高階論理型プログラム言語NUの解釈系

1992

笹田 耕一

高階論理型プログラム言語NUの解釈系

1992

池田靖雄

目次

1 序

ν - 定義可能行為[5] (ν -definable act 以下ν 行為ν act) はプログラムの数学的表現である。ν 行為を用いて、プログラムを表現する事によりプログラムの性質の検証を形式的に厳密に行う事が出来る[11]。他の論理的手段、例えば時制論理[10] (Temporal logic) ではプログラムからトランスというプログラムのコントロールの流れを示すものをつくり、それからプログラムの流れを表す公理を作って、その他時制論理記号 (temporal operator) に関する推論規則と通常の論理の推論を用いて証明を行う。一方、ν 行為を用いる場合では一度ν 行為でプログラムを表現してしまえば後は通常の論理的手段でその形式的扱いが行われる。また、ν 行為への変換はトランスを作る事と比べるとより簡単であると思われる。また、時制論理では並行プロセスは決して同時 (concurrent) には実行されない、つまりインターリーブ (interleave) の仮定がある。ν 行為を用いた証明ではこの仮定がない。更にν 行為を用いれば時間を明示的に扱うことが可能である。[17]

ν 行為の解釈は形式的に定義されているが、この解釈を検証などの目的のため計算機で行うことを考える。この目的のために作成されたのが、高階論理型プログラム言語NU[18]である。本研究の目的は、このプログラム言語NUの解釈系[6], [7], [8]を設計することである。ν 行為によるプログラムの表現は、仕様の一種としてもとらえることが出来る。よって、NUの解釈系の研究は仕様をそのまま動かそうとする研究という視点でとらえることもできる。このような研究には論理プログラミングや、制約解消の研究がある。しかし、これらの研究では仕様そのものではなく、なんらかの形で手続きを与えていたり、表現に大きな制限があり通常の論理式とは大きく異なる表現しか許されない。例えば、Prologでは本当の意味での $\neg$ を扱っていず、存在記号も扱っていない。これに対してν 行為はこれまでの論理プログラムの表現などと比べてより自然で、より仕様に近い表現となっている。

従来のNU解釈系の研究では、次節で定義する制限を満たすような範囲のν 行為に対して解釈を行うものが製作されている。本研究では束縛変数に対する制限をある程度緩和出来たので、その新しいアルゴリズムについて述べる。

またこの課程で、スコーレムがPresburger算術[12]の決定性を示す際に導入した理論[15]、すなわち有理数上で $+, -, 1/N, =, <, Z$ 及び、有理定数からなる数学理論も決定可能であることが分かった。スコーレム自身はPresburger算術の決定性を示しただけで、この理論自体の決定性については触れていなっかたのであるが、決定性のためにはどのような公理が必要であるか明らかにし、同時に理論自体の決定性の証明を行った[4]。

またこのことから項が一次である式は決定可能である事が解り、一次の式が決定可能と言うことからこの理論を有理Presburger算術[3]と名付けた。また、そのようなν 行為に対し解釈系は強正当性を満たす。

高階の量記号について、量記号消去が行なえる形をいくつか見いだし、これを解釈系に応用した。

2　ν 行為、プログラム言語 NU と従来の NU 解釈系

2.1　ν 行為とプログラム言語 NU

この節では ν 行為とその解釈の定義及びプログラム言語 NU について述べる。

述語論理を基にする理論 T の言語 L(T) の論理式（以下単に式という）$A[\underline{x}]$（下線は変数の並びを表す）の自由変数の出現を少なくとも一つ、質変数と呼ばれる $\nu\underline{x}$ という表現で置き換えたもの $A[\nu\underline{x},\underline{x}]$ を ν 行為と呼ぶ。T の変数への、T のモデル M 上の現在の値の割当 (assignment)σ ，ν 行為 $A[\nu\underline{x},\underline{x}]$ に対して、$\sigma(\underline{x})$ の表す値の列の名前 (name) の列を $\underline{a}$ で表すとき、

1. $M \models \exists\underline{y}A[\underline{y},\underline{a}]$ の場合
   $A[\nu\underline{x},\underline{x}]$ は行動可能といい $\underline{x}$ の次の値として $A[\underline{b},\underline{a}]$ なる $\underline{b}$ を非決定的に選ぶ。
2. $M \not\models \exists\underline{y}A[\underline{y},\underline{a}]$ の場合
   $A[\nu\underline{x},\underline{x}]$ は行動不能といい次の値は未定義となる。

プログラム言語 NU では型論理を基底の論理とし自然数論の保存的拡張となっている数学理論 FA[16]の上の ν 行為を表現できるようになっている。NU の型の定義のうち基本的な部分を述べる。

定義 2.1　　型

1. 0 は型である。
2. $\tau_1,\ldots,\tau_n(1 \leq n)$ が型であるとき、$[\tau_1,\ldots,\tau_n]$ も型である。

直観的には、型 0 の対象は有理数を表し、型 $[\tau_1,\ldots,\tau_n]$ の対象は型 τ_1 の対象 $,\ldots,$ 型 τ_n の対象の n 組を元とするような集合、また見方を変えれば型 τ_1 の対象 $,\ldots,$ 型 τ_n の対象の n 項関係を表す。各型には十分な数の変数の集合があると仮定する。また式および項の定義として、関数記号 $+,-,\times,/$, 述語記号 $=,<$,（整数であることを示す）Z からなる通常の一階の有理数論の定義に加えて、以下の部分がある。また、項を型 0 のアブストラクトともいう。

定義 2.2　　式、算術的な式、アブストラクト

1. $\alpha,\alpha_1,\ldots,\alpha_n$ がそれぞれ型 $[\tau_1,\ldots,\tau_n],\tau_1,\ldots,\tau_n$ の変数であるとき、$\alpha(\alpha_1,\ldots,\alpha_n)$ は式である。
2. $A[\alpha]$ が式であり、α,φ が型 τ の変数であるとき、$\exists\varphi A[\varphi],\forall\varphi A[\varphi]$ も式である。
3. 式 A が高階の量記号を含まないとき A は算術的であるという。
4. $A[\alpha_1,\ldots,\alpha_n]$ が算術的な式であり、$\alpha_1,\ldots,\alpha_n$ がそれぞれ型 $\tau_1,\ldots,\tau_n$ の変数であり、$\varphi_1,\ldots,\varphi_n$ がそれぞれ型 $\tau_1,\ldots,\tau_n$ の変数であるとき、$\{\varphi_1,\ldots,\varphi_n\}A[\varphi_1,\ldots,\varphi_n]$ を型 $[\tau_1,\ldots,\tau_n]$ のアブストラクトという。
5. α が型 $[\tau_1,\ldots,\tau_n]$ の変数であり、$V_1,\ldots,V_n$ がそれぞれ型 $\tau_1,\ldots,\tau_n$ のアブストラクトであるとき、$\alpha(V_1,\ldots,V_n)$ は素論理式である。

アブストラクト $\{\varphi_1,\ldots,\varphi_n\}A[\varphi_1,\ldots,\varphi_n]$ は直観的には集合 $\{\langle\varphi_1,\ldots,\varphi_n\rangle \mid$

$A[\varphi_1,\ldots,\varphi_n]\}$ を表している。また、素論理式

$$\alpha(V_1,\ldots,V_n)$$

は α を集合ととらえれば、直観的には

$$\langle V_1,\ldots,V_n\rangle \in \alpha$$

を表している。さらに省略形として次のものを追加する。

定義 2.3　省略形

$\alpha(V_1,\ldots,V_n)$ が式で、V_n が型 τ のアブストラクトであるとき、$\alpha(V_1,\ldots,V_{n-1})$ は型 τ のアブストラクトである。ただし、このとき α が一意性、つまり

$$\forall\varphi_1\ldots\varphi_{n-1}\psi\omega(\alpha(\varphi_1,\ldots,\varphi_{n-1},\psi)\wedge\alpha(\varphi_1,\ldots,\varphi_{n-1}\omega)\supset\forall\underline{x}(\psi(\underline{x})\equiv\omega(\underline{x})))$$

を満たしているとする。ただし ψ,ω の型が 0 であるとき $\forall\underline{x}(\psi(\underline{x})\equiv\omega(\underline{x}))$ の部分は $\psi=\omega$ とする。

2.2　従来の NU 解釈系

従来の NU 解釈系が解釈を行っていた範囲の ν 行為である解釈可能な ν 行為の定義及び、この定義に必要な定値可能項、範囲指定式、解釈可能な項の定義を述べる。これらは相互定義になっている。

定義 2.4 定値可能項、範囲指定式、解釈可能な項、解釈可能な ν 行為

1. 有理定数、変数（質変数以外）は定値可能項である。
2. s,t がそれぞれ定値可能項であるとき、$s+t, s-t, s\times t, s/t$ はそれぞれ定値可能項である。
3. 定値可能項は解釈可能な項である。
4. 型 0 の質変数 νx は解釈可能な項である。
5. g,h が解釈可能な項であるとき、$g+h, g-h$ は解釈可能な項である。
6. g が解釈可能な項であり、s が定値可能項であるとき、$s\times g, g\times s, g/s$ はそれぞれ解釈可能な項である。
7. g,h が解釈可能な項であるとき、$Z(g), g=h, g<h, g\leq h$ はそれぞれ解釈可能な ν 行為である。
8. νp が型 $[0,\ldots,0]$（0 が n 個並んだ型）の質変数であり、$g_1,\ldots,g_n$ が解釈可能な項であるとき、$\nu p(g_1,\ldots,g_n)$ は解釈可能な ν 行為である。
9. A,B がそれぞれ解釈可能な ν 行為であるとき、$\neg A, A\supset B, A\equiv B, A\vee B, A\wedge B$ はそれぞれ解釈可能な ν 行為である。
10. x が型 0 の束縛変数であるとき、次の三つの形の素論理式それぞれ少なくとも一つずつと、解釈可能な ν 行為との論理積を x の範囲指定式と呼ぶ。
    (a) $Z(x)$
    (b) $s<x$ または、$s\leq x$

(c) $x < s$ または、$x \leq s$

ここで、s は x が現れない定値可能項である。

11. x が型 0 の束縛変数であり、$s_1, \ldots, s_n$ $(1 \leq n)$ が x の現れない定値可能項であるとき、$x = s_1 \vee \cdots \vee x = s_n$ と解釈可能な ν 行為との論理積は x の範囲指定式である。
12. A が x の範囲指定式であり、B が解釈可能な ν 行為であるとき、$\exists x(A \wedge B), \forall x(A \supset B)$ は解釈可能な ν 行為である。

解釈系は、この解釈可能な ν 行為で自由変数が全て現在の割当を持っているものの解釈を行う。

以上が厳密な定義であるが、本質的には以下のような範囲となる。

1. 型 0 の質変数は一次で現れる。
2. 高階の質変数の型は $[0, \ldots, 0]$ という 0 が並んだものに限る。
3. 束縛変数は本質的に整数値をとり、以下の例で示されるように外側からそのとるべき値の上界、下界が定まるものに限る。

例

$$\begin{aligned}
&\forall x(Z(x) \wedge a < x < b \supset \\
&\quad \exists y(Z(y) \wedge s[x] < y < t[x] \wedge \\
&\quad A[x, y, \nu \underline{\mathrm{w}}]))
\end{aligned}$$

ここで、a, b は定数、s, t は項である。

本研究ではこれらの制限のうち三番目の制限を緩和することを目指した。つまり、

1. 型 0 の束縛変数の整数値、上界、下界の制限をなくす。
2. ある範囲で高階の束縛変数を扱えるようにする。

また、解釈系は $A[\nu \underline{\mathrm{x}}]$ という ν 行為が与えられたとき、$\exists \underline{\mathrm{y}} A[\underline{\mathrm{y}}]$ という論理式を証明する、一種の証明系として設計された。ただし、$\exists x B[x]$ は本来は何か存在することが示せれば真であるが、解釈系として実行するため B を満たすようなものが具体的に得られるとき真とすることにする。

3 有理 Presburger 算術の決定アルゴリズムの NU 解釈系への応用

3.1 有理 Presburger 算術とその決定アルゴリズム

解釈系のうちもっとも基本的な部分は型0の対象つまり有理数を扱う部分である。つまり、高階の変数が出現しない場合の処理が最も基礎となる。このとき、質変数や、束縛変数が一次で現れる場合は完全に扱える、つまり必ず停止して、新しい割当を返すか行動不可能であることを知らせることが可能であると考えられる。（参考文献[9]はこの範囲の不等式を解くものであるが、完全には扱えていない）このことから、証明系を考えたときに完全に扱える範囲(class)として考え出されたのが有理 Presburger 算術である。

Presburger 算術[1], [12], [13], [14], [19]は整数上で、$+, <, =$, 及び定数 $0, 1$ からなる数学理論である。そして例えば $x+x+x$ の略記法として $3x$ という表現もある。この理論の論理式は決定可能であることが知られている。

この理論を変数と係数のとる値を有理数上に拡張し、等号、不等号に加えて述語 Z も扱うようにし、これらと有理定数からなる理論、有理 Presburger 算術も項が一次であれば以下に示すように決定可能である。

言語を有理 Presburger 算術の、項が一次の式だけからなる様にし、その意味が通常の和と積の意味となるようにした形式理論[4]の公理系を以下に述べる。

3.2 公理系

3.2.1 言語

定数 $0, 1$

関数 2項関数 $+$

1項関数 $\frac{1}{n}$　　全ての自然数 n に対して。

述語 2引数の述語記号 $=, <$

1引数の述語記号 Z

意味論的には $\frac{1}{n}$ は n で割る関数であり、Z は整数であることを表す述語である。

略記法

$$\underbrace{x+x+\cdots+x}_{n}=nx$$

$$\underbrace{\frac{1}{n}x+\cdots+\frac{1}{n}x}_{m}=m\frac{1}{n}x=\frac{m}{n}x$$

$$\underbrace{1+\cdots+1}_{n}=n$$

$$\underbrace{\frac{1}{n}1+\cdots+\frac{1}{n}1}_{m}=m\frac{1}{n}1=\frac{m}{n}$$

これから明らかに

$$mx+nx=(m+n)x$$

$$\frac{l}{m}x + \frac{n}{m}x = \frac{l+n}{m}x$$

ここで $(m+n), l+n$ は通常の整数の和である。以上のことから項は直観的には有理定数係数の線形項である。また、

$$x \leq y \equiv x < y \vee x = y$$

とする。

3.2.2 公理

- 等号の公理
- 不等号の公理

反対称律

$$x < y \supset \neg(y < x) \tag{O1}$$

推移律

$$x < y \wedge y < z \supset x < z \tag{O2}$$

全順序

$$x < y \vee x = y \vee y < x \tag{O3}$$

- $+$ に関する公理（アーベル群）

結合則

$$x + (y + z) = (x + y) + z \tag{A1}$$

交換律

$$x + y = y + x \tag{A2}$$

単位元

$$x + 0 = x \tag{A3}$$

逆元の存在

$$\forall x \exists y . x + y = 0 \tag{A4}$$

(A4) で定義される加法の逆元はただ一つ存在し、任意の元 x に対してこの逆元を $-x$ と表す。減法は以下で定義される。

$$x - y = x + (-y).$$

これによって、

$$(-n)x = -(nx), (-\frac{n}{m})x = \frac{-n}{m}x = -(\frac{n}{m}x)$$

とする。また、

$$0x = \frac{0}{m}x = 0$$

とする。

- 0 と 1 に関する公理

$$0 < 1$$

- $+$ と不等号に関する公理 (preservation of order)

$$x < y \supset x + z < y + z \qquad (PO)$$

- $\frac{1}{n}$ に関する公理

$$n\frac{1}{n}x = x \qquad (DA)$$

（無限個公理がある）

- Z に関する公理

$$Z(0) \tag{Z1}$$

$$Z(x) \equiv Z(x+1) \tag{Z2}$$

- 整数の部分群の公理

$$Z(x) \wedge Z(y) \supset Z(x-y). \tag{Z3}$$

- 整数の間隔

$$\forall x \exists y (Z(y) \wedge y \leq x < y+1). \tag{Z4}$$

-

$$\forall x (0 < x < 1 \supset \neg Z(x)). \tag{Z5}$$

（0 と 1 の間には整数が存在しない）

3.2.3 公理に関する考察

以上で述べた公理のうち、Z に関する五つの公理の独立性を考える。

(Z3) の独立性 領域を $\{a\omega + b \mid a, b \in \mathcal{Q}\}$ とし、$Z(a\omega + b)$ が真となるのは

- $0 \leq a$ のとき $b \in \mathcal{Z}$
- $a < 0$ のとき $b + \frac{1}{2} \in \mathcal{Z}$

のときかつこのときに限るとする。

このモデルが (Z3) を満たさず、他の公理を満たすのは明らか。

(Z4) の独立性 領域を $\{a\omega + b \mid a, b \in \mathcal{Q}\}$ とし $Z(a\omega + b)$ を $a = 0$ かつ b が整数とする。このモデルは (Z4) を満たさず、他の公理を全て満たす。

(Z5) の独立性 領域は変えずに（有理数のまま）Z の解釈を $Z(a)$ となるのは $2a$ が整数のとき、かつこのときに限るとする。これは (Z5) を満たさず、他の公理を全て満たす。

以上のように (Z3),(Z4),(Z5) の三つの公理は他の公理と独立である。

しかし (Z1),(Z2) の二つの公理は以下のように他の公理から導かれる。

(Z1) の証明

(Z4) より整数が存在することが導ける。よって、ある整数を a とすれば、(Z3) より $Z(a-a) \equiv Z(0)$

□

(Z2) の証明

$Z(1)$ とすれば (Z3) より (Z2) を導くことが出来る。よって、背理法により $Z(1)$ を導く。

$\neg Z(1)$ を仮定する。(Z4) より、$Z(y) \wedge y \leq 2 < y+1$ なる y が存在する。(Z5)、$\neg Z(1)$、(Z4) より $1 < y$ である。さらに $\frac{1}{2}(1+y)$ を考える。$1 < \frac{1}{2}(1+y) < y$ であるのは他の公理から導ける。（3.4節を参

照)

再び (Z4) により $Z(y') \wedge y' \leq \frac{1}{2}(1+y) < y'+1$ なる y' が存在する。そして $0 < y - y' < 1$ であり (Z3) より $Z(y-y')$ となるので、(Z5) と矛盾する。□

次に、形式的帰納法をつけ加えた公理系について少し考えてみる。

帰納法

$$A[0] \wedge \forall x(Z(x) \wedge 0 \leq x \wedge A[x] \supset A[x+1]) \supset \forall x(Z(x) \wedge 0 \leq x \supset A[x])$$

帰納法を公理につけ加える代わりに、他の公理を取り除けないか考える。

(Z2) が無い場合 帰納法が有ってもモデルとして領域は変えずに、Z の解釈を $Z(a)$ となるのは $a = 0$ のときに限るようにする。このモデルでは (Z2) 以外の公理は全て真になる。

(Z4) が無い場合 モデルとして帰納法があっても前記のモデル $\{a\omega + b \mid a, b \in \mathcal{Q}\}$ がとれる。つまり、ある有理数が存在してそれが全てのどの整数よりも大きいことになる。このとき、(Z4) ほど強くない条件 ((Z4) から導かれる条件)

$$\forall x \exists y(Z(y) \wedge x < y) \tag{1}$$

を加えれば標準的なモデルしか作れなくなる。

よって、前節で述べた公理系から (Z3) と (Z4) を除き、代わりに (1) をつけ加えた公理系を考える。この公理系を $\mathcal{S}$ とする。

以下で、$\mathcal{S}$ で (Z3) と (Z4) が導かれる事を示す。

まず、$\mathcal{S}$ における二つの補題を先に証明する。

補題 3.1

$$\forall y(Z(x) \wedge 0 \leq y \wedge Z(y) \supset Z(x-y))$$

証明

y に関する帰納法による。

1. 明らかに $Z(x) \supset Z(x-0)$
2. $Z(x) \wedge Z(y) \supset Z(x-y)$ を仮定する。また、$Z(x), Z(y+1)$ を仮定すると $Z(x-y) \equiv Z(x-y-1) \equiv Z(x-(y+1))$ である。

よって結論を得る。□

同様に次の補題を得る。

補題 3.2

$$Z(x) \wedge 0 \leq x \wedge Z(y) \supset Z(x+y)$$

上記二つの補題より、(Z3) を導く。

定理 3.1

$$\mathcal{S} \vdash Z(x) \wedge Z(y) \wedge Z(x-y)$$

証明

補題 3.1より

$$Z(x) \wedge y < 0 \wedge Z(y) \supset Z(x-y)$$

を導けば良い。

$Z(x), y < 0, Z(y)$ を仮定する。

$y < 0$ より $0 < -y$ であり、条件1より $0 < -y < N_0$ なる整数が存在する。$Z(N_0), 0 < N_0, Z(y)$ と補題 3.2より $Z(N_0 + y)$。同様に $Z(N_0 + x)$。$0 < N_0 + y$ と補題 3.1より $Z((N_0 + x) - (N_0 + y))$ であるから、結論を得る。□

