ソフトウェア検証のためのプレスバーガー算術を含む論理の決定可能性

伊藤 宗平　龍田 真

ソフトウェアの検証のために算術とリストの入った一階述語論理は重要である．第一の結果として，プレスバーガー算術とリストの入った一階述語論理の真偽が決定可能であることを示す．また，メモリを扱うソフトウェアの検証のために分離論理は重要であり，さらに実際的なソフトウェアではアドレス計算のため算術が必要である．第二の結果として，points-to, *だけから成る分離論理にプレスバーガー算術を追加した論理の真偽が決定不可能であることを示す．

1　はじめに

論理による演繹的なソフトウェア検証においてはエンテイルメント判定が重要である．エンテイルメント判定とは「A ならば B」の形の論理式の妥当性，すなわちその論理式が可能なすべての構造で真であるかどうかを判定することである．したがってエンテイルメント判定が決定可能である論理は，ソフトウェア検証において有用である．

ソフトウェアは計算を表現するものであるため，自然数上の演算に関する性質の検証が可能であることが望ましい．自然数上の演算を持つ一階の理論には自然数の和のみを持つプレスバーガー算術や自然数の和と積を持つペアノ算術などが知られている．任意の論理式の妥当性判定について，プレスバーガー算術は決定可能であるが，ペアノ算術は決定不能であることが知られている．また，ソフトウェアはリストや木などのデータ構造を用いることが多いため，そのようなデータ構造を扱える論理が望ましい．しかしながら，これまで自然数の算術とリストなどのデータ構造をともに備えた論理の研究は十分なされてこなかった．

一方で，ソフトウェア検証においては，計算に関する性質のみならず，メモリの安全性も重要な要件である．メモリ上のポインタ構造を扱える論理に分離論理がある [13]．分離論理においては決定可能なフラグメントとして，構文を記号的ヒープに限定した分離論理が知られている [1] [2] [6]．また，記号的ヒープにプレスバーガー算術や定数の加法 $+k$ を加えた論理も決定可能である [15] [4]．

一方，記号的ヒープに限らない一般的な一階の分離論理については決定不能であることが示されている [5] [3] [7] が，分離含意 $-\!\!*$ を除き，points-to 演算が 1 フィールドの場合には決定可能であることも知られている [3]．このように分離論理の決定可能性について様々な考察がされてきたが，構文制約のない場合に算術を考慮した分離論理についてはこれまで明らかにされていなかった．

したがって，本研究では次の事実を明らかにする．

1. プレスバーガー算術とリストをシグネチャに持つ一階論理は決定可能である．
2. プレスバーガー算術を持ち，分離含意がなく points-to 演算が 1 フィールドの分離論理は決定不能である．

---

*Decidability of logics with Presburger arithmetic for software verification

Sohei Ito, 長崎大学情報データ科学部, Dept. of Information and Data Sciences, Nagasaki University.

Makoto Tatsuta, 国立情報学研究所 / 総合研究大学院大学, National Institute of Informatics / Sokendai.

事実 1 より，加法とリストを扱うプログラムの検証において有用な論理体系を発見することができた．一方で，事実 2 より記号的ヒープによらない分離論理において決定可能なフラグメントに基本的な算術を追加すると決定不能となることが明らかになった．したがって，算術を考慮した決定可能なフラグメントの探索には記号的ヒープあるいはそれに類する記述への限定が有望なアプローチであることが明らかになった．

本稿の構成は以下の通りである．2 節では関連研究について述べる．3 節ではプレスバーガー算術とリストを備えた一階の論理の決定可能性を証明する．4 節では, プレスバーガー算術を備えた一階の分離論理の決定不可能性を証明する．5 節ではまとめと今後の課題を述べる．

2 関連研究

自然数上の演算を持つ一階の理論においては加法のみのプレスバーガー算術は決定可能であるが加法と乗法を持つペアノ算術は決定不能であることは良く知られた事実である．プレスバーガー算術の拡張については，単項述語記号を追加した場合に決定不能となることが示されている [9]．同様の関係がスコーレム算術 (乗法のみの算術) においても成り立つ [14]．また，プレスバーガー算術に列，すなわち i 番目の要素を取り出す演算 $(a)_i$ を追加した場合には，加法と列から以下のように乗法が定義できるため決定不能である．

$$x \times y = z \text{ iff } \exists a.((a)_0 = 0 \wedge (a)_y = z \wedge \forall i \leq y((a)_i + x = (a)_{i+1}))$$

一方，本研究の事実 1 では，プレスバーガー算術にリストを追加した場合には決定可能であることを明らかにする．

分離論理においては決定可能なフラグメントとして記号的ヒープとして知られる, (不) 等号と連言に限定した限量子なしの分離論理 [1] [2] [6] や, 記号的ヒープに帰納的に定義された述語と存在限量を含むもの [10] [16] [11] 等が知られている．

また，分離論理に算術を加えた決定可能なフラグメントとしては，記号的ヒープにプレスバーガー算術を追加した論理がある [15]．また，それよりもさらに制限の強い，定数の加算 $+k$ のみを追加した論理の計算複雑性が Π_2^P 完全であることも明らかになっている [4]．一方，記号的ヒープに限らない場合については決定不能であることが知られている．まず 2 フィールドのメモリモデルにおいて決定不能であることが明らかになった [5]．この結果はのちに厳格化され，1 フィールドのメモリモデルでも分離含意 $-\!\!*$ を持つ場合決定不能であること [3]，さらに，変数の個数を二つに限定しても決定不能であること [7] が明らかになった．しかし，分離含意を除いた場合には決定可能であることも知られている [3]．ただし，この結果は points-to 演算は緩い points-to ($\hookrightarrow$) を用いた場合にのみ示されている．

一方，本研究の事実 2 では，分離連言 $*$ と points-to 演算 $\hookrightarrow$ のみの分離論理 (1 フィールドのメモリモデル) であっても，プレスバーガー算術を追加した場合には決定不能であることを明らかにする．

3 プレスバーガー算術とリストを備えた一階の論理の決定可能性

本節では，プレスバーガー算術 [12] とリストを備えた一階の論理の決定可能性を証明する．証明の方針は，リスト $[a_1, a_2, \ldots, a_k]$ を以下の関数 τ で符号化することである [17].

$$\begin{aligned}&\tau(a_k, a_{k-1}, \ldots, a_1)\\ =&2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+k-1} \quad (1)\end{aligned}$$

この符号化は 2 進数で以下のような値であることを示している．

$$1\overbrace{0\ldots0}^{a_k}1\ldots1\overbrace{0\ldots0}^{a_2}1\overbrace{0\ldots0}^{a_1} \quad (2)$$

この符号化を用い，プレスバーガー算術とリストを備えた一階の論理の式を，プレスバーガー算術と指数を持つ一階の論理の式に変換する．プレスバーガー算術と指数を持つ一階の論理は決定可能であることが示されている [12] ため，我々の主張が証明される．

3.1 プレスバーガー算術とリストを備えた一階の論理

本節ではプレスバーガー算術とリストを備えた一階の論理 $\mathrm{LI}_{\mathrm{Pres}}$ を導入する．$\mathrm{LI}_{\mathrm{Pres}}$ は自然数のソー

トとリストのソートを持つ多ソート論理である．

N, L をソートとする．$0, 1$ をソート N の定数記号，nil をソート L の定数記号とする．$+$ を型 $N \times N \to N$ の二項関数記号，$\leq$ を型 $N \times N$ の述語記号，cons を型 $N \times L \to L$ の二項関数記号，hd を型 $L \to N$ の単項関数記号，tl を型 $L \to L$ の単項関数記号とする．ソート N の変数記号の集合を $\mathrm{Var}_N = \{x, y, \ldots\}$，ソート L の変数記号の集合を $\mathrm{Var}_L = \{\alpha, \ldots\}$ とし，$\mathrm{Var}_N \cap \mathrm{Var}_L = \emptyset$ とする．

ソート N, L の項 t_N, t_L はそれぞれ以下の文法で与えられる．

$$t_N ::= x \mid 0 \mid 1 \mid t_N + t_N \mid \mathsf{hd}(t_L)$$
$$t_L ::= \alpha \mid \mathsf{nil} \mid \mathsf{cons}(t_N, t_L) \mid \mathsf{tl}(t_L)$$

$\mathrm{LI}_{\mathrm{Pres}}$ の式は以下の文法で与えられる．

$$\begin{aligned} A ::= & t_N = t_N \mid t_N \leq t_N \mid t_L = t_L \\ & \mid \neg A \mid A \wedge A \mid A \vee A \mid A \to A \\ & \mid \exists x A \mid \forall x A \mid \exists \alpha A \mid \forall \alpha A \end{aligned}$$

$\mathbb{N}$ を自然数の集合とする．$\mathbb{L} = \{[a_1, \ldots, a_n] \mid a_i \in \mathbb{N}\}$ とする．$\mathrm{LI}_{\mathrm{Pres}}$ の標準モデル $\mathcal{M}$ はソート N の宇宙 $\mathbb{N}$ とソート L の宇宙 $\mathbb{L}$ を持つ一階の構造である．

ここで，$\mathcal{M}$ による $\mathrm{LI}_{\mathrm{Pres}}$ の非論理記号の解釈は以下の通りとする．

$$\begin{aligned} 0^{\mathcal{M}} &= 0 \\ 1^{\mathcal{M}} &= 1 \\ \leq^{\mathcal{M}} &= \leq \\ \mathsf{nil}^{\mathcal{M}} &= [\,] \\ \mathsf{cons}^{\mathcal{M}}(a, [a_1, \ldots, a_n]) &= [a, a_1, \ldots, a_n] \\ \mathsf{hd}^{\mathcal{M}}([\,]) &= 0 \\ \mathsf{hd}^{\mathcal{M}}([a_1, \ldots, a_n]) &= a_1 \\ \mathsf{tl}^{\mathcal{M}}([\,]) &= [\,] \\ \mathsf{tl}^{\mathcal{M}}([a_1, \ldots, a_n]) &= [a_2, \ldots, a_n] \end{aligned}$$

ここで，通常のプログラム言語では $\mathsf{hd}^{\mathcal{M}}([\,])$ と $\mathsf{tl}^{\mathcal{M}}([\,])$ は定義されないが，論理の構造においては関数は全域的でなければならないため定義されている．

