アルゴリズム 28－1
（1992．7．17）

命題論理における推論と充足の代数化

山崎　勇
（株）東芝　総合研究所

命題論理における節集合の充足可能性問題を考える。加法が推論に相当する加群（推論加群）を定義すると、陰 Horn 条件を満たす節集合の充足可能性問題は、推論加群の上での一次方程式（証明方程式）に非負の解があるかどうかという可解問題に変換できる [1]。この代数的証明原理と線形不等式論の Farkas の定理 [5] とはその言明がよく似ている。そこで、推論だけでなく割当てと充足をも代数化し、離散的 Farkas の定理と関係をつけることで、代数的証明原理における陰 Horn 条件を必要十分条件である一般 Horn 条件にまで拡大できることを明らかにした。証明方程式は多項式時間で解けるから、この一般 Horn 条件を満たす節集合の充足可能性は多項式時間で解ける。

Algebraization of inference and satisfiability in Propositional Logic

Isamu Yamazaki

Information Systems Laboratory, Toshiba Research and Development Center.

Abstract. By constructing a *deductive module D*, where addition corresponds to a kind of deduction, we can prove that a set of *hidden* Horn clauses S is unsatisfiable if and only if the linear *Proving Equation* derived from S has a nonnegative integral solution. This fact, named 'the Algebraic Proving Principle', is analogous to the Farkas's theorem on linear inequality systems. In order to reveal the relation between them, we have algebraized the *interpretation* and the *satisfiability*, as well as the deduction. Furthermore, using discrete Farkas's theorem, we have derived the weakest condition to S, named 'generalized Horn condition', under which the Algebraic Proving Principle still holds.

1 はじめに

本論文で対象とする問題は、命題論理の節集合 S の「充足可能性問題」である。筆者は推論の代数化によって、この充足可能性問題が、ある条件の下で、推論加群 D における一次方程式（証明方程式）の可解問題に変換できることを示し、これを代数的証明原理と名付けた [1]。d を節の全体から D へのある写像、□を空節とすると、代数的証明原理は次のように述べられる。

「節集合 $S=\{c_i\}_{i\in I}$ が陰 Horn 条件を満足していれば、S が充足不可能であるための必要十分条件は、証明方程式：

$$\sum_{i\in I} d(c_i)\cdot z_i = d(\square)$$

が非負の整数解 z_i を持つことである。」

この結論の形は線形不等式論における Farkas の定理によく似ている。 A を m 行 n 列の行列、u を m 列の行ベクトル、b を m 行の列ベクトル、x を n 行の列ベクトルとすると、Farkas の定理は次のように述べられる [5]。

「$uA\geq 0$ なる全ての u に対して $ub\geq 0$ であるための必要十分条件は、

$$Ax=b$$

が $x\geq 0$ なる解を持つことである。」

そこでこれらの関係を追及し、割当てを代数化した割当加群 U を定義し、Farkas の定理を用いて代数的証明原理を導くことを試みた。その結果、Farkas の定理と本理論との関係が明らかになるとともに、代数的証明原理の成立条件として陰 Horn 条件なる十分条件から、一般 Horn 条件なる必要十分条件に拡大することができた。以下にこれらの結果について述べる。なお次の記号を用いる。

$Z^+\cdots$非負の整数の全体,	$Z\cdots$整数の全体,
$\lambda\cdots$命題記号の個数,	$n\cdots$節集合の節の個数,
$K=\{1,2,\cdots,\lambda\}$,	$I=\{1,2,\cdots,n\}$,
$K_0=\{0\}\cup K$,	$J=\{1,2,\cdots,m\}$,
$\emptyset\cdots$空集合,	$(m\cdots$任意の数$)$.

2 命題論理 L

本論文で対象とする命題論理 L を定義する。λ 個の命題記号 $P_k(k\in K)$ を含む命題論理の節集合 $S=\{c_i\}_{i\in I}$ を考える。$\Gamma=\{P_k\}_{k\in K}$ とし、Γ の命題記号を用いて作られる節集合の全体を C と記す。

Γ から { 真 , 偽 } への写像を割当てと呼ぶ。割当ての全体を W と記す。ある割当て w に従って節 c の各命題記号を真理値で置き換え、さらに否定記号と論理和記号の通常の規則で論理演算した結果が真となるとき、w は c を充足する、あるいは w は c のモデルであるといい、$w\models c$ と記す。w が節集合 S のすべての節を充足するとき w は S を充足する、あるいは w は S のモデルであるといい $w\models S$ と記す。S を充足する割当て $w\in W$ が存在するとき S は充足可能であると言い、そうでないとき S は充足不能であるという。

3 凸錐論理 M

本節では凸錐論理というものを導入する。そのためにまず推論加群と割当加群というものを定義する。

3.1 推論加群 D と割当加群 U

Γ に加えて、基準命題と呼ぶ命題記号 P_0 を考え、これを含めた命題記号の集合を Γ_0 と記す。

命題記号 P_k を固定したとき、$P_k\cdot z\,(z\in Z)$ なる表現の全体：

$$D_k \stackrel{\text{def}}{=} \{P_k\cdot z \mid z\in Z\}$$

は、Z の算法を通して右 Z 加群となる。すなわち、

$$P_k\cdot z_1+P_k\cdot z_2=P_k\cdot(z_1+z_2),$$
$$(P_k\cdot z_1)\cdot z_2=P_k\cdot(z_1\cdot z_2).$$

