

単純型付き等式系に基づく  
定理自動証明に関する研究

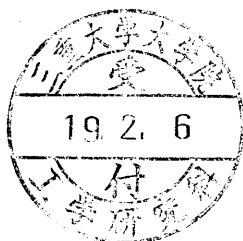
平成 18 年 度

三重大学大学院工学研究科  
博士前期課程 情報工学専攻

岡 村 洋

# 修士論文

## 単純型付き等式系に基づく 定理自動証明に関する研究



平成18年度修了  
三重大学大学院 工学研究科  
博士前期課程 情報工学専攻

岡村 洋

# 目 次

<b>第 1 章 準備</b>	<b>2</b>
1.1 単純型付き等式系 . . . . .	2
1.2 ソート付き等式系 . . . . .	4
<b>第 2 章 振舞等価性</b>	<b>6</b>
2.1 ソート付き項の振舞等価性 . . . . .	6
2.2 単純型付き項の振舞等価性 . . . . .	7
<b>第 3 章 本研究の手法</b>	<b>9</b>
<b>第 4 章 例</b>	<b>10</b>
4.1 関数型等式の引数補完 . . . . .	10
4.2 振舞等価な等式 . . . . .	10
4.3 従来例 . . . . .	11
<b>第 5 章 まとめ</b>	<b>14</b>
<b>謝辞</b>	<b>16</b>
<b>参考文献</b>	<b>17</b>

# はじめに

定理自動証明はプログラムの仕様の正当性の検証に応用できる。プログラムが期待された結果を出すことを証明できれば、作成されたプログラムの正当性を保証できる。そのため作成されたプログラムが予定した動作をするかどうかを検証することは重要なことである。

本論文での定理自動証明は、等式系のもとで与えられた等式が定理であるか自動的に検証することを対象とする。これまで完備化手続きを用いた様々な定理自動証明法が提案され、盛んに研究されてきた。定理の証明法にはKnuth-Bendix アルゴリズムに基づく Inductionless Induction [3] や構造帰納法によるものがある。高階の定理証明法には、文献 [4] や [5] などがある。従来は高階の定理証明には高階の等式系を用いられてきたため、これまで十分研究がなされてきた一階の合流性や停止性を求める手法がそのままでは用いることができない問題があった。

そこで本論文ではまず、単純型付き等式系における振舞等価性を定式化する。また、文献 [6] の変換手法を用いて、高階の等式系の一つである単純型付等式系に基づく定理証明から、一階の等式系の一つであるソート付き等式系に基づく定理証明に還元する方法を明らかにし、振舞の等価性や非等価性の証明法を提示する。

以下に本論文の構成を示す。第 1 章で諸定義、第 2 章でソート付き項の振舞等価性と単純型付き項の振舞等価性、第 3 章で本研究の手法、第 4 章で本研究の手法が有効な例、最後にまとめと今後の課題について述べる。

# 第1章 準備

この章では、単純型付き等式系と単純型付き項書換え系、ソート付き項書換え系に関する諸定義・諸性質について述べる。

書換えの用語や記法は文献 [2] に準ずる。単純型付き等式系に関する定義は文献 [1],[4],[6] に基づく。

単純型付き等式系について定義する。

## 1.1 単純型付き等式系

### 定義 1.1.1. (単純型)

基本型 (*basictype*) の集合  $B$  から得られる単純型 (*simpletype*) の最小の集合  $ST(B)$  を以下のように帰納的に定義する。

1.  $B \subseteq ST(B)$
2.  $\tau_0, \dots, \tau_n \in ST(B) \Rightarrow \tau_1 \times \dots \times \tau_n \rightarrow \tau_0 \in ST(B)$

明らかな時は、単純型は型、 $ST(B)$  は  $ST$  と略す。

型  $\tau$  の定数記号 (シグネチャ) や変数の集合をそれぞれ  $\Sigma^\tau$ ,  $V^\tau$  と表す。  $\Sigma$  と  $V$  はそれぞれ、  $\Sigma = \bigcup_{\tau \in ST} \Sigma^\tau$ ,  $V = \bigcup_{\tau \in ST} V^\tau$  と表す。  $V^\tau$  は任意の  $\tau \in ST$  に対して加算無限とする。