$\rho : (\mathrm{Var}_N \to \mathbb{N}) \cup (\mathrm{Var}_L \to \mathbb{L})$ を変数の付値とする．ρ を定数記号 c に対し $\rho(c) = c^{\mathcal{M}}$，項 $t_1, \ldots, t_n$ と関数記号 f に対し $\rho(f(t_1, \ldots, t_n)) = f^{\mathcal{M}}(\rho(t_1), \ldots, \rho(t_n))$ として項に拡張する．また，$d \in \mathbb{N} \cup \mathbb{L}$ に対し $\rho[x := d]$ で，x に対し d を割り当て，x 以外の変数 y に対しては ρ の通りに値を割り当てる付値を表す．

標準モデル $\mathcal{M}$ と付値 ρ で $\mathrm{LI}_{\mathrm{Pres}}$ の式 A が真であることを $\mathcal{M}, \rho \models A$ と表す．$\mathcal{M}, \rho \models A$ は以下のように帰納的に定義される．

$\mathcal{M}, \rho \models t_N = u_N$ iff $\rho(t_N) = \rho(u_N)$
$\mathcal{M}, \rho \models t_N \leq u_N$ iff $\rho(t_N) \leq^{\mathcal{M}} \rho(u_N)$
$\mathcal{M}, \rho \models t_L = u_L$ iff $\rho(t_L) = \rho(u_L)$
$\mathcal{M}, \rho \models \neg A$ iff $\mathcal{M}, \rho \not\models A$
$\mathcal{M}, \rho \models A_1 \wedge A_2$ iff $\mathcal{M}, \rho \models A_1$ かつ $\mathcal{M}, \rho \models A_2$
$\mathcal{M}, \rho \models A_1 \vee A_2$ iff $\mathcal{M}, \rho \models A_1$ または $\mathcal{M}, \rho \models A_2$
$\mathcal{M}, \rho \models A_1 \to A_2$ iff $\mathcal{M}, \rho \not\models A_1$ または $\mathcal{M}, \rho \models A_2$
$\mathcal{M}, \rho \models \exists x A$ iff $\exists a \in \mathbb{N} : \mathcal{M}, \rho[x := a] \models A$
$\mathcal{M}, \rho \models \forall x A$ iff $\forall a \in \mathbb{N} : \mathcal{M}, \rho[x := a] \models A$
$\mathcal{M}, \rho \models \exists \alpha A$ iff $\exists a \in \mathbb{L} : \mathcal{M}, \rho[\alpha := a] \models A$
$\mathcal{M}, \rho \models \forall \alpha A$ iff $\forall a \in \mathbb{L} : \mathcal{M}, \rho[\alpha := a] \models A$

定義 1. $\mathrm{LI}_{\mathrm{Pres}}$ の式 A が**妥当**であるとは，全ての付値 ρ に対し，$\mathcal{M}, \rho \models A$ であることをいう．$\mathrm{LI}_{\mathrm{Pres}}$ の式 A が**充足可能**であるとは，ある付値 ρ に対し，$\mathcal{M}, \rho \models A$ であることをいう．

3.2 決定可能な論理 $\mathrm{Pres}_{\mathrm{Exp}}$

本節では，プレスバーガー算術に指数関数を追加した論理 $\mathrm{Pres}_{\mathrm{Exp}}$ を導入する．

$\mathrm{Pres}_{\mathrm{Exp}}$ のシグネチャは定数記号 0,1, 二項関数記号 $+, \dot{-}$, 二項述語記号 $\leq$, 単項関数記号 $2^x, \ell_2(x), \lambda_2(x)$ である．$\mathrm{Var} = \{x, y, z, \ldots, \alpha, \ldots\}$ を変数の集合とする．$\mathrm{Pres}_{\mathrm{Exp}}$ の項 t は以下の文法で与えられる．

$$\begin{aligned} t ::= & x \mid 0 \mid 1 \mid t + t \mid t \dot{-} t \mid t \leq t \mid \\ & 2^t \mid \ell_2(t) \mid \lambda_2(t) \end{aligned}$$

$\mathrm{Pres}_{\mathrm{Exp}}$ の式は以下の文法で与えられる．

$$\begin{aligned} A ::= & t = t \mid t \leq t \mid \neg A \mid A \wedge A \mid A \vee A \mid \\ & A \to A \mid \exists x A \mid \forall x A \end{aligned}$$

定義 2. $\mathrm{Pres}_{\mathrm{Exp}}$ の標準モデルを $\mathcal{N}$ とする．$\mathcal{N}$ は宇宙を $\mathbb{N}$ とし，$+$ を自然数の $+$, 2^x を自然数上の 2 の指数関数, $0, 1$ をそれぞれ自然数の $0, 1$ と解釈する構造である．$\dot{-}, \ell_2, \lambda_2$ は以下のような演算として解釈

される．

$$x \dot{-} y = \begin{cases} x - y & (x \geq y) \\ 0 & (x < y) \end{cases}$$
$$\ell_2(x) = \max\{y \mid 2^y \leq x\}$$
$$\lambda_2(x) = 2^{\ell_2(x)}$$

変数の付値を $\rho : \mathrm{Var} \to \mathbb{N}$ とする．また，ρ を $\rho(0) = 0, \rho(1) = 1$, 項 $t_1, \ldots, t_n$ と関数記号 f に対して $\rho(f(t_1, \ldots, t_n)) = f(\rho(t_1), \ldots, \rho(t_n))$ として項に拡張する．このとき，$\rho \models A$ で，式 A が自由変数の解釈 ρ の下で標準モデルにおいて真であることを表す．この関係は以下のように帰納的に定義される．

$$\begin{aligned}
\rho \models t = u \quad & \textit{iff} \quad \rho(t) = \rho(u) \\
\rho \models t \leq u \quad & \textit{iff} \quad \rho(t) \leq \rho(u) \\
\rho \models \neg A \quad & \textit{iff} \quad \rho \not\models A \\
\rho \models A \wedge B \quad & \textit{iff} \quad \rho \models A \text{ かつ } \rho \models B \\
\rho \models A \vee B \quad & \textit{iff} \quad \rho \models A \text{ または } \rho \models B \\
\rho \models A \to B \quad & \textit{iff} \quad \rho \not\models A \text{ または } \rho \models B \\
\rho \models \exists x A \quad & \textit{iff} \quad \exists n \in \mathbb{N} : \rho[x := n] \models A \\
\rho \models \forall x A \quad & \textit{iff} \quad \forall n \in \mathbb{N} : \rho[x := n] \models A
\end{aligned}$$

定義 3. 全ての変数の付値 ρ に対して $\rho \models A$ のとき，A は**妥当**であるという．ある変数の付値 ρ に対して $\rho \models A$ のとき，A は**充足可能**であるという．

定理 1 ([12])**.** $\mathrm{Pres}_{\mathrm{Exp}}$ の任意の閉式 A が妥当であるかどうかは決定可能である．

3.3 $\mathrm{LI}_{\mathrm{Pres}}$ から $\mathrm{Pres}_{\mathrm{Exp}}$ への変換

本節では $\mathrm{LI}_{\mathrm{Pres}}$ の式を $\mathrm{Pres}_{\mathrm{Exp}}$ の式に変換する写像 $(\cdot)^\bullet$ を定義する．まず $\mathrm{LI}_{\mathrm{Pres}}$ の項の変換を定義する．

$$\begin{aligned}
0^\bullet &= 0 \\
1^\bullet &= 1 \\
\mathsf{nil}^\bullet &= 0 \\
x^\bullet &= x \\
(t+u)^\bullet &= t + u \\
\mathsf{tl}(l)^\bullet &= l^\bullet \dot{-} \lambda_2(l^\bullet) \\
\mathsf{hd}(l)^\bullet &= \ell_2(l^\bullet) \dot{-} \ell_2(\mathsf{tl}(l)^\bullet) \dot{-} 1 \\
\mathsf{cons}(a, \mathsf{nil})^\bullet &= 2^{a^\bullet} \\
\mathsf{cons}(a, l)^\bullet &= 2^{\ell_2(l^\bullet) + a^\bullet + 1} + l^\bullet (\text{for } l \neq \mathsf{nil})
\end{aligned}$$

次に $\mathrm{LI}_{\mathrm{Pres}}$ の式の変換を定義する．

$$\begin{aligned}
(t = u)^\bullet &= t^\bullet = u^\bullet \\
(t \leq u)^\bullet &= t^\bullet \leq u^\bullet \\
(\neg A)^\bullet &= \neg A^\bullet \\
(A \Box B)^\bullet &= A^\bullet \Box B^\bullet \quad (\Box \in \{\wedge, \vee, \to\}) \\
(\forall x A)^\bullet &= \forall x A^\bullet \\
(\exists x A)^\bullet &= \exists x A^\bullet
\end{aligned}$$

以下では項の変換において成り立つ性質を示す．そのためにまずは幾つかの代数的な性質を示す．

補題 1. 全ての自然数 x, y に対し，$2^x + 2^{x+y} < 2^{x+y+1}$ が成り立つ．

証明. $2^{x+y+1} - (2^x + 2^{x+y}) = 2^{x+y+1} - 2^{x+y} - 2^x = 2^{x+y}(2-1) - 2^x = 2^{x+y} - 2^x > 0$ より成り立つ． □

補題 2. 全ての自然数 $a_1, \ldots, a_k$ に対し，$2^{a_1} + a^{a_1+a_2+1} + \ldots + 2^{a_1+\ldots+a_k+k-1} < 2^{a_1+\ldots+a_k+k}$ が成り立つ．

証明.

$$\begin{aligned}
& 2^{a_1+\ldots+a_k+k} - \ldots - a^{a_1+a_2+1} - 2^{a_1} \\
>& 2^{a_1+\ldots+a_k+k} - \ldots - a^{a_1+a_2+a_3+2} \\
& \quad - a^{a_1+a_2+2} && \text{(補題 1)} \\
>& 2^{a_1+\ldots+a_k+k} - \ldots - a^{a_1+a_2+a_3+a_4+3} \\
& \quad - a^{a_1+a_2+a_3+3} && \text{(補題 1)} \\
& \ldots \\
>& 2^{a_1+\ldots+a_k+k} - 2^{a_1+\ldots+a_k+k-1} > 0
\end{aligned}$$

□

補題 3. 全ての自然数 $a_1, \ldots, a_k$ に対し，$\ell_2(2^{a_1} + a^{a_1+a_2+1} + \ldots + 2^{a_1+\ldots+a_k+k-1}) = a_1 + \ldots + a_k + k - 1$ が成り立つ．