そこでこれらの $D_0,D_1,D_2,\cdots,D_\lambda$ の直和を D と定義し、推論加群と呼び、その元を文と呼ぶ。

$$D \stackrel{\text{def}}{=} \Big\{\sum_{k\in K_0} P_k\cdot z_k \;\Big|\; P_k\in\Gamma_0, z_k\in Z\Big\}$$

D は整数を要素とする $\lambda+1$ 次元のベクトル空間と同形である。文 d への $z\in Z$ の右作用を $d\cdot z$ と記す。

次に $\lambda+1$ 個の割当記号 Ψ_k なるものを考える。

$$\Delta_0 \stackrel{\text{def}}{=} \{\Psi_k\}_{k\in K_0}$$

この Ψ_k を生成元とする左 Z 加群を考え、これを割当加群 U と定義する。

$$U \stackrel{\text{def}}{=} \Big\{\sum_{k\in K_0} x_k\cdot\Psi_k \;\Big|\; \Psi_k\in\Delta_0, x_k\in Z\Big\}$$

U も整数を要素とする $\lambda+1$ 次元のベクトル空間と同形である。$u\in U$ への $x\in Z$ の左作用を $x\cdot u$ と記す。

次に U の元 u と、D の元 d との『内積』とよぶ、結果が整数になる乗法を、次の様に定義する。

$$\Big(\sum_{k\in K_0} x_k\cdot\Psi_k\Big)*\Big(\sum_{k\in K_0} P_k\cdot z_k\Big) \stackrel{\text{def}}{=} \sum_{k\in K_0} x_k\cdot z_k$$

これは次のように定義したことと同等である。

$$\Psi_k * P_j=\delta_{kj}\quad(\text{クロネッカーのデルタ})$$

3.2 有限錐と双対錐、離散的 Farkas の定理

次にこの D と U に関して、有限錐と双対錐なる概念を定義し、離散的 Farkas の定理を導入する。

まづ B を D の有限部分集合 $\{d_i\}_{i\in I}$ としたとき、B の有限錐 $\langle B\rangle$ とは、B の元の非負一次結合の全体と定める。

$$\langle B\rangle \stackrel{\text{def}}{=} \Big\{\sum_{i\in I} d_i\cdot z_i \;\Big|\; d_i\in B, z_i\in Z^+\Big\}$$

また B の**密有限錐** $\langle\!\langle B \rangle\!\rangle$ とは、その適当な整数倍が B の元の非負一次結合で表されるような D の元の全体と定義する。明らかに $\langle\!\langle B \rangle\!\rangle \supset \langle B \rangle$ である。

$$\langle\!\langle B \rangle\!\rangle \stackrel{\text{def}}{=} \left\{ d \in D \;\middle|\; \exists z \in Z \backslash 0 [\, d \cdot z \in \langle B \rangle \,] \right\}$$

次に B の**双対錐** B^* とは、B の全ての元との内積が非負であるような U の元の全体と定義する。

$$B^* \stackrel{\text{def}}{=} \left\{ u \in U \;\middle|\; \forall d \in B [\, u * d \geq 0 \,] \right\}$$

U の部分集合 X の双対錐 X^* も同様に定義する。

$$X^* \stackrel{\text{def}}{=} \left\{ d \in D \;\middle|\; \forall u \in X [\, u * d \geq 0 \,] \right\}$$

B の双対錐の双対錐を B^{**} と記す。$d \in B^{**}$ ということは、$\forall u \in U [\, u \in B^* \;\Rightarrow\; u * d \geq 0 \,]$ と同等である。

◇補題 1　$B = \{d_i\}_{i \in I}$ とすると $u \in B^*$ ならば、$\langle\!\langle B \rangle\!\rangle$ の任意の元 d に対して $u * d \geq 0$ である。すなわち、$d \in \langle\!\langle B \rangle\!\rangle$ ならば $d \in B^{**}$ である。あるいは、

$$B^{**} \supset \langle\!\langle B \rangle\!\rangle.$$

［証明］　$d \in \langle\!\langle B \rangle\!\rangle$ とする。ある $z > 0$ があって $d \cdot z = \sum_{i \in I} d_i \cdot z_i$ $(z_i \geq 0)$ である。任意の $u \in B^*$ をとると、全ての d_i に対して $u * d_i \geq 0$ であるから $u * (d \cdot z) \geq 0$ である。従って $u * d \geq 0$ でなければならない。■