公理 (Z4) も $\mathcal{S}$ において導ける。

定理 3.2

$$\mathcal{S} \vdash \forall x \exists y (Z(y) \wedge y \leq x < y + 1)$$

証明

x が 0 以上の場合と負の場合との場合分け。

- $0 \leq x$ の場合背理法による。

$$\neg \forall x (0 \leq x \supset \exists y (Z(y) \wedge y \leq x < y + 1))$$

を仮定する。

$$\begin{aligned}
&\neg \forall x (0 \leq x \supset \exists y (Z(y) \wedge y \leq x < y + 1)) \\
&\equiv \exists x (0 \leq x \wedge \forall y (\neg Z(y) \vee \neg (y \leq x \wedge x < y + 1))) \\
&\equiv \exists x (0 \leq x \wedge \forall y (\neg Z(y) \vee \neg y \leq x \vee \neg x < y + 1)) \\
&\equiv \exists x (0 \leq x \wedge \forall y (Z(y) \wedge y \leq x \supset y + 1 \leq x))
\end{aligned}$$

ここで存在するものを q とすれば

$$0 \leq q \wedge \forall y (Z(y) \wedge y \leq q \supset y + 1 \leq q) \tag{2}$$

である。形式的帰納法によって、

$$\forall y (Z(y) \wedge 0 \leq y \supset y \leq q)$$

また $0 \leq q$ なので明らかに

$$\forall y (Z(y) \wedge y < 0 \supset y \leq q)$$

よって、

$$\forall y(Z(y) \supset y \leq q)$$

しかしこれは (1) と矛盾。よって、

$$\forall x(0 \leq x \supset \exists y(Z(y) \wedge y \leq x < y+1))$$

- $x < 0$ の場合

このとき $0 < -x$。よって上の結果より

$$\exists y(Z(y) \wedge y \leq -x < y+1)$$

また (Z3) より $Z(x) \equiv Z(-x)$ は容易に導ける。

$$\begin{aligned}
&\exists y(Z(-y) \wedge -y \leq -x \wedge -x-1 < -y) \\
&\quad\equiv\ \exists y(Z(-y) \wedge y-1 < x \leq y) \\
&\quad\equiv\ \exists y(Z(y) \wedge y' < x < y'+1 \vee x = y'+1) \qquad \text{公理 (Z2) より} \\
&\quad\equiv\ \exists y(Z(y) \wedge y < x < y+1) \vee \exists y(Z(y) \wedge x = y) \\
&\quad\equiv\ \exists y(Z(y) \wedge y \leq x < y+1)
\end{aligned}$$

よって $x < 0$ の場合も $\exists y(Z(y) \wedge y \leq x < y+1)$ である。

□

公理系 $\mathcal{S}$ の公理の数は少し減る。しかし、帰納法はとても強い条件であるから現在の形の公理系を採用する。

3.3 決定アルゴリズム

前節で述べた理論が決定可能であることの証明の概略は以下である。

新しい量記号 υ を導入し、$\upsilon_s^t uA[u]$ で項 s,t 間に整数 u がただ一つ存在し、それが $A[u]$ を満たすことを表すとする。これを存在記号で表現すれば $\exists u(Z(u) \wedge s < u < t \wedge t-1 \leq u \leq s+1 \wedge A[u])$ となる。この新しい量記号 υ はその否定がこれと同値な肯定の形が常に存在するという性質を持っている。有理 Presburger 算術の任意の式はこれと同値な、以下で定義される閉じた拡大 υ 式に変換できる。そしてこの閉じた拡大 υ 式が決定可能であるのは明らかである。

定義 3.1 基本 υ 式、拡大 υ 節、拡大 υ 式

1. $\top, \bot$ は基本 υ 式である。
2. $A[u]$ が基本 υ 式及び不等式から $\wedge$ を用いて作られる論理式であるとき $\upsilon_s^t uA[u]$ も基本 υ 式である。
3. 基本 υ 式、Z の式、$\neg Z$ の式、等式及び不等式から $\wedge$ を用いて作られる論理式を拡大 υ 節と呼ぶ。
4. 拡大 υ 節の論理和を拡大 υ 式と呼ぶ。

本節では決定アルゴリズムのうち、与えられた式と同値な拡大 υ 式を求めるアルゴリズムを述べる。手続き S は与えられた式を簡単化し、手続き M は

この簡単化された式を他のいくつかの手続きを用いて拡大 v 式に同値変形する。

手続き S 式の簡単化を行なう

S-1 移行などを行って、同類項をまとめる。すなわち各素論理式中の変数の出現をまとめて、次のような形にする。

$$t < a, t = a, Z(t + a)$$

ここで t は係数 × 変数の形の和でこの和の中には一つの変数は一度しか出現しないとする。また、a は定数項である。

例

$2x + 2y - x - 3 = y + 1$ を

$x + y = 4$ とする。

S-2 変数の出現しない素論理式はその真偽が定まるので、それらを $\top$、$\bot$ で置き換える。

S-3 論理記号 $\equiv, \supset, \forall$ を消去する。即ち、部分論理式 $A \equiv B, A \supset B, \forall x A[x]$ をそれぞれ $A \wedge B \vee \neg A \wedge \neg B, \neg A \vee B, \neg \exists x \neg A[x]$ で置き換える。

S-4 $\neg$ を内側へ移動する。例えば、$\neg(A \wedge B)$ を $\neg A \vee \neg B$、$\neg\neg A$ を A とする。ただしこのとき $\neg \exists x A$ は A 中の $\neg$ は内側へ移動するが外の $\neg$ はこれ以上動かさない。

S-5 $\neg t = s$ を $t < s \vee s < t$、$\neg t < s$ を $t = s \vee s < t$ とする。

（注）以上二つの操作によって、$\neg$ は $\exists$ の所、及び $\neg Z$ の形でしか現れなくなる。

S-6 $A \wedge \top, \top \wedge A, A \vee \bot, \bot \vee A$ を A に,

$A \wedge \bot, \bot \wedge A, A \wedge \neg A, \neg A \wedge A, \exists x \bot, \neg \exists x \top, \neg \top$ を $\bot$ に,

$A \vee \top, \top \vee A, A \vee \neg A, \neg A \vee A, \exists x \top, \neg \exists x \bot, \neg \bot$ を $\top$ にそれぞれ置き換える。

S-7 $A \vee A, A \wedge A$ を A で置き換える。

また、以下で簡単化と言うとき、この 1,2,6,7 の操作をこの順で行うことを指す。

手続き M 簡単化された式（$\neg, \exists, \wedge, \vee$ からなる式で、$\neg$ は $\exists$ と Z の所にしか現れない）を拡大 v 式にする。

M-1 与えられた式に $\exists$ が無ければ手続きは終了。

M-2 与えられた式に $\exists$ がある場合

一番内側の $\exists x A[x]$ に着目する。以下の手続きによって、この $\exists x A[x]$、$\neg \exists x A[x]$ を拡大 v 式にする。$\neg$ の有無は 6 にだけ影響する。

M-3 A に手続き NF を施す。この結果を $A_1[x] \vee \cdots \vee A_n[x]$ とする。

M-4 $\exists x(A_1[x] \vee \cdots \vee A_n[x])$ を $\exists x_1 A_1[x_1] \vee \cdots \vee \exists x_n A_n[x_n]$ とする。ここで、$x_1, \cdots, x_n$ は新しい変数である。

M-5 各 $\exists x_i A_i[x_i]$ に対して次の操作を行い、それぞれを拡大 v 式に変形する。そして全体の論理和をとる。

M-6 節 A_i を x_i を含む部分 $B[x_i]$ と x_i を含まない部分 C_i とに分け、$C_i \wedge \exists x_i B[x_i]$ とし、$\exists x_i B[x_i]$ に手続き C を施す。
その結果を $D_{i1} \vee \cdots \vee D_{im_i}$ とする。ここで、$D_{ij}(1 \leq j \leq m_i)$ は拡大 v 節である。

(a) 着目した $\exists$ に $\neg$ がついている場合。

i. $\neg C_i, \neg D_{ij}(1 \leq j \leq m_i)$ を手続き S-4、S-5 の操作によって $\neg$ の内側への移動を行う。
この結果を $E_{i0}, \ldots, E_{im_i}$ とする。

ii. $E_{i0} \vee E_{i1} \wedge \ldots \wedge E_{im_i}$ 中に出現する $\neg$ のついた基本 v 式に対して、手続き IN を実行する。

iii. $1 \leq i \leq n$ についての上の結果の論理積をとり、これに手続き NF を施す。

(b) 着目した $\exists$ に $\neg$ がついていない場合。$\exists x_i A_i$ を $C_i \wedge D_{i1} \vee \cdots \vee C_i \wedge D_{im_i}$ で置き換える。（ここで、D_{ij} は拡大 v 節である）

M-7 得られた結果に M を施す。

手続き NF 基本 v 式の論理積と、Z の式、$\neg Z$ の式、不等式、等式と $\wedge\vee$ からなる式 Γ を拡大 v 式に変形する手続き
基本 v 式を素論理式と考えた積和標準形にする。

1. $\Gamma \equiv A \vee B$ のとき A, B それぞれに手続き NF を施し、それらの論理和をとる。
2. $\Gamma \equiv A \wedge B$ のとき A, B それぞれに手続き NF を施した結果をそれぞれ $A_1 \vee \cdots \vee A_n, B_1 \vee \cdots \vee B_m$ とする。

$$\bigvee_{1 \leq i \leq n, 1 \leq j \leq m} A_i \wedge B_j$$

3. Γ が基本 v 式、Z の式、$\neg Z$ の式、不等式、等式のいずれかであるとき Γ 自身が手続きの結果である。

手続き C $\exists x B[x]$ を拡大 v 式に変換する手続き
ここで $B[x]$ は基本 v 式、不等式、等式と $Z, \neg Z$ の式の論理積である。

C-1 $B[x]$ 中に x に関する等式がある場合。
それを x について解いて、その結果の $x = s$ より s を B に代入した $B[s]$ を簡単化して手続きは終了。

C-2 $B[x]$ の中に基本 v 式が無い場合は手続き Ba を施して、手続きは終了。

C-3 $B[x]$ の中に基本 v 式が複数ある場合には、例えば $\mho_t^s uD$ と $\mho_{s'}^{t'} vE$ を

$$\overset{t}{\underset{s}{\mho}} u(D \wedge \overset{t'}{\underset{s'}{\mho}} vE)$$

というようにそれらを一つにまとめる。また基本 v 式以外のリテラルの

論理積を B' とする。この結果得られる式を、$\exists x(B' \wedge \mathcal{V}_s^t uD)$ とする。

C-4 B' の中に Z の式がある場合

(a) $B' \wedge \mathcal{V}_s^t uD$ に手続き OZ を施す。この結果は

$$\bigvee_{i=1}^{n} E_i \wedge \exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge \mathop{\mathcal{V}}_{a_i y_i + e_i}^{a_i' y_i + e_i'} uD_i[y_i, u])$$

となる。ただし、y_i は新しい変数で、E_i には y_i は出現せず、$E_i'[y_i]$ には Z の式、$\neg Z$ の式は現れず、x もこの結果には出現しない。

(b) 各 $\exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge \mathcal{V}_{a_i y_i + e_i}^{a_i' y_i + e_i'} uD_i[y_i, u])$ を次の操作により拡大 v 式に変換し、それと E_i との論理積に手続き NF を施して終了。

a_i, a_i' と 0 との大小関係による場合分け。

i. $a_i = a_i' = 0$ の場合

$\exists$ と v の順序を交換して処理する。

A. $\exists y_i(Z(y_i) \wedge E_i' \wedge D_i)$ に手続き C を施して、拡大 v 式に変形する。この結果を $F_{i1} \vee \cdots \vee F_{im}$ とする。ここで、$F_j (1 \leq j \leq m)$ は拡大 v 節である。

B. 全ての $j (1 \leq j \leq m)$ に対して $\mathcal{V}_{e_i}^{e_i'} uF_{ij}$ に手続き EX を施したものの論理和をとる。

ii. $a_i = a_i' \neq 0$ の場合

A. a_i の分母、分子を M, N とする。（ただし、N, M は互い素な整数で、M は正）$Mv + Nu = 1$ の整数解の組の一つを v_0, u_0 とする。（ただし、$|v_0| \leq |N/2|$ をとる）

B. $\exists u(Z(u) \wedge E_i'[\frac{(1-Nv_0)y_i}{M} + Nu] \wedge D[\frac{(1-Nv_0)y_i}{M} + Nu, My_i - v_0 y_i])$ を手続き C によって拡大 v 式に直す。この結果を $F_{i1}[y_i] \vee \cdots \vee F_{il}[y_i]$ とする。

C. a の正負各々の場合に対応する、次の $vy_i \ldots$ の部分に手続き EX を施したものが i に対応する拡大 v 式である。

$0 < a$ のとき

$$\begin{aligned}
&\bigvee_{j=1}^{l} \{ \\
&\qquad \bigvee_{k=1}^{N} \mathop{\mathcal{V}}_{-Ne'+k-1}^{-Ne'+k} y_i(-N(e+1) < y_i < -Ne \wedge F_{ij}[y_i]) \\
&\quad \vee \quad (Z(Ne') \\
&\qquad \wedge (\bigvee_{k=1}^{N} -N(e+1) < -Ne' + k < -Ne \wedge F_{ij}[-Ne' + k]) \\
&\quad \vee \quad Z(Ne) \wedge -e' < -e < -e' + 1 \wedge F_{ij}[-Ne - 1]\}
\end{aligned}$$

$a<0$ のとき（M は正より N は負）

$$\bigvee_{j=1}^{l}\{$$

$$\bigvee_{k=N}^{-1} \overset{-Ne'+k+1}{\underset{-Ne'+k}{\mathcal{U}}} y_i(-Ne < y_i < -N(e+1) \wedge F_{ij}[y_i])$$

$$\vee \ (Z(Ne')$$

$$\wedge (\bigvee_{k=N}^{-1} -Ne < -Ne'+k+1 < -N(e+1) \wedge F_{ij}[-Ne'+k])$$

$$\vee \ Z(Ne) \wedge -e' < -e < -e'+1 \wedge F_{ij}[-Ne-1]\}$$

iii. $a_i \neq a'_i$ の場合

A. $a_iy_i+e_i = a'_iy_i+e'_i, a_iy_i+e_i+2 = a'_iy_i+e'_i$ の解を求める。それぞれを c_0, c_2 とする。

B. 次の式に手続き C を施して拡大 v 式にする。

$$\exists y_i(Z(y_i) \wedge a_iy_i+e_i < u < a'_iy_i+e'_i$$
$$\wedge \ a'_iy_i+e'_i-1 \leq u \leq a_iy_i+e_i+1 \wedge E'_i \wedge D_i)$$

この結果を $F_{i1} \vee \cdots \vee F_{il}$ とする。（各 F_{ij} は拡大 v 節である）

C. $0, a_i, a'_i$ の大小関係によって以下のように定まる区間 $t_0 < u < t_m$ を幅 1 の区間 $(t_0, t'_1], (t'_1, t'_2], \ldots, (t'_{m-2}, t_{m-1}]$ と幅 1 未満の区間 (t_{m-1}, t_m) に分ける。ただし、$t'_{i+1} = t'_i+1 (0 \leq i < m-1), t_{m-1} < t_m \leq t_{m-1}+1$ とする。

- $0 < a_i < a'_i, a'_i < a_i < 0$ の場合
  $t_0 = s[c_0], t_m = t[c_2]$
- $a_i \leq 0 \leq a'_i, a'_i \leq 0 \leq a_i$ の場合（共には等号はつかない）
  $t_0 = s[c_2], t_m = t[c_2]$
- $a_i < a'_i < 0, 0 < a'_i < a_i$ の場合
  $t_0 = s[c_2], t_m = t[c_0]$

D. 各 $0 \leq j \leq m-1, 1 \leq i \leq l$ にたいして

$$\overset{t'_{j+1}}{\underset{t'_j}{\mathcal{U}}} uF_i$$

を手続き EX により拡大 v 式に変換し、それらの論理和をとる。ただし、$t'_0 = s[c_0], t'_{m+1} = t[c_2], t'_{i+1} = t'_i+1 (0 \leq i < m)$ とする。

E. 式

$$Z(t_0) \wedge (\bigvee_{i=1}^{l}(\bigvee_{j=1}^{m} F_i[t_j])) \vee Z(t_m) \wedge \bigvee_{i=1}^{l} F_i[t_m]$$

を簡単化し手続き NF を施して拡大 v 式に変換したものと上の結果との論理和をとる。

C-5 Z の式がない場合

(a) $\exists x(B' \wedge s < u < t \wedge t-1 \leq u \leq s+1 \wedge D)$ を手続きCにより拡大 v 式に変換する。その結果を $E_1 \vee \cdots \vee E_n$ とする。（E_i は拡大 v 節）

(b)

$$\bigvee_{i=1}^{n} \exists u(Z(u) \wedge E_i)$$

の各 $\exists u(Z(u) \wedge E_i)$ を手続きCにより拡大 v 式にし、この結果の論理和で $\exists x(B' \wedge \mathcal{V}_s^t u D)$ を置き換え終了。

手続き OZ 式 $\exists x(A[x] \wedge B[x])$（ここで、$A$ は Z の式、$\neg Z$ の式、不等式の論理積、B は基本 v 式の論理積である）を $C \wedge \exists y(Z(y) \wedge A' \wedge B')$（ここで A' は不等式の論理積）という $\exists$ 中に $\neg Z$ の式が現れない式の論理和にする手続き

OZ-1 A 中の Z の式に手続き EZ を施し、この結果を $C \wedge Z(ax+b)$ とする。また、A 中の Z の式以外の式を $A'[x]$、とする。

OZ-2

$$\exists y(Z(y) \wedge A'[\frac{y-b}{a}] \wedge B[\frac{y-b}{a}])$$

に手続き NZ を施す。この結果を $D_1 \vee \cdots \vee D_n$ とする。

OZ-3

$$C \wedge D_1 \vee \cdots \vee C \wedge D_n$$

手続き EX $\mathcal{V}_s^t u(B \wedge C)$ を拡大 v 式にする手続き

ここで、B は不等式と Z の式の論理積であり、C は基本 v 式である。

EX-1 $\mathcal{V}_s^t u(B \wedge C)$ に対して B 中に Z の式があるとき、それらを $Z(a_1 u + e_1), \ldots, Z(a_k u + e_k)$ としそれら以外の B の式つまり不等式と C との論理積を B' として次の手続きを行う。
Z の式が無ければ終了。

EX-2 上の Z の式と $Z(u)$ を手続き EZ により、変数 u の出現する Z の式を一つにする。その結果を $Z(e'_1), \ldots, Z(e'_k), Z(a'u + e')$ とする。（$e'_1, \ldots, e'_k$ には u は出現しない）

EX-3 $\mathcal{V}_{a's+e'}^{a't+e'} y(a't - a' + e' < y < a's + a' + e' \wedge B'[(y - e')/a'])$
$\vee Z(t-1) \wedge s < t-1 < s+1 \wedge B'[t-1]$
$\vee Z(s+1) \wedge t-1 < s+1 < t \wedge B'[s+1]$ の簡単化を行う。

EX-4 上で得られた式と $Z(e'_1) \wedge \ldots \wedge Z(e'_k)$ との論理積に手続き NF を施して拡大 v 式に変形する。

手続き Ba $\exists x A[x]$ の $A[x]$ 中に基本 v 式が出現していない場合の手続き

Ba-1 $A[x]$ の中に Z の式が出現しない場合は $\neg Z$ の式を取り除き手続き Ra を実行して終了。

Ba-2 $\exists x A[x]$ に手続き OZ を施す。この結果を

$$\bigvee_{i=0}^{m} D_i \wedge \exists y_i(Z(y_i) \wedge B_i)$$

とする。(B_i は不等式の論理積)

Ba-3 $1 \leq i \leq m$ なる i に対して $\exists y_i(Z(y_i) \wedge B_i)$ に次の操作を施し、それと D_i との論理積に手続き NF を施したもの m 個の論理和をとる。

(a) 手続き Pr を行う。その結果得られた式を

$$\bigvee_{j=1}^{n} E_j \wedge \exists y_{ij}(Z(y_{ij}) \wedge l_j < y_{ij} < h_j)$$