証明. $b = 2^{a_1} + a^{a_1+a_2+1} + \ldots + 2^{a_1+\ldots+a_k+k-1}$ とおく．明らかに $2^{a_1+\ldots+a_k+k-1} \leq b$. これと補題 2 より $a_1 + \ldots + a_k + k - 1 \leq \ell_2(b) < a_1 + \ldots + a_k + k$ より成り立つ． □

以下では $\mathsf{cons}(a_k, \mathsf{cons}(a_{k-1}, \ldots, \mathsf{cons}(a_1, \mathsf{nil})))$ を $[|a_k, \ldots, a_1|]$ と表す．

次の命題はリストの符号化が式 (1) の通りであるこ

とを示している．

命題 1. 全ての変数の付値 ρ に対し，$\rho([|a_k,\ldots,a_1|]^\bullet) = 2^{b_1} + 2^{b_1+b_2+1} + \ldots + 2^{b_1+b_2+\ldots+b_k+k-1}$ が成り立つ．ここで $b_i = \rho(a_i^\bullet)$ である．

証明. k の帰納法で示す．$k = 1$ のとき，$\rho(\mathsf{cons}(a_1,\mathsf{nil})^\bullet) = \rho(2^{a_1^\bullet}) = 2^{\rho(a_1^\bullet)}$ より成り立つ．$k = n+1$ のとき，定義より $[|a_{n+1},\ldots,a_1|]^\bullet = 2^{\ell_2([|a_n,\ldots,a_1|]^\bullet)+a_{n+1}^\bullet+1}+[|a_n,\ldots,a_1|]^\bullet$ である．帰納法の仮定より，$\rho([|a_n,\ldots,a_1|]^\bullet) = 2^{b_1} + 2^{b_1+b_2+1} + \ldots + 2^{b_1+b_2+\ldots+b_n+n-1}$．ここで，補題 3 より，$\ell_2(2^{b_1} + 2^{b_1+b_2+1} + \ldots + 2^{b_1+b_2+\ldots+b_n+n-1}) = b_1 + b_2 + \ldots + b_n + n - 1$ であるので，$\rho([|a_{n+1},\ldots,a_1|]^\bullet) = 2^{b_1+b_2+\ldots+b_n+n-1+b_{n+1}+1} + 2^{b_1} + 2^{b_1+b_2+1} + \ldots + 2^{b_1+b_2+\ldots+b_n+n-1} = 2^{b_1} + 2^{b_1+b_2+1} + \ldots + 2^{b_1+b_2+\ldots+b_n+b_{n+1}+n}$．□

補題 4. ρ を変数の付値とする．ある自然数 $a_1,\ldots,a_k$ に対し $\rho(l^\bullet) = 2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+k-1}$ と表せるとき，$\rho(\mathsf{cons}(a,l)^\bullet) = 2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k}$ である．

証明. 定義より $\mathsf{cons}(a,l)^\bullet = 2^{\ell_2(l^\bullet)+a^\bullet+1} + l^\bullet$ である．よって $\rho(\mathsf{cons}(a,l)^\bullet) = \rho(2^{\ell_2(l^\bullet)+a^\bullet+1}) + \rho(l^\bullet)$ である．ここで，$\rho(2^{\ell_2(l^\bullet)+a^\bullet+1}) = 2^{\ell_2(\rho(l^\bullet))+\rho(a^\bullet)+1}$ であり，

$$\begin{aligned}
&\ell_2(\rho(l^\bullet)) + \rho(a^\bullet) + 1\\
=&\ell_2(2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+k-1})\\
&\quad + \rho(a^\bullet) + 1\\
=&a_1 + a_2 + \ldots + a_k + k - 1 + \rho(a^\bullet) + 1 \quad \text{(補題 3)}\\
=&a_1 + a_2 + \ldots + a_k + \rho(a^\bullet) + k
\end{aligned}$$

よって，$\rho(2^{\ell_2(l^\bullet)+a^\bullet+1}) + \rho(l^\bullet) = 2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+k-1} + 2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k}$．□

次の命題は hd,tl の $(\cdot)^\bullet$ による変換が正しいことを述べている．

命題 2. 全ての変数の付値 s に対し

$$s \models \mathsf{hd}(\mathsf{cons}(a,l))^\bullet = a^\bullet \tag{3}$$
$$s \models \mathsf{tl}(\mathsf{cons}(a,l))^\bullet = l^\bullet \tag{4}$$

が成り立つ．

証明. $l = \mathsf{nil}$ のときは明らかなので，以下では $l \neq \mathsf{nil}$ とする．まず (4) を示す．定義より $\mathsf{tl}(\mathsf{cons}(a,l))^\bullet = \mathsf{cons}(a,l)^\bullet \dot{-} \lambda_2(\mathsf{cons}(a,l)^\bullet)$．ここで，$l \neq \mathsf{nil}$ より $\rho(l^\bullet) > 0$ なので，ある自然数 $a_1,\ldots,a_k$ を用いて $\rho(l^\bullet) = 2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+k-1}$ と表せるのは明らかである ($\rho(l^\bullet)$ の 2 進表現から $a_1,\ldots,a_k$ を求めることができる)．したがって補題 4 より $\rho(\mathsf{cons}(a,l)^\bullet) = 2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k}$．このとき

$$\begin{aligned}
&\lambda_2(2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k})\\
=&2^{\ell_2(2^{a_1}+2^{a_1+a_2+1}+\ldots+2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k})}\\
=&2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k} \quad \text{(補題 2)}
\end{aligned}$$

したがって，

$$\begin{aligned}
&\rho(\mathsf{cons}(a,l)^\bullet \dot{-} \lambda_2(\mathsf{cons}(a,l)^\bullet))\\
=&2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k}\\
&\dot{-} 2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k}\\
=&2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+k}\\
=&\rho(l^\bullet)
\end{aligned}$$

次に (3) を示す．

$$\begin{aligned}
&\mathsf{hd}(\mathsf{cons}(a,l))^\bullet\\
=&\ell_2(\mathsf{cons}(a,l)^\bullet) \dot{-} \ell_2(\mathsf{tl}(\mathsf{cons}(a,l))^\bullet) \dot{-} 1\\
=&\ell_2(\mathsf{cons}(a,l)^\bullet) \dot{-} \ell_2(l^\bullet) \dot{-} 1 \quad \text{((4) より)}
\end{aligned}$$

ここで，ある自然数 $a_1,\ldots,a_k$ が存在し $\rho(l^\bullet) = 2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+k-1}$ と表せる．したがって補題 4 より $\rho(\mathsf{cons}(a,l)^\bullet) = 2^{a_1} + 2^{a_1+a_2+1} + \ldots + 2^{a_1+a_2+\ldots+a_k+\rho(a^\bullet)+k}$．したがって，補題 2 より，$\rho(\ell_2(\mathsf{cons}(a,l)^\bullet)) = a_1 + a_2 + \ldots + a_k + \rho(a^\bullet) + k$，$\rho(\ell_2(l^\bullet)) = a_1 + a_2 + \ldots + a_k + k - 1$．したがって，$\rho(\mathsf{hd}(\mathsf{cons}(a,l))^\bullet) = a_1 + a_2 + \ldots + a_k + \rho(a^\bullet) + k \dot{-} (a_1 + a_2 + \ldots + a_k + k - 1) \dot{-} 1 = \rho(a^\bullet)$．□

3.4 $\mathrm{LI}_{\mathrm{Pres}}$ の決定可能性

本節では，$\mathrm{LI}_{\mathrm{Pres}}$ の決定可能性を証明する．目標は以下の定理を示すことである．

定理 2. $\mathrm{LI}_{\mathrm{Pres}}$ の式 A に対し，ある変数の付値 ρ_1 が存在し $\mathcal{M},\rho_1 \models A$ が成り立つのは，ある変数の付値 ρ_2 が存在し $\rho_2 \models A^\bullet$ のとき，かつその時に限る．

定理 2 は言い換えると，$\mathrm{LI}_{\mathrm{Pres}}$ の式 A が充足可能であるのは，$\mathrm{Pres}_{\mathrm{Exp}}$ の式 $A^\bullet$ が充足可能のとき，かつその時に限るということである．

これより次の系を得る．

系 1. $\mathrm{LI}_{\mathrm{Pres}}$ の式の妥当性判定は決定可能である.

証明. 定理 2 より, $\mathrm{LI}_{\mathrm{Pres}}$ の式 A が充足可能であることと $A^\bullet$ が充足可能であることは等価である. これより $\mathrm{LI}_{\mathrm{Pres}}$ の式 $\neg A$ が妥当であることと $\neg A^\bullet$ が妥当であることは等価である. 定理 1 より後者は決定可能である. □

以下では定理 2 を示すために必要な準備を行っていく. まず, リストの集合 $\mathbb{L}$ から自然数の集合 $\mathbb{N}$ への写像 τ を定める.

定義 4. $\tau : \mathbb{L} \to \mathbb{N}$ を以下のように定める.

$$\begin{aligned}\tau([\,]) =& 0\\ \tau([a_1,\ldots,a_n]) =& 2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots +\\ & 2^{a_n+\ldots+a_1+n-1}\end{aligned}$$

命題 3. τ は全単射である.

証明. $\tau(l) = 0$ なら $l = [\,]$, $\tau(l) > 0$ なら, $\tau(l) = \tau([a_1,\ldots,a_n])$ となる $a_1,\ldots,a_n$ は式 (2) のように自然数の 2 進表現から一意に定まることから明らかである. □

定義 5. $\rho : (\mathrm{Var}_N \to \mathbb{N}) \cup (\mathrm{Var}_L \to \mathbb{L})$ を $\mathrm{LI}_{\mathrm{Pres}}$ の付値とする. このとき, $\rho' : \mathrm{Var} \to \mathbb{N}$ をソート N の変数 x に対しては $\rho'(x) = \rho(x)$, ソート L の変数 l に対しては $\rho'(l) = \tau(\rho(l))$ であるような付値とする. ρ' は $\rho'(0) = 0, \rho'(1) = 1$, 項 $t_1,\ldots,t_n$ と関数記号 f に対して $\rho'(f(x_1,\ldots,x_n)) = f(\rho(x_1),\ldots,\rho(x_n))$ として $\mathrm{Pres}_{\mathrm{Exp}}$ の項に拡張する.

ここで, τ が全単射であることから, 任意の ρ に対し $\sigma' = \rho$ となる付値 σ は一意に定まることに注意されたい.

