証明方程式の線形時間解法アルゴリズム

山崎　勇

（株）東芝　総合研究所

命題論理における節集合 S の充足可能性問題は、S が一般 Horn 条件を満たすならば、同次証明方程式に非負の整数解があるかどうかという問題と等価である（代数的証明原理）[1]。一般 Horn 条件とは、S の充足可能性問題と等価な 0, 1 整数計画問題の 0, 1 制約を実数にまで緩和した問題によって充足可能性が判定できる、という条件と考えてよい。ところでこの緩和問題に実数の解があれば区間 $[0,1]$ での解もある、という補題が導ける。従ってこの緩和問題は $[0,1]$ の範囲の解だけを探せばよく、リテラル数に線形の時間で解ける。この解法から、（同次）証明方程式の線形時間解法が導ける。

一方リテラル数の線形時間で充足可能性が判定できる節集合のクラスについて、Chandru らは (hidden) extended Horn sets なるクラスを導いているが [4]、このクラスはさらに拡大できることを示した。

Linear Time Algorithm for solving the Proving Equation

Isamu Yamazaki

Information Systems Laboratory, Toshiba Research and Development Center.

Abstract. Let S denote a set of clauses of propositional logic, and m the total number of literals in S. According to the Algebraic Proving Principle, a generalized Horn set S is unsatisfiable if and only if the linear ***Homogeneous Proving Equation*** derived from S has a nonnegative integral solution. A ***generalized Horn set*** is an S that is satisfiable if there exists an unconstrained real solution to the 0, 1 integer programming problem equivalent to the original satisfiability problem. The author proved the lemma that if this relaxed problem has unconstrained real solution, then it has also $[0,1]$ solution. Hence this relaxed problem is solvable in $O(m)$ time. This leads us to an $O(m)$ time algorithm for solving the (Homogeneous) Proving Equation. It is also shown that there is a super class to the class of (***hidden***) ***extended Horn sets*** given by Chandru and Hooker, whose satisfiability is still solvable in $O(m)$ time.

1 はじめに

組み合わせ問題、計画問題、自動プログラミングなど、命題論理の証明問題、あるいは充足可能性問題に帰着させることができる問題は多数存在する。この充足可能性問題はNP問題として良く知られている。筆者は [1] において一般Horn条件を満たす節集合の充足可能性問題は、同次証明方程式と名付けた斉一次方程式に非負の解があるかどうかと言う問題と等価であるという、代数的証明原理を導いた。

一般Horn条件を満たすという限定された範囲内ではあるが、この代数的証明原理によって、充足可能性問題を一次方程式を解く問題に置き換えることができる。しかし新たに同次証明方程式を能率的に解くアルゴリズムを求めるという課題が生じる。同次証明方程式は線形計画法の実行可能解探索問題となるから、この方法を用いればとりあえず規模の多項式時間で証明方程式を解くことができる。

ところで、解を持つ同次証明方程式を観察すると、その主要部はすでに半分解けた形をしている。すなわちその連立方程式の行列の主要部は、行と列を適当に並べ変えれば、必ず上三角行列に変形できて、しかもその対角要素は1か−1になっている。大雑把に言えば前進消去がほとんど済んでおり、後退代入だけが残されているようなものである。そしてその対角要素を見付ける手順は、Davis と Putnam の1リテラル規則の繰り返しと本質的に等価であって、全体としてリテラル数の線形時間の手順になる。そこで本論文の前半ではその間の事情をより直接的に示すことを目標とする。

鍵となる事実は3つある。第1は、一般Horn条件とは、節集合 S の充足可能性問題と等価な $0,1$ 整数計画問題の $0,1$ 制約を実数にまで緩和した問題によって充足可能性が判定できる、という条件であることである。第2は、この緩和問題に実数の解があれば $[0,1]$ の範囲の解もある、という事実である。第3は、$[0,1]$ の範囲ではこの緩和問題を解く線形時間アルゴリズムが存在するという事実である。このアルゴリズムから証明方程式の線形時間解法アルゴリズムを構成することができる。さらにこのアルゴリズムから、同次証明方程式に解があれば、非同次の証明方程式にも解があることを示すことができる。

そもそもHorn節集合 [3] やこれを拡張したChandru らによる (hidden) extended Horn set [4] は線形時間で充足可能性が判定できることが知られているが、一般Horn条件はそれらを含んだより広い条件になっている。またChandru らの (hidden) extended Horn sets より大きいクラスであって、Chandru らと同様の議論ができる、興味あるクラスが存在することが分かった。本論文の後半ではこれらについて述べる。

