g4[1]=1
```

以上の例は2値論理の範疇で考える事ができ、実は手計算でも比較的容易に解答可能である。

しかし次に示す例は必然的に3値以上の値をとり、手計算で解くためにはかなり頭を使わなければならない。一方与えられた主張がどのくらい正しいか間違っているかは、グレブナー基底計算によりおおよそ把握することができる。

よって計算機を用いて判断推理の問題を解けるという事実は非常に有益であると考えられる。

真偽判定

男 A.B.C.D と女 E.F.G はそれぞれ 0～2 のカードのうち 1 種類を 1 枚ずつ持っている
このうち、0 のカードを持っているのは 2 人だけであることがわかっている。

7 人が以下のように主張した。

A 「B は 1 のカードを持っている」

B 「女のうち 1 人だけ 2 のカードを持っている」

C 「A も B も嘘をついている」

D 「男に 0 のカードを持っている人はいない」

E 「私は 1 のカードを持っていない」

F 「男で 1 のカードを持っている人は 2 人だけいる」

G 「E と F の少なくとも一方は本当のことを言っている」

ただし、本当のことを言っているのはこのうち 2 人のみである。

次のうち、必ず正しい主張はどれか

1 E は 2 のカードを持っている

2 C と D は嘘をついている

3 1 のカードは 3 枚ある

4 G が 1 のカードを持っているならば、D は 2 のカードを持っている

5 A が嘘をついているならば、D は本当のことを言っている

6 2 のカードは 1 枚もない

参考文献

- [1] D.Cox, J.Little and D.Oshea. *Ideals, Varieties and Algorithms*, Springer-Verlag International Switzerland 2015. [CLO1]
- [2] D.Cox, J.Little and D.Oshea. *Using Algebraic Geometry*, Second edition, Springer Science+Business Media, Inc 2005. [CLO2]
- [3] Zhenyu HUANG. *Parametric Equation Solving and Quantifier Elimination in Finite Fields with The Characteristic Set Method*. Springer-Verlag Berlin Heidelberg 2012 [ZH]
- [4] Sicun Gao, Andre Platzer, and Edmund M. Clarke. *Quantifier Elimination over Finite Fields Using Grobner Bases*. pp. 140–157, Springer-Verlag Berlin Heidelberg 2011 [GPC]
- [5] J. CHAZARAIN, A. RISCOS, J. A. ALONSO, E. BRIALES. *Multi-valued Logic and Grobner Bases with Applications to Modal Logic*. University of Nice, Department of Mathematics, Pare Valrose, 06034 Nice, France University of Sevilla, Faculty of Mathematics, 41012 Seoilla, Spain. April 1988 [CRAB]
- [6] 穴井宏和, 横山和弘 QE の計算アルゴリズムとその応用—数式処理による最適化 東京大学出版会 2011. [AY]
- [7] 公務員試験数的処理解法テクニック教室の KOMARO <https://komaro.net/>