補題 5. $\mathrm{LI}_{\mathrm{Pres}}$ の項 t に対し, t がソート N の項なら $\rho(t) = \rho'(t^\bullet)$ が, t がソート L の項なら $\tau(\rho(t)) = \rho'(t^\bullet)$ が, 成り立つ.

証明. t の構造に関する帰納法で示す.

$t = 0$ のとき, $\rho(0) = 0$ で, $\rho'(0^\bullet) = \rho'(0) = 0$ である. $t = 1$ のときも同様. $t = \mathsf{nil}$ のとき, $\tau(\rho(\mathsf{nil})) = \tau([\,]) = 0$. $\rho'(\mathsf{nil}^\bullet) = \rho'(0) = 0$ より成り立つ.

$t = x + y$ のとき, $\rho(x+y) = \rho(x) + \rho(y) = \rho'(x^\bullet) + \rho'(x^\bullet)$(帰納法の仮定より) $= \rho'(x^\bullet + y^\bullet) = \rho'((x+y)^\bullet)$ より成り立つ.

$t = \mathsf{cons}(a, \mathsf{nil})$ のとき, $\tau(\rho(\mathsf{cons}(a,\mathsf{nil}))) = \tau(\mathsf{cons}^{\mathcal{M}}(\rho(a), \rho([\,]))) = \tau([\rho(a)]) = 2^{\rho(a)}$. 一方, $\rho'(\mathsf{cons}(a,\mathsf{nil})^\bullet) = 2^{\rho'(a)}$. 帰納法の仮定より $\rho(a) = \rho'(a)$ なので成り立つ.

$t = \mathsf{cons}(a, l)$ で $l \neq \mathsf{nil}$ のとき, $\tau(\rho(\mathsf{cons}(a,l))) = \tau(\mathsf{cons}^{\mathcal{M}}(\rho(a), \rho(l)))$. ここで $\rho(l) = [a_1,\ldots,a_n]$ となる $a_1,\ldots,a_n \in \mathbb{N}$ が存在する. したがって, $\tau(\mathsf{cons}^{\mathcal{M}}(\rho(a),\rho(l))) = \tau(\mathsf{cons}^{\mathcal{M}}(a,[a_1,\ldots,a_n])) = \tau([a,a_1,\ldots,a_n]) = 2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_1+a+n}$. 一方, 帰納法の仮定より $\rho'(l^\bullet) = \tau(\rho(l)) = 2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_1+n-1}$ なので, 補題 4 より, $\rho'(\mathsf{cons}(a,l)^\bullet) = 2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_1+a+n}$ である.

$t = \mathsf{hd}(\mathsf{nil})$ のとき, $\rho(\mathsf{hd}(\mathsf{nil})) = \mathsf{hd}^{\mathcal{M}}(\mathsf{nil}^{\mathcal{M}}) = \mathsf{hd}^{\mathcal{M}}([\,]) = 0$. 一方, $\rho'(\mathsf{hd}(\mathsf{nil})^\bullet) = \rho'(\ell_2(\mathsf{nil}^\bullet) \dot{-} \ell_2(\mathsf{tl}(\mathsf{nil})^\bullet) \dot{-} 1) = \rho'(\ell_2(0) \dot{-} \ell_2(\mathsf{tl}(\mathsf{nil})^\bullet) \dot{-} 1) = \ell_2(\rho'(0)) \dot{-} \ell_2(\rho'(\mathsf{tl}(\mathsf{nil})^\bullet)) \dot{-} \rho'(1) = \ell_2(0) \dot{-} \ldots = 0$.

$t = \mathsf{hd}(l)$ で $l \neq \mathsf{nil}$ のとき, $\rho(\mathsf{hd}(l)) = \mathsf{hd}^{\mathcal{M}}(\rho(l))$. ここで, $l \neq \mathsf{nil}$ より, ある $a_1,\ldots,a_n \in \mathbb{N}$ が存在し, $\rho(l) = [a_1,\ldots,a_n]$ である. したがって, $\mathsf{hd}^{\mathcal{M}}(\rho(l)) = \mathsf{hd}^{\mathcal{M}}([a_1,\ldots,a_n]) = a_1$. 一方, $\rho'(\mathsf{hd}(l)^\bullet) = \rho'(\ell_2(l^\bullet) \dot{-} \ell_2(\mathsf{tl}(l)^\bullet) \dot{-} 1) = \ell_2(\rho'(l^\bullet)) \dot{-} \ell_2(\rho'(\mathsf{tl}(l)^\bullet)) \dot{-} 1$. また, $\rho'(\mathsf{tl}(l)^\bullet) = \rho'(l^\bullet \dot{-} \lambda_2(l^\bullet)) = \rho'(l^\bullet) \dot{-} \lambda_2(\rho'(l^\bullet))$. ここで帰納法の仮定より $\rho'(l^\bullet) = \tau(\rho(l)) = \tau([a_1,\ldots,a_n])$ なので, $\rho'(l^\bullet) \dot{-} \lambda_2(\rho'(l^\bullet)) = \tau([a_1,\ldots,a_n]) \dot{-} \lambda_2(\tau([a_1,\ldots,a_n])) = 2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_1+n-1} \dot{-} \lambda_2(2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_1+n-1}) = 2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_1+n-1} \dot{-} 2^{a_n+\ldots+a_1+n-1} = 2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_2+n-2}$. よって, $\ell_2(\rho'(l^\bullet)) \dot{-} \ell_2(\rho'(\mathsf{tl}(l)^\bullet)) + 1 = a_n + \ldots + a_1 + n - 1 \dot{-} (a_n + \ldots + a_2 + n - 2) + 1 = a_1$(補題 3 を利用).

$t = \mathsf{tl}(\mathsf{nil})$ のとき, $\tau(\rho(\mathsf{tl}(\mathsf{nil}))) = \tau(\mathsf{tl}^{\mathcal{M}}(\mathsf{nil}^{\mathcal{M}})) = \tau(\mathsf{tl}^{\mathcal{M}}([\,])) = \tau([\,]) = 0$. 一方, $\rho'(\mathsf{tl}(\mathsf{nil})^\bullet) = \rho'(\mathsf{nil}^\bullet \dot{-} \lambda_2(\mathsf{nil}^\bullet)) = \rho'(0 \dot{-} \lambda_2(0)) = \rho'(0) \dot{-} \lambda_2(\rho'(0)) = 0 \dot{-} 0 = 0$.

$t = \mathsf{tl}(l)$ で $l \neq \mathsf{nil}$ のとき, $\tau(\rho(\mathsf{tl}(l))) = \tau(\mathsf{tl}^{\mathcal{M}}(\rho(l)))$. ここで $l \neq \mathsf{nil}$ より, ある $a_1,\ldots,a_n \in$

$\mathbb{N}$ が存在し，$\rho(l) = [a_1, \ldots, a_n]$ である．したがって，$\tau(\mathsf{tl}^{\mathcal{M}}(\rho(l))) = \tau(\mathsf{tl}^{\mathcal{M}}([a_1, \ldots, a_n])) = \tau([a_2, \ldots, a_n])$．一方，$\rho'(\mathsf{tl}(l)^\bullet) = \rho'(\mathsf{tl}(l)^\bullet \dot{-} \lambda_2(l^\bullet)) = \rho'(l^\bullet) \dot{-} \lambda_2(\rho'(l^\bullet))$．帰納法の仮定より $\rho'(l^\bullet) = \tau(\rho(l)) = \tau([a_1, \ldots, a_n])$．したがって，$\lambda_2(\rho'(l^\bullet)) = \lambda_2(\tau([a_1, \ldots, a_n])) = \lambda_2(2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_1+n-1}) = 2^{a_n+\ldots+a_1+n-1}$($\lambda_2$ の定義と補題 3 より)．これより，$\rho'(l^\bullet) \dot{-} \lambda_2(\rho'(l^\bullet)) = 2^{a_n} + 2^{a_n+a_{n-1}+1} + \ldots + 2^{a_n+\ldots+a_2+n-2} = \tau([a_2, \ldots, a_n])$． □

命題 4. 全ての ρ に対し，$\mathcal{M}, \rho \models A \Leftrightarrow \rho' \models A^\bullet$ が成り立つ．

証明．A の帰納法で示す．

$A = (t = u)$ で t と u がソート N の項のとき，補題 5 より $\rho'(t^\bullet) = \rho(t)$ かつ $\rho'(u^\bullet) = \rho(u)$．よって $\rho(t) = \rho(u) \Leftrightarrow \rho'(t^\bullet) = \rho'(u^\bullet)$．

$A = (t \leq u)$ のときも同様に成り立つ．

$A = (t = u)$ で t と u がソート L の項のとき，補題 5 より $\rho'(t^\bullet) = \tau(\rho(t))$ かつ $\rho'(u^\bullet) = \tau(\rho(u))$．命題 3 より，$\tau$ は全単射なので $\rho'(t^\bullet) = \rho'(u^\bullet) \Leftrightarrow \tau(\rho(t)) = \tau(\rho(u)) \Leftrightarrow \rho(t) = \rho(u)$．

$A = \neg B$ のとき，$\mathcal{M}, \rho \models \neg B \Leftrightarrow \mathcal{M}, \rho \not\models B \Leftrightarrow \rho' \not\models B^\bullet$(帰納法の仮定の対偶) $\Leftrightarrow \rho' \models \neg B^\bullet$．

$A = A \wedge B$ のとき，$\mathcal{M}, \rho \models A \wedge B \Leftrightarrow \mathcal{M}, \rho \models A$ かつ $\mathcal{M}, \rho \models B \Leftrightarrow \rho' \models A^\bullet$ かつ $\rho' \models B^\bullet$(帰納法の仮定) $\Leftrightarrow \rho' \models A^\bullet \wedge B^\bullet$．

$A = \exists \alpha B$ で α がソート L のとき，まず $\mathcal{M}, \rho \models \exists \alpha B \Rightarrow \rho' \models B^\bullet$ を示す．$\mathcal{M}, \rho \models \exists \alpha B \Leftrightarrow$ ある $l \in \mathbb{L}$ が存在し$\rho[\alpha := l] \models B$．$\rho_1 = (\rho[\alpha := l])'$ と定めると，帰納法の仮定より $\rho_1 \models B^\bullet$．ここで，$\rho'[\alpha := \tau(l)] = \rho_1$ であることから，$\rho'[\alpha := \tau(l)] \models B^\bullet$．よって $\rho' \models \exists \alpha B^\bullet$．次に，$\rho' \models B^\bullet \Rightarrow \mathcal{M}, \rho \models \exists \alpha B$ を示す．$\rho' \models \exists \alpha B^\bullet \Leftrightarrow$ ある $n \in \mathbb{N}$ が存在し，$\rho'[\alpha := n] \models B^\bullet$．ここで，命題 3 より，$\tau$ は全単射なので，ある $l \in \mathbb{L}$ が存在し $n = \tau(l)$ である．よって，$\rho'[\alpha := \tau(l)] \models B^\bullet$．帰納法の仮定より $\rho[\alpha := l] \models B$．したがって，$\rho \models \exists \alpha B$．