2 代数的証明原理

ここでは筆者による代数的証明原理の理論展開を簡単に追ってみよう。命題論理の節集合 $S = \{c_i\}_{i\in I}$ の充足可能性問題を考える。($I = \{1,2,\cdots,n\}$)。S が含む命題記号の集合を $\{P_k\}_{k\in K}$ とする。($K = \{1,2,\cdots,\lambda\}$)。次の言明を考える。

$$S\text{は充足不可能である。} \tag{1}$$

S の節 $c = \bigvee_{j\in J} L_j$ がある割当てで充足されるということは、次のような線形不等式を成り立たせる λ 個の $0,1$ 変数 $\{u_k\}_{k\in K}$ が存在するということと同等である。ただし節 c がリテラル L を含むということを $L\in c$ と記す。

$$\sum_{P_k\in c} u_k + \sum_{(\neg P_k)\in c} (1-u_k) - 1 \geq 0 \tag{2}$$

上式の左辺の u_k の係数を k の昇順に並べてできる列ベクトルを $a(c)$ と、定数項を $r(c)$ と記す。そして

$$\begin{aligned}
\text{行ベクトル}\quad & r \stackrel{\text{def}}{=} (r(c_1),\cdots,r(c_n))\text{、}\\
\text{行列}\quad & A \stackrel{\text{def}}{=} (a(c_1),\cdots,a(c_n))\text{、}\\
\text{行ベクトル}\quad & v = (u_1,\cdots,u_\lambda)\text{、および}\\
\text{行ベクトル}\quad & e = (1,1,\cdots,1)
\end{aligned}$$

を考える。すると (1) は、線形不等式 (2) を節の個数だけ集めた連立不等式系に対する次の言明と同等である。

$$(1,v)\begin{pmatrix} r, & 0, & e \\ A, & E, & -E \end{pmatrix} \geq 0\text{に整数解がない} \tag{3}$$

ただし E は単位行列とする。ここで、

$$\begin{aligned}
V &\stackrel{\text{def}}{=} \{(1,u_1,u_2,\cdots,u_\lambda) \mid u_k\in Z\}\\
W &\stackrel{\text{def}}{=} \{(1,u_1,u_2,\cdots,u_\lambda) \mid u_k\in \{0,1\}\}
\end{aligned}$$

と置くと、写像 r と a の性質に起因して、次の補題が成り立つ [1]。ただし C を $\{P_k\}_{k\in K}$ からできる節の全体とする。

◇補題 1　写像 $h: V \to W$ であって次の条件を満足するものが存在する。

$$\forall u\in V\Big[\forall c\in C\Big[u\begin{pmatrix} r(c)\\ a(c)\end{pmatrix} \geq 0 \;\Rightarrow\; h(u)\begin{pmatrix} r(c)\\ a(c)\end{pmatrix} \geq 0\Big]\Big]$$

この補題から (3) における $0,1$ 条件は不要であるので、(3) は次と同等である。

$$(1,v)\begin{pmatrix} r\\ A\end{pmatrix} \geq 0 \quad\text{に整数解がない} \tag{4}$$

ここで

$$\left\{\begin{array}{l} (u_0,v)\begin{pmatrix} r\\ A\end{pmatrix} \geq 0 \\ u_0 \geq 1 \end{array}\right\}\text{に整数解がない} \tag{5}$$

なる言明を考え、『(4) ならば (5) である』という A に対する条件を一般Horn条件と称し、H_G と記す。すると、

当然の事ながら一般 Horn 条件のもとで (4) は (5) と同等である。そして (5) は次と同等である。

$$\left\{\begin{array}{l}(u_0, \boldsymbol{v})\begin{pmatrix}\boldsymbol{r}\\ A\end{pmatrix} \geq 0\\ u_0 > 0\end{array}\right\} \text{に有理数解がない} \tag{6}$$

なぜなら (5) で整数解があれば明らかにその解は (6) でも解である。逆に (6) で有理数解があれば、その有理数解の分母の最小公倍数を乗じれば (5) の整数解が得られるからである。

さらに (6) は次と同等である。

$$\left\{\begin{array}{l}(u_0, \boldsymbol{v})\begin{pmatrix}\boldsymbol{r}\\ A\end{pmatrix} \geq 0 \quad \text{となる全ての有理数}\\ \text{ベクトルは} \quad (u_0, \boldsymbol{v})\begin{pmatrix}-1\\ 0\end{pmatrix} \geq 0 \quad \text{を満たす}\end{array}\right\} \tag{7}$$

線形不等式論における Farkas の定理は任意の順序体に対して成り立つ [2] から、有理数体に対しても成り立つ。そこで有理数体に対する Farkas の定理から、(7) は次と同等である。ただし $\boldsymbol{x}$ を列ベクトルとする。

$$\left\{\begin{array}{l}\begin{pmatrix}\boldsymbol{r}\\ A\end{pmatrix}\boldsymbol{x} = \begin{pmatrix}-1\\ 0\end{pmatrix}\\ \boldsymbol{x} \geq 0\end{array}\right\} \text{は有理数解を持つ} \tag{8}$$

(8) に有理数解があればその各有理数の分母の最小公倍数を乗ずれば次の解を得るから、(8) は次と同等である。ただし $\boldsymbol{z}$ を列ベクトルとする。

$$\left\{\begin{array}{l}\begin{pmatrix}\boldsymbol{r}\\ A\end{pmatrix}\boldsymbol{z} = \begin{pmatrix}-1\\ 0\end{pmatrix}z_0\\ \boldsymbol{z} \geq 0, \quad z_0 \geq 1\end{array}\right\} \text{は整数解を持つ} \tag{9}$$

以上から S が一般 Horn 条件 H_G を満たすならば、(1) と (9) とが同等であることが示された。以上が代数的証明原理の理論展開の概要である。(9) における方程式系を同次証明方程式と称する。