◇定理 1 (離散的 Farkas の定理)　$B = \{d_i\}_{i \in I} \subset D$ に対して次が成り立つ。

$$B^{**} = \langle\!\langle B \rangle\!\rangle$$

［証明］　補題1の逆、$B^{**} \subset B$、すなわち $d \in B^{**}$ であれば、適当な整数 $z > 0, z_i \geq 0$ によって、

$$d \cdot z = \sum_{i \in I} d_i \cdot z_i$$

が成り立つこと、を証明すれば十分である。以下帰納法を用いる。

（$n = 1$ のとき）　対偶を証明する。すなわち $d \notin \langle\!\langle d_1 \rangle\!\rangle$ ならば、$u * d_1 \geq 0$ かつ $u * d < 0$ なる $u \in U$ が存在すること（$d \notin \{d_1\}^{**}$）を示す。

(1)　$d_1 = 0$ の場合。$d = \sum_{k \in K_0} P_k \cdot z_k \notin \langle\!\langle d_1 \rangle\!\rangle = \{0\}$ に対して、$u = -\sum_{k \in K_0} z_k \cdot \Psi_k$ と選べば、$u * d = -\sum_{k \in K_0} z_k \cdot z_k < 0$、$u * d_1 = 0$ である。

(2)　$d_1 \neq 0$ の場合。$v * d_1 > 0$ となる $v \in U$ が必ず存在する。d は 0 ではあり得ない。その中で特に $v * d \geq 0$ なる $v \in U$ を選ぶ（もしそのような v が存在しないなら，$u * d_1 > 0$ ならば $u * d < 0$ を意味するから直ちに $d \notin \{d_1\}^{**}$ と言える）。そこで、

$$e = d \cdot (v * d_1) - d_1 \cdot (v * d)$$

と置くと、仮定によりあらゆる $z > 0$, $x \geq 0$ に対して $d \cdot z \neq d_1 \cdot x$ であるから、$e \neq 0$。そこで $u' * e > 0$ を満たす u' が存在する。そのような u' を用いて

$$u = (v * (d + d_1)) \cdot u' - (u' * (d + d_1)) \cdot v$$

と置けば、

$$u * d_1 = u' * e > 0, \quad u * d = -u' * e < 0$$

となるから、$d \notin \{d_1\}^{**}$ である。

（$n = n$ のとき）　$n - 1$ では定理が成立するものと仮定する。$C = \{d_1, \cdots, d_{n-1}\}$ とする。任意の $d \in B^{**}$ を考える。

(1)　$d \in C^{**}$ の場合。帰納法の仮定により $d \in \langle\!\langle C \rangle\!\rangle \subset \langle\!\langle B \rangle\!\rangle$ であるから $d \in \langle\!\langle B \rangle\!\rangle$ である。

(2)　$d \in C^{**}$ でない場合。ある $v \in C^*$ が存在して、$v * d < 0$ となる。$d \in B^{**}$ であるから v は B^* の元ではない。これは $v * d_n < 0$ を意味する。ここで、

$$\begin{cases} d' = d \cdot (-v * d_n) + d_n \cdot (v * d) \\ d'_i = d_i \cdot (-v * d_n) + d_n \cdot (v * d_i) \quad (1 \leq i \leq n-1) \end{cases}$$

と置く。任意の $u \in \{d'_1, \cdots, d'_{n-1}\}^*$ に対して、

$$u' = (-v * d_n) \cdot u + (u * d_n) \cdot v$$

とすると、

$$\begin{cases} u' * d_i = u * d'_i \geq 0 \quad (1 \leq i \leq n-1), \\ u' * d_n = 0. \end{cases}$$

であるから $u' \in B^*$ であり、従って $u * d' = u' * d \geq 0$ である。これは $d' \in \{d'_1, \cdots, d'_{n-1}\}^{**}$ を意味する。そこで帰納法の仮定から、適当な整数 $x > 0$、$x_i \geq 0$ $(1 \leq i \leq n-1)$ を用いて、

$$d' \cdot x = \sum_{i=1}^{n-1} d'_i \cdot x_i$$

と表せる。そこで、

$$\begin{cases} z = (-v * d)x \;> 0 \\ z_i = (-v * d)x_i \;\geq 0 \qquad (1 \leq i \leq n-1) \\ z_n = (-v * d)x + \sum_{i=1}^{n-1} (v * d_i)x_i \;\geq 0 \end{cases}$$

と置けば、$d \cdot z = \sum_{i=1}^{n} d_i \cdot z_i$ が成り立つ。■

3.3　凸錐論理 M

以上の準備の下に、凸錐論理 M なるものを定義する。

凸錐論理 M では、物事は D の元の集合 $B = \{d_i\}_{i \in I} \subset D$ で表す。

凸錐論理 M での B からの推論は、B の非負一次結合：

$$\sum_{i \in I} d_i \cdot z_i \quad (z_i \geq 0)$$

とする。また、B を前提とすると d が成り立つ、ということの論証は、d の適当な正の整数倍が B からの推論で導かれ得ること、すなわち、次の一次方程式に非負の整数解があること、を示すことであるとする。