とする。(このとき $\top$ または $\bot$ が得られる場合もある)

(b) 得られた結果が $\top, \bot$ でない場合。各 $j(1 \leq j \leq n)$ に対応する式 $E_j \wedge \exists y_{ij}(Z(y_{ij}) \wedge l_j < y_{ij} < h_j)$ に対して次の操作を行う。($\exists$ がなければそのまま)

i. l_j, h_j に変数がなければ真偽を求める。このとき

A. $\bot$ の場合式を取り除く。

B. $\top$ の場合は E_j で式を置き換える。

ii. 変数がある場合

$$E_j \quad \wedge \quad l_j + 1 < h_j \vee \mathop{\mathcal{U}}_{l_j}^{h_j} y_i(0 < h_j - l_j < 1)$$
$$\vee\ h_j - l_j = 1 \wedge \neg Z(l_j)$$

手続き NZ $\exists x(Z(x) \wedge \neg Z(b_1 x + f_1) \wedge \ldots \wedge \neg Z(b_l x + f_l) \wedge E[x])$ という式を、$D \wedge \exists y(Z(y) \wedge E[f(y)])$ という $\neg Z$ が $\exists$ の中に現れない形の式の論理和にする手続き

1. $b_1, \ldots, b_l$ の分母の最小公倍数 M を求める。
2.

$$\bigvee_{i=0}^{M-1} \neg Z(b_1 i + f_1) \wedge \ldots \wedge \neg Z(b_l i + f_l) \wedge \exists y_i(Z(y_i) \wedge E[M y_i + i])$$

が求める式である。ここで、y_i は新しい変数である。

手続き Pr $\exists x B[x]$ を (B は $Z(x)$ と不等式の論理積) $D \wedge \exists x(Z(x) \wedge l < x < h)$ または $\top, \bot$ と変形する手続き

1. $B[x]$ 中の不等式を x について解き、x の下界 ($l_1 < x, \ldots, l_p < x$) と上界 ($x < h_1, \ldots, x < h_q$) とに分ける。
2. 求める式は上界下界のどちらかが無い場合は $\top$ とし、両方ある場合は次の式とする。

$$\bigvee_{0 \leq i \leq p, 0 \leq j \leq q} \{ \bigwedge_{0 \leq i' \leq p, i' \neq i} (l_{i'} \leq l_i) \}$$

$$\wedge\{\bigwedge_{0\le j'\le q, j'\ne j}(h_j \le hj')\} \wedge \exists x(l_i < x < h_j \wedge Z(x))$$

手続き Ra $\exists x B[x]$ で $B[x]$ はすべて不等式の場合の手続き

1. $\exists x B[x]$ の $B[x]$ （の不等式全て）を x について解き、x の上界を表すもの（$x < h_1, \ldots, x < h_n$）、下界を表すもの（$l_1 < x, \ldots, l_m < x$）それぞれに分ける。
2. 上界下界の少なくとも片方が現われない場合、$\top$
3. 上界下界両方がある場合 $\bigwedge_{1\le i\le m, 1\le j\le n} l_i < h_j$

手続き EZ $Z(t_1[x]), \ldots, Z(t_n[x])$ という式の連言を $Z(t'_1), \ldots, Z(t'_{n-1}), Z(ax+e)$ $(a > 0)$ という式の連言にする手続き

ここで $t'_1, \ldots, t'_{n-1}$ には x が出現しない。

EZ-1 $n = 1$ のとき。つまり、x の出現する Z の式がただ一つしか存在しないとき手続きは終了。ただし、$Z(ax+e)$ の a が負の場合は $Z(-ax-e)$ で置き換える。

EZ-2 $2 \le n$ のとき。$t_1 = ax+b, t_2 = cx+d$ とする。

EZ-3 a, c どちらかあるいは両方が負の場合。負の方の項（両方とも負ならば両方の項）に -1 を掛ける。

EZ-4 $a = c$ の場合　$Z(t_2[x]), \ldots, Z(t_n[x])$ に手続き EZ を施し、その結果に、$Z(b-d)$ を付け加える。

EZ-5 $a \ne b$ の場合　a, c の大きい方の項から小さい方の項を引き、その結果で大きい方の項を含む式を置き換え、EZ-4 へ。

例えば $a < c$ なら $Z(cx+d)$ を $Z((c-a)x+d-b)$ で置き換える。

手続き IN $\neg \mathcal{V}_s^t u A[u]$ を $\neg$ の出現しない拡大 v 式にする手続き

IN-1 項 s, t 両方に変数が現れない場合

(a) 開区間 (s, t) 中の整数が一つのときその値 N を求め、$A[N]$ の結果に $\neg$ を付け、S-4,S-5 によって簡単化する。

(b) (s, t) 間の整数が複数あるか、全く無いときは $\top$

IN-2 少なくとも片方に変数が現れる場合

次の三つの結果の論理和をとり、手続き NF を施して拡大 v 式にする。

(a) 手続き Ba によって式 $\exists x(Z(x) \wedge s+1 < x < t)$ を拡大 v 式にする。

(b) 次の手続きにより $\mathcal{V}_s^t u \neg A$ を拡大 v 式にする。

i. $\neg A$ に手続き S-4,S-5 を施す。

ii. 上の結果中の $\neg v$ に手続き IN を施す。

iii. 手続き NF によって拡大 v 式にする。その結果を $D_1[u] \vee \cdots \vee D_n[u]$（ここで、$D_i[u] (1 \le i \le n)$ は拡大 v 節）とする。

iv.

$$\overset{t}{\underset{s}{\mathcal{V}}} u_1 D_1[u_1] \vee \cdots \vee \overset{t}{\underset{s}{\mathcal{V}}} u_n D_n[u_n]$$

を作り、各 $\mathcal{V}_s^t u_i D_i[u_i]$ を手続き EX によって拡大 v 式にする。

(c) $s = ax + e, t = a'x + e'$ とする。$\neg\exists x(Z(x) \wedge s < x < t)$ を以下のように a, a' の大小関係の場合分けによって拡大 v 式にする。

i. $0 < a < a'$ の場合

$$\exists u(Z(u) \wedge \frac{a'e - ae'}{a' - a} < u \leq \frac{a'e - ae' + a'}{a' - a} \wedge \frac{u - 1 - e}{a} \leq x \leq \frac{u - e'}{a'})$$

を拡大 v 式にしたものと、$x \leq \frac{e-e'}{a'-a}$ との論理和

ii. $0 = a < a'$ の場合

$$\exists u(Z(u) \wedge e < u \leq e + 1 \wedge x \leq \frac{u - e'}{a'})$$

を拡大 v 式にしたものと、$x \leq \frac{e-e'}{a'-a}$ との論理和

iii. $0 \neq a = a'$ の場合

$$e < e' \wedge \exists u(Z(u) \wedge ax + e' \leq u \leq ax + e + 1)$$

を拡大 v 式にしたものと、$e' \leq e$ の論理和

iv. $a < 0 < a'$ の場合

$$\exists u(Z(u) \wedge \frac{a'e - ae' + a}{a' - a} \leq u \leq \frac{ae' - a'e + a'}{a' - a} \wedge (x \leq \frac{u - e'}{a'} \vee x \leq \frac{u - e}{a}))$$

を拡大 v 式にしたものと $x \leq \frac{e-e'}{a'-a}$ との論理和

v. $a < a' < 0$ の場合

$$\exists u(Z(u) \wedge \frac{a'e - ae' + a}{a' - a} \leq u \leq \frac{a'e - ae'}{a' - a} \wedge \frac{u + 1 - e'}{a'} \leq x \leq \frac{u - e}{a})$$

を拡大 v 式にしたものと $x \leq \frac{e-e'}{a'-a}$ との論理和

vi. $a < a' = 0$ の場合

$$\exists u(Z(u) \wedge e' - 1 \leq u \leq e' \wedge x \leq \frac{u - e}{a})$$

を拡大 v 式にしたものと $x \leq \frac{e'-e}{a}$ との論理和

vii. $0 < a' < a$ の場合

$$\exists u(Z(u) \wedge \frac{a'e - ae' + a}{a' - a} \leq u \leq \frac{a'e - ae'}{a' - a} \wedge \frac{u - e}{a} \leq x \leq \frac{u + 1 - e'}{a'})$$

を拡大 v 式にしたものと $\frac{e-e'}{a'-a} \leq x$ との論理和

viii. $0 = a' < a$ の場合

$$\exists u(Z(u) \wedge e' - 1 \leq u \leq e' \wedge \frac{u - e}{a} \leq x)$$

を拡大 v 式にしたものと $\frac{e'-e}{a} \leq x$ との論理和

ix. $a' < 0 < a$ の場合

$$\exists u(Z(u) \wedge \frac{a'e - ae' + a}{a' - a} \leq u \leq \frac{a'e - ae' + a'}{a' - a} \wedge (\frac{u - e}{a} \leq x \vee \frac{u - e'}{a'} \leq x))$$

を拡大 v 式にしたものと $\frac{e-e'}{a'-a} \leq x$ との論理和

x. $a' < a = 0$ の場合

$$\exists u(Z(u) \wedge e \leq u \leq e+1 \wedge x \leq \frac{u-e'}{a'})$$

を拡大 v 式にしたものと $\frac{e-e'}{a'} \leq x$ との論理和

xi. $a' < a < 0$ の場合

$$\exists u(Z(u) \wedge \frac{a'e-ae'}{a'-a} \leq u \leq \frac{a'e-ae'+a'}{a'-a} \wedge \frac{u+1-e'}{a'} \leq x \leq \frac{u-e}{a})$$

を拡大 v 式にしたものと $\frac{e-e'}{a'-a} \leq x$ との論理和

3.4 初等的定理

この節では前節で示した手続きの正当性を証明するために必要ないくつかの性質を公理から形式的に導く。

定理 3.3

1. $x = y \equiv x - y = 0$
2. $x < y \equiv x - y < 0$
3. $x < 0 \equiv 0 < -x$
4. $x < y \supset \neg x = y$
5. $\neg x < y \equiv y \leq x$

定理 3.4 $0 < n$ とする。

1. $nx = 0 \equiv x = 0$
2. $0 < nx \equiv 0 < x$
3. $nx < 0 \equiv x < 0$

証明

- $x = 0$ ならば $nx = 0$
- $x < 0$ と仮定すると (OP) より、$2x < x, 3x < 2x, \ldots$ であるから推移律により、

$$nx < 0$$

- $0 < x$ と仮定すれば、同様に $0 < nx$

これらと (O3) $x < 0 \vee x = 0 \vee 0 < x$、(O1) 反対称律、定理 3.3より明らか。 □

定理 3.5 分配則

$$\frac{1}{n}(x+y) = \frac{1}{n}x + \frac{1}{n}y$$

証明

$$n\frac{1}{n}(x+y) = x + y = n\frac{1}{n}x + n\frac{1}{n}y = n(\frac{1}{n}x + \frac{1}{n}y)$$

よって、$n(\frac{1}{n}(x+y)-(\frac{1}{n}x+\frac{1}{n}y))=0$であるから定理 3.4、3.3により

$$\frac{1}{n}(x+y)=\frac{1}{n}x+\frac{1}{n}y$$

□

系 3.1

1.

$$\frac{m}{n}(x+y)=\frac{m}{n}x+\frac{m}{n}y$$

2.

$$\frac{1}{n}mx=m\frac{1}{n}x$$

3.

$$-\frac{1}{n}x=\frac{1}{n}(-x)$$

証明

1. のみ示す。

$$\frac{m}{n}(x+y)=m(\frac{1}{n}x+\frac{1}{n}y)=m\frac{1}{n}x+m\frac{1}{n}y$$

□

定理 3.6 順序保存

任意の正の整数 m,n に対して、

$$x<y\supset\frac{m}{n}x<\frac{m}{n}y$$

証明

$$x-y<0\equiv\frac{m}{n}(x-y)<0\equiv\frac{m}{n}x-\frac{m}{n}y<0$$

定理 3.7 約分・通分

$$\frac{nd}{md}x=\frac{n}{m}x$$

証明

$$m(\frac{nd}{md}x-\frac{n}{m}x)=m\frac{nd}{md}x-m\frac{n}{m}x=md\frac{n}{md}x-nx=0$$

系 3.2

$$Cx+C'x=(C+C')x$$

ここで $(C+C')$ は通常の有理数の和である。

また二つの有理数 C と C' とが与えられたとき、その和である d をとれば $C+C'=d$ が成り立つ。

定理 3.8 順序保存

$0<\frac{n}{m}<\frac{n'}{m'}$ であるとき

$$0<x\supset\frac{n}{m}x<\frac{n'}{m'}x$$

証明

$0<\frac{n}{m}<\frac{n'}{m'}$ より $m'n<mn'$。よって、

$$\frac{n'}{m'}x-\frac{n}{m}x=\frac{mn'}{mm'}x-\frac{m'n}{mm'}x=\frac{m'n-mn'}{mm'}x$$

ここで $0<\frac{n'm-m'n}{mm'}$ であるから $0<x$ と定理 3.6 より

$$\frac{n'm-m'n}{mm'}0<\frac{n'm-m'n}{mm'}x$$

従って結論を得る。□

定理 3.9

$$\frac{n}{m}(\frac{p}{q}x)=\frac{np}{mq}x$$

証明

$$\begin{aligned}
&mq(\frac{n}{m}(\frac{p}{q}x)-\frac{np}{mq}x)\\
&= qn(\frac{p}{q}x)-npx\\
&= npx-npx=0
\end{aligned}$$

従って結論を得る。□

定理 3.10

$$Z(x)\equiv Z(-x)$$

証明 $Z(0)$ と公理 (Z3) より $Z(x)\supset Z(0-x)$。逆向きも同様。

定理 3.11

$$Z(n)$$

証明

n に関する帰納法で示す。

$0 < n$ の場合

$$Z(0) \equiv Z(0+1) \equiv Z(0+1+1) \equiv \cdots \equiv Z(0+\underbrace{1+1+\cdots+1}_{n})$$

から明らか。
$n < 0$ の場合は $Z(-x)$ より直ちにいえる。□

定理 3.12

$$Z(x) \wedge Z(y) \supset Z(x+y)$$

証明
$Z(x)$ より $Z(-x)$ であり、また $Z(y)$ より $Z(-x-y)$ 即ち $Z(-(x+y))$ よって $Z(x+y)$ である。□

系 3.3

$$Z(x) \supset Z(nx)$$

$$Z(x) \wedge Z(x+y) \supset Z(y)$$

$$\neg Z(x) \supset \neg Z(\frac{1}{n}x)$$

証明
1番目については明らかなので、2番目、3番目の式について証明する。
2番目
$Z(x)$ より $Z(-x)$。ゆえに定理3.12より、$Z(-x+(x+y)) \equiv Z(y)$
3番目
対偶をとって $Z(\frac{1}{n}x) \supset Z(x)$ を示す。$Z(\frac{1}{n}x)$ を仮定すると、1番目の式より $Z(x)$ である。□

系 3.4

$$Z(x) \wedge \neg Z(x+y) \supset \neg Z(y)$$

定理 3.13

$$\forall x \exists y (Z(y) \wedge x < y \leq x+1)$$

証明
公理 (Z4) より、

$$\forall x \exists y (Z(y) \wedge y \leq x < y+1)$$

これから

$$\exists y (Z(y) \wedge y \leq a < y+1)$$

を仮定する。存在するものを b とすると、

$$Z(b) \wedge b \leq a < b+1。$$

これより

$$\begin{aligned} & Z(b) \wedge a < b+1 \leq a+1 \\ \equiv\ & Z(b+1) \wedge a < b+1 \leq a+1 \\ \rightarrow\ & \exists y(Z(y) \wedge a < y \leq a+1) \\ \equiv\ & \exists y(Z(y) \wedge a \leq y < a+1) \end{aligned}$$

最後に $\forall$ を導入すればよい。□

定理 3.14

$$Z(y) \wedge y < x < y+1 \supset \neg Z(x)$$

証明

背理法による。

$Z(y) \wedge y < x < y+1$ と $Z(x)$ を仮定する。$y < x < y+1$ より $0 < x-y < 1$ である。$Z(y)$ と $Z(x)$、公理 (Z3) より $Z(x-y)$ しかしこれは公理 (Z4) と矛盾。□

補題 3.3　n を正の自然数とする。このとき

$$Z(x) \supset \exists w, y(Z(w) \wedge Z(y) \wedge x = ny + w \wedge 0 \leq w < n)$$

証明

$Z(x)$ と仮定する。公理 (Z4) より

$$\exists y(Z(y) \wedge y \leq \frac{1}{n}x < y+1)$$

であるから、存在するものを y_0 とおく。

$$\begin{aligned} & y_0 \leq \frac{1}{n}x < y_0+1 \\ \equiv\ & ny_0 \leq x < ny_0+n \end{aligned}$$

このとき $x - ny_0 \geq 0$ かつ $x - ny_0 < n$、また $Z(x), Z(y_0)$ より $x - ny_0 = w$ とおけば、

$$\exists w(Z(w) \wedge x = ny_0 + w \wedge 0 \leq w < n)$$

であるので、結論を得る。□

定理 3.15

$$Z(x) \equiv \bigvee_{i=0}^{n-1} Z(\frac{1}{n}(x-i))$$

証明

$(\rightarrow)$

公理より $Z(x) \equiv Z(x+n)$。

上の補題から

$$Z(x) \supset \exists w, y(Z(w) \wedge Z(y) \wedge x = ny + w \wedge 0 \leq w < n)$$

また定理 3.14 より

$$Z(w) \wedge 0 \leq w < n \supset w = 0 \vee \cdots \vee w = n-1$$

よって、

$$\begin{aligned}
&\exists w, y(Z(w) \wedge Z(y) \wedge x = ny + w \wedge 0 \leq w < n) \\
&\equiv \exists y(Z(y) \wedge x = ny + 0) \vee \exists y(Z(y) \wedge x = ny + 1) \\
&\quad \vee \cdots \vee \exists y(Z(y) \wedge x = ny + n - 1) \\
&\equiv \exists y(Z(y) \wedge \frac{1}{n}x = y) \vee \exists y(Z(y) \wedge \frac{1}{n}(x-1) = y) \\
&\quad \vee \cdots \vee \exists y(Z(y) \wedge \frac{1}{n}(x-(n-1)) = y) \\
&\equiv Z(\frac{1}{n}x) \vee Z(\frac{1}{n}(x-1) \vee \cdots \vee Z(\frac{1}{n}(x-(n-1))) \\
&\equiv \bigvee_{i=0}^{n-1} Z(\frac{1}{n}(x-i))
\end{aligned}$$

$(\leftarrow)$

$Z(\frac{1}{n}(x-i))$ とすると系 3.3 より $Z(n\frac{1}{n}(x-i))$。よって、$Z(x-i)$ であるから $Z(x)$ である。□

x, y の平均 $\frac{x+y}{2}$ をとる事により次の補題が成立する。

補題 3.4

$$x < y \supset \exists r(x < r < y)$$

定理 3.16

$$x < y \supset \exists r(x < r < y \wedge \neg Z(m_1 r + n_1) \wedge \cdots \wedge \neg Z(m_l r + n_l))$$

証明

$1 < y - \frac{1}{2}(x+y)$ であるとき $d = 1$、そうでないとき $d = y - \frac{1}{2}(x+y)$ とする。
$Z(m_1 r + n_1)$ を満たす元を r_0 とすれば

$$Z(m_1 r_0 + n_1) \equiv Z(m_1 r_0 + n_1 + 1) \equiv Z(m_1(r_0 + \frac{1}{m_1}) + n_1)$$

より、$r_0, r_0 + \frac{1}{m_1}, r_0 + \frac{2}{m_1}, \ldots$ も $Z(m_1 r + n_1)$ を満たす。しかも区間 $[r_0, r_0 + 1)$ にはこれ以外に存在しない。よって、$d \leq 1$ より区間 $\frac{1}{2}(x+y) \leq r < \frac{1}{2}(x+y) + d$ には $Z(m_1 r + n_1)$ を満たす元は高々 m_1 個しかない。同様にこの区間に $Z(m_2 r + n_2), \ldots, Z(m_l r + n_l)$ を満たす元はそれぞれ高々 $m_2, \ldots, m_l$ 個しかないので、$Z(m_1 r + n_1) \vee \cdots \vee Z(m_l r + n_l)$ を満たす元もこの区間には高々 $m_1 + m_2 + \cdots + m_l$ 個しかない。これより、

$$\frac{1}{2}(x+y), \frac{1}{m_1 + \cdots + m_l + 1} d + \frac{1}{2}(x+y), \ldots, \frac{m_1 + \cdots + m_l}{m_1 + \cdots + m_l + 1} d + \frac{1}{2}(x+y)$$