A が他の場合も同様に示される． □

これで定理 2 の証明の準備が整った．

定理 2. $\mathrm{LI}_{\mathrm{Pres}}$ の式 A に対し，ある変数の付値 ρ_1 が存在し $\mathcal{M}, \rho_1 \models A$ が成り立つのは，ある変数の付値 ρ_2 が存在し $\rho_2 \models A^\bullet$ のとき，かつその時に限る．

証明. only if 方向．ある変数の付値 ρ_1 が存在し $\mathcal{M}, \rho_1 \models A$ が成り立つとする．このとき，命題 4 より，$\rho_1' \models A$ である．

if 方向．ある変数の付値 ρ_2 が存在し $\rho_2 \models A^\bullet$ とする．このとき，$\rho_1 = \rho_2'$ となるような付値が存在する．命題 4 より，$\mathcal{M}, \rho_1 \models A$ である． □

4 プレスバーガー算術を備えた一階分離論理の決定不能性

4.1 分離論理 $\mathrm{SL}_{\mathrm{Pres}}$

本節では，本研究で考えるプレスバーガー算術を備えた一階の分離論理 $\mathrm{SL}_{\mathrm{Pres}}$ の定義を与える．変数の集合を $\mathrm{Var} = \{x, y, \ldots\}$ とする．アドレスの集合と値の集合をともに $\mathbb{N}$ とする．項は以下の文法で与えられる．

$$t ::= x \mid 0 \mid 1 \mid t + t$$

式は以下の文法で与えられる．

$$A ::= t = t \mid t \leq t \mid t \hookrightarrow t \mid A * A \mid \neg A \mid A \wedge A \mid A \vee A \mid A \to A \mid \exists x A \mid \forall x A$$

$x < y$ を $x \leq y \wedge x \neq y$ により定義される述語とする．$x \mapsto -$ を $\exists y(x \mapsto y)$ の略記，$\forall x \leq t\ A$ を $\forall x(x \leq t \to A)$ の略記，true を $0 = 0$ の略記とする．

$s : \mathrm{Var} \to \mathbb{N}$ を変数の付値とする．s を $s(0) = 0, s(1) = 1$, 項 $t_1, \ldots, t_n$ と関数記号 f に対して $s(f(t_1, \ldots, t_n)) = f(s(t_1), \ldots, s(t_n))$ として項に拡張する．また，$n \in \mathbb{N}$ に対し $s[x := n]$ で，x に対し n を割り当て，x 以外の変数 y に対しては $s(y)$ を割り当てる変数の付値を表す．ヒープ $h : \mathbb{N} \to \mathbb{N}$ をドメインが有限となるような部分関数とする．ヒープはメモリの状態を表している．ヒープ h_1 と h_2 に対し，$h_1 \perp h_2 \Leftrightarrow \mathsf{Dom}(h_1) \cap \mathsf{Dom}(h_2) = \emptyset$ と定義する．$h_1 \perp h_2$ のとき，$h_1 \uplus h_2$ を h_1 と h_2 の和ヒープとする．$\mathrm{SL}_{\mathrm{Pres}}$ の式 A が変数の付値 s とヒープ h に対し真である，という関係を $s, h \models A$ と表す．この

関係は以下のように帰納的に定義される．

$$
\begin{array}{lll}
s,h \models t_1 = t_2 & \text{iff} & s(t_1) = s(t_2) \\
s,h \models t_1 \leq t_2 & \text{iff} & s(t_1) \leq s(t_2) \\
s,h \models t_1 \hookrightarrow t_2 & \text{iff} & h(s(t_1)) = s(t_2) \\
s,h \models A_1 * A_2 & \text{iff} & \exists h_1, h_2 : h_1 \perp h_2 \text{ かつ} \\
 & & h_1 \uplus h_2 = h \text{ かつ} \\
 & & s,h_1 \models A_1 \text{ かつ } s,h_2 \models A_2 \\
s,h \models \neg A & \text{iff} & s,h \not\models A \\
s,h \models A_1 \wedge A_2 & \text{iff} & s,h \models A_1 \text{ かつ } s,h \models A_2 \\
s,h \models A_1 \vee A_2 & \text{iff} & s,h \models A_1 \text{ または } s,h \models A_2 \\
s,h \models A_1 \to A_2 & \text{iff} & s,h \not\models A_1 \text{ または } s,h \models A_2 \\
s,h \models \exists x A & \text{iff} & \exists n \in \mathbb{N} : s[x := n], h \models A \\
s,h \models \forall x A & \text{iff} & \forall n \in \mathbb{N} : s[x := n], h \models A
\end{array}
$$

全ての s と h で $s,h \models A$ が成り立つとき，A は**妥当**であるという．

$\hookrightarrow$ の定義より，本論理は 1 フィールドのメモリモデルを採用していることに注意されたい．プレスバーガー算術を除けばこの論理は決定可能である [3].

4.2 一階算術の論理 L_{bPA}

この節では一階算術の論理 L_{bPA} の定義を与える．

定義 6. L_{bPA} を二項関数記号 $+$, 二項述語記号 $\leq$, 三項述語記号 Mult, 定数記号 $0, 1$ をシグネチャとする一階の論理とする．$\mathrm{Var} = \{x, y, \ldots\}$ を変数の集合とする．項は以下の文法で与えられる．

$$t ::= x \mid 0 \mid 1 \mid t + t$$

L_{bPA} の式は以下の文法の A で与えられる．

$$
\begin{aligned}
B ::= & t = t \mid t \leq t \mid \mathsf{Mult}(t,t,t) \mid \neg B \mid \\
& B \wedge B \mid B \vee B \mid B \to B \\
A ::= & B \mid \exists x A \mid \forall x \leq t\ A
\end{aligned}
$$

この文法の定義より，L_{bPA} の式は全て冠頭標準形である．L_{bPA} の**標準モデル**を $\mathcal{N}$ とする．$\mathcal{N}$ は宇宙を $\mathbb{N}$ とし，$+$ を自然数の $+$, $0, 1$ をそれぞれ自然数の $0, 1$ と解釈する構造である．変数の付値を $s : \mathrm{Var} \to \mathbb{N}$ とする．s を $s(0) = 0, s(1) = 1$, 項 $t_1, \ldots, t_n$ と関数記号 f に対して $s(f(t_1, \ldots, t_n)) = f(s(t_1), \ldots, s(t_n))$ として項に拡張する．また，$n \in \mathbb{N}$ に対し $s[x := n]$ で，x に対し n を割り当て，x 以外の変数 y に対しては $s(y)$ を割り当てる変数の付値を表す．このとき，$s \models A$ で，式 A が自由変数の解釈 s の下で標準モデルにおいて真であることを表す．この関係は以下のように帰納的に定義される．

$$
\begin{array}{lll}
s \models t = u & \textit{iff} & s(t) = s(u) \\
s \models t \leq u & \textit{iff} & s(t) \leq s(u) \\
s \models \mathsf{Mult}(t,u,v) & \textit{iff} & s(t) \times s(u) = s(v) \\
s \models \neg A & \textit{iff} & s \not\models A \\
s \models A \wedge B & \textit{iff} & s \models A \text{ かつ } s \models B \\
s \models A \vee B & \textit{iff} & s \models A \text{ または } s \models B \\
s \models A \to B & \textit{iff} & s \not\models A \text{ または } s \models B \\
s \models \exists x A & \textit{iff} & \exists n \in \mathbb{N} : s[x := n] \models A \\
s \models \forall x \leq t\ A & \textit{iff} & \forall n \leq s(t) : s[x := n] \models A
\end{array}
$$

全ての変数の付値 s に対して $s \models A$ のとき，A は**妥当**であるという．

定理 3. L_{bPA} の任意の文 A が妥当であるかどうかは決定不能である．

証明. クリーネの T 述語は原始帰納的であるため L_{bPA} の式で表現可能である (例えば [8] Theorem 1.2.19 参照)．すると停止集合 (Halting set) は $\{x \mid \exists z T(x,x,z)\}$ として表現できることによる． □

4.3 L_{bPA} から $\mathrm{SL}_{\mathrm{Pres}}$ への変換

本節では L_{bPA} の式を $\mathrm{SL}_{\mathrm{Pres}}$ の式に変換する写像を定義する．ここでは L_{bPA} の式 A は冠頭標準形で，本体は選言標準形であるとする (以下では冠頭選言標準形と呼ぶ)．すなわち，$A = Q_1 x_1 \ldots Q_n x_n (B_1 \vee \ldots \vee B_n)$, $B_i = C_1^i \wedge \ldots \wedge C_{i_k}^i (i \in \{1, \ldots, n\})$, $C_j^i (j \in \{1, \ldots, i_k\})$ はリテラル (原子論理式またはその否定), $Q_i x_i$ は $\exists x_i$ か $\forall x_i \leq t_i$ とする．

このとき，変換 $(\cdot)^\circ$ を次のように定義する．

$$
\begin{aligned}
(t = u)^\circ &= t = u \\
(t \neq u)^\circ &= t \neq u \\
(t \leq u)^\circ &= t \leq u \\
(t \not\leq u)^\circ &= t \not\leq u \\
\mathsf{Mult}(x,y,z)^\circ &= \exists b(\forall i(i \leq x \leftrightarrow b + i \hookrightarrow -) \\
&\qquad \wedge b \hookrightarrow 0 \wedge b + y \hookrightarrow z \\
&\qquad \wedge \forall i(i < y \rightarrow \forall w(b + i \hookrightarrow w \\
&\qquad\qquad \rightarrow b + i + 1 \hookrightarrow w + x))) \\
(\neg\mathsf{Mult}(x,y,z))^\circ &= \exists w(\mathsf{Mult}(x,y,w)^\circ \wedge z \neq w) \\
(C_1 \wedge \ldots \wedge C_k)^\circ &= C_1^\circ * \mathsf{true} \wedge \ldots \wedge C_k^\circ * \mathsf{true} \\
(B_1 \vee \ldots \vee B_k)^\circ &= B_1^\circ \vee \ldots \vee B_k^\circ \\
(\exists x A)^\circ &= \exists x A^\circ \\
(\forall x \leq t\ A)^\circ &= \forall x \leq t(A^\circ * \mathsf{true})
\end{aligned}
$$