なお筆者は [1] において、一般 Horn 条件 H_G を補題 1 の言い方に倣って次のように定義しているが、どちらも等価である。ただし次のように置く。

$$Y \stackrel{\text{def}}{=} \{(u_0, u_1, u_2, \cdots, u_\lambda) \mid u_0 \geq 1,\ u_i \in Z\}$$

一般 Horn 条件: 写像 $p : Y \to V$ であって次の条件を満足するものが存在する。

$$\forall \boldsymbol{u} \in Y\left[\boldsymbol{u}\begin{pmatrix}\boldsymbol{r}\\ A\end{pmatrix} \geq 0 \ \Rightarrow\ p(\boldsymbol{u})\begin{pmatrix}\boldsymbol{r}\\ A\end{pmatrix} \geq 0\right]$$

さらに H_G より狭い次の条件を定義している。

条件 H_V (拡大 Horn 条件) :

$$\exists \boldsymbol{u} \in V\left[\boldsymbol{u}\begin{pmatrix}-\boldsymbol{r}\\ -A\end{pmatrix} \geq 0\right]$$

条件 H_W (陰 Horn 条件) :

$$\exists \boldsymbol{u} \in W\left[\boldsymbol{u}\begin{pmatrix}-\boldsymbol{r}\\ -A\end{pmatrix} \geq 0\right]$$

条件 H (Horn 条件) :

$$(1, 1, \cdots, 1)\begin{pmatrix}-\boldsymbol{r}\\ -A\end{pmatrix} \geq 0$$

$(1, 1, \cdots, 1) \in W \subset V$ であるから、上記の条件は後者ほど強い条件である。すなわち一般に条件 J を満たす節集合のクラスを $S(J)$ と記すことにすると、

$$S(H_G) \supset S(H_V) \supset S(H_W) \supset S(H)$$

である[1]。(右側は左側の真部分集合)

なお、以上の議論を [1] における表記法に翻訳するには次のような対応を行えばよい。

推論加群 D は $\lambda+1$ 次元整数列ベクトル空間と同形であり、D の生成元 P_k は整数列ベクトル空間の基底に対応する。

$$P_k = (\underbrace{0, 0, \cdots, 0}_{k}, 1, \underbrace{0, \cdots, 0}_{\lambda-k})^T$$

割当加群 U は $\lambda+1$ 次元整数行ベクトル空間と同形であり、U の生成元 Ψ_k は整数行ベクトル空間の基底に対応する。

$$\Psi_k = (\underbrace{0, 0, \cdots, 0}_{k}, 1, \underbrace{0, \cdots, 0}_{\lambda-k})$$

$d(c) \in D$ は次の $\lambda+1$ 次元列ベクトルに対応する。

$$\boldsymbol{d}(c) = \begin{pmatrix}r(c)\\ \boldsymbol{a}(c)\end{pmatrix}$$

内積 $u * d$ $(u \in U,\ d \in D)$ はベクトルの内積 $\boldsymbol{ud}$ に対応する。

$$u * d = \boldsymbol{ud}$$

そこで $d_0 = -P_0 \in D$ とすると同次証明方程式 (9) は [1] の表記法では

$$\sum_{i \in I} d(c_i) \cdot z_i = d_0 \cdot z_0, \quad z_i \geq 0, z_0 > 0$$

となる。また $a_{0i} = r(c_i)$、$a_{ki} = \boldsymbol{a}(c_i)$ の第 k 要素、と置くと (9) は次のようにも書ける。

$$\left\{\begin{array}{l}\sum_{i \in I} a_{0i} z_i = z_0 > 0\\ \sum_{i \in I} a_{ki} z_i = 0 \quad (k \in K)\end{array}\right. \quad z_i \geq 0 \tag{10}$$

(9) または (10) において $z_0 = 1$ とした方程式を証明方程式と称する。

$$\left\{\begin{array}{l}\sum_{i \in I} a_{0i} z_i = 1\\ \sum_{i \in I} a_{ki} z_i = 0 \quad (k \in K)\end{array}\right. \quad z_i \geq 0 \tag{11}$$

[1] 最初の包含関係 $S(H_G) \supset S(H_V)$ については [1] 参照のこと。

3 証明方程式の解法アルゴリズム

この節では、証明方程式 (11) の解法アルゴリズムを示し、それを用いて、(10) に解があれば (11) に解があることを示す。

3.1 $0 \le u_k \le 1$ での (4) の解法

まず連立不等式系 (4) から整数条件を外し、$0 \le u_k \le 1$ $(k \neq 0)$ なる条件を追加した問題を考える[2]。この問題に対しては次のアルゴリズム a によって、リテラル数の線形時間で解 u_k を求めることができる。(4) の不等式の集合を N_1 とする。また単項の不等式とは、

$$u_k - 1 \ge 0 \quad \text{、または} \quad u_k \le 0$$

の形の不等式とする。

（アルゴリズム a）

(a0) $j := 1$ とする。

(a1) N_j が単項の不等式を含む限り次を行う。

(a1-1) N_j の単項の不等式を 1 個選び、それが $u_{k_1} - 1 \ge 0$ ならば $u_{k_1} := 1$ と、$u_{k_1} \le 0$ ならば $u_{k_1} := 0$ と置く。この値を N_j の全ての不等式に代入したものを N とする。その結果満足し得ない不等式が N にあれば不能として終了する。そうでなければ、残された変数 u_k が $0 \le u_k \le 1$ である限りは満足されることが明らかな不等式を N から除く。$N_{j+1} := N$、$j := j+1$ とする。