$$\sum_{i \in I} d_i \cdot z_i = d \cdot z \quad (z_i \geq 0, z > 0)$$

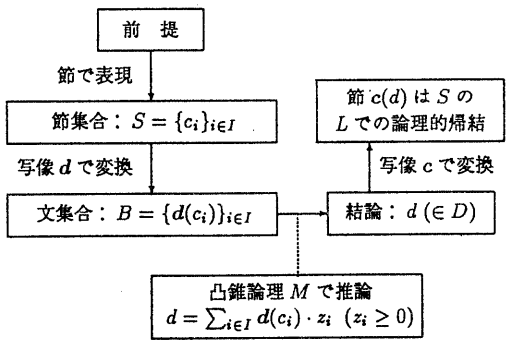

図 1: 命題論理 L の推論に凸錐論理 M の推論法を利用

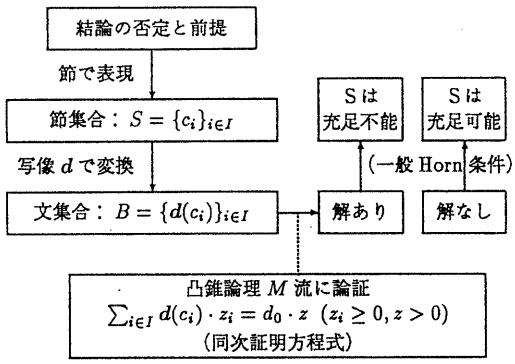

図 2: 命題論理 L の論証に凸錐論理 M の論証法を利用

すると B から推論できる元の全体は $\langle B\rangle$ と一致する。また。B から論証できる元の全体は $\langle\langle B\rangle\rangle$ と一致する。

次に、剰当加群 U と内積とを用いて、凸錐論理 D のセマンティクスを定義する。すなわち「u が d を充足する」あるいは「u は d の U モデルである」とは、u と d との内積が非負であること、と定め、これを $u\models_* d$ と記す。

$$u\models_* d \quad \stackrel{\text{def}}{=} \quad u*d\geq 0 \qquad (u\in U, d\in D)$$

すると、B の U モデルの全体は、B^* と一致する。また B の論理的帰結の全体は、B^{**} と一致する。また離散的 Farkas の定理は、このセマンティクスのもとで、M の推論が健全であること、および M の論証法が完全であることを、意味する。

4　代数的導出原理と代数的証明原理

上述の凸錐論理は、健全かつ完全とは言っても、そのセマンティクスが人工的な物である限り、我々の住む世界との結び付きがなく、実際の問題解決に役立たない。そこで次に凸錐論理を通常の命題論理と結び付けることを考える。

まず命題論理 L の推論に凸錐論理 M の推論を利用することを考えよう。すなわち、まず、前提を命題論理の節集合 S で表現し、S をある写像 d で D の部分集合 B へ変換する。次に B から凸錐論理 M の推論法を用いて推論を行い、ある結論 d を得て、この d をある写像 c で節に変換すると、その結果が、命題論理 L に於ける S からの論理的帰結になっている、と言うように写像 d と c を定めたい。実際、以下に述べる写像でこのようなことが可能である。この事実（健全性）を「代数的導出原理」と名付けた。図 1参照。

また命題論理の論証に凸錐論理の論証法を利用することを考えよう。すなわち、まず、前提と証明したい結論の否定とを節集合 S で表す。これを写像 d で D の部分集合 B に変換する。次に、この B が矛盾を含むことを凸錐論理流に論証する。すなわち、命題論理における矛盾に対応する元を d_0 とし、B が矛盾を含むとは、次の方程式（同次証明方程式）に非負の解があることである、と考えることができるように、写像 d と矛盾 d_0 とを定めたい。

$$\sum_{i\in I} d(c_i)\cdot z_i = d_0\cdot z \quad (z_i\geq 0, z>0)$$

以下に述べる写像によればこのようなことが条件付きで可能である。すなわちこの方程式に解があれば S は充足不可能であることが言える。一方、解がなかったときは、S は充足可能である、と無条件には言えず、言えるためには S が一般 Horn 条件を満たしている必要がある。この事実（条件つき完全性）を「代数的証明原理」と名付けた。図 2参照。

4.1　代数的導出原理

まず健全性について考える。写像 $\boldsymbol{d}: C\to D$ と $\boldsymbol{c}: D\to C$ は次を満たすように定義したい。

$$w\models\{c_i\}_{i\in I} \quad\Rightarrow\quad w\models \boldsymbol{c}\Big(\sum_{i\in I}\boldsymbol{d}(c_i)\cdot\alpha_i\Big) \quad (\alpha_i\in R^+) \tag{1}$$

これを成り立たせるには、凸錐論理の健全性を考慮すれば、ある写像 $\boldsymbol{u}: W\to U$ があって、次の 2 条件が成り立てば十分である。

$$w\models c \quad\Rightarrow\quad \boldsymbol{u}(w)\models_* \boldsymbol{d}(c) \quad (w\in W, c\in C) \tag{2}$$

$$\boldsymbol{u}(w)\models_* d \quad\Rightarrow\quad w\models \boldsymbol{c}(d) \quad (w\in W, d\in D) \tag{3}$$

そこでまず (2) を成立させる写像 $\boldsymbol{d}$ と写像 $\boldsymbol{u}$ を定める。C から D への写像 $\boldsymbol{d}$ は次のように定める。ただしリテラル

