

判断推理の多項式モデルによる計算アルゴリズム

数学応用数理専攻 楯研究室所属 5117A032-6 高橋拓也

1 Abstract

与えられた条件を仮定して結論を導くという推理論理の問題は、多値論理の構造を有限体上で多項式表現することにより、イデアル従属判定問題に帰着させることができる。しかしこの事実を具体的な事例に活用した事例はあまり知られていない。そこで我々は有限体上の多項式環の性質を利用し、判断推理の問題を計算機上で解くアルゴリズム的手法を考案した。

2 Basic Fact

2.1 Definition

- $G = \{g_1, \dots, g_s\}$ が $J \subset k[x_1, \dots, x_n]$ のグレブナー基底 $\iff \langle LT(J) \rangle = \langle LT(g_1), \dots, LT(g_s) \rangle$
- 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

2.2 Theorem

- (Elimination Theorem)
 G : J のグレブナー基底のとき、 $G_l = G \cap k[x_{l+1}, \dots, x_n]$ は J_l のグレブナー基底
- (Fermat's Little Theorem)
 $\mathbb{F}_p$ を標数 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。
- (Nullstellensatz in finite field)

$$I(V(J)) = J + \langle x_1^p - x_1, \dots, x_n^p - x_n \rangle \quad (J \subset \mathbb{F}_p[x_1, \dots, x_n])$$

- $J \subset \mathbb{F}_p[\mathbf{x}, \mathbf{y}]$ 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と、以下が成立

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

- T を命題論理式からそれに対応する多項式への写像とすると、

$$\Phi_1, \dots, \Phi_m \models \Psi \iff T(\Psi) - 1 \in \langle T(\Phi_1) - 1, \dots, T(\Phi_m) - 1, x_1^p - x_1, \dots, x_n^p - x_n \rangle$$

3 Idea

- 具体的な判断推理問題は、仮定イデアルと結論イデアルの関係を調べることで解くことができる。
- $\mathbb{F}_2[x_1, \dots, x_n]$ 上で $x_1, \dots, x_n$ は 0, 1 のいずれか一方の値を取るとする。
 $S_i(x_1, \dots, x_n)$ が $x_1, \dots, x_n$ の i 次対称多項式とすると
 $x_1 \sim x_n$ に 1 がちょうど i 個ある $\iff S_i(x_1, \dots, x_n) = 1$ かつ $S_{n-i}(x_1 - 1, \dots, x_n - 1) = 1$

4 Example

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、逆上がりできる子が 2 人いることが分かっている。A ～ G は以下の発言をしたが、本当のことを言っているのは 2 人である。

A : B は逆上がりできるよ。

B : A は間違っただけを言っているよ。

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 の少なくともどっち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次のうちどれか。

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 は間違っただけを言っている。
3. B は逆上がりができ、間違っただけを言っていない。
4. F が逆上がりできるならば、G は逆上がりできない

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。0 のカードを持っているのは 2 人だけであることが分かっている。7 人が以下のように主張したが、本当のことを言っているのは 2 人である。

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」

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, Fourth edition, Springer-Verlag International Switzerland 2015.
- [2] D.Cox, J.Little and D.Oshea. Using Algebraic Geometry, Second edition, Springer Science+Business Media, Inc 2005.
- [3] Sicun Gao, Andre Platzer, and Edmund M. Clarke. Quantifier Elimination over Finite Fields Using Grobner Bases. F. Winkler (Ed.): CAI 2011, LNCS 6742, pp. 140-157, Springer-Verlag Berlin Heidelberg 2011.
- [4] Zhenyu HUANG. Parametric Equation Solving and Quantifier Elimination in Finite Fields with The Characteristic Set Method. The Editorial Office of JSSC Springer-Verlag Berlin Heidelberg 2012.
- [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.
- [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.
- [7] 公務員試験数式的処理法テクニック教室の KOMARO <https://komaro.net/>