(a2) N_j が空なら得られた解を解として終了する。空でなければ N_j は単項の不等式を含まないので、全ての値の決まっていない変数 u_k を $\frac{1}{2}$ と置き、それまでに得られた解を合わせて解として終了する。

このアルゴリズムが正しく働くことは次の 2 個の事実による。

(1) ステップ (a1-1) において、N_j が

$$\sum_{k \in K_1} u_k + \sum_{k \in K_2} (1 - u_k) - 1 \ge 0 \qquad (2')$$

の形の不等式だけからなるならば、N_{j+1} も (2′) の形をした不等式だけからなる。なぜならば、(2′) の形の不等式に $u_{k_1} = 1$ または $u_{k_1} = 0$ を代入すると、生じ得る場合は次の 3 通りしかないからである。

(A) $k_1 \notin K_1 \cup K_2$。この場合は (2′) 式は不変である。

(B) $k_1 \in K_1$ かつ $u_{k_1} = 0$、または $k_1 \in K_2$ かつ $u_{k_1} = 1$。この場合は代入の結果 (2′) 式はやはり (2′) 式の形である。

(C) $k_1 \in K_1$ かつ $u_{k_1} = 1$、または $k_1 \in K_2$ かつ $u_{k_1} = 0$。この場合は (2′) 式は残りの u_k によらずに満たされることが確定するから、N_{j+1} には含まれない。

なお (B) の場合でもとの式が単項の不等式であれば、不能な不等式となるから、アルゴリズムは不能として終了する。

(2) 上記の (B) の場合に変数 (u_k) を 1 個しか含まない不等式が得られたならば、それは (2′) 式の形なのだから単項の不等式である。従ってステップ (a2) へ進んだならば、変数を 1 個しか含まない不等式は削除されており、ステップ (a2) の決定によって残された不等式は全て満たされる。

このアルゴリズムは、適当なデータ構造を仮定すれば、各リテラルが高々定数回だけ処理の対象となるようにできるから、時間計算量はリテラル数に線形である。

3.2 $u_k \in R$ での (4) の解法

次に連立不等式系 (4) の整数条件を外したものを考える。これは $k \neq 0$ ならば u_k はあらゆる実数値を許すということであるが、次の補題 2 によって、$0 \le u_k \le 1$ に制限して解を探しても良いことが保証される。従ってアルゴリズム a は連立不等式系 (4) の整数条件を外したものに対する解法にもなっている。

V と W において整数条件を外したものをそれぞれ V_R と W_R と記すことにする。

$$V_R \stackrel{\text{def}}{=} \{(1, u_1, u_2, \cdots, u_\lambda) \mid u_k \in \boldsymbol{R}\}$$
$$W_R \stackrel{\text{def}}{=} \{(1, u_1, u_2, \cdots, u_\lambda) \mid u_k \in \boldsymbol{R},\ 0 \le u_k \le 1\}$$

◇補題 2 写像 $h : V_R \to W_R$ であって次の条件を満足するものが存在する。

$$\forall u \in V_R \Big[\forall c \in C \big[ud(c) \ge 0 \ \Rightarrow\ h(u)d(c) \ge 0 \big] \Big]$$

［証明］ 次を満たす写像 h を具体的に示す。

$$\forall u \in V_R \Big[\forall c \in C \big[h(u)d(c) < 0 \ \Rightarrow\ ud(c) < 0 \big] \Big]$$

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

$$s(x) \stackrel{\text{def}}{=} \begin{cases} 0 \cdots \text{if } x \le 0, \\ x \cdots \text{if } 0 \le x \le 1, \\ 1 \cdots \text{if } 1 \le x. \end{cases}$$

さらに写像 $h : V_R \to W_R$ を次のように仮定する。

$$h((1, u_1, u_2, \cdots, u_\lambda)) = (1, s(u_1), s(u_2), \cdots, s(u_\lambda)) \ \in W_R$$

[2] これは連立不等式系 (3) の整数条件を外したものと同等である。

この h が補題で言う写像になっていることを示す。$u \in V_R$ とする。y_k $(k \in K)$ を、

$$y_k = u_k - s(u_k)$$

と置き、$w_k \in W_R$ を、

$$\begin{cases} u_k < 0 \quad (\Leftrightarrow y_k < 0) \ \Rightarrow \ w_k = h(u) + \Psi_k, \\ 0 \leq u_k \leq 1 \quad (\Leftrightarrow y_k = 0) \ \Rightarrow \ w_k = h(u), \\ 1 < u_k \quad (\Leftrightarrow y_k > 0) \ \Rightarrow \ w_k = h(u) - \Psi_k. \end{cases}$$