の内すくなくとも一つは

$$\neg Z(m_1 r + n_1) \wedge \cdots \wedge \neg Z(m_l r + n_l))$$

を満たすので結論を得る。□

次の定理は公理 (Z4) より明らかである。

定理 3.17 *Cofinality*

$$\forall x \exists y (Z(y) \wedge x < y)$$
$$\forall x \exists y (Z(y) \wedge y < x)$$

定理 3.18 m, n を互いに素な整数とする。$m \neq 1$ であれば

$$\neg Z(\frac{n}{m})$$

証明

$$n = mq + r$$

$(1 \leq r < m)$ と書ける。(互いに素であるから $r \neq 0$) よって、

$$\frac{n}{m} = q + \frac{r}{m}$$

であり、

$$Z(q), q < \frac{r}{m} < q + 1$$

となって定理 3.14 より $\neg Z(\frac{n}{m})$ である。□

注 1 以上の議論によって、

1. a が定数 (変数の出現しない項) であるとき、a より大きい最小の整数を求めることができる。

2. 閉じた素論理式の真偽を定めることができる。

3.5 正当性の証明

この節では前節で示した手続きによって、閉じた一次の有理 Presburger 算術の式が決定できることを示す。

手続き S、手続き NF の検証と補題 手続き S、手続き NF の正当性は全てよく知られた論理的手続き（ブール則など）と有理数の性質より明らか。また、手続き NF によっては v 記号の数は減ることはあっても決して増えない。

よって、他の手続きについて次節以降でそれらの正当性を証明する。またその前に検証に必要となる補題を証明しておく。

補題 3.5 $1 \leq t - s$ であるとき、

$$\exists x(Z(x) \wedge s < x < t \wedge A) \equiv \overset{t}{\underset{s}{\mho}} x A$$

である。

明らかなので証明は省く。

補題 3.6 式 $\exists x(Z(x) \wedge t < x < t + a \wedge A[x])$（ここで、$t$ は x の出現しない項、a は定数、A は式である）は次の式と同値である。

a が整数の場合

$$\bigvee_{i=0}^{a-1} \overset{t+i+1}{\underset{t+i}{\mho}} x A[x]$$
$$\vee \quad Z(t) \wedge (\bigvee_{i=1}^{a-1} A[t+i])$$

a が整数でない場合

$$\bigvee_{i=0}^{\lfloor a-1 \rfloor} \overset{t+i+1}{\underset{t+i}{\mho}} x A[x]$$
$$\vee \quad \overset{t+a}{\underset{t+\lfloor a \rfloor}{\mho}} x A[x]$$
$$\vee \quad Z(t) \wedge (\bigvee_{i=1}^{\lfloor a \rfloor} A[t+i])$$

ここで、$\lfloor x \rfloor$ は x を越えない最大の整数を示す。

証明

$$t < x < t + a \equiv$$
$$t < x < t + 1 \vee x = t + 1 \vee t + 1 < x < t + 2 \vee \cdots \vee$$
$$t + \lfloor a - 1 \rfloor - 1 < x < t + \lfloor a - 1 \rfloor \vee t = \lfloor a - 1 \rfloor \vee t + \lfloor a - 1 \rfloor < x < t + a$$

である事は明らか。よって、補題 3.5より

$$
\begin{aligned}
&\exists x(Z(x) \wedge t < x < t + a \wedge A[x]) \equiv \\
&\quad \exists x(Z(x) \wedge \\
&\quad ((t < x < t+1 \vee t+1 < x < t+2 \vee \cdots \vee t + \lfloor a-1 \rfloor < x < t+a) \wedge A \\
&\quad \vee (x = t+1 \vee x = t+2 \vee \cdots \vee x = t + \lfloor a-1 \rfloor) \wedge A)) \\
&\equiv \bigcup_{t}^{t+1} xA \vee \cdots \vee \bigcup_{t+\lfloor a-1 \rfloor}^{t+a} xA \\
&\quad \vee \exists x(Z(x) \wedge x = t+1 \wedge A) \vee \cdots \vee \exists x(Z(x) \wedge x = t + \lfloor a-1 \rfloor \wedge A) \\
&\equiv \bigcup_{t}^{t+1} xA \vee \cdots \vee \bigcup_{t+\lfloor a-1 \rfloor}^{t+a} xA \\
&\quad \vee Z(t) \wedge (A[t+1] \vee \cdots \vee A[t + \lfloor a-1 \rfloor]) \qquad \square
\end{aligned}
$$

次節から各手続きについて証明して行くが、その順番はボトムアップになっている。また、各手続きの仕様中でいう式の変形は同値変形を意味する。

手続き EZ 仕様 $Z(t_1[x]), \ldots, Z(t_n[x])$ という形の式の連言を $Z(t'_1), \ldots, Z(t'_{n-1}), Z(ax+e)$ $(a > 0)$ という式の連言にする。
ここで、$t'_1, \ldots, t'_{n-1}$ には x は出現しない。また、$t_i = x$ である i があれば、$0 < a \leq 1$。

証明 $Z(t_1) \wedge \cdots \wedge Z(t_n)$ で（x の現れる）Z の式の数の上の帰納法。
$n = 1$ であれば明か。（EZ-1）$n = k \geq 1$ で成り立っているとして、$n = k+1$ の場合を考える。$Z(t_1) \wedge Z(t_2)$ で $t_1 = \frac{n_1}{m_1}x + e_1$、$t_2 = \frac{n_2}{m_2}x + e_2$ とする。（n_1, m_1、n_2, m_2 は互いに素）$LCM(m_1, m_2) = a_1 m_1 = a_2 m_2$、$GCD(n_1, n_2) = d$、$n_1 = d_1 d$、$n_2 = d_2 d$ とする。このとき $GCD(a_1 n_1, a_2 n_2) = d$ である。従って、ある整数 k_0, k_1 が存在して、$a_1 n_1 k_0 + a_2 n_2 k_1 = d$ となる。$s_0 = dx/l + k_0 e_1 + k_1 e_2$、$s_1 = a_1 d_1 e_2 - a_2 d_2 e_1$ と置く。$s_0 = k_0 t_1 + k_1 t_2$、$s_1 = -a_2 d_2 t_1 + a_1 d_1 t_2$ である。よって、行列

$$
M = \begin{bmatrix} k_0 & k_1 \\ -a_2 d_2 & a_1 d_1 \end{bmatrix}
$$

と置くと、

$$
\begin{bmatrix} s_0 \\ s_1 \end{bmatrix} = M \begin{bmatrix} t_1 \\ t_2 \end{bmatrix}
$$

である。$det(M) = 1$ なので M^{-1} も整数係数の行列になる。よって、$Z(t_1) \wedge Z(t_2) \equiv Z(s_0) \wedge Z(s_1)$ となり、$n_0 = 1$ ならば $d = 1$ である。ここで s_1 は x を含まないので、x が現れる式の数が k となり、帰納法の仮定より結論がいえる。

手続き NZ 仕様 式

$$
\Gamma \equiv \exists x(Z(x) \wedge \neg Z(t_1) \wedge \cdots \wedge \neg Z(t_n) \wedge A[x])
$$

を

$$\bigvee_{i=0}^{M-1} C_i \wedge \exists y_i(Z(y_i) \wedge A[My_i + i])$$

という $C_i(0 \leq i \leq M-1)$ には x, y_i が現れず、M は $t_1, \ldots t_n$ の x の係数の分母の最小公倍数である論理式にする。

証明 整数 x を $t_1, \ldots t_n$ の x の係数の分母の最小公倍数 M で割った余りの場合分け、定理 3.15 より

$$Z(x) \equiv Z(x/M) \vee Z((x-1)/M) \vee \cdots \vee Z((x-(M-1))/M)$$

よって、

$$\begin{aligned}
\Gamma \equiv & \\
& \exists x((Z(x/M) \vee Z((x-1)/M) \vee \cdots \vee Z((x-(M-1))/M)) \\
& \wedge \neg Z(t_1[x]) \wedge \cdots \wedge \neg Z(t_n[x]) \wedge A[x]) \\
\equiv & \bigvee_{i=0}^{M-1} \exists x(Z((x-i)/M) \wedge \neg Z(t_1[x]) \wedge \cdots \wedge \neg Z(t_n[x]) \wedge A[x]) \\
\equiv & \bigvee_{i=0}^{M-1} \exists x(Z((x-i)/M) \wedge \neg Z(t_1[i]) \wedge \cdots \wedge \neg Z(t_n[i]) \wedge A[x]) \\
\equiv & \bigvee_{i=0}^{M-1} \neg Z(t_1[i]) \wedge \cdots \wedge \neg Z(t_n[i]) \wedge \exists x(Z((x-i)/M) \wedge A[x]) \\
\equiv & \bigvee_{i=0}^{M-1} \neg Z(t_1[i]) \wedge \cdots \wedge \neg Z(t_n[i]) \wedge \exists y_i(Z(y_i) \wedge A[My_i + i])
\end{aligned}$$

また、明らかに $1 \leq M$ である。□

手続き OZ 仕様 式 $\exists x(A[x] \wedge B[x])$ （ここで、A は Z の式、$\neg Z$ の式不等式の論理積、B は基本 υ 式の論理積である）を $C \wedge \exists y(Z(y) \wedge A' \wedge B')$ （ここで A' は不等式の論理積）という $\exists$ の束縛範囲内に $\neg Z$ の式が現れない式の論理和にする

証明

$$A[x] \equiv Z(t_1) \wedge \cdots \wedge Z(t_n) \wedge A'[x]$$

とする。（A' にはの Z 式は現れない） $Z(t_1) \wedge \cdots \wedge Z(t_n)$ に手続き EZ を施した結果を

$$Z(t'_1) \wedge \cdots \wedge Z(t'_{n-1}) \wedge Z(ax+b)$$

とすれば手続き EZ の証明より、

$$Z(t_1) \wedge \cdots \wedge Z(t_n) \equiv Z(t'_1) \wedge \cdots \wedge Z(t'_{n-1}) \wedge Z(ax+b)$$

(OZ-1)

また、

$$
\begin{aligned}
&\exists x(A[x] \wedge B[x]) \\
&\quad \equiv \exists x(Z(t_1) \wedge \cdots \wedge Z(t_n) \wedge A'[x] \wedge B[x]) \\
&\quad \equiv \exists x(Z(t'_1) \wedge \cdots \wedge Z(t'_{n-1}) \wedge Z(ax+b) \wedge A'[x] \wedge B[x]) \\
&\quad \equiv Z(t'_1) \wedge \cdots \wedge Z(t'_{n-1}) \wedge \exists x(Z(ax+b) \wedge A'[x] \wedge B[x]) \\
&\quad \equiv Z(t'_1) \wedge \cdots \wedge Z(t'_{n-1}) \wedge \exists y(Z(y) \wedge A'[\frac{y-b}{a}] \wedge B[\frac{y-b}{a}])
\end{aligned}
$$

である。これに手続き NZ を施した結果を

$$\bigvee_{i=1}^{M} C_i \wedge \exists y_i(Z(y_i) \wedge D[y_i])$$

とすれば

$$
\begin{aligned}
&\exists x(A[x] \wedge B[x]) \\
&\quad \equiv \bigvee_{i=1}^{M} Z(t'_1) \wedge \cdots \wedge Z(t'_{n-1}) \wedge C_i \wedge \exists y_i(Z(y_i) \wedge D[y_i])
\end{aligned}
$$

(OZ-2、OZ-3) □

手続き Pr 仕様 $\exists x A[x]$ を $D \wedge \exists x(l < x < h \wedge A')$ または $\top, \bot$ と変形する。ここで、$A[x]$ は不等式と Z の式、$\neg Z$ の式との論理積であり、A' は Z の式、$\neg Z$ の式との論理積である。

証明 A 中の不等式を x について解いたものを $l_1 < x, \ldots, l_n, x < h_1, \ldots, x < h_m$ とし、残りの Z の式、$\neg Z$ の式の論理積を A' とすれば明らかに、

$$
\begin{aligned}
&\exists x A[x] \equiv \\
&\quad \bigvee_{1 \le i \le n, 1 \le j \le m} \{ \bigwedge_{1 \le i' \le n, i' \ne i} l_{i'} \le l_i \} \wedge \bigwedge_{1 \le j' \le n, j' \ne j} \{ h_j \le h_{j'} \wedge \exists x(l_i < x < h_j \wedge A') \}
\end{aligned}
$$

また、$l_i < x, x < h_j$ のどちらかの形の式がなければ定理 3.17 (cofinality) より $\top$ である。□

手続き Ba 仕様 手続き Ba は、$\exists x B[x]$（ここで、B は不等式、Z の式、$\neg Z$ の式の連言）を拡大 υ 式に変換する。このとき B に $\neg Z$ の式が現れなければその結果にも $\neg Z$ の式が現れない。

証明 手続き Pr、手続き OZ の証明の結果と、Ba-1、Ba-2 から明らかに $\exists x(Z(x) \wedge l < x < h)$ の形の式を扱えば良い。そしてこれが

$$\overset{h}{\underset{l}{\upsilon}} x(h-l<1) \vee h-l=1 \wedge \overset{h}{\underset{l}{\upsilon}} x\top \vee 1 < h-l$$

と同値であるのは全順序の公理、定理 3.13 と補題 3.5 より導ける。また、$h-l=1 \wedge \upsilon_l^h x\top \equiv \neg Z(l) \wedge h-l=1$ は定理 3.13 より導ける。□

手続き EX 仕様 A が Z の式と基本 v 式からなる拡大 v 節であるとき $\mathcal{V}_s^t xA$ という式を拡大 v 式にする。

証明 $\mathcal{V}_s^t xA$ の A が Z の式、不等式と基本 v 式との論理積であるから、Z の式が現れなければ $\mathcal{V}_s^t xA$ はすでに基本 v 式である。(EX-1) よって、Z の式がいくつか現れた場合を考える。$A \equiv Z(t_1) \wedge \cdots \wedge Z(t_n) \wedge A'$ とする。手続き EZ の証明より、$Z(x) \wedge A \equiv Z(t'_1) \wedge \cdots \wedge Z(t'_n) \wedge Z(ax+e) \wedge A'$ とすることが出来る。(EX-2) ここで、$t'_1, \ldots, t'_{n-1}$ には x が現れず、

$$0 < a \leq 1 \tag{3}$$

である。よって、

$$\begin{aligned}
&\overset{t}{\underset{s}{\mathcal{V}}} xA \\
&\equiv \exists x(Z(x) \wedge s < x < t \wedge t-1 \leq x \leq s+1 \wedge A) \\
&\equiv \exists x(Z(x) \wedge s < x < t \wedge t-1 \leq x \leq s+1 \\
&\quad \wedge Z(t_1) \wedge \cdots \wedge Z(t_n) \wedge A') \\
&\equiv \exists x(s < x < t \wedge t-1 \leq x \leq s+1 \\
&\quad \wedge Z(t'_1) \wedge \cdots \wedge Z(t'_n) \wedge Z(ax+e) \wedge A') \\
&\equiv Z(t'_1) \wedge \cdots \wedge Z(t'_n) \wedge \\
&\quad \exists y(Z(y) \wedge as+e < y < at+e \\
&\qquad \wedge at+e-a \leq y \leq as+e+a \wedge A'[\frac{y-e}{a}])
\end{aligned}$$

ここで、条件 (3) 及び補題 3.5 より

$$\begin{aligned}
&\exists y(Z(y) \wedge as+e < y < at+e \\
&\qquad \wedge at+e-a \leq y \leq as+e+a \wedge A'[\frac{y-e}{a}]) \\
&\equiv \overset{at+e}{\underset{as+e}{\mathcal{V}}} yA'[\frac{y-e}{a}]
\end{aligned}$$

である。□

手続き C 仕様 式 $\exists x(A \wedge B)$ を（ここで A は Z の式、$\neg Z$ の式、不等式、等式の連言であり、B は基本 v 式の連言である）を拡大 v 式 $C_1 \vee \cdots \vee C_m$ に変換する。このとき $A \wedge B$ 中の v の数が N であるならば、各拡大 v 節 $C_i (1 \leq i \leq m)$ の中には v は高々 $N+1$ 個しか現れない。そして Z の式が A に無ければ各拡大 v 節中の v の数は高々 N である。さらに、A に $\neg Z$ の式がなければ各 $C_i (1 \leq i \leq m)$ の中にも $\neg Z$ の式は現れない。

証明 A に等式があれば C-1 より明かなので、A に等式がない場合を扱う。v の個数 N に関する帰納法を用いる。

1. $N = 0$ の場合

   C-2 より Ba を行う。手続き Ba の証明により、$\exists x B[x]$（ここで、B は不等式、Z の式、$\neg Z$ の式の連言）は拡大 v 式に変換され、このと

き B に $\neg Z$ の式が現れなければその結果にも $\neg Z$ の式が現れない事がいえる。

2. $N = k+1$ の場合

ただし k 以下のときは正しいとする。C-3 の手続きは同値変形であるから $\exists x(B' \wedge \mathcal{V}_s^t uD)$ が条件にあるような拡大 v 式に出来ることを言えば良い。

- B' に Z の式がある場合

  $\exists x(B' \wedge \mathcal{V}_s^t uD)$ は OZ の証明より

$$\bigvee_{i=1}^{n} E_i \wedge \exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge \mathop{\mathcal{V}}_{a_i y_i + e_i}^{a_i' y_i + e_i'} uD_i[y_i, u])$$

  という形にできる。(C-4(a)) 以下 a_i, a_i' の大小関係の場合分けとなる。

(a) $a_i = a_i' = 0$

明らかに

$$\begin{aligned} & E_i \wedge \exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge \mathop{\mathcal{V}}_{a_i y_i + e_i}^{a_i' y_i + e_i'} uD_i[y_i, u]) \\ \equiv\ & E_i \wedge \mathop{\mathcal{V}}_{e_i}^{e_i'} u \exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge D_i[y_i, u]) \end{aligned}$$

また、$\exists \mathcal{V}_{e_i}^{e_i'} u \exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge D_i[y_i, u])$ は $\neg Z$ が現れないので、帰納法の仮定より $\neg Z$ が現れない拡大 v 式に直せる。よって、EX,NF によれば全体も拡大 v 式に直せる。

(b) $a_i = a_i' \neq 0$

$a_i = N/M$、N, M は互いに素とし、Mv+Nu=1 の解の組の一つを (v_0, u_0) とすると

$a_i > 0$ の場合

$$\begin{aligned} & E_i \wedge \exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge \mathop{\mathcal{V}}_{a_i y_i + e_i}^{a_i' y_i + e_i'} uD_i[y_i, u]) \\ \equiv\ & E_i \wedge \ \exists y_i(Z(y_i) \wedge -Ne' < y_i < -Ne \\ & \wedge -N(e+1) \leq y_i \leq N(-e'+1) \\ & \wedge \exists u(Z(u) \wedge E_i'[\frac{(1-Nv_0)y_i}{M} + Nu] \\ & \wedge D_i[\frac{(1-Nv_0)y_i}{M} + Nu, Mu - v_0 y_i])) \end{aligned}$$

$a_i < 0$ の場合

$$\begin{aligned} & E_i \wedge \exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge \mathop{\mathcal{V}}_{a_i y_i + e_i}^{a_i' y_i + e_i'} uD_i[y_i, u]) \\ \equiv\ & E_i \wedge \ \exists y_i(Z(y_i) \wedge -Ne < y_i < -Ne' \\ & \wedge N(-e'+1) \leq y_i \leq -N(e+1) \end{aligned}$$

$$\wedge \exists u(Z(u) \wedge E_i'[\frac{(1-Nv_0)y_i}{M} + Nu] \wedge$$
$$D_i[\frac{(1-Nv_0)y_i}{M} + Nu, Mu - v_0 y_i]))$$

である。内側の $\exists u(\cdots)$ の部分は帰納法の仮定により手続きCによって拡大 v 式にできる。外側の $\exists y(\cdots)$ は $-Ne' < y < N(-e'+1)$、$N(-e'+1) < y < -Ne'$ より補題3.6より、$vy(\cdots)$ という形の式の論理和に出来る。さらにこの $vy(\cdots)$ の部分はEXによって拡大 v 式にする事が出来る。