### 定義 1.1.2. (単純型付き項)

任意の  $\Sigma, V$  に対して、型  $\tau$  の単純型付き項の集合  $T_{ST}(\Sigma, V)^\tau$  を以下のように定義する。

1.  $\Sigma^\tau \cup V^\tau \subseteq T_{ST}(\Sigma, V)^\tau$
2.  $s \in T_{ST}(\Sigma, V)^{\tau_1 \times \dots \times \tau_n \rightarrow \tau}$  かつ  $\forall i \in \{1, \dots, n\}, t_i \in T_{ST}(\Sigma, V)^{\tau_i} \Rightarrow (s \ t_1 \dots t_n) \in T_{ST}(\Sigma, V)^\tau$

混乱が生じない場合、単純型付き項の最外括弧ははずすことが可能である。型  $\tau$  を持つ単純型付き項  $s \in T_{ST}(\Sigma, V)^\tau$  は  $s^\tau$  と表す。

全ての単純型付き項の集合  $T_{ST}(\Sigma, V)$  は  $\bigcup_{\tau \in ST} T_{ST}(\Sigma, V)^\tau$  と表し、明らかな時は  $T_{ST}(\Sigma, V)$  は  $T_{ST}$  と略す。単純型付き項の頭部記号を再帰的に定義する。

1.  $\text{head}(t) = t$  if  $t \in \Sigma \cup V$ .
2.  $\text{head}((st_1 \cdots t_n)) = \text{head}(s)$ .

単純型付き項  $t$  に現れる変数の集合を  $V(t)$  と表す.

### 定義 1.1.3. (代入)

代入は関数  $\sigma : V \rightarrow T_{ST}$  で表され, 次の条件を満たす.

1.  $\text{Dom}(\sigma) = \{x | \sigma(x) \neq x\}$  は有限.
2. 各  $x \in \text{Dom}(\sigma)$  に対して,  $x$  と  $\sigma(x)$  は同じ型を持つ.

代入  $\sigma$  の定義域を  $T_{ST}(\Sigma, V)$  へと広げた準同型拡張も  $\sigma$  で示される. 通常  $\sigma(t)$  は  $t\sigma$  と表す. また, 関数  $\sigma : V \rightarrow T_{ST}(\Sigma, \emptyset)$  を基礎項代入と呼ぶ.

### 定義 1.1.4. (文脈)

文脈はある出現位置  $u$  が空になっている型  $t \in T_{ST}$  を返す単純型付き項である. 空になっているとは  $t$  を返す項の位置  $u$  の部分項と同じ型ならば, どのような単純型付き項とでも置き換え可能であることをいう. 文脈を  $C[]$  と表記し,  $C[T_{ST}]$  は文脈  $C[]$  の空の位置を  $T_{ST}$  で置き換えて得られる項のことである.  $C[] \in T_{ST}(\Sigma, \emptyset)$  を満たす文脈を基礎項文脈と呼ぶ.

### 定義 1.1.5. (単純型付き等式系)

単純型付き項の組  $\langle l, r \rangle$  は  $l, r$  が同じ型を持っている時, 単純型付き等式である. 単純型付き等式  $\langle l, r \rangle$  は  $l \approx r$  のように表す. 基本型の集合  $B$ , 定数記号の集合  $\Sigma$ , 単純型付き等式の集合  $E$  から構成される 3 つ組  $\langle B, \Sigma, E \rangle$  を単純型付き等式系と呼ぶ.

### 定義 1.1.6. (単純型付き項書換え系)

単純型付き項書換え系  $\mathcal{R} = \langle B, \Sigma, R \rangle$  によって導かれる書換え関係  $\rightarrow_{\mathcal{R}}$  は次の条件を満たす  $T_{ST}(\Sigma, V)$  上の最小の関係である.

1. 全ての  $l \rightarrow r \in R$ , 全ての代入  $\sigma$  に対して  $l\sigma \rightarrow_{\mathcal{R}} r\sigma$
2. 全ての  $s_0, \dots, s_n$  に対して,  $s \rightarrow_{\mathcal{R}} t$  ならば  $(s_0 \cdots s \cdots s_n) \rightarrow_{\mathcal{R}} (s_0 \cdots t \cdots s_n)$

### 定義 1.1.7. (合同関係)

$\mathcal{E}$  を等式系とすると, 合同関係  $\equiv_{\mathcal{E}}$  は,  $\mathcal{E}$  の等式集合に含まれる等式によって導かれる同値関係である.