とすると、

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

と変形できる。いまある節 c が相補対を n (≥ 0) 対含むとすると、

$$d(c) = \sum_{k \in K_1} P_k + \sum_{k \in K_2} (P_0 - P_k) + P_0 \cdot n - P_0$$

となるから、

$$h(u)d(c) = \sum_{k \in K_1} s(u_k) + \sum_{k \in K_2} (1 - s(u_k)) + n - 1$$

である。そこで $h(u)d(c) < 0$ であるとすると、次が成り立っているはずである。

$$\begin{cases} n = 0, \\ k \in K_1 \ \Rightarrow \ s(u_k) < 1 \ \Rightarrow \ u_k < 1, \\ k \in K_2 \ \Rightarrow \ 0 < s(u_k) \ \Rightarrow \ 0 < u_k. \end{cases}$$

そこで、いずれにしても

$$(h(u) - w_k)d(c) \leq 0$$

となるから次が成り立つ。

$$ud(c) - h(u)d(c) = \sum_{k \in K} |y_k| \ ((h(u) - w_k)d(c)) \leq 0.$$

従って $h(u)d(c) < 0$ ならば $ud(c) < 0$ である。■

一般 Horn 条件 H_G とは、(4) が整数条件を外した解を持てば整数条件を満たす解を持つ、という条件であるから、この条件を満たす節集合の充足可能性はもともとアルゴリズム a によってリテラルの線形時間で判定できることが分った。またアルゴリズム a の主要部 (a1-1) は Davis-Putnam の1リテラル規則 [6] と本質的に同じものであり、従って条件 H_G とは、1リテラル規則を適用できる限り適用するだけで充足可能性が判定できる[3]ための十分条件になっている。さらにこれは必要条件でもある。なぜなら、S が充足可能ならば H_G を満たす[4]。そこで S が充足不能であって H_G を満たさなかったとすると、不等式系 (4) は W での解はないが W_R での解はある[5]ということになり、1リテラル規則を適用できる限り適用するだけの方法＝アルゴリズム a では充足可能と判定してしまう。従ってそのようにならないために一般 Horn 条件 H_G は必要である。

[3] 途中で単リテラル節がなくなったら充足可能と判定して良い、という意味。

[4] (4) が偽なら、「(4) ならば (5)」は自動的に真だから。

[5] もし W_R での解がないとすると V_R での解がなく、(5) は真となって「(4) ならば (5)」は真となり、H_G が満たされてしまう。

3.3 証明方程式の解法

次にこのアルゴリズム a から証明方程式の解法アルゴリズムを構成することを考える。ここでアルゴリズム a の各時点で、不等式系 N に対応する証明方程式を $Q(N)$ とする。すなわち、N が $uB \geq 0$ のとき $Q(N)$ は $Bz = -P_0$ である。

証明方程式 $Q(N_1)$ に解があるなら元の節集合は充足不能であるから、N_1 にアルゴリズム a を適用するとステップ (a2) に進むことはない。つまりステップ (a1) において、不能が判明するまで N_j には単項の不等式が1個以上存在するという状況が続くはずである。これは $Q(N_j)$ には、第0行を除くと1個の式（第 k_1 行）にしか出現しない未知数 z_{i_1} が存在することを意味する。このときアルゴリズム a では N_j 中の単項の不等式を満たすように変数 u_{k_1} を決めてそれを他の不等式に代入して規模の小さい不等式系 N_{j+1} を得る。これは証明方程式 $Q(N_j)$ の第 k_1 行を用いて未知数 z_{i_1} を（第0行から）消去する過程に正確に対応する。次にこのことを示す。

（X）アルゴリズム a で単項の不等式が $u_{k_1} - 1 \geq 0$ の形であるとき。$u_{k_1} = 1$ となる。証明方程式 $Q(N_j)$ は第0行と第 k_1 行だけが未知数 z_{i_1} を含む。未知数 z_{i_1} の係数は第 k_1 行では1、第0行では -1 である。従って第 k_1 行を用いて第0行から未知数 z_{i_1} を消去するとは、第 k_1 行を第0行に加えることである。$Q(N_k)$ の第0行は不等式系 N_j では各不等式の定数項に相当するから、この消去は u_{k_1} に1を代入することと等価である。

（Y）アルゴリズム a で単項の不等式が $u_k \leq 0$ の形であるとき。$u_{k_1} = 0$ となる。証明方程式 $Q(N_j)$ は第 k_1 行だけが未知数 z_{i_1} を含む。従って他の式から z_{i_1} を消去する必要はない。従って単に第 k_1 行を除くだけである。これは u_{k_1} に0を代入することと等価である。

またアルゴリズム a では成立することが確定した不等式（第 i 不等式）を除くが、これに対応して上記の未知数消去を行った方程式系で、さらに未知数 z_i を0と置けば、その結果得られる方程式系は $Q(N_{j+1})$ と一致する。これは前記 (C) の場合であるから、その様な未知数 z_i とは第 k_1 式において z_{i_1} と同じ（符号の）係数をもつ z_i である。

以上によって、次のような証明方程式の解法アルゴリズムを得る。$|I|$ を I の要素数、$|K|$ を K の要素数とする。

(アルゴリズムb)