(c) $a_i \neq a_i'$ の場合

$0 < a_i < a_i'$ の場合のみ示すがこれ以外も同様である。$a_i y_i + e_i = a_i' y_i + e_i', a_i y_i + e_i + 2 = a_i' y_i + e_i'$ の解をそれぞれ c_0, c_2 とすると

$$\begin{aligned}
& E_i \wedge \exists y_i(Z(y_i) \wedge E_i'[y_i] \wedge \overset{a_i' y_i + e_i'}{\underset{a_i y_i + e_i}{\mathcal{U}}} u D_i[y_i, u]) \\
\equiv\ & E_i \wedge\ \exists u(Z(u) \wedge \exists y_i(Z(y_i) \wedge a_i y_i + e_i < u < a_i' y_i + e_i' \\
& \qquad \wedge a_i' y_i + e_i' - 1 \leq u \leq a_i y_i + e_i + 1 \\
& \qquad\qquad \wedge E_i'[y_i] \wedge D_i[y_i, u])) \\
\equiv\ & E_i \wedge\ \exists u(Z(u) \wedge c_0 < u \leq c_2 \wedge \\
& \qquad \exists y_i(Z(y_i) \wedge a_i y_i + e_i < u < a_i' y_i + e_i' \\
& \qquad\quad \wedge a_i' y_i + e_i' - 1 \leq u \leq a_i y_i + e_i + 1 \qquad (4) \\
& \qquad\qquad \wedge E_i'[y_i] \wedge D_i[y_i, u]))
\end{aligned}$$

帰納法の仮定より、

$$\begin{aligned}
& \exists y_i(Z(y_i) \wedge a_i y_i + e_i < u < a_i' y_i + e_i' \\
& \quad \wedge\ a_i' y_i + e_i' - 1 \leq u \leq a_i y_i + e_i + 1 \wedge E_i'[y_i] \wedge D_i[y_i, u]))
\end{aligned}$$

は拡大 v 式に直せる。また、$c_2 - c_0$ は定数であるから補題3.6及び手続きNFにより、式(4)も拡大 v 式にすることが出来る。

□

手続きIN 仕様 $\neg \mathcal{U}_s^t uA[u]$ を $\neg$ の出現しない拡大 v 式にする。

証明 まず、

$$\begin{aligned}
& \neg \overset{t}{\underset{s}{\mathcal{U}}} uA[u] \\
& \quad \equiv\ \exists x(Z(x) \wedge s+1 < x < t) \qquad (5) \\
& \qquad \vee \overset{t}{\underset{s}{\mathcal{U}}} u \neg A \qquad (6) \\
& \qquad \vee \neg \exists x(Z(x) \wedge s < x < t) \qquad (7)
\end{aligned}$$

を示す。

1. 十分性

$\neg \mho_s^t uA[u]$ と、(5)(7) それぞれの否定を仮定し、(6) を導けば良い。

$$\exists u(Z(u) \wedge s < u < t) \equiv \exists u(Z(u) \wedge s < u < t \wedge t-1 \leq u)$$

である。また、(5) の否定と $\exists u(Z(u) \wedge s < u \leq s+1)$ より $\exists u(Z(u) \wedge s < u < t \wedge t-1 \leq u \leq s+1)$ である。よって、存在するものを u_0 とする。これはただ一つだけ存在する。しかし、$\neg \mho_s^t uA[u]$ より $\neg A[u_0]$。よって $\mho_s^t u \neg A$ を得る。

2. 必要性

左向きは、式 (5),(6),(7) それぞれと $\mho_s^t uA$ を仮定して矛盾を導けば良い。

υ 記号の定義より、

$$\begin{aligned} &\overset{t}{\underset{s}{\mho}} uA \\ &\quad \equiv \quad \exists u(Z(u) \wedge s < u < t \wedge t-1 \leq u \leq s+1 \wedge A[u]) \end{aligned}$$

である。$\mho_s^t uA$ を仮定すると、式 (5) と (7) は式

$$Z(u) \wedge s < u < t \wedge t-1 \leq u \leq s+1$$

と矛盾する。

また、式 (6) と $\mho_s^t uA$ を仮定して矛盾するのは明らかである。

よって、式 (5)、(6)、(7) それぞれが拡大 υ 式にできれば良いことになる。(5) については手続き C の証明より明らかであり、(IN-2(a)) υ 記号の数の上の帰納法を用いると、(6) については明らかである。(IN-2(b)) 変数が s, t に現れない場合は (IN-1) 式 (7) は真偽が定まる。よって、s, t に変数が現れる場合について、式 (7) と同値な拡大 υ 式を得れば良い。

s, t に変数が出現すると仮定したので、$s = ay + e, t = a'y + e'$ とおける。

0、a、a' の大小関係による場合分け。$0 < a < a'$ のとき $s = t, s+1 = t$ を y について解いた解をそれぞれ c_0, c_1 とし、$s = x, t = x$ を y について解いた解をそれぞれ $s^{-1}[x], t^{-1}[x]$ とする。

$$\begin{aligned} &\neg \exists x(Z(x) \wedge s < x < t) \equiv \\ &\quad y < c_0 \vee \exists x(Z(x) \wedge s[c_0] < x \leq t[c_1] \wedge s^{-1}[x-1] \leq y \leq t^{-1}[x]) \end{aligned}$$

これが、拡大 υ 式にできるのは手続き C の証明より明らか。

$0 < a = a'$ の場合。

$$\begin{aligned} &\neg \exists x(Z(x) \wedge s < x < t) \equiv \\ &\quad e' \leq e \vee e < e' \wedge \exists x(Z(x) \wedge ay + e' \leq x \leq ay + e + 1) \end{aligned}$$

これも同様に拡大 υ 式に直せる。他の場合も同様である。□

手続き M 仕様 任意の有理 Presburger 算術の式を拡大 v 式に変換し、停止する。

証明 M-2 以下で $\exists$ が一つしか現れない式が拡大 v 式に変形できれば、全体として式を拡大 v 式に変形して止まることは、$\exists$ 記号の数の上の帰納法を用いれば明らか。よって、M-2 〜 M-7 でそれを証明する。

M-2、M-3 の手続きはよく知られた論理的同値変形である。M-6 において

$$\neg\exists x(A_1 \vee \cdots \vee A_n) \equiv \neg\exists x_1 A_1 \wedge \cdots \wedge \neg\exists x A_n$$

であり、

$$\begin{aligned}
\neg\exists x_i A_i &\equiv \neg C_i \vee \neg\exists x_i B[x_i] \\
&\quad (\exists x_i B[x_i] \text{に手続き C を施した結果を} D_{i1} \vee \cdots \vee D_{im} \text{とすると} \\
&\equiv \neg C_i \vee \neg(D_{i1} \vee \cdots \vee D_{im}) \\
&\quad C_i, D_{i1}, \ldots, D_{im} \text{の} \neg \text{を内側に移動し、} \\
&\quad \text{手続き IN を施した結果をそれぞれ} E_{i0}, \ldots, E_{im} \text{とすると} \\
&\equiv E_{i0} \vee E_{i1} \wedge \cdots \wedge E_{im}
\end{aligned}$$

でありこれらの論理積は NF の結果より拡大 v 式に変換できる。

M-7 も手続き C の結果より上と同様に

$$\begin{aligned}
\exists x_i A_i &\equiv C_i \wedge \exists x_i B_i \\
&\equiv C_i \wedge (D_{i1} \vee \cdots \vee D_{im_i}) \\
&\equiv C_i \wedge D_{i1} \vee \cdots \vee C_i \wedge D_{im_i}
\end{aligned}$$

より明らか。□

3.6 有理 Presburger 算術の決定アルゴリズムの NU 解釈系への応用

有理 Presburger 算術の決定アルゴリズムを NU 解釈系へ応用した解釈アルゴリズムを述べる。

3.6.1 値の対応と値の決定列

解釈アルゴリズムを述べる前にアルゴリズムの記述に必要な概念である値の対応、値の決定列などを定義する。

定義 3.2 変数の対応

質変数と項の組、及び質変数と、項の三つの集合の組の集合

$$\begin{aligned}
&\{\langle \nu x_1, t_1\rangle, \ldots, \langle \nu x_n, t_n\rangle, \\
&\quad \langle \nu x_{n+1}, S_{11}, S_{12}, S_{13}\rangle, \ldots, \langle \nu x_{n+m}, S_{m1}, S_{m2}, S_{m3}\rangle\}
\end{aligned}$$

を変数の対応と呼ぶ。

質変数と項の三つの集合の組 $\langle \nu x_i, S_{i1}, S_{i2}, S_{i3}\rangle$ の、項の三つの集合はそれぞれ質変数のとるべき値を次のように制限するものである。S_{i1} は質変数 νx_i の値の下界、S_{j2} は値の上界を表し、S_{i3} は非整数値であるべき $(\neg Z(t_j[\nu x_i])$

と現れた）項の集合を表す。

定義 3.3 変数の対応への代入

変数の対応 ρ と変数 x、項 t に対し $\rho\{t/x\}$ で変数の対応の元それぞれの項、及び項の集合中の項に出現する変数 x に項 t を代入して得られる新しい変数の対応を表すとする。つまり、

$$\begin{aligned}\rho \;=\; & \{\langle \nu x_1, t_1[x]\rangle, \ldots, \langle \nu x_n, t_n[x]\rangle, \\ & \langle \nu x_{n+1}, S_{11}[x], S_{12}[x], S_{13}[x]\rangle, \ldots, \langle \nu x_{n+m}, S_{m1}[x], S_{m2}[x], S_{m3}[x]\rangle\}\end{aligned}$$

であるとき、（ここで S が項の集合であるとき $S[x]$ で集合 S 中の各項の変数 x の出現を表す。また、以下のアルゴリズムでは $\langle \nu x, a\rangle$ が変数の対応にある場合 $\rho\{b/\nu x\}$ というような代入は行われない）

$$\begin{aligned}\rho\{s/x\} \;=\; & \{\langle \nu x_1, t_1[s]\rangle, \ldots, \langle \nu x_n, t_n[s]\rangle, \\ & \langle \nu x_{n+1}, S_{11}[s], S_{12}[s], S_{13}[s]\rangle, \ldots, \langle \nu x_{n+m}, S_{m1}[s], S_{m2}[s], S_{m3}[s]\rangle\}\end{aligned}$$

次に定義する値の決定列は、最終的に質変数のとるべき値の制限に自由度がある場合の値の決め方に関するものである。この場合の値の決め方は本来の解釈の定義では適当でよく、かつ非決定的でなければならないのだが、解釈系の解釈としては以下のように定める。

定義 3.4 値の決定列

変数の対応中の元で、束縛変数が現れず質変数と項の三つの集合の組になっているもの $\langle \nu x, S_1, S_2, S_3\rangle$ に対して（ここで S_1, S_2 の元は定数、S_3 の元は変数を一つだけ含む項である）質変数 νx の値の決定列 $a_0, a_1, \ldots$ を以下のように定義する。S_1 の元の最大値を L、S_2 の元の最小値を H とする。S_3 中の項の変数の係数の分子の最小公倍数に 1 を加えたものを M とする。$(0 \leq i)$

$S_3 \neq \phi$ の場合

$$a_0 = \begin{cases} L + 1/M & S_2 \text{が空の場合} \\ H - 1/M & S_1 \text{が空の場合} \\ 0 & S_1, S_2 \text{ともに空の場合} \\ (L+H)/2 & \text{その他} \end{cases}$$

$$a_{i+1} = \begin{cases} a_i + 1/M & S_2 \text{が空の場合} \\ a_i - 1/M & S_1 \text{が空の場合} \\ a_i + (-1)^i \times \lfloor i/2 \rfloor \times 1/2 & S_1\text{、}S_2 \text{ともに空の場合} \\ (L + a_i)/2 & S_1\text{、}S_2 \text{空でなく、}i\text{が奇数の時} \\ (H + a_i)/2 & S_1\text{、}S_2 \text{空でなく、}i\text{が偶数の時} \end{cases}$$

$S_3 = \phi$ の場合（このとき決定列は定数の列となる）

$$a_i = \frac{L+H}{2}$$

定義 3.5 部分論理式の出現

論理式 A 中の部分論理式 B の出現の一つだけを $A[B]$ で表す。このとき $A[B]$ に対して変数 x が B で自由で $A[B]$ では束縛されていても、$A[C[x]]$ という置き換えを許すことにする。もちろん $B[x] \equiv C[x]$ ならば $A[B[x]] \equiv A[C[x]]$ である。

3.6.2 解釈アルゴリズム

以下で簡単化と言うのは手続き S の 1,2,4,5,6 の操作である。

ν 行為 $A[\underline{x}, \nu\underline{x}]$（ここで、式 $A[\underline{x}, \underline{y}]$ は有理 Presburger 算術の式）が与えられたとする。

1. 質変数 $\nu\underline{x}$ に対して新しい束縛変数 $\underline{y}$ をつくる。
   そして、これらから変数の対応

$$\rho = \{\langle \nu x_1, y_1 \rangle, \ldots, \langle \nu x_n, y_n \rangle\}$$

   を作る。
2. 式 $A[\underline{x}, \underline{y}]$ を拡大 υ 式 $B[\underline{y}]$ に変換する。
   このとき拡大 υ 式の定義より明らかに $B[\underline{y}]$ には $\neg Z$ 以外の $\neg$ は現れない。
3. 以上で得られた拡大 υ 式 $B[\underline{y}]$ と変数の対応 ρ に対して、式と変数の組の集合 $S = \{\langle \exists \underline{y} B[\underline{y}], \rho \rangle\}, S' = \phi$ に対して以下の手続きを施す。
   ここで S' が空でないときは与えられた ν 行為の部分式を解釈中であることを表し、このとき S' には部分式の解釈結果が入る。

(a) $S = \phi$ のとき。
- $S' = \phi$ であれば手続きは終了し、解釈結果は ' 行動不能 ' となる。
- $S' \neq \phi$ のとき。S' を結果として返す。

(b) S から元 $\langle A_i, \rho_i \rangle$ を一つ選ぶ。

i. A_i が閉じた拡大 υ 節の場合。
- $S' = \phi$ であるとき外側から変数の値を決定していく。この時その値を式に代入すると共に、変数の対応（これは集合であるから）の元それぞれにも代入する。
  その結果
  - 式が $\perp$ のとき、この元を S から取り除く。
  - 式が $\top$ のとき、変数の対応を簡単化する。変数の対応中の元が全て、質変数と項の組になっていればそれが解釈結果である。
    質変数と項の三つの集合の組がある場合。質変数の値の決ったものを次々代入していき、二番目、三番目の集合中に束縛変数のなくなったものに対してその値を決定する。その値の決定の仕方は次のとおりである。

    A. 値の決定列の要素を順に四番目の集合の各元の変数に代入し簡単化する。

    B. この集合の全ての元が整数でなくなる要素のうち一番最初のものを対応する質変数の値とする。
- $S' \neq \phi$ のとき。この元を S から取り除き S' に加える。

ii. A_i が閉じた拡大 v 節でない場合

A_i の一番内側の存在記号に着目する。以下でその部分を $\exists x B$ とし、($A_i \equiv A_i[\exists x B]$) 選んだ $\langle A_i, \rho \rangle$ を S から取り除き、B の形による場合分けで以下の操作を行った後、3b へ。S' は変化しない。(上から順に条件を確かめていくとする)

- B 中に $\vee$ があるとき。B に手続き NF を施す。その結果を $C_1 \vee \cdots \vee C_n$ とする。$\langle A_i[\exists x C_1], \rho \rangle, \ldots, \langle A_i[\exists x C_n], \rho \rangle$ を S に加える。
- B に x が出現しない不等式、等式、Z の式、$\neg Z$ の式がある場合
  それらの論理積を C とし、B の残りの部分の論理積を $D[x]$ とする。$\langle C \wedge \exists x D[x], \rho \rangle$ を S に加える。
- B 中に等式がある場合
  その等式を x について解いた結果を $x = t$ とし、$B \equiv x = t \wedge C[x]$ とする。$C[t]$ を簡単化した結果を C' とする。

  A. $C' \equiv \top$ の場合
  $A_i[\top]$ を簡単化したものを A' とする。$\langle A', \rho\{t/x\} \rangle$ を S に加える。

  B. $C' \equiv \bot$ の場合
  S には何も加えない。

  C. 上のどちらでもない場合
  $\langle A_i[\exists x C'], \rho\{t/x\} \rangle$ を S に加える。
- B 中に基本 v 式でない $\mathcal{V}_s^t uC$ という式が存在する場合
  B を $B \equiv D \wedge \mathcal{V}_s^t uC$ となるように変形し、(u の現れる部分 C と現れない部分 D に分ける) $C \equiv Z(t_1) \wedge \ldots \wedge Z(t_n) \wedge E$ とする。(E には Z の式は現れない) $Z(t_1), \ldots, Z(t_n)$ と $Z(u)$ に手続き EZ を施した結果を $Z(t'_1), \ldots, Z(t'_n), Z(au+e)$ とする。$\langle A_i[\exists x(D \wedge Z(t'_1) \wedge \ldots \wedge Z(t'_n) \wedge \mathcal{V}_{as+e}^{at+e} u' E[\frac{u'-e}{a}])], \rho\{\frac{u'-e}{a}/u\} \rangle$ を S に加える。
- B 中に基本 v 式が複数ある場合
  $B \equiv C \wedge \mathcal{V}_s^t uD \wedge E$ とする。ここで C は Z の式、不等式、$\neg Z$ の式の論理積であり、E は基本 v 式の論理積である。$\langle A_i[\exists x(C \wedge \mathcal{V}_s^t u(D \wedge E))], \rho \rangle$ を S に加える。
- $B \equiv C \wedge D[x]$ で C は Z の式の論理積であり、$D[x]$ は不等式、$\neg Z$ の式、基本 v 式の論理積である場合
  C に手続き EZ を施した結果を $C' \wedge Z(ax+b)$ とする。$\langle A_i[C' \wedge \exists y(Z(y) \wedge D[\frac{y-b}{a}])], \rho\{\frac{y-b}{a}/x\} \rangle$ を S に加える。
- $B \equiv Z(x) \wedge C[x] \wedge D[x]$ で $C[x]$ は $\neg Z$ の式の論理積であり、$D[x]$ は不等式、基本 v 式の論理積である場合
  $C[x]$ の各 $\neg Z$ の式の x の係数の分母の最小公倍数を M とする。次の操作を $j = 0$ から $j = M - 1$ まで繰り返す。$C[j]$ を簡単化し、その結果 F' が

  A. $\top$ のとき

$\langle A_i[\exists y(Z(y) \wedge D[My+j])], \rho\{My+j/x\}\rangle$ を S に加える。

B. $\perp$ のとき

S には何も加えない。

C. $\top, \perp$ いずれでもないとき

$\langle A_i[F' \wedge \exists y(Z(y) \wedge D[My+j])], \rho\{My+j/x\}\rangle$ を S に加える。

- $B \equiv Z(x) \wedge C[x]$ $C[x]$ は不等式の論理積である場合

C を x について解いて $l_1 < x, \ldots, l_n < x$、 $x < h_1, \ldots, x < h_m$ とする。

A. l_j または h_k がない場合

$A_i[\top]$ を簡単化し、その結果が $\perp$ のときは S に何も加えない

簡単化の結果が $\perp$ 以外の A' のとき

ρ の元に $\langle \nu y, x\rangle$ という組がある場合 ρ の $\langle \nu y, x\rangle$ という組を $\langle \nu y, \{l_1, \ldots, l_n\}, \{h_1, \ldots, h_m\}, \phi\rangle$ で置き換えた変数の対応を ρ' とする。 ($\{l_1, \ldots, l_n\}$、 $\{h_1, \ldots, h_m\}$ のどちらかが空である筈) S に $\langle A', \rho'\rangle$ を加える。

ρ の元に $\langle \nu y, x\rangle$ という組がない場合新しい質変数 νy を作り

$$\langle \nu y, \{l_1, \ldots, l_n\}, \{h_1, \ldots, h_m\}, \phi\rangle$$

を $\rho\{\nu y/x\}$ に加えたものを ρ' とし、 S に $\langle A', \rho'\rangle$ を加える。

B. $1 \leq j \leq n, 1 \leq k \leq m$ に対して

$$L_j \equiv \bigwedge_{1 \leq q \leq n, q \neq j} l_q \leq l_j, H_k \equiv \bigwedge_{1 \leq p \leq m, p \neq k} h_k \leq h_p$$

とする。

$$\langle A_i[L_j \wedge H_k \wedge 1 < h_k - l_j], \rho'_k\rangle,$$
$$\langle A_i[L_j \wedge H_k \wedge h_k - l_j = 1 \wedge \neg Z(l_j)], \rho'_k\rangle,$$
$$\langle A_i[\mathop{\mathcal{O}}_{l_j}^{h_k} x(L_j \wedge H_k \wedge h_k - l_j < 1)], \rho'_k\rangle$$