L が節 c に含まれることを $L \in c$ と記す。

$$d(c) = \sum_{P_k \in c} P_k + \sum_{(\neg P_k) \in c} (P_0 - P_k) - P_0$$

空節□は変換 d によって $-P_0$ に変換される。これを d_0 と置く。すなわち命題論理 L における「矛盾」は D ではこの d_0 によって表されることになる。

$$d_0 \stackrel{\text{def}}{=} d(\square) = -P_0$$

節集合 S の全ての元に変換 d を施して得られる文の集合を $d(S)$ と記す。

$$d(S) \stackrel{\text{def}}{=} \{d(c) \mid c \in S\}$$

次に命題論理における各命題記号への真偽の割当の全体を W とし、W から U への写像 u を次のように定める。

$$u(w) \stackrel{\text{def}}{=} \Psi_0 + \sum_{k \in K} \nu_k \cdot \Psi_k, \quad \nu_k = \begin{cases} 1 \cdots \text{if} & w \models P_k \\ 0 \cdots \text{if} & w \models \neg P_k \end{cases}$$

w を割当てとすると定義から次が成り立つ。

	if $w \models P_k$	if $w \models \neg P_k$
$u(w) * P_k =$	1	0
$u(w) * (P_0 - P_k) =$	0	1

(4)

これより、$w \models c$ ならば、

$$u(w) * d(c) = \sum_{P_k \in c} u(w) * P_k + \sum_{(\neg P_k) \in c} u(w) * (P_0 - P_k) - 1 \geq 0$$

となる。従って (2) が成り立つ。

次に (3) を成立させる、D から C への写像 c として次のものを考える。ただし□∨□=□とする。

$$d = \textstyle\sum_{k \in K} P_k \cdot z_k + P_0 \cdot z_0 \quad \Rightarrow$$

$$c(d) = \Big(\bigvee_{z_k > 0} P_k\Big) \vee \Big(\bigvee_{z_k < 0} \neg P_k\Big) \vee c'(d)$$

$$c'(d) \stackrel{\text{def}}{=} \begin{cases} \square \cdots\cdots\cdots\cdots \text{if } \beta(d) \leq -1 \\ P_1 \vee \neg P_1 \quad \cdots \text{if } \beta(d) \geq 0 \end{cases}$$

$$\beta(d) \stackrel{\text{def}}{=} \sum_{k \in K, z_k < 0} z_k + z_0$$

この定義に現れた $\beta(d)$ を文 d の底数と称する[1]。節 c に含まれる相補対の個数を n とすると、

$$\beta(d(c)) = n - 1 \tag{5}$$

が成り立つ。また一般に $d = \sum_{k \in K} P_k \cdot z_k + P_0 \cdot z_0$ は、

$$d = \sum_{k \in K, z_k > 0} P_k \cdot z_k + \sum_{k \in K, -z_k > 0} (P_0 - P_k) \cdot (-z_k) + P_0 \cdot \beta(d)$$

と変形できるから、次が成り立つ。

$$u(w) * d = \sum_{k \in K, z_k > 0} u(w) * P_k \cdot z_k + \sum_{k \in K, -z_k > 0} u(w) * (P_0 - P_k) \cdot (-z_k) + \beta(d) \tag{6}$$

ここで $w \not\models c(d)$ とすると、写像 c の定義から $z_k > 0$ なら $w \not\models P_k$ つまり $u(w) * P_k = 0$、$z_k < 0$ なら $w \not\models \neg P_k$ つまり $u(w) * (P_0 - P_k) = 0$ を意味するから、(6) より $u(w) * d = \beta(d)$ を得る。従って $w \in W, d \in D$ とすると次が成り立つ。

$$w \not\models c(d) \quad \Rightarrow \quad u(w) * d = \beta(d) \tag{7}$$

(7) から (3) が成り立つことがいえる。なぜならば、まず $\beta(d) \leq -1$ の場合は、$u(w) \models_* d$ とすると、$u(w) * d \geq 0$ であるから $u(w) * d \neq \beta(d)$ であり、(7) から $w \models c(d)$ となるからである。また $\beta(d) \geq 0$ の場合は、c の定義から $c(d)$ は恒真であるから、全ての $w \in W$ は $w \models c(d)$ を満たすからである。

以上より (1)、すなわち次の定理が成り立つ。

◇定理 2 (代数的導出原理)　節集合 $S = \{c_i\}_{i \in I}$ に対して、$d(c_i)$ の非負一次結合を

$$d = \sum_{i \in I} d(c_i) \cdot \alpha_i \qquad (\alpha_i \in R^+)$$

とすると、節 $c(d)$ は S の論理的帰結である。

ここで後の議論に用いる事実を導いておく。まず (4) と (6) から次は明らかである。

$$u(w) * d \geq \beta(d) \qquad (w \in W, d \in D) \tag{8}$$

また $w \in W, d \in D$ とすると次が成り立つ。

$$\beta(d) \leq -1 \quad \Rightarrow \quad (u(w) * d = \beta(d) \quad \Rightarrow \quad w \not\models c(d)) \tag{r7}$$