(b0) Q_1 を証明方程式(11)、$K_1 := K, I_1 := I, j := 1$ とする。

(b1) (前進消去) $|K_j| = 0$ となるまで次を繰り返す。

(b1-1) Q_j において、$a_{0i_2} = 1, a_{ki_2} = 0(k \in K_j)$ なる i_2 (矛盾列) が存在するならば、$z_{i_2} = 1$、$z_i = 0(i \in I_j \backslash i_2)$ として(b3)へ進む。存在しないならば、$a_{k_1 i_1} = 1$, $a_{ki_1} = 0$ $(k \in K_j \backslash k_1)$ なる (k_1, i_1) (孤立点) を探す。それが存在しなければ、不能として終了する。存在すれば、第 k_1 行を z_{i_1} について解いたもの:

$$z_{i_1} = -a_{k_1 i_1} \sum_{i \in I_j \backslash i_1} a_{k_1 i} z_i \qquad \text{(a)}$$

を第0行へ代入して z_{i_1} を消去する。また、

$$I' \stackrel{\text{def}}{=} \{i \in I_j \backslash i_1 \mid a_{k_1 i} = a_{k_1 i_1}\}$$

に含まれる i に対して、

$$z_i := 0, \qquad (i \in I') \qquad \text{(b)}$$

と置いて、(b) を k_1 以外の行へ代入する。その結果の方程式系を Q_{j+1}、$K_{j+1} := K_j \backslash k_1$、$I_{j+1} := I_j \backslash I'$、$j := j+1$ とする。

(b2) いまや $|K_j| = 0$ である。$a_{0i} = 1$ となっている i を探す。そのような i が存在しなければ、不能として終了する。存在すれば、その i を i_1 とし、$z_{i_1} = 1, z_i = 0$ $(i \neq i_1)$ として(b3)へ進む。

(b3) (後退代入) ステップ(b1)での各(a)式を j の降順に計算して z_i の値を決める。

なお(a)式において $a_{k_1 i_1}^2 = 1$ なる事実を利用している。またここでは不能とは証明方程式が不能という意味である(充足不能という意味ではない)。またこのアルゴリズムが解 z_i を出力したとき、それが確かに非負であることは、(a)式において負の係数を持つ未知数 z_i $(i \in I_j \backslash i_1)$ は(b)式によって0とされていることによって保証される。

このアルゴリズムの終了までに各式の各項は高々2回だけ操作の対象となる(前進消去と後退代入)。また矛盾列や孤立点の探索、並びにある命題記号を含む節の探索の時間については、適当なデータ構造を用意する[6]ことで一定とすることができる。従って総合的にはこのアルゴリズムはリテラル数(=項数)の線形時間で終了する。

[6] 例えば矛盾列への pointer list と、孤立点への pointer list と、各命題記号ごとにそれを含む式への pointer list を用意する。

同次証明方程式(10)に解があれば、不等式系(4)は整数条件を外しても解を持たないから、アルゴリズムbによって(11)の解が得られることが分かった。ここで notation を[1]に合わせると、結局次の定理が成り立つ。

◇定理 1 $d_0 = -P_0$ とし、$\{c_i\}_{i \in I}$ を節集合とする。同次証明方程式:

$$\sum_{i \in I} d(c_i) \cdot z_i = d_0 \cdot z_0, \quad z_i \in Z^+ \ (i \in I), \quad z_0 > 0 \quad (12)$$

に解 z_i, z_0 が有ることと、証明方程式:

$$\sum_{i \in I} d(c_i) \cdot z_i = d_0, \quad z_i \in Z^+ \ (i \in I) \qquad (13)$$

に解 z_i があることとは同等である。

4 Chandru の理論

Chandru らは、充足可能性がリテラル数の線形時間で判定できる節集合のクラスについて (hidden) extended Horn sets なるものを導いている。この理論との比較を行うため、本節では Chandru らの理論の概要を述べる。

Chandru らの理論は、(3) までは第2節と同じである。そのあと Chandru らは次の定理を利用する。ただし $\lfloor x \rfloor$ は x を越えない最大の整数であり、$v = (u_1, u_2, \cdots, u_\lambda)$ としたとき $\lfloor v \rfloor \stackrel{\text{def}}{=} (\lfloor u_1 \rfloor, \lfloor u_2 \rfloor, \cdots, \lfloor u_\lambda \rfloor)$ とする。

◇定理 2 (Chandrasekaran) A' を整数行列、c' を行ベクトルとすると、線形不等式系:

$$vA' + c' \geq 0$$

は、次の条件を満たす行列 T が存在するならば、実数解 v を持つとき整数解 $\lfloor vT^{-1} \rfloor T$ を持つ[5]。

(1) T と T^{-1} はともに整数行列。

(2') TA' の各列は正の要素を高々1個だけ持ち、それは必ず1である。

(3)の整数解の存否を線形計画法で判定するためにこの定理を利用することを考える。行列 A' として $(A, E, -E)$ と取ることによって、T に対する条件は次のようになる。