を S に加える。ここで ρ'_k は ρ の元に $\langle \nu y, x\rangle$ という組がある場合 ρ の $\langle \nu y, x\rangle$ という組を $\langle \nu y, \lfloor h_k \rfloor\rangle$ で置き換えた変数の対応であり、 $\langle \nu y, x\rangle$ という組がない場合新しい質変数 νy を作り

$$\langle \nu y, \lfloor h_k \rfloor\rangle$$

を $\rho\{\nu y/x\}$ に加えたものである。また、 $\lfloor t \rfloor$ は t を越えない最大の整数を表す。

- $B \equiv D[x] \wedge C[x]$ で $C[x]$ は不等式の論理積、 $D[x]$ は $\neg Z$ の式の論理積である場合

C を x について解いて $l_1 < x, \ldots, l_n < x$、 $x < h_1, \ldots, x < h_m$ とし、 D に含まれる $\neg Z$ の式中の項を集めたものを T とする。

A. l_j または h_k がない場合

$A_i[\top]$ を簡単化し、その結果が $\perp$ のときは S に何も加えない

簡単化の結果が $\perp$ 以外の A' のとき
○ρ の元に $\langle \nu y, x\rangle$ という組がある場合
ρ の $\langle \nu y, x\rangle$ という組を $\langle \nu y, \{l_1, \ldots, l_n\}, \{h_1, \ldots, h_m\}, T\rangle$ で置き換えた変数の対応を ρ' とする。S に $\langle A', \rho'\rangle$ を加える。
○ そのような元がない場合
新しい質変数 νy を作り

$$\langle \nu y, \{l_1, \ldots, l_n\}, \{h_1, \ldots, h_m\}, T\rangle$$

を $\rho\{\nu y/x\}$ に加えたものを ρ' とし、S に $\langle A', \rho'\rangle$ を加える。

B. 両方ある場合 $1 \leq j \leq n, 1 \leq k \leq m$ に対して

$$\langle A_i[\bigwedge_{1\leq j\leq n, 1\leq k\leq m} l_j < h_k], \rho'\rangle$$

を S に加える。ここで ρ' は ρ の元に $\langle \nu y, x\rangle$ という組がある場合 ρ の $\langle \nu y, x\rangle$ という組を $\langle \nu y, \{l_1, \ldots, l_n\}, \{h_1, \ldots, h_m\}, T\rangle$ で置き換えた変数の対応であり、そのような元がない場合新しい質変数 νy を作り

$$\langle \nu y, \{l_1, \ldots, l_n\}, \{h_1, \ldots, h_m\}, T\rangle$$

を $\rho\{\nu y/x\}$ に加えたものである。

- $B \equiv Z(x) \wedge C[x] \wedge \mathcal{V}_s^t\, uD[x, u]$ で $C[x]$ は不等式の論理積である場合

A. s, t 両方に x が現れないとき
$\{\langle \exists x(Z(x) \wedge C[x] \wedge D[x]), \rho\rangle\}$ にこの手続きを施す。この結果を $\{\langle E_1, \rho_1\rangle, \ldots, \langle E_n, \rho_n\rangle\}$ とする。S を S と

$$\{\langle A_i[\overset{t}{\underset{s}{\mathcal{V}}} uE_1], \rho_1\rangle, \ldots, \langle A_i[\overset{t}{\underset{s}{\mathcal{V}}} uE_n], \rho_n\rangle\}$$

の和集合とする。

B. s, t 中の x の係数が等しい場合
- x の係数の分母、分子を N, M とする。（ただし、N, M は互い素な整数で、M は正）$Mv + Nu = 1$ の整数解の組の一つを v_0, u_0 とする。（ただし、$[v_0] \leq [N/2]$）
- 現在の S, S' を保存し、$S = \{\langle \exists u(Z(y) \wedge C[\frac{(1-Nv_0)w}{M} + Ny] \wedge D[\frac{(1-Nv_0)w}{M} + Ny, My - v_0w]), (\rho\{(\frac{w}{M} - \frac{u}{a})/x\})\{(My - v_0w)/u\}\rangle\}, S' = \{\langle \perp, \phi\rangle\}$ としてこの手続きを施す。この結果から $\langle \perp, \phi\rangle$ を除いたものを $\{\langle F_1[w], \rho_1'\rangle, \ldots, \langle F_l[w], \rho_l'\rangle\}$ とする。
- a の正負各々の場合に対応してそれぞれ以下のものを、保存しておいた S に加える。また、S' を保存しておいた S' に戻す。
$0 < a$ のとき

$$\langle A_i[\overset{-Ne'+1}{\underset{-Ne'}{\mathcal{V}}} w(-N(e+1) < w < -Ne \wedge F_1)], \rho_1'\rangle,$$

$$\vdots$$

$$\langle A_i[\overset{-Ne'+1}{\underset{-Ne'}{\mathcal{U}}} w(-N(e+1) < w < -Ne \wedge F_l)], \rho_l' \rangle,$$
$$\langle A_i[\overset{-Ne'+2}{\underset{-Ne'+1}{\mathcal{U}}} w(-N(e+1) < w < -Ne \wedge F_1)], \rho_1' \rangle,$$
$$\vdots$$
$$\langle A_i[\overset{-Ne'+2}{\underset{-Ne'+1}{\mathcal{U}}} w(-N(e+1) < w < -Ne \wedge F_l)], \rho_l' \rangle,$$
$$\vdots$$
$$\vdots$$
$$\langle A_i[\overset{-Ne'+N}{\underset{-Ne'+N-1}{\mathcal{U}}} w(-N(e+1) < w < -Ne \wedge F_1)], \rho_1' \rangle,$$
$$\vdots$$
$$\langle A_i[\overset{-Ne'+N}{\underset{-Ne'+N-1}{\mathcal{U}}} w(-N(e+1) < w < -Ne \wedge F_l)], \rho_l' \rangle,$$
$$\langle A_i[Z(Ne') \wedge -N(e+1) < -Ne'+1 < -Ne \wedge F_1[-Ne'+1]], \rho_1' \rangle,$$
$$\vdots$$
$$\langle A_i[Z(Ne') \wedge -N(e+1) < -Ne'+1 < -Ne \wedge F_l[-Ne'+1]], \rho_l' \rangle,$$
$$\vdots$$
$$\vdots$$
$$\langle A_i[Z(Ne') \wedge -N(e+1) < -Ne'+N < -Ne \wedge F_1[-Ne'+N]], \rho_1' \rangle,$$
$$\vdots$$
$$\langle A_i[Z(Ne') \wedge -N(e+1) < -Ne'+N < -Ne \wedge F_l[-Ne'+N]], \rho_l' \rangle,$$
$$\langle A_i[Z(Ne) \wedge -e' < -e < -e'+1 \wedge F_1[-Ne-1]], \rho_1' \rangle,$$
$$\vdots$$
$$\langle A_i[Z(Ne) \wedge -e' < -e < -e'+1 \wedge F_l[-Ne-1]], \rho_l' \rangle$$

$a < 0$ のとき（M は正より N は負）

$$\langle A_i[\mathcal{U}_{-Ne'+N}^{-Ne'+N+1}\, w(-Ne < w < -N(e+1) \wedge F_1)], \rho_1\rangle,$$
$$\vdots$$
$$\langle A_i[\mathcal{U}_{-Ne'+N}^{-Ne'+N+1}\, w(-Ne < w < -N(e+1) \wedge F_l)], \rho_l\rangle,$$
$$\vdots$$
$$\vdots$$
$$\langle A_i[\mathcal{U}_{-Ne'-1}^{-Ne'}\, w(-Ne < w < -N(e+1) \wedge F_1)], \rho_1\rangle,$$
$$\vdots$$
$$\langle A_i[\mathcal{U}_{-Ne'-1}^{-Ne'}\, w(-Ne < w < -N(e+1) \wedge F_l)], \rho_l\rangle,$$
$$\langle A_i[Z(Ne') \wedge -Ne < -Ne' + N < -N(e+1) \wedge F_1[-Ne' + N]], \rho_1'\rangle$$
$$\vdots$$
$$\langle A_i[Z(Ne') \wedge -Ne < -Ne' + N < -N(e+1) \wedge F_l[-Ne' + N]], \rho_l'\rangle,$$
$$\vdots$$
$$\vdots$$
$$\langle A_i[Z(Ne') \wedge -Ne < -Ne' < -N(e+1) \wedge F_1[-Ne']], \rho_1'\rangle,$$
$$\vdots$$
$$\langle A_i[Z(Ne') \wedge -Ne < -Ne' - 1 < -N(e+1) \wedge F_l[-Ne' - 1]], \rho_l'\rangle,$$
$$\langle A_i[Z(Ne) \wedge -e' < -e < -e' + 1 \wedge F_1[-Ne - 1]], \rho_1'\rangle,$$
$$\vdots$$
$$\langle A_i[Z(Ne) \wedge -e' < -e < -e' + 1 \wedge F_l[-Ne - 1]], \rho_l'\rangle$$

C. $a_i \neq a_i'$ の場合まず、S, S' を保存し、新しく S, S' をそれぞれ

$$\{\langle \exists x(Z(x) \wedge s < u < t \wedge C[x] \wedge D[x]), \rho\rangle\}, \{\langle \bot, \phi\rangle\}$$

としてこの手続きを施す。この結果を

$$\{\langle E_1, \rho_1\rangle, \ldots, \langle E_n, \rho_n\rangle\}$$

とする。ここで E_j は拡大 v 節である。E_j 中の Z の式と $Z(u)$ とに手続き EZ を施した結果を $E_j' \wedge Z(a_j u + e_j)$ とし、E_j から Z の式を除いたものを E_j'' とする。つぎに手続き C と同様に s, t 中の x の係数によって次のように項の列 $t_0, \ldots, t_m$ を定め S を保存しておいた S と

$$\{\langle A_i[E_1' \wedge \overset{a_1 t_1 + e_1}{\underset{a_1 t_0 + e_1}{\mathcal{U}}} u E_1''], \rho_1\rangle, \ldots,$$
$$\langle A_i[E_n' \wedge \overset{a_n t_1 + e_n}{\underset{a_n t_0 + e_n}{\mathcal{U}}} u E_n''], \rho_n\rangle,$$
$$\langle A_i[E_1' \wedge \overset{a_1 t_2 + e_1}{\underset{a_1 t_1 + e_1}{\mathcal{U}}} u E_1''], \rho_1\rangle, \ldots,$$
$$\langle A_i[E_n' \wedge \overset{a_n t_2 + e_n}{\underset{a_n t_1 + e_n}{\mathcal{U}}} u E_n''], \rho_n\rangle,$$

$$\vdots$$

$$\langle A_i[E'_1 \wedge \overset{a_1 t_m + e_1}{\underset{a_1 t_{m-1}+e_1}{\mathcal{U}}} uE''_1], \rho_1\rangle, \ldots,$$

$$\langle A_i[E'_n \wedge \overset{a_n t_m + e_n}{\underset{a_n t_{m-1}+e_n}{\mathcal{U}}} uE''_n], \rho_n\rangle\}$$

の和集合とする。S' を保存しておいた S' にする。

$s = ax+e, t = a'x+e'$ とし、$ax+e = a'x+e', ax+e+2 = a'x+e'$ の解を求めそれぞれを c_0, c_2 とする。以下で $t'_{i+1} = t'_i + 1 (0 \leq i < m-1), t_{m-1} < t_m \leq t_{m-1}+1$ とする。

- $0 < a < a', a' < a < 0$ の場合
  $t_0 = s[c_0], t_m = t[c_2]$
- $a \leq 0 \leq a', a' \leq 0 \leq a$ の場合（共には等号はつかない）
  $t_0 = s[c_2], t_m = t[c_2]$
- $a < a' < 0, 0 < a' < a$ の場合
  $t_0 = s[c_2], t_m = t[c_0]$

以上。

3.7 使用例

上で述べた解釈系アルゴリズムの使用例、上で述べた範囲で表現できる ν 行為の例を示す。

3.7.1 同値の証明

二つのプログラム

プログラム 1

```
if a>b then x:= a
       else x:= b;
```

プログラム 2

```
if a>b or a=b then x:= a
              else x:= b;
```

はどちらも a, b の大きい方の値を x に代入するものである。

この二つのプログラムの同値性は次の式に帰結する。

$$\begin{aligned} &\nu p \\ &\equiv \forall a, b, x((a > b \supset x = a) \wedge (\neg a > b \supset x = b) \\ &\quad \equiv (a \geq b \supset x = a) \wedge (\neg a \geq b \supset x = b)) \end{aligned}$$

ここで変数 p は Boolean 型の変数であり、この値が $\top$ であれば二つのプログラムは同値となる。（厳密にはこの ν 行為は、有理 Presburger 式の範囲を越えているが、その解釈アルゴリズムは本質的には同じ様に動くのでここで示す）

3.7.2 線分の移動

制約論理で行われていることであるが、与えられた線分をいくつかの条件のもとで、それらに優先順位があるときにどのような移動を行うかを考える。[2]

今、平面上の線分の端点の座標が $(x_0, y_0), (x_1, y_1)$ であったとする。条件

1. 直線 $ax + by + c = 0$ に関して対称移動
2. 原点に対称移動
3. 直線 $a'x + b'y + c' = 0$ に関して平行移動
4. 片方の端点を保存

はそれぞれ

1.

$$\begin{aligned} & a\frac{\nu x_0 + x_0}{2} + b\frac{\nu y_0 + y_0}{2} + c = 0 \\ \wedge\ & b(\nu x_0 - x_0) + a(\nu y_0 - y_0) = 0 \\ \wedge\ & a\frac{\nu x_1 + x_1}{2} + b\frac{\nu y_1 + y_1}{2} + c = 0 \\ \wedge\ & b(\nu x_1 - x_1) + a(\nu y_1 - y_1) = 0 \end{aligned}$$

2.

$$\nu x_0 + x_0 = 0 \wedge \nu y_0 + y_0 = 0 \wedge \nu x_1 + x_1 = 0 \wedge \nu y_1 + y_1 = 0$$

3.

$$b'(\nu y_1 - \nu y_0) = a'(\nu x_1 - \nu x_0) \vee b'(\nu y_1 - \nu y_0) = a'(\nu x_0 - \nu x_1)$$

4.

$$\nu x_0 = x_0 \wedge \nu y_0 = y_0 \vee \nu x_1 = x_1 \wedge \nu y_1 = y_1$$

と表現できる。

そして優先条件は次のように表せる。例えば三つの条件を ν 行為で表すと $A[\underline{x}, \nu\underline{x}], B[\underline{x}, \nu\underline{x}], C[\underline{x}, \nu\underline{x}]$ となるとする。

$$\begin{aligned} \Gamma \equiv\ & \neg\exists\underline{y}(A[\underline{x}, \underline{y}] \wedge B[\underline{x}, \underline{y}] \wedge C[\underline{x}, \underline{y}]) \\ \Gamma_0 \equiv\ & \Gamma \wedge \neg\exists\underline{y}(A[\underline{x}, \underline{y}] \wedge B[\underline{x}, \underline{y}]) \wedge \neg\exists\underline{y}(B[\underline{x}, \underline{y}] \wedge C[\underline{x}, \underline{y}]) \wedge \neg\exists\underline{y}(C[\underline{x}, \underline{y}] \wedge A[\underline{x}, \underline{y}]) \end{aligned}$$

と置くとき、最も多くの条件を満たすように動かすという ν 行為は次のように表現できる。

$$\begin{aligned} & A[\underline{x}, \nu\underline{x}] \wedge B[\underline{x}, \nu\underline{x}] \wedge C[\underline{x}, \nu\underline{x}]) \\ \vee\ & \Gamma \wedge A[\underline{x}, \nu\underline{x}] \wedge B[\underline{x}, \nu\underline{x}]) \\ \vee\ & \Gamma \wedge B[\underline{x}, \nu\underline{x}] \wedge C[\underline{x}, \nu\underline{x}]) \\ \vee\ & \Gamma \wedge C[\underline{x}, \nu\underline{x}] \wedge A[\underline{x}, \nu\underline{x}]) \\ \vee\ & \Gamma_0 \wedge A[\underline{x}, \nu\underline{x}] \end{aligned}$$

$$\vee \quad \Gamma_0 \wedge B[\underline{x}, \nu\underline{x}]$$

$$\vee \quad \Gamma_0 \wedge C[\underline{x}, \nu\underline{x}]$$

4　高階の変数の解釈アルゴリズム

2節で述べたように従来の解釈系は高階の束縛変数を扱っていず、高階の質変数の値も有限集合となっていた。

本節ではこれらの制限をやや解消出来たのでそれについて述べる。

4.1　高階の量記号の消去

新しいアルゴリズムでは、次の定理、及びその系に示されるように高階の量記号の部分を、高階の量記号の現れないそれと同値な式で置き換える。

補題 4.1　φ を高階の束縛変数とし、A_i, E_j, C を $(1 \leq i, j \leq n)$ を φ の出現しない論理式とする。

$$\begin{aligned}
&\exists\varphi(\forall\underline{x_1}(A_1[\underline{x_1}] \supset \exists\underline{y_1}(E_1[\underline{x_1}, \underline{y_1}] \wedge \forall\underline{x_2}(A_2[\underline{x_1}, \underline{y_1}, \underline{x_2}] \\
&\quad \supset \exists\underline{y_2}(E_2[\underline{x_1}, \underline{y_1}, \underline{x_2}, \underline{y_2}] \wedge \forall\underline{x_3}(A_3[\underline{x_1}, \ldots, \underline{x_3}] \\
&\quad \supset \cdots \supset \exists\underline{y_n}(E_n[\underline{x_1}, \ldots, \underline{y_n}] \wedge \varphi(\underline{y_n}))\cdots)))) \\
&\wedge \quad \forall\underline{x}(C[\underline{x}] \supset \neg\varphi(\underline{x})))
\end{aligned}$$

と

$$\begin{aligned}
&\forall\underline{x_1}(A_1[\underline{x_1}] \supset \exists\underline{y_1}(E_1[\underline{x_1}, \underline{y_1}] \\
&\quad \wedge \forall\underline{x_2}(A_2[\underline{x_1}, \underline{y_1}, \underline{x_2}] \supset \cdots \supset \exists\underline{y_n}(E_n[\underline{x_1}, \ldots, \underline{y_n}] \wedge \neg C[\underline{y_n}])\cdots))
\end{aligned}$$

は同値である。

証明

$n = 1$ の場合を示すが、それ以上の場合も同様である。（添え字を省く。）

1. 上式から下式を導く。

$$\forall\underline{x}(A[\underline{x}] \supset \exists\underline{y}(E[\underline{x}, \underline{y}] \wedge V(\underline{y}))) \tag{8}$$

と

$$\forall\underline{x}(C[\underline{x}] \supset \neg V(\underline{x})) \tag{9}$$

を仮定する。

(8) より、

$$A[\underline{a}] \supset \exists\underline{y}(E[\underline{a}, \underline{y}] \wedge V(\underline{y}))。$$

ここで

$$A[\underline{a}] \tag{10}$$

を仮定すると

$$\exists\underline{y}(E[\underline{a}, \underline{y}] \wedge V(\underline{y})) \tag{11}$$

を得るので、

$$E[\underline{a}, \underline{b}] \wedge V(\underline{b}) \tag{12}$$

を仮定する。また (9) より

$$V(\underline{a}) \supset \neg C[\underline{a}]$$

であるから先ほどの仮定より、

$$E[\underline{a}, \underline{b}] \wedge \neg C[\underline{a}]$$

$\exists$ を導入し、

$$\exists \underline{y}(E[\underline{a}, \underline{y}] \wedge \neg C[\underline{a}])$$

よって、(11) より (12) の仮定を消去できる。$\supset$ の導入により仮定 (10) を消去し、

$$A[\underline{a}] \supset \exists \underline{y}(E[\underline{a}, \underline{y}] \wedge \neg C[\underline{a}])$$

最後に $\forall$ を導入して結論を得る。

2. 下式より上式

下式

$$\forall \underline{x}(A[\underline{x}] \supset \exists \underline{y} E[\underline{x}, \underline{y}] \wedge \neg C[\underline{y}])$$

とおく。これより明らかに

$$\forall \underline{x}(A[\underline{x}] \supset \exists \underline{y} E[\underline{x}, \underline{y}] \wedge (\{\underline{w}\}\neg C[\underline{w}])(\underline{y}))$$

また、明らかに $\forall \underline{x}(C[\underline{x}] \supset \neg\neg C[\underline{x}]$ であるから

$$\forall \underline{x}(C[\underline{x}] \supset \neg(\{\underline{w}\}\neg C[\underline{w}])(\underline{x}))$$