### 定義 1.1.8. (アリティ)

アリティの集合は以下の条件を満たす最小の集合  $Ar(B)$  とする.

1.  $B \subseteq Ar(B)$
2.  $n \geq 1, a_0, a_1, \dots, a_n \in Ar(B) \Rightarrow \langle a_1, a_2, \dots, a_0 \rangle \in Ar(B)$

関数  $ar : ST(B) \rightarrow Ar(B)$  を以下のように定義する.

$$ar(\tau) = \begin{cases} \tau & \text{if } \tau \in B \\ \langle ar(\tau_1) \cdots ar(\tau_n) ar(\tau_0) \rangle & \text{if } \tau = \tau_1 \times \cdots \times \tau_n \rightarrow \tau_0 \end{cases}$$

文献 [6] の変換手法を用いて単純型付き等式系からソート付き等式系へ変換を行なう.

### 定義 1.1.9. (変換)

単純型付きシグネチャ (項, 等式系) から対応するソート付きシグネチャ (項, 等式系) への変換  $\theta$  を定義する.

1.  $\theta(\Sigma) = \Sigma \cup \{ @_a | a \in Ar(B) \setminus B \}$

( $\theta(\Sigma)$  における各定数記号を以下のようにそのソートと関連づける)

$$sort(f) = \begin{cases} ar(\tau) & \text{if } f \in \Sigma^\tau \\ \langle a_1 \cdots a_n a_0 \rangle \times a_1 \times \cdots \times a_n \rightarrow a_0 & \text{if } f = @_a \langle a_1 \cdots a_n a_0 \rangle \end{cases}$$

$$2. \theta(t) = \begin{cases} t & \text{if } t \in \Sigma \cup V \\ @_a ar(\tau)(\theta(s), \theta(t_1), \dots, \theta(t_n)) & \text{if } t = (s^\tau t_1 \cdots t_n) \end{cases}$$

$$3. \theta(E) = \{ \theta(l) \approx \theta(r) | l \approx r \in E \}$$

$$4. \theta(\langle B, \Sigma, E \rangle) = \langle Ar(B), \theta(\Sigma), \theta(E) \rangle$$

### 定義 1.1.10. (論理値を備えた単純型付き等式系)

単純型付き等式系  $\mathcal{E}$  が論理値を備えるとは,  $\mathcal{E}$  の基本型のひとつとして論理値型  $Bool$  があり, 論理値型の定数記号として  $True$  と  $False$  をもつことである.

単純型付き等式系の変換後のソート付き等式系に説明する.

## 1.2 ソート付き等式系

### 定義 1.2.1. (ソート付き書換え規則)

ソート付き書換え規則  $l \rightarrow r$  とは,  $sort(l) = sort(r)$  かつ  $V(l) \supseteq V(r)$  かつ  $l \notin V$  を満たすソート付き項の対  $(l, r)$  である.

関係  $\rightarrow$  の反射推移閉包 (0 回以上の書換え) を  $\rightarrow^*$  と表記する. 項  $t_1$  に対して  $t_1 \rightarrow t_2$  のような書換え規則がない場合  $t_1$  を正規形と呼ぶ.

また, ソート付き書換え系  $\mathcal{R}$  が合流性を満たすとは  $(\leftarrow^* \cdot \rightarrow^*) \subseteq (\rightarrow^* \cdot \leftarrow^*)$  が成り立つことをいう.  $\mathcal{R}$  が停止性を満たすとは, 無限の書換え  $t \rightarrow_{\mathcal{R}} t_1 \rightarrow_{\mathcal{R}} t_2 \rightarrow_{\mathcal{R}} \cdots$  が存在しないことをいう. 合流性と停止性をともに満たすことを完備であるといい, 与えられた等式系と等価で完備な項書換え系を得る手続きを完備化手続きと呼ぶ.

### 定義 1.2.2. (論理値を備えたソート付き等式系)

ソート付き等式系  $\mathcal{E}$  が論理値を備えるとは,  $\mathcal{E}$  がソートのひとつとして *Bool* をもち, ソート *Bool* の定数記号として *True* と *False* をもつことである.