(1) T と T^{-1} はともに整数行列。

(2) TA の各列は正の要素を高々1個だけ持ち、それは必ず1である。

(3) T の各列は, 高々1個の1と高々1個の -1 を持ち、それ以外は皆0である。

このような行列 T が存在するという A に対する条件を(これは結局 S にたいする条件である)、条件 H_E と記すこと

にする[7]。S が条件 H_E を満たせば線形計画法を用いて S の充足可能性が判定できる。

条件 (1),(3) によって、行列 T はある有向木の結合行列[8]から根点の行を取り除いたものと解釈できる。そして、A の各列、すなわち $a(c_i)$ を、有向木の各辺の流量を表すと考えると、縦ベクトル $Ta(c_i)$ はその流れに伴う各点での吸い込み量を与える。そこで条件 (2) は、流れ $a(c_i)$ に伴う吸い込み点が、根点を除けば高々 1 個であることを意味する。$a(c_i)$ の要素は 1 か -1 であるから、流量の絶対値が各辺とも 1 である。これは流れというより有向路の集まりである。そこで、条件 H_E を節集合 S に対する言葉で表現すれば、『その辺が命題記号に対応する有向木が存在して、各節とも、節をその木の上の有向路の集まりに対応させると、根点以外の点を終点とする有向路は高々 1 個しか存在しない』という条件となる。ただし合流点は一方の有向路の終点と見る。有向木が star である場合には、(陰) Horn 節集合に対する条件となる。

このあと Chandru らは、この条件を満たす節集合の充足可能性は単位導出のみを用いてリテラル数の線形時間で判定できることを示している。

5 各種 Horn 条件の比較

ここでは充足可能性がリテラル数の線形時間で判定できる節集合のクラスに関して前節までに得られた結果を比較し、さらに中間に位置する新たなクラスを提示する。

まず H_E より H_G のほうが適用範囲が広いこと、すなわち H_G を満たす節集合の全体 $S(H_G)$ は H_E を満たす節集合の全体 $S(H_E)$ を含むことを示す。

A が条件 H_E を満たすならば、次のような写像 $p : Y \to V$ を構成できる。

$$p((u_0, v)) = (1, \lfloor \frac{v}{u_0} T^{-1} \rfloor T)$$

すると、

$$(u_0, v)\begin{pmatrix} r \\ A \end{pmatrix} \geq 0 \quad \text{すなわち} \quad \frac{v}{u_0}A + r \geq 0$$

であれば、Chandrasekaran の定理から

$$\lfloor \frac{v}{u_0} T^{-1} \rfloor TA + r \geq 0 \quad \text{すなわち} \quad p((u_0, v))\begin{pmatrix} r \\ A \end{pmatrix} \geq 0$$

となるから、この写像によって一般 Horn 条件が満たされる。すなわち H_E を満たせば H_G を満たす。

ところでこの議論を行うには、T が条件 (3) を満たしている必要はない。そこで条件 (1),(2) を満たす T が存在す

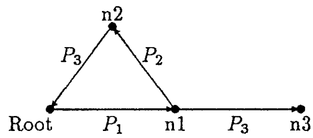

図 1:

ると言う条件を H_F と記すことにする[9]。条件 H_F を満たせば一般 Horn 条件 H_G を満たすからアルゴリズム a によって、リテラル数の線形時間で充足可能性が判定できる。

H_F は H_E よりも真に広い条件である。すなわち H_F を満たすが H_E を満たさない節集合が存在する。次にこれを示す。次のような T を考える。

$$T = \begin{pmatrix} 1 & -1 & -1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \quad T^{-1} = \begin{pmatrix} 1 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

この T は (3) を満たさない。このとき A_1 として、

$$A_1 = \begin{pmatrix} 1 & -1 & -1 & -1 & 1 & -1 \\ 1 & -1 & 1 & -1 & 0 & 0 \\ 1 & -1 & 1 & 1 & 1 & -1 \end{pmatrix}$$
$$\qquad \underbrace{\qquad\quad}_{\alpha}\underbrace{\qquad\quad}_{\beta}\underbrace{\qquad\quad}_{\gamma}$$

を考えると、

$$TA_1 = \begin{pmatrix} -1 & 1 & -3 & -1 & 0 & 0 \\ 0 & 0 & 0 & -2 & -1 & 1 \\ 1 & -1 & 1 & 1 & 1 & -1 \end{pmatrix}$$

となるから (2) を満たしている。この A_1 に対しては (3) を満たす T は存在しない。つまり対応する有向木が存在しない。なぜなら、A_1 の α 部分から対応する有向木は枝別れの無い形、つまり 1 本道の形しか許されない。また A_1 の β 部分から、辺 3 辺 2 辺 1 根または辺 1 辺 2 辺 3 根のいずれかしか許されない。ところが A_1 の γ 部分から、どちらの有向木も (2) を満たせない。

一般に条件 (1),(2) だけを満たす T は、複数の辺に対応する命題記号と閉路とを許す有向連結グラフに対応させることができる。実際上例の T に対応するグラフは図 1のように閉路を含み、命題記号 P_3 は 2 個の辺に対応している。このグラフの上で A の各列に対応する節を、流れ、あるいは道として描いてみると、いずれも根点以外の終点が高々 1 個の道になるが、これは条件 (2) から当然である。このように H_F は H_E の拡張になっている。