なぜならば、$d = \sum_{k \in K} P_k \cdot z_k + P_0 \cdot z_0$ とすると、(6) において、$u(w) * P_k \geq 0$、$u(w) * (P_0 - P_k) \geq 0$ であって、かつこれらに乗ぜられている係数はみな正であるから、$u(w) * d = \beta(d)$ となるとすると、$u(w) * P_k = 0$ $(z_k > 0)$、$u(w) * (P_0 - P_k) = 0$ $(z_k < 0)$ でなければならない。これは $z_k > 0$ なら $w \not\models P_k$、$z_k < 0$ なら $w \not\models \neg P_k$、すなわち $w \not\models c(P_k \cdot z_k)$ を意味する。また $\beta(d) \leq -1$ であるから $c'(d) = \square$ である。よって $w \not\models c(d)$ となるからである。

これらより $w \in W, d \in D$ とすると次が成り立つ。

$$\beta(d) = -1 \quad \Rightarrow \quad (u(w) \not\models_* d \quad \Rightarrow \quad w \not\models c(d)) \tag{r3}$$

なぜなら $u(w) \not\models_* d$ とすると $u(w) * d \leq -1$ である。一方 (8) により $u(w) * d \geq \beta(d) = -1$ であるから、$u(w) * d = -1 = \beta(d)$ とならざるを得ない。従って (r7) から $w \not\models c(d)$

[1] 文の底数とは、[1, 2] の用語でいえば、文の重真度の符号を変えたものである。すなわち $\beta(d) = -m[d]$。

となるからである。

一般に $d(c(d)) = d$ とは限らない[2]。これとは対称的に次の補題が成り立つ。

◇補題 2　節 c が相補対を含まなければ $c(d(c)) = c$ である。

［証明］　$c = (\bigvee_{k\in K_1} P_k) \vee (\bigvee_{k\in K_2} \neg P_k)$ とする。c が相補対を含まなければ、$K_1 \cap K_2 = \emptyset$ である。そこで、

$$\begin{aligned} c(d(c)) &= c\Big(\sum_{k\in K_1} P_k + \sum_{k\in K_2} (P_0 - P_k) - P_0\Big) \\ &= \Big(\bigvee_{k\in K_1} P_k\Big) \vee \Big(\bigvee_{k\in K_2} \neg P_k\Big) \vee \Box \\ &= c \end{aligned}$$ ■

4.2　代数的証明原理

次に完全性について考察する。全ての命題に真を割り当てる割当を w^+ とする。また

$$u^+ \stackrel{\text{def}}{=} u(w^+)$$

とする。

次に割当を写像 u で変換したものの全体を $u(W)$ とする。これは u^+ を含む。

$$u(W) \stackrel{\text{def}}{=} \{u(w) \mid w\in W\}$$

次に P_0 との内積が 1 である U の元の全体を V と定める。V は $u(W)$ を含む。

$$V \stackrel{\text{def}}{=} \{u\in U \mid u * P_0 = 1\}$$

次に P_0 との内積が 1 以上である U の元の全体を Y と定める。Y は V を含む。

$$Y \stackrel{\text{def}}{=} \{u\in U \mid u * P_0 \geq 1\}$$

これは u の表現において Ψ_0 の係数が正であるものの全体に他ならない。

$$Y = \Big\{\sum_{k\in K_0} z_k \cdot \Psi_k \;\Big|\; z_k\in Z,\ z_0 > 0\Big\}$$

さらに、$\{d_0\}^*$ は u の表現において Ψ_0 の係数が 0 または負であるものの全体と一致する。つまりこれは U に関する Y の補集合である。従って

$$Y = U \backslash \{d_0\}^*$$

◇補題 3　写像 $h : V \to u(W)$ であって次の条件を満足するものが存在する。

$$u\in V \;\Rightarrow\; \forall d\in d(C)[\, h(u) * d < 0 \;\Rightarrow\; u * d < 0\,]$$

ただし、$d(C) = \{d(c) \mid c\in C\}$ とする。

[2]例えば $d(c(P_1 \cdot 3 - P_0 \cdot 2)) = d(P_1) = P_1 - P_0 \neq P_1 \cdot 3 - P_0 \cdot 2$

［証明］　まず次の写像 $s : Z \to \{0, 1\}$ を考える。

$$\text{if } z \leq 0 \text{ then } s(z) = 0,\ \text{ if } z \geq 0 \text{ then } s(z) = 1$$

この写像を用いて写像 h を次のように仮定する。

$$h(\sum_{k\in K_0} z_k \cdot \Psi_k) = \sum_{k\in K_0} s(z_k) \cdot \Psi_k$$

この h が定理で言う写像になっていることを示す。$u = \sum_{k\in K_0} z_k \cdot \Psi_k \in V$ とする。まず u の z_0 は 1 であり従って $h(u)$ の Ψ_0 の係数は 1 である。また $h(u)$ の Ψ_k の係数は 0 か 1 である。よって $h(u)\in u(W)$。次に n_k $(k\in K)$ を、

$$n_k = z_k - s(z_k)$$

と置き、u_k を、

$$\begin{aligned} z_k \geq 1 (\Leftrightarrow n_k \geq 0) &\;\Rightarrow\; u_k = h(u) - \Psi_k \in u(W), \\ z_k \leq 0 (\Leftrightarrow n_k < 0) &\;\Rightarrow\; u_k = h(u) + \Psi_k \in u(W). \end{aligned}$$