これらから上式を得る。

□

また、この補題 4.1で

$$E_n \equiv \bigwedge_i^p B_i$$

とおけば以下の補題が導かれる。ここで

$$B_i \equiv \begin{cases} x_{ni} = y_{ni} & y_{ni}\text{の型が } 0 \text{ のとき} \\ \forall \underline{\eta}(x_{ni}(\underline{\eta}) \equiv y_{ni}(\underline{\eta})) & \text{その他} \end{cases}$$

とする。

補題 4.2 φ を高階の束縛変数とし、A_i, E_j, C $(1 \leq i \leq n, 1 \leq j \leq n-1)$ を φ が出現しない論理式とする。

$$\begin{aligned} &\exists \varphi(\forall \underline{x_1}(A_1[\underline{x_1}] \supset \exists \underline{y_1}(E_1[\underline{x_1}, \underline{y_1}] \wedge \forall \underline{x_2}(A_2[\underline{x_1}, \underline{y_1}, \underline{x_2}] \\ &\qquad \supset \exists \underline{y_2}(E_2[\underline{x_1}, \underline{y_1}, \underline{x_2}, \underline{y_2}] \wedge \cdots \wedge \forall \underline{x_n}(A_n[\underline{x_1}, \ldots, \underline{y_{n-1}}, \underline{x_n}] \supset \varphi(\underline{x_n}))\cdots))) \\ &\wedge \quad \forall \underline{x}(C[\underline{x}] \supset \neg\varphi(\underline{x}))) \end{aligned}$$

と

$$\forall \underline{x_1}(A_1[\underline{x_1}] \supset \exists \underline{y_1}(E_1[\underline{x_1}, \underline{y_1}]$$

$$\wedge \cdots \wedge \neg\exists \underline{x_n}(A_2[\underline{x_1}, \ldots, \underline{y_{n-1}}, \underline{x_n}] \wedge C[\underline{x_n}]) \cdots))$$

は同値である。

補題 4.3 φ を型 $[\tau_1, \cdots, \tau_p]$ の束縛変数とする。

$$\begin{array}{l}
\exists\varphi(\forall \underline{x_{11}}(A_{11}[\underline{x_{11}}] \supset \cdots \supset \exists \underline{y_{1n_1}}(E_{1n_1}[\underline{x_1}, \ldots, \underline{y_{1n_1}}] \wedge \varphi(\underline{y_{1n_1}})) \cdots) \\
\quad \wedge \quad \forall \underline{x_{21}}(A_{21}[\underline{x_{21}}] \supset \cdots \supset \exists \underline{y_{2n_2}}(E_{2n_2}[\underline{x_{21}}, \ldots, \underline{y_{2n_2}}] \wedge \varphi(\underline{y_{2n_2}})) \cdots) \\
\quad \wedge \\
\quad \vdots \\
\quad \wedge \quad \forall \underline{x_{m1}}(A_{m1}[\underline{x_{m1}}] \supset \cdots \supset \exists \underline{y_{mn_m}}(E_{mn_m}[\underline{x_{m1}}, \ldots, \underline{y_{mn_m}}] \wedge \varphi(\underline{y_{mn_m}})) \cdots) \\
\quad \wedge \quad \forall \underline{x_1}(C_1[\underline{x_1}] \supset \neg\varphi(\underline{x_1})) \\
\quad \wedge \\
\quad \vdots \\
\quad \wedge \quad \forall \underline{x_l}(C_l[\underline{x_l}] \supset \neg\varphi(\underline{x_l})))
\end{array}$$

は $\Gamma[\underline{x}] \equiv C_1[\underline{x}] \vee \cdots \vee C_l[\underline{x}]$ とおけば、

$$\begin{array}{l}
\exists\varphi(\forall \underline{x_{11}}(A_{11}[\underline{x_{11}}] \supset \cdots \supset \exists \underline{y_{1n_1}}(E_{1n_1}[\underline{x_1}, \ldots, \underline{y_{1n_1}}] \wedge \neg\Gamma[\underline{y_{1n_1}}]) \cdots) \\
\quad \wedge \quad \forall \underline{x_{21}}(A_{21}[\underline{x_{21}}] \supset \cdots \supset \exists \underline{y_{2n_2}}(E_{2n_2}[\underline{x_{21}}, \ldots, \underline{y_{2n_2}}] \wedge \neg\Gamma[\underline{y_{2n_2}}]) \cdots) \\
\quad \wedge \\
\quad \vdots \\
\quad \wedge \quad \forall \underline{x_{m1}}(A_{m1}[\underline{x_{m1}}] \supset \cdots \supset \exists \underline{y_{mn_m}}(E_{mn_m}[\underline{x_{m1}}, \ldots, \underline{y_{mn_m}}] \wedge \neg\Gamma[\underline{y_{mn_m}}]) \cdots))
\end{array}$$

と同値である。

補題 4.3は $\forall \underline{x}(A[\underline{x}] \vee \exists \underline{y}(E \wedge \cdots \wedge \varphi(\underline{y}')))$ 及び $\forall \underline{x}(C[\underline{x}] \supset \neg\varphi(\underline{x}))$ という形の式が φ の束縛範囲に複数出現してもこの φ を消去できる事を示している。この証明は補題 4.1とほぼ同様なので省略する。

V を高階の変数またはアブストラクトとする。論理式 $A[V]$ 中で V が他の高階の変数の引数に出現しないとき、 $A[V]$ 中の $V(\underline{V'})$ という出現を $\neg V(\underline{V'})$ で置き換えた論理式、例えば

$$A[V] \equiv \neg V(\underline{V'}) \vee \exists \underline{\psi}(E[\underline{\psi}] \wedge V(\underline{\psi}))$$

（ここで、 E は V を含まない論理式）であるとき、

$$\neg\neg V(\underline{V'}) \vee \exists \underline{\psi}(E[\underline{\psi}] \wedge \neg V(\underline{\psi}))$$

を $A[\neg V]$ で表す。

補題 4.4

$$\exists\varphi A[\varphi] \equiv \exists\varphi A[\neg\varphi]$$

証明 $A[\varphi]$ に対して $A[\neg\neg\varphi]$ なども同様に定義する。
十分性 $A[V]$ を仮定する。

$$\begin{aligned} A[V] &\vdash A[\neg\neg V] \\ &\vdash A[\neg(\{\underline{\psi}\}\neg V(\underline{\psi}))] \\ &\vdash \exists\varphi A[\neg\varphi] \end{aligned} \tag{13}$$

ここで $\exists\varphi A[\varphi]$ を仮定すれば最初の仮定を消去できる。
式 (13) を導く部分であるが、これは以下のように論理式 $A[\neg\neg V]$ の構造上の帰納法により導ける。

1. $A[\neg\neg V] \equiv \neg\neg V(\underline{\eta})$ の場合

$$\neg\neg V(\underline{\eta}) \equiv \neg(\{\underline{\psi}\}\neg V(\underline{\psi}))(\underline{\eta})$$

2. A が $\neg B, B \vee C, B \wedge C, B \supset C$ の形のときは帰納法の仮定から直接導ける。
3. $A \equiv \exists\underline{x}B$ の場合

$$\begin{aligned} & B[\underline{a}, \neg\neg V] \\ \vdash\ & B[\underline{a}, \neg(\{\underline{\psi}\}\neg V(\underline{\psi}))] && \text{帰納法の仮定より} \\ \vdash\ & \exists\underline{x}B[\underline{x}, \neg(\{\underline{\psi}\}\neg V(\underline{\psi}))] && \psi \text{ は新しい変数} \end{aligned}$$

最後に $\exists\underline{x}B$ より最初の仮定を消去する。

4. $A \equiv \forall\underline{x}B$ の場合

$$\forall\underline{x}B[\underline{x}, \neg\neg V] \tag{14}$$

$$\begin{aligned} \vdash\ & B[\underline{a}, \neg\neg V] \\ \vdash\ & B[\underline{a}, \neg(\{\underline{\psi}\}\neg V(\underline{\psi}))] && \text{帰納法の仮定より} \\ \vdash\ & \forall\underline{x}B[\underline{x}, \neg(\{\underline{\psi}\}\neg V(\underline{\psi}))] && \underline{a}\text{は式 (14) に出現しない} \end{aligned}$$

必要性 十分性の証明より、$\exists\varphi A[\neg\varphi] \supset \exists\varphi A[\neg\neg\varphi]$ である。また、論理式 A の構造上の帰納法により、$A[\neg\neg V] \equiv A[V]$ は容易に示せる。
よって

$$\begin{aligned} A[\neg\neg V] &\vdash A[V] \\ &\vdash \exists\varphi A[\varphi] \end{aligned}$$

であるから $\exists\varphi A[\neg\varphi]$ を仮定する事により $\exists\varphi A[\neg\neg\varphi]$ が導けて、最初の仮定を消去できる。
□

定理 4.1 高階の量記号の消去

φ を型 $[0,\cdots,0]$ の束縛変数とし、項 $\underline{t_1},\ldots,\underline{t_m},\underline{s_1},\ldots\underline{s_l}$ では束縛変数が一次でしか出現しないとする。

$$
\begin{aligned}
&\exists\varphi(\forall\underline{x_{11}}(A_{11}[\underline{x_{11}}]\supset\cdots\supset\exists\underline{y_{1n_1}}(E_{1n_1}[\underline{x_1},\ldots,\underline{y_{1n_1}}]\wedge\varphi(\underline{t_1}))\cdots)\\
&\quad\wedge\ \forall\underline{x_{21}}(A_{21}[\underline{x_{21}}]\supset\cdots\supset\exists\underline{y_{2n_2}}(E_{2n_2}[\underline{x_{21}},\ldots,\underline{y_{2n_2}}]\wedge\varphi(\underline{t_2}))\cdots)\\
&\quad\wedge\\
&\quad\vdots\\
&\quad\wedge\ \forall\underline{x_{m1}}(A_{m1}[\underline{x_{m1}}]\supset\cdots\supset\exists\underline{y_{mn_m}}(E_{mn_m}[\underline{x_{m1}},\ldots,\underline{y_{mn_m}}]\wedge\varphi(\underline{t_m}))\cdots)\\
&\quad\wedge\ \forall\underline{x_1}(C_1[\underline{x_1}]\supset\neg\varphi(\underline{s_1}))\\
&\quad\wedge\\
&\quad\vdots\\
&\quad\wedge\ \forall\underline{x_l}(C_l[\underline{x_l}]\supset\neg\varphi(\underline{s_l})))
\end{aligned}
$$

と同値で、φ の出現しない式を求める手続きが存在する。

証明

$\underline{y_{in_i}}$ を $\underline{y_i}$ とおく。

$$\forall\underline{x_{i1}}(A_{i1}[\underline{x_{i1}}]\supset\cdots\supset\exists\underline{y_i}(E_{in_i}\wedge\varphi(t_{i1},\ldots,t_{ik}))\cdots)$$

から新しい変数 $x'_1,\ldots,x'_k$ をつくり、等式 $x'_1=t_{i1},\ldots,x'_k=t_{ik}$ とおく。これを行列表現で表すと

$$\begin{bmatrix} x'_1\\ \vdots\\ x'_k\end{bmatrix}=M\begin{bmatrix} y_{i1}\\ \vdots\\ y_{im}\end{bmatrix}+L$$

とおく。ここで、M は有理数を要素とする k 行 m 列の行列、L は k 行 1 列の行列で自由変数を含む場合があり、例えば $t_{ij}=a_1y_{i1}+\cdots+a_my_{im}+a_{m+1}$ ならば M の第 i 行は

$$[\ a_1\ \ \cdots\ \ a_m\ ]$$

となり、L の第 i 要素は a_{m+1} である。k 行 m 列行列 M の階数(rank)を l とすると $(l\leq k,m)$ $y_{i1},\ldots,y_{im}$ の内 l 個選べて、

$$
\begin{aligned}
y_{i_{j_1}} &= f_1(x'_1,\ldots,x'_n,y_{i_{j_{l+1}}},\ldots,y_{i_{j_m}})\\
x_{i_2} &= f_2(x'_1,\ldots,x'_n,y_{i_{j_{l+1}}},\ldots,y_{i_{j_m}})\\
&\vdots\\
x_{i_l} &= f_l(x'_1,\ldots,x'_n,y_{i_{j_{l+1}}},\ldots,y_{i_{j_m}})
\end{aligned}
\tag{15}
$$

とすることが出来る。そして、式

$$E_{in_i}[\underline{y_i}]\wedge\underline{x'}=\underline{t_i}$$

に (15) を代入して簡単化した結果を $A'[x'_1,\ldots,x'_n,y_{i_{l+1}},\ldots,y_{i_{jm}}]$ とし、同様に $C_h[\underline{x_h}]$ についても、変数 $x_{h_1},\ldots,x_{h_{l'}}$ について解いた結果を $\neg C_h[\underline{x_h}] \wedge \underline{x'} = \underline{s_h}$ に代入した結果を $C'_h[x'_1,\ldots,x'_n,y_{h_{l'+1}},\ldots,y_{h_{n'}}]$ とする。この様に変数変換を行うことで、補題 4.3 に帰着する。□

これら定理の直観的意味は以下である。

$$\forall\underline{x}(A[\underline{x}] \supset \varphi(\underline{x}))$$

$$\forall\underline{x}(B[\underline{x}] \supset \neg\varphi(\underline{x}))$$

という形の式は直観的に φ を集合と考えればそれぞれ

$$\{\underline{x} \mid A[\underline{x}]\} \subset \varphi$$

$$\{\underline{x} \mid B[\underline{x}]\} \subset \overline{\varphi}$$

を表していると考えることが出来る。同様に

$$\forall\underline{x}(A[\underline{x}] \supset \exists\underline{y}(E[\underline{x},\underline{y}] \wedge \varphi(\underline{y}))$$

は

$$(\{\underline{y} \mid \exists\underline{x}A[\underline{x}] \wedge E[\underline{x},\underline{y}]\} \cap \varphi) \neq \phi$$

を意味している。そして、明らかに φ と $\overline{\varphi}$ には共通部分があってはいけないし、共通部分がなければ条件を満たすように φ をとることが出来る。

これらのことと変数変換をまとめて、最も簡単な場合の証明を示す。

$$\begin{aligned}
&\exists\varphi(\forall\underline{x}\underline{x'}(\underline{x'} = \underline{t} \supset A[\underline{x}] \vee \varphi(\underline{x'})) \\
&\qquad \wedge \forall\underline{y}\underline{x'}(\underline{x'} = \underline{s} \supset B[\underline{y}] \vee \neg\varphi(\underline{x'}))) \\
\equiv\ &\exists\varphi(\forall\underline{x}\underline{x'}(\underline{x'} \neq \underline{t} \vee A[\underline{x}] \vee \varphi(\underline{x'})) \\
&\qquad \wedge \forall\underline{y}\underline{x'}(\underline{x'} \neq \underline{s} \vee B[\underline{y}] \vee \neg\varphi(\underline{x'}))) \\
\equiv\ &\exists\varphi(\forall\underline{x'}(\forall\underline{x}(\underline{x'} \neq \underline{t} \vee A[\underline{x}]) \vee \varphi(\underline{x'})) \\
&\qquad \wedge \forall\underline{x'}(\forall\underline{y}\underline{x'} \neq \underline{s} \vee B[\underline{y}]) \vee \neg\varphi(\underline{x'}))) \\
\equiv\ &\exists\varphi(\forall\underline{x'}(\exists\underline{x}(\underline{x'} = \underline{t} \wedge \neg A[\underline{x}]) \supset \varphi(\underline{x'})) \\
&\qquad \wedge \forall\underline{x'}(\exists\underline{y}\underline{x'} = \underline{s} \wedge \neg B[\underline{y}]) \supset \neg\varphi(\underline{x'}))) \\
\equiv\ &\exists\varphi(\forall\underline{x'}(\exists x_{i_{l+1}}\cdots x_{i_m}A'[\underline{x'},x_{i_{l+1}},\ldots,x_{i_m}] \supset \varphi(\underline{x'})) \\
&\wedge \forall\underline{x'}(\exists y_{j_{l'+1}}\cdots y_{j'_m}B'[\underline{x'},y_{j_{l'+1}},\ldots,y_{j'_m}] \supset \neg\varphi(\underline{x'})) \\
\equiv\ &\exists\varphi((\{\underline{x'} \mid \exists x_{i_{l+1}}\cdots x_{i_m}A'[\underline{x'},x_{i_{l+1}},\ldots,x_{i_m}]\} \subset \varphi) \\
&\wedge (\{\underline{x'} \mid \exists y_{j_{l'+1}}\cdots y_{j'_m}B'[\underline{x'},y_{j_{l'+1}},\ldots,y_{j'_m}]\} \subset \overline{\varphi})) \\
\equiv\ &\neg\exists\underline{x'}(\exists x_{i_{l+1}}\cdots x_{i_m}A'[\underline{x'},y_{j_{l'+1}},\ldots,y_{j'_m}] \\
&\qquad \wedge \exists y_{j_{l'+1}}\cdots y_{j'_m}B'[\underline{x'},y_{j_{l'+1}},\ldots,y_{j'_m}])
\end{aligned}$$

また、補題 4.4 と上の定理より次の定理を導く。

定理 4.2 高階の量記号の消去 *2*

φ を型 $[0,\cdots,0]$ の束縛変数とし、項 $\underline{t_1},\ldots,\underline{t_m},\underline{s_1},\cdots\underline{s_l}$ では束縛変数が一次でしか出現しないとする。

$$
\begin{aligned}
&\exists\varphi(\forall\underline{x_{11}}(A_{11}[\underline{x_{11}}]\supset\cdots\supset\exists\underline{y_{1n_1}}(E_{1n_1}[\underline{x_1},\ldots,\underline{y_{1n_1}}]\wedge\neg\varphi(\underline{t_1}))\cdots)\\
&\quad\wedge\quad\forall\underline{x_{21}}(A_{21}[\underline{x_{21}}]\supset\cdots\supset\exists\underline{y_{2n_2}}(E_{2n_2}[\underline{x_{21}},\ldots,\underline{y_{2n_2}}]\wedge\neg\varphi(\underline{t_2}))\cdots)\\
&\quad\wedge\\
&\quad\vdots\\
&\quad\wedge\quad\forall\underline{x_{m1}}(A_{m1}[\underline{x_{m1}}]\supset\cdots\supset\exists\underline{y_{mn_m}}(E_{mn_m}[\underline{x_{m1}},\ldots,\underline{y_{mn_m}}]\wedge\neg\varphi(\underline{t_m}))\cdots)\\
&\quad\wedge\quad\forall\underline{x_1}(C_1[\underline{x_1}]\supset\varphi(\underline{s_1}))\\
&\quad\wedge\\
&\quad\vdots\\
&\quad\wedge\quad\forall\underline{x_l}(C_l[\underline{x_l}]\supset\varphi(\underline{s_l})))
\end{aligned}
$$

と同値で、φ の出現しない式を求める手続きが存在する。

さらに、高階の量記号に関しても一階（型 0）の量記号の場合と同様に、次の事が成立する。

- $\forall\psi A\equiv\neg\exists\neg\psi A$
- $\exists\varphi\exists\psi A[\varphi,\psi]\equiv\exists\psi\exists\varphi A[\varphi,\psi]$
- A に ψ が現れないとき

$$\exists\psi(A\wedge B)\equiv A\wedge\exists\psi B$$

これらのことと定理4.1から次の系がいえる。

系 4.1　次の条件を満たすとき高階の量記号を消去することが出来る。

1. 高階の束縛変数の型は $[0,\ldots,0]$ である。
2. 高階の束縛変数の引数には他の束縛変数（型 0）は一次で現れる。
3. 高階の量記号の種類（$\exists$ か $\forall$ か）と異なる種類の型 0 の量記号がこの高階の量記号の束縛範囲内に現れる場合この異なる種類の量記号の束縛範囲内には
   (a) 高階の量記号と同じ種類の量記号は現れない。
   (b) この高階の束縛変数の出現は一つしかない。

4.2　NU 解釈系への応用

系 4.1を NU 解釈系に応用したアルゴリズムを述べる。これは 3 節で示した手続き NF と新しい二つの手続き EQ と NF2 からなり、手続き EQ を実行することで高階の量記号の消去が行われる。（手続き NF、NF2 は EQ から呼ばれる手続きである）ただし、NF はこのために NF-3 の後に