次に条件 H_G を満たすが条件 H_F を満たさない節集合が存在することを示す。次で表される節集合を考える。

$$A_2 = \begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

---

[7] 条件 H_E を満たす節集合を Chandru らは (hidden) extended Horn set と呼んでいる。

[8] 行が点、列が辺に対応し、有向木の点 i が辺 j の出発点なら i, j 要素は -1、到着点なら 1、他は 0 なる行列。

[9] これは Chandru の理論の出発点を、(3) ではなく、補題 1を用いた後の (4) としたことにに相当する。

$$r_2 = (-1,1,1,1)$$

これは充足可能である。実際 $v_1 = (1,1,1)$ とすれば、

$$v_1 A_2 + r_2 = (2,0,0,0) \geq 0$$

である。そこで Y の全ての元を $(1, v_1) \in V$ へ写像する写像を p とすれば、条件 H_G が満たされる。しかしながら、条件 (2) を満たす行列 T は存在しない。かりにそれが存在して

$$T = \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix}$$

であったとする。条件 (2) を

$$\exists j \in J\,[\,TA_2 \leq A'_j\,]$$

の形に書くと、A'_j として可能性があるのは全部で $3^4 = 81$ 通りであるが、A_2 の対称性と、T の行の交換で一致するものは 1 度だけ考慮すれば良いことから、結局次の 3 個だけを考慮すれば良い。

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{pmatrix}$$

特に整数 a, b, c を考えると、条件 (1) からそのうち少なくとも 1 個は非 0 であって、条件 (2) から次のいずれかの case を満たさなければならない。

case 1 と case 2	case 3
$a+b+c \leq 0$	$a+b+c \leq 0$
$a-b-c \leq 0$	$a-b-c \leq 0$
$-a+b-c \leq 0$	$-a+b-c \leq 0$
$-a-b+c \leq 0$	$-a-b+c \leq 1$

しかしそれはどの case でも不可能である。結局 A_2 は条件 H_F を満たさない。

以上より、リテラルの線形時間で充足可能性が判定できる節集合のクラスに関して、次のことが分かった（いずれも右側は左側の真部分集合）。

$$S(H_G) \supset S(H_F) \supset S(H_E)\ (\supset S(H_W) \supset S(H)\,)$$

5.1 各条件判定の計算量

節集合 S が $S(H_G)$ に属するかどうかの判定の計算量は、P≠NP である限りは NP である。なぜなら $S(H_G)$ に属さないことが分かれば直ちに充足不能であると判定できるし、属すことが分かればリテラルの線形時間で充足可能性が判定できるから、$S(H_G)$ の所属判定問題が P 問題ならば充足可能性問題は P 問題となってしまうからである。

$S(H_E)$ と $S(H_F)$ の場合には、その所属判定法で多項式時間のものは知られていない。具体的に T が指定されれば、条件 (2) を満たすかどうかは線形時間で判定できることは明らかである。$S(H_W)$ への所属判定は 2 充足問題に変換することで P 問題となる。$S(H_V)$ の場合もその所属判定法で多項式時間のものは知られていない。

6 おわりに

代数的証明原理における証明方程式をリテラル数の線形時間で解くアルゴリズムを導いた。一般 Horn 条件を満たす節集合の充足可能性判定問題はリテラル数の線形時間で解ける。一般 Horn 条件を満たす節集合のクラス $S(H_G)$ は、充足可能性がリテラル数の線形時間で判定できる節集合のクラスとしてこれまでに知られているもののうち、Horn 節集合のクラス $S(H)$[3] と (hidden) extended Horn sets $S(H_E)$[4] とを含んでいる。また $S(H_G)$ と $S(H_E)$ の中間に、興味あるクラス $S(H_F)$ が存在することも分った。

一般 Horn 条件の判定問題は NP 問題であるので、一般 Horn 条件よりは狭いが、多項式時間で判定できる条件を探すことが現実的な課題である。例えば条件 H_E や H_F の判定問題の計算量は現在未解決であるが、もし多項式時間であればその条件は価値がある。また $S(H_G)$ より広いクラスであってその所属判定の計算量とその中での充足可能性判定の計算量とがほぼ同等の多項式時間である、というクラスが存在してはいけないという理由はない。そこでそのようなクラスが存在するかどうかということも興味ある問題である。

参考文献

[1] 山崎勇：「命題論理における推論と充足の代数化」，情報処理学会アルゴリズム研究会, AL-28（本予稿集），1992.

[2] 岩掘長慶：「線形不等式とその応用」岩波講座基礎数学ー代数学 vii，岩波書店, 1977.

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

[4] Chandru,V.,Hooker,J.N. : Extended Horn Sets in Propositional Logic, *J. ACM*, Vol.38, No.1, pp.205-221, 1991.

[5] Chandrasekaran,R. : Integer programming problems for which a simple rounding type of algorithm works. In W. R. Pulleyblank, ed. *Progress in Combinatorial Optimization.* Academic Press Canada, Toronto, Ontario, Canada. pp.101-106, 1984.

[6] Davis,M.,Putnam,H. : A Computing Procedure for Quantification Theory, *J. ACM*, Vol. 7, No. 3, pp.201-215, 1960.