$(\mathsf{Mult}(x,y,z))^\circ$ は，あるベースアドレス b に値 0 を格納し，隣り合う y 個のメモリセルに x を次々に足していった値が格納されたメモリ状態を表している．これにより，最後のセル (アドレス $b+y$) には値 $x \times y$ が格納されることになり，これが z となる．

4.4 分離論理 $\mathrm{SL}_{\mathrm{Pres}}$ の決定不能性

本節では $\mathrm{SL}_{\mathrm{Pres}}$ の決定不能性を証明する．目標は，次の定理を示すことである．

定理 4. A を L_{bPA} の式とするとき，ある s が存在して $s \models A$ であるのは，ある s とヒープ h が存在して $s, h \models A^\circ$ のとき，かつその時に限る．

この定理より以下が成り立つ．

系 2. A を L_{bPA} の文とするとき，A が妥当である *iff* $\neg A^\circ$ が妥当ではない．

証明. L_{bPA} の文が充足可能であることと妥当であることは等価なので，定理 4 より，L_{bPA} の文 A が妥当であることと，A° が充足可能であることは等価である．これより L_{bPA} の式 A が妥当であることと，$\neg A^\circ$ が妥当でないことは等価である． □

定理 3 と系 2 より，$\mathrm{SL}_{\mathrm{Pres}}$ の決定不能性を得る．

定理 5. $\mathrm{SL}_{\mathrm{Pres}}$ の式 A の妥当性判定は決定不能である．

したがって，以下では定理 4 を証明していく．その方針は，まず L_{bPA} の選言標準形の A が限量子なしのときに，$s \models A \Leftrightarrow \exists h(s, h \models A^\circ)$ が成り立つことを示す (命題 5)．次に，A が $s \models A \Leftrightarrow \exists h(s, h \models A^\circ)$ を満たす場合に，$\exists x A$ と $\forall x \leq t\ A$ の場合についても成り立つことを示す (命題 6, 7)．最後に，定理 4 は限量子の数に関する帰納法により証明する．

したがって，まずは次の命題を証明する．

命題 5. A が限量子なしの選言標準形の L_{bPA} の式のとき，$s \models A$ *iff* あるヒープ h が存在して $s, h \models A^\circ$.

このために次の二つの補題が必要になるのでそれを示す．

補題 6. 以下の二つが成り立つ．*(i)* $s \models \mathsf{Mult}(x,y,z)$ *iff* あるヒープ h が存在し $s, h \models \mathsf{Mult}(x,y,z)^\circ$. *(ii)* $s \models \neg\mathsf{Mult}(x,y,z)$ *iff* あるヒープ h が存在し $s, h \models (\neg\mathsf{Mult}(x,y,z))^\circ$.

証明. (i) の証明．only if 方向を示す．$s \models \mathsf{Mult}(x,y,z)$ より，$s(x) \times s(y) = s(z)$．このとき，ある $b \in \mathbb{N}$ に対し，$h(b) = 0$, $h(b+1) = s(x)$, $h(b+2) = s(x) \times 2$, ..., $h(b + s(y)) = s(x) \times s(y)$ となる h を選べばよい．次に if 方向を示す．仮定より，ある h である $b \in \mathbb{N}$ に対し，$h(b) = 0$, $h(b+1) = s(x)$, $h(b+2) = s(x) \times 2$, ..., $h(b + s(y)) = s(z)$．ここで，全ての $i \in \{0, \ldots, s(y)\}$ に対し，$h(b+i) = s(x) \times i$ であることは容易にわかる．よって $s(x) \times s(y) = s(z)$ すなわち $s \models \mathsf{Mult}(x,y,z)$.

(ii) の証明．$s \models \neg\mathsf{Mult}(x,y,z)$ iff $s \models \exists w(\mathsf{Mult}(x,y,z) \wedge w \neq z)$ であることは容易にわかる．したがって，$s \models \exists w(\mathsf{Mult}(x,y,z) \wedge w \neq z)$ iff あるヒープ h が存在して $s, h \models \exists w(\mathsf{Mult}(x,y,z)^\circ \wedge w \neq$

$z)$ を示せばよい．

$s \models \exists w(\mathsf{Mult}(x,y,z) \wedge w \neq z)$
$\Leftrightarrow \exists n \in \mathbb{N} : (s[w := n] \models \mathsf{Mult}(x,y,w) \wedge w \neq z)$
$\Leftrightarrow \exists n \in \mathbb{N} : (s[w := n] \models \mathsf{Mult}(x,y,w)$ かつ
$s[w := n] \models w \neq z)$
$\Leftrightarrow \exists n \in \mathbb{N} : (\exists h : (s[w := n], h \models \mathsf{Mult}(x,y,w)^\circ)$ かつ
$s[w := n] \models w \neq z)$ ((i) より)
$\Leftrightarrow \exists n \in \mathbb{N} : (\exists h : (s[w := n], h \models \mathsf{Mult}(x,y,w)^\circ$ かつ
$s[w := n], h \models w \neq z))$
(h に依存しないため)
$\Leftrightarrow \exists n \in \mathbb{N} : (\exists h : s[w := n], h \models \mathsf{Mult}(x,y,w)^\circ \wedge w \neq z)$
$\Leftrightarrow \exists h : (s, h \models \exists w(\mathsf{Mult}(x,y,z)^\circ \wedge w \neq z))$
以上により示された． □

補題 7. $s, h \models \mathsf{Mult}(x,y,z)^\circ$ なら，ある h' が存在し，$s, h' \models \mathsf{Mult}(x,y,z)^\circ$ かつ $\max \mathsf{Dom}(h') - \min \mathsf{Dom}(h') = s(y)$.

証明. ある $b \in \mathbb{N}$ に対し，$\mathsf{Dom}(h') = \{b, b+1, \ldots, b+s(y)\}$, $h'(b) = 0$, $h'(b+1) = s(x)$, $h'(b+2) = s(x) \times 2$ …, $h'(b+s(y)) = s(x) \times s(y)$ とすれば所望の h' を得る． □

次に，ヒープの平行関係を定義する．自然数の集合 S と整数 d に対し，集合 $S + d = \{x + d \mid x \in S\}$ とする．

定義 7. ヒープ h と h' が平行である *($h \parallel h'$)* とは，ある整数 d が存在し $\min \mathsf{Dom}(h) + d \geq 0$ かつ $\mathsf{Dom}(h') = \mathsf{Dom}(h) + d$ かつ $h(x) = h'(x+d)$ のとき，かつそのときに限る．

ヒープ間の平行関係は，あるヒープの内容を全て一定のアドレスだけ左（あるいは右）にずらした関係にあることを意味している．

補題 8. 以下の二つが成り立つ．*(i)* $s, h \models \mathsf{Mult}(x,y,z)^\circ$ のとき，h と平行な全ての h' に対し，$s, h' \models \mathsf{Mult}(x,y,z)^\circ$ が成り立つ．*(ii)* $s, h \models \neg\mathsf{Mult}(x,y,z)^\circ$ のとき，h と平行な全ての h' に対し，$s, h' \models (\neg\mathsf{Mult}(x,y,z))^\circ$ が成り立つ．

証明. (i) の証明．$s, h \models \mathsf{Mult}(x,y,z)^\circ$ なので，補題 7 より，h はある $b \in \mathbb{N}$ で $h(b) = 0$, $h(b+1) = s(x)$, $h(b+2) = s(x) \times 2$, …, $h(b + s(y)) = s(x) \times s(y)$ となるように選んでよい．このとき，h' を h と平行なヒープとすると，ある整数 d が存在し，$b + d \geq 0$ で，$h'(b+d) = 0$, $h'(b+d+1) = s(x)$, $h'(b+d+2) = s(x) \times 2$, …, $h'(b+d+s(y)) = s(x) \times s(y)$ となる．よって明らかに $s, h' \models \mathsf{Mult}(x,y,z)^\circ$ である．

(ii) の証明．

$s, h \models \mathsf{Mult}(x,y,z)^\circ$
$\Leftrightarrow s, h \models \exists w(\mathsf{Mult}(x,y,z)^\circ \wedge w \neq z)$
$\Leftrightarrow \exists n \in \mathbb{N} : s[w := n], h \models \mathsf{Mult}(x,y,z)^\circ \wedge w \neq z$
$\Leftrightarrow \exists n \in \mathbb{N} : s[w := n], h \models \mathsf{Mult}(x,y,z)^\circ$ かつ
$s[w := n], h \models w \neq z$ (1)

ここで h' を h と平行なヒープとすると，(i) より

(1) $\Leftrightarrow \exists n \in \mathbb{N} : s[w := n], h' \models \mathsf{Mult}(x,y,z)^\circ$ かつ
$s[w := n], h \models w \neq z$
$\Leftrightarrow \exists n \in \mathbb{N} : s[w := n], h' \models \mathsf{Mult}(x,y,z)^\circ$ かつ
$s[w := n], h' \models w \neq z$
(ヒープと関係ないため)
$\Leftrightarrow \exists n \in \mathbb{N} : s[w := n], h' \models \mathsf{Mult}(x,y,z)^\circ \wedge w \neq z$
$\Leftrightarrow s, h' \models \exists w(\mathsf{Mult}(x,y,z)^\circ \wedge w \neq z)$
$\Leftrightarrow s, h' \models (\neg\mathsf{Mult}(x,y,z))^\circ$

□

準備が整ったので命題 5 を証明する．

命題 5 の証明. A の構造に関する帰納法で示す．

(i) $A = (t \bowtie u)(\bowtie \in \{=, \neq, \leq, \not\leq\})$ のとき，$A = A^\circ$ より明らか．$A = \mathsf{Mult}(x,y,z)$, $A = \neg\mathsf{Mult}(x,y,z)$ のときは補題 6 より従う．

(ii) $A = B_1 \wedge \ldots \wedge B_n$ で $B_i (i \in \{1, \ldots, n\})$ がリテラルとする．まず only if 方向を示す．

$s \models A \Leftrightarrow s \models B_1$ かつ … かつ $s \models B_n$
$\overset{\text{i.h.}}{\Leftrightarrow} \exists h_1(s, h_1 \models B_1^\circ)$ かつ … かつ
$\exists h_n(s, h_n \models B_n^\circ)$ (5)