## 第2章 振舞等価性

本章では、ソート付き等式系と単純型付き等式系の振舞等価性について定義する。

### 2.1 ソート付き項の振舞等価性

本節では、ソート付き等式系における振舞等価性を定義する。

#### 定義 2.1.1. (ソート付き項の振舞等価性)

論理値を備えるソート付き等式系  $\mathcal{E}$  のもとでソート付き項  $l$  と  $r$  が振舞等価であるとは、 $Bool$  ソートの任意の基礎項文脈  $C$  と任意の基礎項代入  $\sigma$  について  $C[l\sigma] \equiv_{\mathcal{E}} C[r\sigma]$  が成り立つことであり、 $l \cong_{\mathcal{E}} r$  と表す。

ソート付き項の振舞の等価性と非等価性は、無矛盾性や強完全性から導かれる。

#### 定義 2.1.2. (ソート付き等式系の無矛盾性と強完全性)

論理値を備えたソート付き等式系  $\mathcal{E}$  が無矛盾であるとは、 $True \not\equiv_{\mathcal{E}} False$  が成り立つことであり、 $\mathcal{E}$  が強完全であるとは、 $Bool$  ソートの任意の項  $t$  について  $t \equiv_{\mathcal{E}} True$  か  $t \equiv_{\mathcal{E}} False$  が成り立つことである。

#### 定理 2.1.3. (ソート付き項の振舞等価性と非等価性の証明法)

論理値を備えたソート付き等式系  $\mathcal{E}$  について 次の 2 つの性質が成り立つ。

1.  $\mathcal{E}$  が強完全であり、 $\mathcal{E} \cup \{l \approx r\}$  が無矛盾ならば、 $l \cong_{\mathcal{E}} r$ .
2.  $\mathcal{E}$  の各ソートに基礎項が存在し、 $\mathcal{E}$  が無矛盾性を満たさないならば、 $l \not\equiv_{\mathcal{E}} r$ .

#### 証明. (性質 1.)

強完全性より  $C[l\sigma] \equiv_{\mathcal{E}} True$  または  $C[l\sigma] \equiv_{\mathcal{E}} False$  が成り立つ。  $C[l\sigma] \equiv_{\mathcal{E}} True$  のとき、 $C[r\sigma] \equiv_{\mathcal{E}} False$  と仮定すると、 $C[l\sigma] \equiv_{\mathcal{E} \cup \{l \approx r\}} C[r\sigma]$  より、 $True \equiv_{\mathcal{E} \cup \{l \approx r\}} False$ . これは前提に矛盾。  
 $C[l\sigma] \equiv_{\mathcal{E}} False$  のときも同様に証明可能である。 □

**証明.** (性質 2.)

背理法を用いて証明する.  $True \equiv_{\mathcal{E} \cup \{l \approx r\}} False$  と仮定すると, 各ソートに基礎項が存在するため, ある基礎項  $r_1, \dots, r_k$  に対して

$$True \leftrightarrow_{\mathcal{E} \cup \{l \approx r\}} r_1 \leftrightarrow_{\mathcal{E} \cup \{l \approx r\}} \dots \leftrightarrow_{\mathcal{E} \cup \{l \approx r\}} r_k \leftrightarrow_{\mathcal{E} \cup \{l \approx r\}} False \quad (2.1)$$

が成立する.

また (1) は  $\equiv_{\mathcal{E}} = \leftrightarrow_{\mathcal{E}}^*$  より,

$$True(\leftrightarrow_{\{l \approx r\}} \cup \leftrightarrow_{\mathcal{E}})^* False$$

と表せる.

$C[l\sigma] \equiv_{\mathcal{E}} C[r\sigma]$  と  $\equiv_{\mathcal{E}}$  と  $\leftrightarrow_{\{l \approx r\}}$  の定義より,  $(\leftrightarrow_{\{l \approx r\}} \cup \leftrightarrow_{\mathcal{E}}) \subseteq \equiv_{\mathcal{E}}$  であるので,

$$True \equiv_{\mathcal{E}} False$$

これは  $\mathcal{E}$  の無矛盾性に矛盾. □

ソート付き等式系の無矛盾性や強完全性は, 対応する項書換え系の性質から導かれる.

#### 補題 2.1.4. (ソート付き等式系の無矛盾性の証明法)

論理値を備えたソート付き等式系  $\mathcal{E}$  と同じシグネチャをもつソート付き項書換え系  $\mathcal{R}$  について次の 3 条件が成り立てば,  $\mathcal{E}$  は無矛盾.