NF-4　　Γ が $\forall xA$ という形の式のとき Γ 自身を結果として終了。

を加える。

手続き EQ

EQ-1 高階の質変数に対し、新しい束縛変数を作りそれで高階の質変数を置き換えて、一番外側で存在記号で束縛する。

EQ-2 一番内側の高階の量記号に着目する。以下で、着目している量記号に束縛されている変数を φ とする。

量記号を Q とすると $Q\varphi A$ に以下の手続きを施し、この部分を高階の量記号が現れない式にする。

- 高階の量記号が存在の場合

(a) $A \supset B$、$A \equiv B$ をそれぞれ $\neg A \vee B$、$A \wedge B \vee \neg A \wedge \neg B$ で置き換える。

(b) $\neg$ を内側へ移動する。

(c) 内側の存在量記号を外へ出す。（存在量記号の交換）例えば

$$\exists\varphi(\cdots \exists x B \cdots)$$

を

$$\exists x \exists\varphi(\cdots B \cdots)$$

とする。

(d) 手続き NF を施す。この結果が $A_1 \vee \cdots \vee A_n$ であるとき、この部分を $\exists\varphi A_1 \vee \cdots \vee \exists\varphi A_n$ とし、各 $\exists\varphi A_i (1 \leq i \leq n)$ に以下の手続きを施し、全体の論理和をとる。

(e) 着目している高階の束縛変数 φ の出現しない素論理式を外へ出す
例えば

$$\exists\varphi(A \wedge B)$$

で A には φ が現れないとき、この式を

$$A \wedge \exists\varphi B$$

とする。

(f) 上の EQ-2eの結果の $\exists\varphi B$ 中の $\forall\underline{x}C$ という部分全てに対し、$\forall$ の束縛範囲 C に手続き NF2 を施す。この結果を $C_1 \wedge \cdots \wedge C_m$ とすると $\forall\underline{x}C$ を

$$\forall\underline{x}C_1 \wedge \cdots \wedge \forall\underline{x}C_m$$

で置き換える。

(g) 定理 4.1 と同様に

$$\forall\underline{x}(A[\underline{x}] \vee \varphi(t_1, \ldots, t_n))$$
$$\forall\underline{x}(B[\underline{x}] \vee \neg\varphi(s_1, \ldots, s_n))$$

の部分を

$$\forall\underline{x}'(A'[\underline{x}'] \vee \varphi(x'_1, \ldots, x'_n))$$
$$\forall\underline{x}'(B'[\underline{x}'] \vee \neg\varphi(x'_1, \ldots, x'_n))$$

と同値変形する。

注 2 $\varphi(t_1,\ldots,t_n)$ で $t_1,\ldots,t_n$ には φ より外側の束縛変数しか現れない場合は（$rank=0$ の場合）

$$\forall\underline{x'}(\neg(x'_1=t_1\wedge\cdots\wedge x'_n=t_n)\vee\varphi(x'_1,\ldots,x'_n))$$

とする。

(h) これまでの操作によって、

$$\begin{array}{lll}\exists & \varphi(& \\ & & \forall\underline{x}(A_1[\underline{x}]\vee\varphi(x_1,\ldots,x_n)) \\ & \wedge & \cdots \\ & \wedge & \forall\underline{x}(A_n[\underline{x}]\vee\varphi(x_1,\ldots,x_n)) \\ & \wedge & \forall\underline{x}(B_1[\underline{x}]\vee\neg\varphi(x_1,\ldots,x_n)) \\ & \wedge & \cdots \\ & \wedge & \forall\underline{x}(B_m[\underline{x}]\vee\neg\varphi(x_1,\ldots,x_n)) \\ &) & \end{array}$$

となっている。この部分を

$$\forall\underline{x}((A_1[\underline{x}]\wedge\cdots\wedge A_n[\underline{x}])\vee(B_1[\underline{x}]\wedge\cdots\wedge B_m[\underline{x}]))$$

で置き換える。（$\forall\underline{x}((A_1[\underline{x}]\wedge\cdots\wedge A_n[\underline{x}])\vee(B_1[\underline{x}]\wedge\cdots\wedge B_m[\underline{x}]))$ は $\neg\exists\underline{x}((\neg A_1[\underline{x}]\vee\cdots\vee\neg A_n[\underline{x}])\wedge(\neg B_1[\underline{x}]\vee\cdots\vee\neg B_m[\underline{x}]))$ と同値である。）このときこの変数 φ が元々は質変数であった場合その値は

$$\{\underline{x}\}(\neg A_1[\underline{x}]\vee\cdots\vee\neg A_n[\underline{x}])$$

となる。

- 着目した量記号が全称記号の場合
  $\forall\varphi A$ を $\neg\exists\varphi\neg A$ とし、2へ。

手続き NF2 式 Γ を選言標準形にする。

- $\Gamma\equiv A\vee B$ のとき
  1. A、B に手続き NF2 を施す。この結果をそれぞれ $A_1\wedge\cdots\wedge A_n$、$B_1\wedge\cdots\wedge B_m$ とする。
  2. $$\bigwedge_{1\le i\le n,1\le j\le m}(A_i\vee B_j)$$
     を結果とする。
- $\Gamma\equiv A\wedge B$ のとき
  1. A、B に手続き NF2 を施す。この結果をそれぞれ A'、B' とする。
  2. $$A'\wedge B'$$

を結果とする。

- Γ がその他のリテラルの場合
  Γ 自身が結果である。

4.3 例

良く知られた問題であるソクラテスの問題について示す。ソクラテスの問題は NU では次のように表現できる。

$$\forall P, M(P(0) \wedge \forall x(P(x) \supset M(x)) \supset M(\nu x))$$

ここでソクラテスに 0 が対応している。解釈は次のように行われる。

1. まず、一番内側の高階の量記号$\forall M$ に着目し、系に当てはまるようにこれを $\exists$ で表現し、$\neg$ を内側へ移動する。

$$\neg\exists P, M(P(0) \wedge \forall x(\neg P(x) \vee M(x)) \wedge \neg M(\nu x))$$

2. M の現れない式を外に出す。

$$\neg\exists P(P(0) \wedge \exists M(\forall x(\neg P(x) \vee M(x)) \wedge \neg M(\nu x)))$$

3. $\forall x(\neg P(x) \vee M(x))$、$\neg M(\nu x)$ の形を整える。

$$\begin{aligned} & \forall x(\neg P(x) \vee M(x)) \\ \equiv\ & \forall x', x(P(x) \wedge x = x' \supset M(x')) \\ \equiv\ & \forall x'(\exists x(P(x) \wedge x = x') \supset M(x')) \\ \equiv\ & \forall x'(P(x') \supset M(x')) \end{aligned}$$

であるから

$$\neg\exists P(P(0) \wedge \exists M(\forall x'(\neg P(x') \vee M(x')) \wedge \forall x'(x' \neq \nu x \vee \neg M(x')))$$

4. M を消去する。

$$\neg\exists P(P(0) \wedge \neg\exists x'(x' = \nu x \wedge P(x')))$$

これは

$$\neg\exists P(P(0) \wedge \forall x'(x' \neq \nu x \vee \neg P(x')))$$

とできる。

5. P を消去する。

$$\neg\neg\exists y(y = 0 \wedge y = \nu x)$$

6. 得られた ν 行為を簡単化すれば

$$\nu x = 0$$

5 結び

5.1 まとめ

1. 決定可能である新しい数学理論を示し、それを有理 Presburger 算術と名付けた。
2. NU 解釈系において型 0 の束縛変数に対する制限（一次という制限以外）を解消した。
3. NU 解釈系において高階の束縛変数に対してもある制限を満たすものに対して解釈を行えるようにした。

加法しか許さない整数論である Presburger 算術の研究はそのアルゴリズムの計算量に関するもの、あるいは式にクラスを定義し、そのクラスの計算量に関するものが行われてきた。本研究ではこのような方向ではなく、変数の範囲を有理数に拡張したものも決定可能であることを示し、その決定アルゴリズムを与えた。また、この決定アルゴリズムを NU 解釈系に応用することにより、有理 Presburger 算術で項が一次の範囲で書かれた ν 行為に対しては行動可能であればその新しい値を求め、行動不能であればそのことを知らせるように出来る。つまり、強正当性が言える。

高階の束縛変数を 4 節で述べたような制限を満たすものの解釈を行えるようにした結果、以前は扱えなかった無限集合を表すような高階の対象もこの制限内で扱えるようになった。例えば、型 [0] の変数 P に 2 と 3 の公倍数の集合を代入する ν 行為

$$\forall x(\nu P(x) \equiv \exists y, w(Z(y) \wedge Z(w) \wedge x = 2y \wedge x = 3w))$$

の解釈は従来の解釈系では行えないが新しい解釈系では可能になり、解釈の結果 P の値は

$$\{x\}(\exists y, w(Z(y) \wedge Z(w) \wedge x = 2y \wedge x = 3w))$$

となる。他の論理型プログラム言語では、通常このような無限集合そのものを直接扱うことは出来ない。例えば Prolog でも 2 の倍数の集合と 3 の倍数の集合の積集合である 6 の倍数の集合を直接求めることは出来ない。

また、前節の例のソクラテスの問題では Prolog では、プログラムテキスト中の唯一つの定数記号であるソクラテスの場合を試して、それでうまくいくのでソクラテスが解釈結果となる。一方 NU 解釈系では型 [0] の対象すべての上で P, M を動かしたとき、与えられた ν 行為を満たすものは必ず、ソクラテスを表す 0 を含むので答は 0 となるのである。

5.2 展望

今後は以下のようなことを研究したい。

1. 決定アルゴリズムの高速化
2. 従来の解釈系では束縛変数は有限の範囲で動いていたので例えば 2 次で出現しても構わなかった。これは新しい解釈系でも可能にしたいので、決定ア

ルゴリズムとの融合を考える。

3. 高階の束縛変数に対する制限をゆるめる。例えば、Prolog などで行われる再帰的定義に当るようなことを可能にしたい。

それぞれについて考察する。

1. 有理 Presburger 算術の決定アルゴリズムでは与えられた式全体を拡大 v 式に変換し、その後真偽を決定している。
しかし、真偽を決定する場合例えば与えられた式が

$$\exists x_1 A_1 \vee \cdots \vee \exists x_n A_n \tag{16}$$

と同値である場合 $\exists x_i A_i$ が真であれば他の式の真偽に関係なく元の式も真である。そこで、まず与えられた式を式 (16) の形に変形し $\exists x_1 A_1$ から順に拡大 v 式に変換し、真偽を決定し、真ならばそれで終了し偽であれば次の $\exists x_i A_i$ に関して同じことをする。このとき $\exists x_n A_n$ の結果も偽であれば、全体も偽で終了する。
このようにすれば、かなり高速化がはかれる。しかし、最初に式 (16) の形にしてしまうと、式自体がかなり大きなものになってしまい、記憶容量に問題が出る。そこで、一度に式 (16) の形にしないで、必要になったら次の $\exists x_i A_i$ を生成するようにする。また、例えば $\exists x_i A_i$ と $\exists x_{i+1} A_{i+1}$ とではほとんど同じ式であると思われるのでこの生成手続きも再帰的に定義し、部分式に対して適用するようにするとかなり高速化がはかれるであろう。
また、$\mathcal{V}_{ax+e}^{a'x+e'} uA$ は例えば $0 < a < a'$ とし、$ax+e = a'x+e', ax+e+2 = a'x+e'$ の解をそれぞれ c_0, c_2 とすれば、

$$\begin{aligned}\exists u(Z(u) \wedge a'c_0 + e' < u < a'c_2 + e' \wedge ax + e < u < a'x + e' \\ \wedge a'x + e' - 1 \leq u \leq ax + e + 1 \wedge A)\end{aligned}$$

と同値である。ここで、$a'c_2 - a'c_0$ は定数であるから決定アルゴリズムに従えば、外側の $\exists$ を、$a'c_0 + e' < u < a'c_2 + e'$ を幅 1 の区間に分割して v 記号にし手続き EX によって拡大 v 式にする。しかしここで、これをこのまま $\exists u(Z(u) \wedge t < u < t + b \wedge B)$ の形で持っていることを考える。この形の式を扱うように出来れば扱わねばならない式の大きさはかなり小さくなるので、アルゴリズムは高速になる。例えば

$$\exists x(A[x] \wedge \exists u(Z(u) \wedge ax + e < u < ax + e + b \wedge B[x, u]))$$

は $0 < a$ とすれば

$$\exists x(Z(x) \wedge -\frac{e+b}{a} < x < -\frac{e}{a} \wedge \exists x(A[\frac{u}{a} + x] \wedge B[\frac{u}{a} + x, u]))$$

と同値になる。よって、$\exists$ 記号の数の上の帰納法を用いれば、$\neg$ が無い場合にはうまくいく。$\neg$ がある場合はこの形の式を補題 3.6で v 式になおして $\neg$ の無い形にする方法が考えられる。この方法でも元々 v で行っていたも

のと比べると、補題 3.6の適用は他の手続きに比べて、非常に簡単なのでこれでも十分に速いと思われる。また、υ 記号を扱わず、上限と下限の幅が定数で整数値をとるというような形の $\forall$ と $\exists$ を扱うことも考えたい。

2. 外から動く範囲が決まる束縛変数は、例えば A 中に x が 2 次以上で現れる場合でも

$$\exists x(Z(x) \wedge 0 \leq x \leq 3 \wedge A[x])$$

は

$$A[0] \vee \cdots \vee A[3]$$

というように先に外側から順に展開してしまって、そのような束縛変数を消去した形を扱うようにすれば良い。
また、上で述べた

$$\exists x(Z(x) \wedge t < x < t + a \wedge B[x])$$

という形との整合性も考えたい。

3. 例えば

$$\begin{aligned} &\exists \varphi(\forall \underline{x}(A[\underline{x}] \supset \varphi(\underline{x})) \\ &\wedge \quad \forall \underline{x}, \underline{y}(p(\underline{x}) \wedge B[\underline{x}, \underline{y}] \\ &\qquad \supset p(\underline{y}))) \end{aligned}$$

の決定アルゴリズムを考える。これは「A を満たすものから始まる B によって作られる列」を表す。
具体的な例としてゲーム・ニムを考える。このゲームは相手が言った数字より小さくてその数字 -2 以上の負でない数字を交り番こに言っていくというものである。そして 0 を言わざるを得なくなった方が負けというものである。
このゲームには必勝形があり先手が 3 の倍数 + 1 を常にいっていればよい。この必勝形 M を求める行為は次のように表現できる。

$$\begin{aligned} &\exists w \nu M(w) \\ &\quad \wedge \quad \forall x(\nu M(x) \supset x > 0) \\ &\quad \wedge \quad \forall x(\nu M(x) \supset \forall y(x - 2 \leq y < x \wedge y \neq 0 \\ &\qquad \supset \neg \nu M(y) \wedge \exists w(w \neq 0 \wedge y - 2 \leq w < y \wedge \nu M(w)))) \end{aligned}$$

以下のように手続き $\mathrm{D}(x_1, \ldots, x_n)$ を定義し、この式を決定するために、A を満たす全ての列について、$\mathrm{D}(s_1, \ldots, s_n)$ を実行する。

手続き $\mathrm{D}(x_1, \ldots, x_n)$

D-1

$$\exists \underline{y} B[\underline{x}, \underline{y}]$$

の真偽を決定する。

- 偽の場合
  結果を T として終了。
- 真の場合

$$B[\underline{x}, \underline{t}]$$

  なる全ての $\underline{t}$ について
  $\mathrm{D}(t_1, \ldots, t_n)$ を実行。

このアルゴリズムは停止しない場合がある。また、先のニムの例では $\forall \underline{x}(A[\underline{x}] \supset \varphi(\underline{x}))$ に当るものがないので適用できない。更に全ての項列についてという部分が必ず計算できるとは限らない。
しかし、このような表現を許すことによって、かなり表現力は増す。また、ニムのように答えが明らかなものについてその答えを得るためにはどのようなアルゴリズムが考えられるのがそしてそのアルゴリズムはどこまで一般に扱えるのかを考えたい。また、扱える表現はどこまで一般化できるか、あるいはどの程度このような表現を許して行けば満足な範囲になるかを調べて行きたい。
また、先に得られた定理 4.1 は φ と $\neg\varphi$ に対して非対称になっている。そこで対称な形、例えば

$$\begin{aligned}
&\Gamma \equiv \\
&\quad \exists\varphi(\quad \forall \underline{x}(A[\underline{x}] \supset \exists \underline{y}(E[\underline{x}, \underline{y}] \wedge \varphi(\underline{y}))) \\
&\quad\quad \wedge \quad \forall \underline{x}(A'[\underline{x}] \supset \exists \underline{y}(E'[\underline{x}, \underline{y}] \wedge \neg\varphi(\underline{y})))) \\
&
\end{aligned}$$

を考える。しかしこれは定理のような形では一般には解けないという予想をしている。残念ながらその証明はまだ出来ていないが、今後はこの証明と、定理のような方法では解けない表現を明らかにしたい。

謝辞

この研究を進めるにあたりご指導いただいた筑波大学教授五十嵐滋先生、筑波大学講師細野千春先生に感謝致します。証明の足りない部分の指摘や、研究の議論に参加していただいた筑波大学助教授辻尚史先生、水谷哲也氏に感謝します。いろいろな励ましをいただいた筑波大学人工知能研究室の皆さんに感謝します。

References

[1] M. Davis :A Computer Program for Presburger's Algorithm, *Automation of Reasoning 1 (Symbolic Computation), J. Siekmann and G. Wrightson (ed.), Springer-Verlag, 1983*, 1957, pp. 41-48.

[2] 服部隆志: 矛盾を含む制約の部分的解決, 応用数学合同研究集会報告集, 1990, pp.100-105.

[3] 細野千春, 池田靖雄: 有理 Presburger 算術の決定性について, コンピュータ・ソフトウェア, Vol. 9, No. 5(1992), pp. 54-61.

[4] C. Hosono and Y. Ikeda : A Formal Derivation of the Decidability of the Theory SA, *Theor. Comput. Sci.*, to appear.

[5] S. Igarashi :The ν -Conversion and an Analytic Semantics, *Inf.Proc.83, R.E.A.Mason(ed.), Elsivier Science Publishers B.V.(North-Holland), IFIP*(1983), pp.764-774.

[6] 池田靖雄, 細野千春, 辻尚史, 五十嵐滋: NU 解釈系の設計, 日本ソフトウェア科学会第 7 回大会論文集, 1990, pp.293-296.

[7] 池田靖雄: 高階論理型プログラム言語 NU の処理系に関する研究, 筑波大学工学研究科修士論文, 1989.

[8] 池田靖雄, 辻尚史, 細野千春: プログラム言語 NU の解釈系とその正当性, 情報処理学会論文誌, 投稿中.

[9] T. Käufl : Reasoning Systems of Linear Inequalities, *E.lusk and R.Overbeek(ed.), 9th International Conference on automated Deduction. Proceedings of conference held in Argonne, Illinois*, 1988, pp.563-572, *(Lecture Notes in Comput. Sci.,* **310**, *Springer-Verlag).*

[10] F. Kröger : Temporal Logic of Programs, *Springer-Verlag*, 1987.

[11] 水谷哲也, 細野千春, 五十嵐滋: ν - 定義可能行為によるプログラムの検証, コンピュータソフトウェア, Vol.2, No.3(1985), pp.47-56.

[12] M. Presburger : Über die Vollständigkit eines gewissen Systems der Arithmetik ganzer Zahlen in welchem die Additon als einzige Operation hervortritt, *Comptes-Rendus du Congres des Mathematicians des Pays Slaves, Warsaw*, 1930, pp.92-101, p.395.

[13] C.R. Reddy and D.W. Loveland :Presburger arithmetic with bounded quantifier alternation, *Conference Record of Tenth Annual ACM Symposium on Theory of Computing(San Diego, Calif.,1978), ACM,*

New York, 1978, pp.320-325,

[14] B. Scarpellimi :Complexity of subcase of Presburger arithmetic, *Trans.Amer.Math.Soc.*, Vol. 284, No.1(1984), pp.203-218.

[15] T. Skolem, Über einige Satzfunktionen in der Arithmetik, *Selected Works in Logic, Universitetsforlaget*, 1970, pp. 281-306.

[16] G. Takeuti :*Two applications of logic to Mathematics, Iwanami Shoten Publisher, and Princeton University Press*, 1978.

[17] 富田康治, 辻尚史, 五十嵐滋: プログラムの実時間問題の ν - 転換による解釈と動作条件, 応用数学合同研究集会報告集, 1989, pp.161-166.

[18] T. Tsuji :The language NU, to appear.

[19] K. Wöhl :Zur Komplexitat der Presburger Arithmetik und des Äquivalenzproblems ein facher Programme, *Theor. Comput. Sci. (Fourth GI Conf., 1979)*, 1979, pp. 310-318, *(Lecture Notes in Comput. Sci.,* **67**, *Springer-Verlag).*

本学関係