ここで，$B_i = (t \bowtie u)(\bowtie \in \{=, \neq, \leq, \not\leq\})$ の場合は，$\mathsf{Dom}(h_i) = \emptyset$ なる h_i が選べる．また，$B_i = \mathsf{Mult}(x,y,z)$ あるいは $B_i = \neg\mathsf{Mult}(x,y,z)$ なら，補題 7,8 より，$\mathsf{Dom}(h_i) = \{\max \mathsf{Dom}(h_{i-1}) + 1, \ldots, \max \mathsf{Dom}(h_{i-1}) + 1 + s(y)\}$ なる h_i が選べる．ただし，$\mathsf{Dom}(h_0) = \emptyset$ とし，$\mathsf{Dom}(h_{i-1}) = \emptyset$

のときは $\max \mathsf{Dom}(h_{i-1}) = 0$ とする．すると，$h_1 \perp \ldots \perp h_n$ である．$h = h_1 \uplus \ldots \uplus h_n$ とすると，式 (5) が成り立つとき，$s, h \models B_1^\circ * \mathsf{true}$ かつ ... かつ $s, h \models B_n^\circ * \mathsf{true}$ である．したがって，ある h が存在して $s, h \models B_1^\circ * \mathsf{true} \wedge \ldots \wedge B_n^\circ * \mathsf{true}$ すなわち $s, h \models (B_1 \wedge \ldots \wedge B_n)^\circ$ を得る．次に if 方向を示す．

$\exists h(s, h \models (B_1 \wedge \ldots \wedge B_n)^\circ)$
$\Leftrightarrow \exists h(s, h \models B_1 * \mathsf{true} \wedge \ldots \wedge B_n * \mathsf{true})$
$\Leftrightarrow \exists h(s, h \models B_1 * \mathsf{true}$ かつ ... かつ $s, h \models B_n * \mathsf{true})$
$\Rightarrow \exists h(s, h \models B_1 * \mathsf{true})$ かつ ... かつ
$\quad \exists h(s, h \models B_n * \mathsf{true})$
$\overset{\text{i.h.}}{\Leftrightarrow} s \models B_1$ かつ ... かつ $s \models B_n$
$\Leftrightarrow s \models B_1 \wedge \ldots \wedge B_n$

(iii) $A = B_1 \vee \ldots \vee B_n$ で各 B_i はリテラルの連言のとき，

$s \models A$
$\Leftrightarrow s \models B_1$ または ... または $s \models B_n$
$\overset{\text{i.h.}}{\Leftrightarrow} \exists h_1(s, h_1 \models B_1^\circ)$ または ... または
$\quad \exists h_n(s, h_n \models B_n^\circ)$
$\Leftrightarrow \exists h(s, h \models B_1^\circ$ または ... または $s, h \models B_n^\circ)$
$\Leftrightarrow \exists h(s, h \models B_1^\circ \vee \ldots \vee B_n^\circ)$

□

次に，$\exists x A$ の場合について証明する．

命題 6. 全ての s に対し，$s \models A$ *iff* あるヒープ h が存在し $s, h \models A^\circ$ ならば，全ての s に対し，$s \models \exists x A$ *iff* あるヒープ h が存在し $s, h \models \exists x A^\circ$．

証明.

$s \models \exists x A$
$\Leftrightarrow \exists x \in \mathbb{N} : s[x := n] \models A$
$\Leftrightarrow \exists x \in \mathbb{N} : \exists h : (s[x := n], h \models A^\circ)$ (仮定より)
$\Leftrightarrow \exists h : \exists x \in \mathbb{N} : s[x := n], h \models A^\circ$
$\Leftrightarrow \exists h : (s, h \models \exists x A^\circ)$

□

最後に，$\forall x \leq t$ A の場合について証明するが，それにはいくつかの補題が必要となる．まず，L_{bPA} の式 A に対し，A° が充足可能，すなわちある s, h に対し $s, h \models A^\circ$ が成り立つなら，h を任意に平行移動したヒープ h' も A° のモデルになること (補題 11) を示す．それを示すためにやはりいくつかの補題が必要となる．

補題 9. A を限量子なしの選言標準形の L_{bPA} の式とする．$s, h \models A^\circ$ ならば，h と平行な全ての h' に対し，$s, h' \models A^\circ$ が成り立つ．

証明. A の構造帰納法で証明する．

(i) $A = (t \bowtie u)(\bowtie \in \{=, \neq, \leq, \not\leq\})$ のとき，ヒープとは関係ないので成り立つ．$A = \mathsf{Mult}(x, y, z)$, $A = (\neg \mathsf{Mult}(x, y, z))^\circ$ のときは補題 8 より成り立つ．

(ii) $A = B_1 \wedge \ldots \wedge B_n$ で $B_i (i \in \{1, \ldots, n\})$ がリテラルとする．

$s, h \models A^\circ$
$\Leftrightarrow s, h \models B_1^\circ * \mathsf{true} \wedge \ldots \wedge B_n^\circ * \mathsf{true}$
$\Leftrightarrow s, h \models B_1^\circ * \mathsf{true}$ かつ ... かつ $s, h \models B_1^\circ * \mathsf{true}$

ここで，$i \in \{1, \ldots, n\}$ に対し，$s, h \models B_i^\circ * \mathsf{true}$ はある h_1, h_2 が存在し $h_1 \perp h_2$ かつ $h = h_1 \uplus h_2$ で $s, h_1 \models B_i^\circ$ かつ $s, h_2 \models \mathsf{true}$ と等価である．(i) より $\forall h_1' \parallel h_1 : s, h_1' \models B_i^\circ$ であり，true はどんなヒープでも真である．したがって $\forall h' \parallel h : s, h' \models B_i^\circ * \mathsf{true}$ である．これより

$\Leftrightarrow s, h \models B_1^\circ * \mathsf{true}$ かつ ... かつ $s, h \models B_1^\circ * \mathsf{true}$
$\Rightarrow \forall h' \parallel h : s, h' \models B_1^\circ * \mathsf{true}$ かつ ... かつ
$\quad \forall h' \parallel h : s, h' \models B_n^\circ * \mathsf{true}$
$\Rightarrow \forall h' \parallel h : (s, h' \models B_1^\circ * \mathsf{true}$ かつ ... かつ
$\quad s, h' \models B_n^\circ * \mathsf{true})$
$\Leftrightarrow \forall h' \parallel h : s, h' \models B_1^\circ * \mathsf{true} \wedge \ldots \wedge B_n^\circ * \mathsf{true}$
$\Leftrightarrow \forall h' \parallel h : s, h' \models A^\circ$

(iii) $A = B_1 \vee \ldots \vee B_n$ で各 B_i はリテラルの連言のとき，

$s, h \models A^\circ$
$\Leftrightarrow s, h \models B_1^\circ \vee \ldots \vee B_n^\circ$
$\Leftrightarrow s, h \models B_1^\circ$ または ... または $s, h \models B_n^\circ$
$\Leftrightarrow \forall h' \parallel h : s, h \models B_1^\circ$ または ... または
$\quad \forall h' \parallel h : s, h \models B_n^\circ$ ((ii) より)
$\Rightarrow \forall h' \parallel h : (s, h \models B_1^\circ$ または ... または $s, h \models B_n^\circ)$
$\Leftrightarrow \forall h' \parallel h : s, h \models B_1^\circ \vee \ldots \vee B_n^\circ$
$\Leftrightarrow \forall h' \parallel h : s, h \models A^\circ$

□

補題 10. L_{bPA} の式 A に対し，任意の s に対し

て，$s,h \models A$ のとき，h と平行な全ての h' に対し $s,h' \models A$ が成り立つとする．このとき以下の二つが成り立つ．*(i)* 任意の s に対して，$s,h \models \exists x A$ が成り立つとき，h と平行な全ての h' に対し $s,h' \models \exists x A$ が成り立つ．*(ii)* 任意の s に対して，$s,h \models \forall x \leq t\ A$ が成り立つとき，h と平行な全ての h' に対し $s,h' \models \forall x \leq t\ A$ が成り立つ．

証明．(i) の証明．

$$
\begin{aligned}
& s,h \models \exists x A \\
\Leftrightarrow & \exists n \in \mathbb{N} : s[x := n], h \models A \\
\Leftrightarrow & \exists n \in \mathbb{N} : \forall h' \parallel h : s[x := n], h' \models A \quad \text{(仮定より)} \\
\Rightarrow & \forall h' \parallel h : \exists n \in \mathbb{N} : s[x := n], h' \models A \\
\Leftrightarrow & \forall h' \parallel h : s,h' \models \exists A
\end{aligned}
$$

(ii) の証明．

$$
\begin{aligned}
& s,h \models \forall x \leq t\ A \\
\Leftrightarrow & \forall n \leq s(t) : s[x := n], h \models A \\
\Leftrightarrow & \forall n \leq s(t) : \forall h' \parallel h : s[x := n], h' \models A \\
& \qquad\qquad\qquad\qquad\qquad\qquad \text{(仮定より)} \\
\Leftrightarrow & \forall h' \parallel h : \forall n \leq s(t) : s[x := n], h' \models A \\
\Leftrightarrow & \forall h' \parallel h : s,h' \models \forall x \leq t\ A
\end{aligned}
$$

□

これで準備が整ったので，我々の目標としていた主張を証明する．

補題 11. A を冠頭選言標準形の L_{bPA} の式とする．$s,h \models A^\circ$ なら，h と平行な全ての h' に対し，$s,h' \models A^\circ$．

証明．A の限量子の数に関する帰納法で証明する．

(i) A が限量子を含まないとき，補題 9 より成り立つ．

(ii) $A = \exists x B$ のとき，$A^\circ = \exists x B^\circ$ である．$s,h \models \exists x B^\circ$ とすると，ある $n \in \mathbb{N}$ で $s[x := n], h \models B^\circ$．帰納法の仮定より h と平行な全ての h' に対し，$s[x := n], h' \models B^\circ$．よって補題 10(i) より，$s[x := n], h' \models \exists x B^\circ$ を得る．$\exists x B^\circ$ 中では x は自由変数ではないので $s,h' \models \exists x B^\circ$ である．

$A = \forall x \leq t\ B$ のとき，$A^\circ = \forall x \leq t(B^\circ * \mathsf{true})$．