- $\mathcal{E}$  と  $\mathcal{R}$  から生成される合同関係が一致する ( $\equiv_{\mathcal{E}} = \leftrightarrow_{\mathcal{R}}^*$ )
- $\mathcal{R}$  が合流性を満たす.
- $True$  と  $False$  は  $\mathcal{R}$  の正規形である.

**証明.**  $True$  と  $False$  が  $\mathcal{R}$  の正規形であり,  $\mathcal{R}$  が合流性を満たすので,  $True \leftrightarrow_{\mathcal{R}}^* False$  のような書換えは存在しない. よって  $True \not\equiv_{\mathcal{E}} False$ . □

## 2.2 単純型付き項の振舞等価性

本節では, 単純型付き等式系における振舞等価性を定式化する. また, ソート付き等式系への変換を利用した振舞の等価性と非等価性の証明法を提示する.

**定義 2.2.1. (単純型付き項の振舞等価性)**

論理値を備える単純型付き等式系  $\mathcal{E}$  のもとで単純型付き項  $l$  と  $r$  が**振舞等価**であるとは、 $Bool$  型の任意の基礎項文脈  $C$  と任意の基礎項代入  $\sigma$  について  $C[l\sigma] \equiv_{\mathcal{E}} C[r\sigma]$  が成り立つことであり、 $l \cong_{\mathcal{E}} r$  と表す。

定義 1.2.1 の変換  $\theta$  を使うと、単純型付き等式系を、生成される合同関係を保ったままソート付き等式系へと変換可能である。変換  $\theta$  を使い、単純型付き等式系における振舞等価性を、ソート付き等式系の振舞等価性の判定問題へと帰着させる手法を提示する。ソート付き項書換え系を用いた既存の自動証明法が活用できる点で、この変換手法は有用である。

**定理 2.2.2. (単純型付き項の振舞非等価性の証明法)**

論理値を備えた単純型付き等式系  $\mathcal{E}$  と単純型付き等式  $l \approx r$  について考える。変換  $\theta$  によるソート付きの等式系や項への変換結果を、 $\mathcal{E}' = \theta(\mathcal{E}), l' = \theta(l), r' = \theta(r)$  で表し、生成される合同関係が  $\mathcal{E}'$  と一致する ( $\equiv_{\mathcal{E}'} = \leftrightarrow_{\mathcal{R}'}$ ) のように定めたソート付き書換え系を  $\mathcal{R}'$  と表す。このとき、次の 2 条件が成立すれば  $l \cong_{\mathcal{E}} r$  である。

- $\mathcal{R}'$  と  $\mathcal{R}' \cup \{l' \approx r'\}$  が共に合流性を満たす。
- $True$  と  $False$  は共に  $\mathcal{R}$  と  $\mathcal{R}' \cup \{l' \approx r'\}$  の正規形である。

**証明.** 変換  $\theta$  が合同関係を保存することと、補題 2.1.4 のソート付き等式系の無矛盾性の条件を満たしていること、定理 2.1.3 のソート付き項の振舞等価性による。  $\square$

## 第3章 本研究の手法

本研究の単純型付き等式系の定理の証明法について説明する。以下にその手続きを示す。

- 入力: 論理値を備えた単純型付き等式系  $\mathcal{E}' (= \mathcal{E} \cup \{e\})$ .
- 出力: *Yes* または *No*.

手順:

1. 単純型付き項をソート付き項へ変換する.
2. 変換後の  $\mathcal{E}'$  が無矛盾であることを示す. すなわち変換後の  $\mathcal{E}'$  を完備化する.
3. 完備化が成功ならば *Yes* を, 失敗ならば *No* を返す.

完備化が失敗するとは, ソート付き等式系  $\mathcal{E}'$  や  $\mathcal{E}'$  に等価なソート付き項書換え系  $\mathcal{R}'$  に矛盾が生じることである. 矛盾が現れた時, 定理 2.1.3 の性質 2. より振舞非等価であり, 単純型付き等式系  $\mathcal{E}$  のもとで定理ではない. 完備化が成功するとは, 完備化が終了するまで矛盾が生じないことである.

完備化手続きには従来の完備化手続きが利用可能である. また, 完備化手続きを用いない場合には, 補題 2.1.4 より, 単純型付き等式系を変換した後のソート付き等式系に対応したソート付き項書換え系の合流性を示すことによって, 定理の判定が行なえる.