とすると、

$$\begin{aligned} u - h(u) &= \sum_{k\in K} (z_k - s(z_k)) \cdot \Psi_k \\ &= \sum_{k\in K} |n_k| \cdot (h(u) - u_k) \end{aligned}$$

と変形できる。そこで $d\in d(C)$ とすると、一般に $u'\in u(W)$ ならば，$u' * d \geq \beta(d) = -1$ であるから、$h(u) * d < 0$ ならば $h(u) * d = -1$ であり、また $-1 - u_k * d \leq 0$ である。よってこのとき u と $d\in d(C)$ との内積を考えると、

$$\begin{aligned} u * d &= h(u) * d + \sum_{k\in K} |n_k| \ (h(u) * d - u_k * d) \\ &= -1 + \sum_{k\in K} |n_k| \ (-1 - u_k * d) < 0 \end{aligned}$$ ■

◇補題 4　S を有限節集合、$B = d(S)$ とすると、

$$u(W) \cap B^* = \emptyset \;\Leftrightarrow\; V \cap B^* = \emptyset$$

［証明］　$V \supset u(W)$ であるから、$V \cap B^* = \emptyset$ であれば、$u(W) \cap B^* = \emptyset$ である。反対に $u(W) \cap B^* = \emptyset$ であるとすると、任意の $u\in u(W)$ には $u * d < 0$ となる $d\in B$ が存在する。そこで V の任意の元を u とする。補題3の写像 h によれば $h(u)\in u(W)$ であるから、$h(u) * d < 0$ となる $d\in B$ が存在するが、補題3によればこの d は $u * d < 0$ をも満たす。これは $V \cap B^* = \emptyset$ を意味する。■

◆一般 Horn 条件　D の部分集合 $B = \{d_i\}_{i\in I}$ に関する次の条件を一般 Horn 条件と呼ぶ。

次のような写像 $p : Y \to V$ が存在する。

$$\forall u\in Y[\, u\in B^* \;\Rightarrow\; p(u)\in B^*\,]$$

節集合 S に対して $d(S)$ が一般 Horn 条件を満たすとき、「S は一般 Horn 条件を満たす」と言うことにする。

◇補題 5　節集合 $S=\{c_i\}_{i\in I}$ が一般 Horn 条件を満足するならば、$B=d(S)$ とするとき、

$$Y\cap B^*=\emptyset \quad\Leftrightarrow\quad V\cap B^*=\emptyset$$

［証明］　$V\subset Y$ であるから、$Y\cap B^*=\emptyset$ であれば $V\cap B^*=\emptyset$ である。逆に $Y\cap B^*\neq\emptyset$ とすると $u\in Y\cap B^*$ が存在するが、一般 Horn 条件の写像 $p: Y\to V$ によれば、$p(u)\in B^*$ かつ $p(u)\in V$ であるから $V\cap B^*\neq\emptyset$ である。■

◇定理 3 (代数的証明原理)　節集合 $S=\{c_i\}_{i\in I}$ が一般 Horn 条件を満足するならば、S が充足不可能であるための必要十分条件は、同次一次方程式（同次証明方程式）：

$$\sum_{i\in I} d(c_i)\cdot z_i = d_0\cdot z$$

に非負の解 $z_1\in Z^+,\cdots,z_n\in Z^+, z\in Z^+\backslash 0$ が存在することである。

［証明］　$B=d(S)$ とする。同次証明方程式に非負の解があるとは、

$$\exists z>0[d_0\cdot z\in\langle B\rangle]$$

すなわち $d_0\in\langle\langle B\rangle\rangle$ ということにほかならない。そこで、

S が充足不可能

$\Leftrightarrow$ $\neg(\exists w\in W[\,\forall c\in S[\,w\models c\,]\,])$ (充足の定義)

$\Leftrightarrow$ $\neg(\exists w\in W[\,\forall c\in S[\,u(w)*d(c)\geq 0\,]\,])$ ((3) と (r3))

$\Leftrightarrow$ $u(W)\cap B^*=\emptyset$ (B^* の定義)

$\Leftrightarrow$ $V\cap B^*=\emptyset$ (補題 4)

$\Leftrightarrow$ $Y\cap B^*=\emptyset$ (一般 Horn 条件と補題 5)

$\Leftrightarrow$ $\{d_0\}^*\supset B^*$ ($Y=U\backslash\{d_0\}^*$)

$\Leftrightarrow$ $d_0\in B^{**}$ (双対錐の性質)

$\Leftrightarrow$ $d_0\in\langle\langle B\rangle\rangle$ (離散的 Farkas の定理) ■

なお、証明方程式に解があるならば、S が一般 Horn 条件を満たさなくても充足不能であることが、定理 2から言える。

5　考察

代数的証明原理により、充足可能性の判定問題を、（同次）証明方程式に非負の整数解があるかどうかを問う問題に置き換えられた。それは見かけ上は整数計画法における実行可能解の存在問題の形をしている。しかし同次証明方程式に非負有理数の解があれば必ず非負整数の解があると言える（非負有理数の解に、その分母の公倍数を乗じたものは非負整数の解になる）ので、線形計画法における実行可能解の探索問題と考えてよく、これはよく知られているとおり線形計画問題に変形できる。そしてこれには規模の多項式時間で解く方法が知られている。