いま，$s,h \models \forall x \leq t(B^\circ * \mathsf{true})$ とする．すると全ての $n \leq s(t)$ に対し，$s[x := n], h \models B^\circ * \mathsf{true}$．帰納法の仮定より，$h$ と平行な全ての h' に対し，$s[x := n], h' \models B^\circ * \mathsf{true}$．すると補題 10(ii) より，全ての $n \leq s(t)$ に対し，h と平行な全ての h' に対し $s[x := n], h' \models \forall x \leq t(B^\circ * \mathsf{true})$ を得る．$\forall x \leq t(B^\circ * \mathsf{true})$ 中では x は自由変数ではないので $s,h' \models \forall x \leq t(B^\circ * \mathsf{true})$．□

これより次の命題を得る．

命題 7. 全ての s に対し，$s \models A$ *iff* あるヒープ h が存在し $s,h \models A^\circ$ ならば，全ての s に対し，$s \models \forall x \leq t\ A$ *iff* あるヒープ h が存在し $s,h \models \forall x \leq t(A^\circ * \mathsf{true})$．

証明．only if の証明．

$$
\begin{aligned}
& s \models \forall x \leq t\ A \\
\Leftrightarrow & \forall n \leq s(t) : s[x := n] \models A \\
\Leftrightarrow & \forall n \leq s(t) : \exists h_n : s[x := n], h_n \models A^\circ \quad \text{(仮定)} \\
\Leftrightarrow & \exists h_0 : (s[x := 0], h_0 \models A^\circ) \text{ かつ } \ldots \text{ かつ} \\
& \quad \exists h_{s(t)} : (s[x := s(t)], h_{s(t)} \models A^\circ)
\end{aligned}
$$

そのような $h_0,\ldots,h_{s(t)}$ をそれぞれ一つ選ぶ．全ての $i \in \{0,\ldots,s(t)\}$ に対し，$s[x := i], h_i \models A^\circ$ と補題 11 より，h_i と平行な全ての h_i' に対し，$s[x := i], h_i' \models A^\circ$ である．したがって，$h_0,\ldots,h_{s(t)}$ とそれぞれ平行な $h_0',\ldots,h_{s(t)}'$ で $h_0' \perp \ldots \perp h_{s(t)}'$ なるものが存在する．このとき $h' = h_0' \uplus \ldots \uplus h_{s(t)}'$ とすると，$s[x := 0], h' \models A^\circ * \mathsf{true}$ かつ $\ldots$かつ $s[x := s(t)], h' \models A^\circ * \mathsf{true}$ が成り立つ．よって，$s,h' \models \forall x \leq t(A^\circ * \mathsf{true})$．

if の証明．

$$
\begin{aligned}
& \exists h : s,h \models \forall x \leq t(A^\circ * \mathsf{true}) \\
\Leftrightarrow & \forall n \leq s(t) : s[x := n], h \models A^\circ * \mathsf{true} \\
\Leftrightarrow & \forall n \leq s(t) : \exists h_1, h_2 \text{ s.t. } h_1 \perp h_2 \wedge h = h_1 \uplus h_2 : \\
& \quad s[x := n], h_1 \models A^\circ \text{ かつ } s[x := n], h_2 \models \mathsf{true} \\
\Rightarrow & \forall n \leq s(t) : \exists h_1 : s[x := n], h_1 \models A^\circ \\
\Leftrightarrow & \forall n \leq s(t) : s[x := n] \models A \qquad \text{(仮定)} \\
\Leftrightarrow & s \models \forall x \leq t\ A
\end{aligned}
$$

□

これで定理 4 の証明の準備が整った．

定理 4. A を L_{bPA} の式とするとき，ある s が存在し

て $s \models A$ であるのは，ある s とヒープ h が存在して $s, h \models A^\circ$ のとき，かつその時に限る．

証明．限量子の数の帰納法で証明する．

(i) A が限量子を含まないとき，命題 5 より従う．

(ii) $A = \exists x B$ のとき，命題 6 より従う．$A = \forall x \leq t\ B$ のとき，命題 7 より従う． □

5 まとめと今後の課題

本稿では演繹的手法によるソフトウェア検証で用いることを念頭に置いた，算術を持つ論理の決定可能性について明らかにした．一つは，通常の一階述語論理にプレスバーガー算術とリストのデータ構造を持つ論理が決定可能であることを明らかにした．また，points-to 演算と $*$ のみをもつ一階の分離論理にプレスバーガー算術を追加した論理は決定不能であることを明らかにした．

本研究の発見により，加法とリストを扱うプログラムの演繹的検証において，エンテイルメントを自動で判定することが可能となった．一方で，ポインタ算術などメモリ上の性質を検証するための論理では，一般的な論理式のエンテイルメントの判定は完全な自動化は不可能であることが明らかになった．

今後の方向性としては，プレスバーガー算術に加え，データ構造として木を持つ場合の論理の決定可能性について明らかにすることが考えられる．算術を持つ分離論理においては，記号的ヒープの場合プレスバーガー算術を追加しても決定可能であることが知られている [15] が，本研究により構文制約がない場合は決定不能であることが明らかになった．そこで，構文制約としてどこまで緩和すると決定不能になるのか明らかにすることは意義のあることである．また，構文制約のない場合に，定数の 1 と後継者関数のみの，いわば最小限の算術を追加した場合の決定可能性について明らかにすることも考えられる．

謝辞 この研究は JSPS 科研費 JP21K11756 と 2023 年度国立情報学研究所公募型共同研究 (23FP03) の助成を受けています．

参 考 文 献

[1] Berdine, J., Calcagno, C., and O'Hearn, P. W.: A Decidable Fragment of Separation Logic, *FSTTCS 2004: Foundations of Software Technology and Theoretical Computer Science, 24th International Conference, Chennai, India, December 16-18, 2004, Proceedings*, Lodaya, K. and Mahajan, M.(eds.), Lecture Notes in Computer Science, Vol. 3328, Springer, 2004, pp. 97–109.

[2] Berdine, J., Calcagno, C., and O'Hearn, P. W.: Symbolic Execution with Separation Logic, *Programming Languages and Systems, Third Asian Symposium, APLAS 2005, Tsukuba, Japan, November 2-5, 2005, Proceedings*, Yi, K.(ed.), Lecture Notes in Computer Science, Vol. 3780, Springer, 2005, pp. 52–68.

[3] Brochenin, R., Demri, S., and Lozes, É.: On the almighty wand, *Inf. Comput.*, Vol. 211(2012), pp. 106–137.

[4] Brotherston, J. and Kanovich, M. I.: On the Complexity of Pointer Arithmetic in Separation Logic, *Programming Languages and Systems - 16th Asian Symposium, APLAS 2018, Wellington, New Zealand, December 2-6, 2018, Proceedings*, Ryu, S.(ed.), Lecture Notes in Computer Science, Vol. 11275, Springer, 2018, pp. 329–349.

[5] Calcagno, C., Yang, H., and O'Hearn, P. W.: Computability and Complexity Results for a Spatial Assertion Language for Data Structures, *The Second Asian Workshop on Programming Languages and Systems, APLAS'01, Korea Advanced Institute of Science and Technology, Daejeon, Korea, December 17-18, 2001, Proceedings*, 2001, pp. 289–300.

[6] Cook, B., Haase, C., Ouaknine, J., Parkinson, M. J., and Worrell, J.: Tractable Reasoning in a Fragment of Separation Logic, *CONCUR 2011 - Concurrency Theory - 22nd International Conference, CONCUR 2011, Aachen, Germany, September 6-9, 2011. Proceedings*, Katoen, J. and König, B.(eds.), Lecture Notes in Computer Science, Vol. 6901, Springer, 2011, pp. 235–249.

[7] Demri, S. and Deters, M.: Expressive completeness of separation logic with two variables and no separating conjunction, *Joint Meeting of the Twenty-Third EACSL Annual Conference on Computer Science Logic (CSL) and the Twenty-Ninth Annual ACM/IEEE Symposium on Logic in Computer Science (LICS), CSL-LICS '14, Vienna, Austria, July 14 - 18, 2014*, Henzinger, T. A. and Miller, D.(eds.), ACM, 2014, pp. 37:1–37:10.

[8] Girard, J.-Y.: *Proof theory and logical complexity. Volume I.*, Bibliopolis, 1987.

[9] Halpern, J. Y.: Presburger Arithmetic with Unary Predicates is Π^1_1 complete, *The Journal of Symbolic Logic*, Vol. 56, No. 2(1991), pp. 637–642.

[10] Iosif, R., Rogalewicz, A., and Simácek, J.: The Tree Width of Separation Logic with Recursive Def-

initions, *Automated Deduction - CADE-24 - 24th International Conference on Automated Deduction, Lake Placid, NY, USA, June 9-14, 2013. Proceedings*, Bonacina, M. P.(ed.), Lecture Notes in Computer Science, Vol. 7898, Springer, 2013, pp. 21–38.

[11] Koji, N., Makoto, T., Daisuke, K., and Mitsuru, Y.: Spatial Factorization in Cyclic-Proof System for Separation Logic, コンピュータ ソフトウェア, Vol. 37, No. 1(2020), pp. 1_125–1_144.

[12] Point, F.: On the expansion $(\mathbb{N}, +, 2^x)$ of Presburger arithmetic, 2007.

[13] Reynolds, J. C.: Separation Logic: A Logic for Shared Mutable Data Structures, *17th IEEE Symposium on Logic in Computer Science (LICS 2002), 22-25 July 2002, Copenhagen, Denmark, Proceedings*, IEEE Computer Society, 2002, pp. 55–74.

[14] Speranski, S. O.: A note on definability in fragments of arithmetic with free unary predicates, *Archive for Mathematical Logic*, Vol. 52(2013), pp. 507–516.

[15] Tatsuta, M., Le, Q. L., and Chin, W.: Decision Procedure for Separation Logic with Inductive Definitions and Presburger Arithmetic, *Programming Languages and Systems - 14th Asian Symposium, APLAS 2016, Hanoi, Vietnam, November 21-23, 2016, Proceedings*, Igarashi, A.(ed.), Lecture Notes in Computer Science, Vol. 10017, 2016, pp. 423–443.

[16] Tatsuta, M., Nakazawa, K., and Kimura, D.: Completeness of Cyclic Proofs for Symbolic Heaps with Inductive Definitions, *Programming Languages and Systems - 17th Asian Symposium, APLAS 2019, Nusa Dua, Bali, Indonesia, December 1-4, 2019, Proceedings*, Lin, A. W.(ed.), Lecture Notes in Computer Science, Vol. 11893, Springer, 2019, pp. 367–387.

[17] Webber, R.: *Computability Theory*, American Mathematical Society, 2012.