## 第4章 例

本研究の手法が有効である例を以下に示す.

### 4.1 関数型等式の引数補完

例 4.1.1. 単純型の集合を  $\mathcal{O}$ , 定数記号の集合を  $\Sigma$ , 等式系を  $\mathcal{E}$  と表す.

$$\begin{aligned}\mathcal{O} &= \{ B, S \} \\ \Sigma &= \{ \begin{array}{ll} a & : S, \\ b & : S, \\ true & : B, \\ false & : B, \\ f & : S \rightarrow B, \\ g & : S \rightarrow B \end{array} \\ &\} \\ \mathcal{E} &= \{ \begin{array}{lll} f\ a & \approx & true, \\ f\ b & \approx & false, \\ g\ a & \approx & true, \\ g\ b & \approx & false, \end{array} \\ &\} \end{aligned}$$

上記の  $\langle \mathcal{O}, \Sigma, \mathcal{E} \rangle$  に対して, 単純型付き関数の等式  $f \approx g$  が  $\mathcal{E}$  のもとで振舞等価であるか判別する時,  $f\ x \approx g\ x$  のように変数の引数を与え定理証明を行なう. これは変換後の一階のソート付き等式系では,  $@_{SB}(f, x) \approx @_{SB}(g, x)$  と表されるが, これは  $f \approx g$  に等しい.

### 4.2 振舞等価な等式

異なる2つの関数  $f, g$  の引数に  $a$  を与えたとき,  $b$  を与えたときそれぞれ等しくなるような例を考える.

例 4.2.1. 単純型の集合を  $\mathcal{O}$ , 定数記号の集合を  $\Sigma$ , 等式系を  $\mathcal{E}$  と表す.

$$\begin{aligned}
\mathcal{O} &= \{ B, S \} \\
\Sigma &= \{ \begin{array}{ll} a & : S, \\ b & : S, \\ true & : B, \\ false & : B, \\ f & : S \rightarrow B, \\ g & : S \rightarrow B \end{array} \\
&\} \\
\mathcal{E} &= \{ \begin{array}{lll} f \ a & \approx & true, \\ f \ b & \approx & false, \\ g \ a & \approx & true, \\ g \ b & \approx & false, \end{array} \\
&\}
\end{aligned}$$

上記の  $\langle \mathcal{O}, \Sigma, \mathcal{E} \rangle$  に対して、単純型付き項の等式  $a \approx b$  を与えた時、 $\mathcal{E}$  のもとで振舞等価であり、定理である。この例は従来の始代数意味論に基づく定理証明では導くことができない。

### 4.3 従来の例

従来の定理証明で導かれる例に対しても、本手法が有効であることを示す。

**例 4.3.1.**  $\mathcal{O}$  を基本型の集合、 $\Sigma$  を関数記号の集合、 $E$  を等式の集合とする。

$$\begin{aligned}
\mathcal{O} &= \{ Nat, List, Bool \} \\
\Sigma &= \{ \begin{array}{ll} 0 & : Nat, \\ s & : Nat \rightarrow Nat, \\ True & : Bool, \\ False & : Bool, \\ isNull & : List \rightarrow Bool, \\ [] & : List, \\ :: & : Nat \times List \rightarrow List, \\ map & : (Nat \rightarrow Nat) \rightarrow (List \rightarrow List), \\ \circ & : (Nat \rightarrow Nat) \times (Nat \rightarrow Nat) \rightarrow (Nat \rightarrow Nat), \\ \bullet & : (List \rightarrow List) \times (List \rightarrow List) \rightarrow (List \rightarrow List) \end{array} \\
E &= \{ \begin{array}{ll} (map \ F) [] & \approx \ [], \\ (map \ F)(x :: xs) & \approx \ (F \ x) :: ((map \ F)xs), \\ (F \circ \ G) \ x & \approx \ F(G \ x), \\ (X \bullet \ Y) \ xs & \approx \ X(Y \ xs) \end{array} \}
\end{aligned}$$

上記の単純型付き等式系  $\mathcal{E} = \langle \mathcal{O}, \Sigma, E \rangle$  に対して、等式  $e = map \ (F \circ \ G) \approx (map \ F) \bullet (map \ G)$  を与えた時、 $e$  が  $\mathcal{E}$  のもとで振舞等価であるか判定を行なう。