一方命題論理における節集合の充足可能性問題は NP 完全である。NP から P へのギャップをどこで飛び越えたのかと言うと、S に一般 Horn 条件を要請したところである。$B=d(S)$ と置けば、補題 5 の証明から、一般 Horn 条件は、

$$Y\cap B^*\neq\emptyset \quad\text{ならば}\quad V\cap B^*\neq\emptyset$$

と同等であるが、$Y\cap B^*\neq\emptyset$ は有理数の実行可能解が存在することに、また $V\cap B^*\neq\emptyset$ は整数の実行可能解が存在することに、正確に対応するのである。

ここで、一般 Horn 条件よりは狭いが、より判定が容易と思われる条件をいくつか定義する。

まず**拡大 Horn 条件**を次の様に定義する。

$$V\cap(-B^*)\neq\emptyset$$

B が拡大 Horn 条件を満たせば、一般 Horn 条件を満たす。なぜならば、$V\cap(-B^*)$ の任意の元を v とすると、$u\in Y\cap B^*$ ならば、$u+(1-u*d_0)\cdot v\in V\cap B^*$ となるからである。

次に**陰 Horn 条件**を、S に含まれる命題記号のうちのあるものの定義をその否定と交換すれば、次に述べる正 Horn 条件を満たすようになる、という条件と定義する。この条件は $B=d(S)$ とおけば、次のように表現できる。

$$u(W)\cap(-B^*)\neq\emptyset$$

B が陰 Horn 条件を満たせば、拡大 Horn 条件を満たす。

正 Horn 条件とは、S の各節が肯定リテラルを高々 1 個しか含まない、という条件である。つまり正 Horn 条件を満たす節集合とは、Horn 節だけからなる節集合である。この条件は次のように表現できる。

$$u^+\cap(-B^*)\neq\emptyset$$

B が正 Horn 条件を満たせば、陰 Horn 条件を満たす。

このように通常の Horn 条件（正 Horn 条件は）一般 Horn 条件の特別な場合に相当している。もともと正 Horn 条件を満たす節集合（Horn 節集合）の充足可能性問題に対しては多項式時間の判定法が知られている [6]。従って代数的証明原理は、多項式時間の判定法の存在領域を一般 Horn 条件にまで拡げられることを示したことに相当する。ただし節集合 S に対する正 Horn 条件は $O(n)$ 時間で、陰 Horn 条件は $O(n^2)$ 時間で判定できる [1] のに対し、整数計画問題の形になる拡大 Horn 条件の判定問題と、一般 Horn 条件の判定問題とは、NP であると予想される [2]。

6　おわりに

命題記号から生成される推論加群 D と割当記号から生成される割当加群 U を定義し、それらの上で密有限錐と双対

錐とを定義して、離散的 Farkas の定理を導入・証明し、これに基づいて凸錐論理 M を定義した。次に通常の命題論理 L の推論と論証に凸錐論理 M の推論法と論証法を流用した結果として、代数的導出原理と代数的証明原理を導いた。この結論はすでに [1, 3] において導出原理の完全性を用いて導かれているが、そこでは代数的証明原理の適用条件は陰 Horn 条件であった。本論文ではそれを上記の方法で一般 Horn 条件にまで拡大するとともに、これらの成立条件を双対錐により統一的に表現し、その意味を NP 問題と関連させて理解する事ができた。

なお、本稿では同次証明方程式を対象とした代数的証明原理を導いたが、[1, 3] では $z = 1$ なる証明方程式を対象とした代数的証明原理を導いていた。しかし同次証明方程式に解があるならば証明方程式に解があるということが証明できる [4]。

また一階述語論理においても本論文の方法に沿った議論が可能である。そしてその結果得られる代数系は非常に有用であって、種々の問題の分析や解決に利用できると思われる。これらに関しては改めて報告したい。

参考文献

[1] 山崎勇：「推論の代数化と代数的証明原理」第 2 回人工知能学会全国大会, 1-3, pp.27-30, 1988.

[2] 山崎勇：「充足可能性問題の代数化－同次証明方程式による判定法」, 第 40 回情報処理全国大会 (I), 7c-7, pp.210-211, 1990.

[3] 山崎勇：「一階述語論理における代数的証明原理」, 人工知能学会誌, Vol.5, No.3, pp.279-290, 1990.

[4] 山崎勇：「証明方程式の線形時間解法アルゴリズム」, 情報処理学会アルゴリズム研究会, AL-28, (本予稿集), 1992.

[5] 岩堀長慶：「線形不等式とその応用」岩波講座基礎数学－代数学 vii , 岩波書店, 1977.

[6] Dowling,W.F., Gallier,J.H. Linear time algorithms for testing the satisfiability of Horn formulae, *J. Logic Prog.* Vol.3, pp.267 -284, 1984.