$E' = E \cup \{e\}, \mathcal{E}' = \langle O, \Sigma, E' \rangle$  とする時, 単純型付き等式系  $\mathcal{E}'$  をソート付き等式系へ変換すると以下ようになる. (表記に関して, 以下のように条件を定める. 混乱が生じない場合,  $Nat$  は  $N$ ,  $List$  は  $L$  と略す. また変換前に  $X \rightarrow X$  であった型は変換後にソートを  $X^2$  と表記し, 変換前に  $X \times X \rightarrow X$  であった型は変換後にソートを  $X^3$  と表記する. 表記上分かりやすくするため,  $@$  の添字にソートでなく関数記号と引数番号を用いる.)

$$Ar(O) = \{ N, B, L, N^2, L^2, LB, NLL, N^2L^2, (N^2)^3, (L^2)^3 \}$$

$$\begin{aligned} \theta(\Sigma) = \{ & 0 : N, \\ & s : N^2, \\ & True : B, \\ & False : B, \\ & isNull : LB, \\ & [] : L, \\ & :: : NLL, \\ & map : N^2L^2, \\ & \circ : (N^2)^3, \\ & \bullet : (L^2)^3, \\ & @_{m1} : N^2L^2 \times N^2 \rightarrow L^2, \\ & @_{m2} : L^2 \times L \rightarrow L, \\ & @_{::} : NLL \times N \times L \rightarrow L, \\ & @_{LB} : LB \times L \rightarrow B, \\ & @_{N^2} : N^2 \times N \rightarrow N, \\ & @_{\circ} : (N^2)^3 \times N^2 \times N^2 \rightarrow N^2, \\ & @_{\bullet} : (L^2)^3 \times L^2 \times L^2 \rightarrow L^2 \} \end{aligned}$$

$$\begin{aligned} \theta(E') = \{ & @_{m2}(@_{m1}(map, F), []) \approx [], & (1) \\ & @_{m2}(@_{m1}(map, F), @_{::}(:, x, xs)) \approx @_{::}(:, @_{N^2}(F, x), @_{m2}(@_{m1}(map, F), xs)), & (2) \\ & @_{N^2}(@_{\circ}(\circ, F, G), x) \approx @_{N^2}(F, @_{N^2}(G, x)), & (3) \\ & @_{m2}(@_{\bullet}(\bullet, X, Y), xs) \approx @_{m2}(X, @_{m2}(Y, xs)) & (4) \\ & @_{m1}(map, @_{\circ}(\circ, F, G)) \approx @_{\bullet}(\bullet, @_{m1}(map, F), @_{m1}(map, G)) & (5) \\ & \} \end{aligned}$$

厳格半順序として辞書式経路順序  $\succ_{lpo}$  ( $[\gamma]$ ) を与える.

$\theta(\Sigma)$  の要素に対して以下のような順序付けをする.

$$@_{m1} > @_{\bullet} > @_{\circ} > @_{m2} > @_{::} > @_{LB} > @_{N^2} > map > \bullet > \circ > :: > [] > isNull > s > 0 > True > False$$

上で求めた  $\theta(E')$  と厳格半順序  $\succ_{lpo}$  を用いて完備化を行なう. この時, 危険対は 2 つ生じるが, そのいずれから新たな書換え規則は得られない. よって完備化が成功するので, 等式  $e$  は単純型付き等式系  $\mathcal{E}$  の定理であることが分かる.

また, 完備化によって以下のような TRS  $R$  を得る.

$$\begin{aligned}
R = \{ \quad & @_{m2}(@_{m1}(map, F), [ ]) && \rightarrow [ ], \\
& @_{m2}(@_{m1}(map, F), @_{::} (::, x, xs)) && \rightarrow @_{::} (::, @_{N^2}(F, x), @_{m2}(@_{m1}(map, F), xs)), \\
& @_{N^2}(@_{\circ}(\circ, F, G), x) && \rightarrow @_{N^2}(F, @_{N^2}(G, x)), \\
& @_{m2}(@_{\bullet}(\bullet, X, Y), xs) && \rightarrow @_{m2}(X, @_{m2}(Y, xs)), \\
& @_{m1}(map, @_{\circ}(\circ, F, G)) && \rightarrow @_{\bullet}(\bullet, @_{m1}(map, F), @_{m1}(map, G)) \}
\end{aligned}$$



## 第5章 まとめ

本論文ではまず，単純型付き等式系における振舞等価性を定式化した．これにより，従来の高階の定理自動証明の研究では複雑であった定理を単純なものにした．

また，単純型付き等式系からソート付き等式系への変換を用いた振舞の等価性や非等価性の証明法を提示した．高階から一階への変換を行なっているため，従来の一階の合流性や停止性などの項書換え系で重要な性質を求める手法が利用可能であることが分かり，従来の定理証明法が利用可能である．

## 今後の課題

以下のような,

1. 様々な例に対してこの手法の証明能力を確認すること
2. 定理 2.1.3 の性質 2 の無矛盾性による証明法を用いて定理であるか判定を行なう手法を用いたが, 強完全性を用いた振舞等価の判定のための十分条件を与えること
3. 停止性を用いない証明法
4. 本手法に適した完備化の戦略の考案

が今後の課題である.

2. については, 従来の強完全性の研究や文献 [8] に参考になると考えている. 3. についても, 従来の停止性の研究が応用できるか考察する必要がある. 4. は, 本手法ではソート付き等式系に関数適応関数が多数現れることを考慮し, 本手法に適した厳格半順序, 関数記号の順序付けを考案することが定理証明の自動化に必要であると考え.

## 謝辞

日頃、丁寧なご指導と助言、御高配を賜わり、研究に関連する話題や様々な資料をいただいた大山口通夫教授に感謝いたします。太田教授には、研究に関する本を貸して頂いたり、論文の査読をしていただくなどお世話になりました。また、忙しいなか時間を見つけて勉強会を開いて頂いたり、学会の引率など、山田俊行講師には本研究を進めていく上でも、日頃の研究室の生活でも大変お世話になりました。深く感謝いたします。ならびに学会発表や論文提出などの事務手続き、研究に必要な物の発注、研究室生活での相談、その他何かとお世話になりました落合美子事務員に感謝いたします。また、山田裕一先輩、三橋一郎先輩には相談にのって頂いたり、アドバイスや研究や学会発表の参考資料を頂き感謝しています。最後に、熱心に議論していただいた研究室の学生諸氏、御世話になりました社会人として活躍されておられる研究室の先輩方に感謝いたします。本当にありがとうございました。

## 参考文献

- [1] Toshiyuki Yamada. *Confluence and termination of simply typed term rewriting systems*. In Proceedings of the 12th International Conference on Rewriting Techniques and Applications, Vol. 2051 of LNCS, pp. 338-352. Springer-Verlag, 2001.
- [2] F. Baader and T. Nipkow, *Term Rewriting and All That*. Cambridge University Press, 1998.
- [3] H. Comon. *Inductionless induction*. In A. Robinson and A. Voronkov, editors, Handbook of Automated Reasoning, volume I, chapter 14, pages 913-962. Elsevier Science, 2001
- [4] Takahito Aoto, Toshiyuki Yamada, and Yoshihito Toyama *Inductive Theorems for Higher-Order Rewriting*. Proceedings of the 15th International Conference on Rewriting Techniques and Applications (RTA'04), Lecture Notes in Computer Science 3091, pp.269-284, June 2004
- [5] Linnestad, H., Prehofer, C., and Lysne, O. 1996. *Higher-Order Proof by Consistency*. In Proceedings of the 16th Conference on Foundations of Software Technology and theoretical Computer Science (December 18 - 20, 1996). V. Chandru and V. Vinay, Eds. Lecture Notes In Computer Science, vol. 1180. Springer-Verlag, London, 274-285.
- [6] Takahito Aoto , Toshiyuki Yamada, *Termination of Simply Typed Term Rewriting Systems by Translation and Labelling*. Proceedings of the 14th International Conference on Rewriting Techniques and Applications (RTA'03), Lecture Notes in Computer Science 2706, pp.380-394, June 2003
- [7] Dershowitz, N. *Termination of rewriting*. J. Symb. Comput. 3, 1-2 (Feb. 1987), 69-116. 1987.
- [8] A. Bouhoula and F. Jacquemard. *Automating Sufficient Completeness Check for Conditional and Constrained TRS*. In Proceedings of the 20th International Workshop on Unification (UNIF'06), Seattle, Washington, USA, August 2006.