自然演繹による算術の形式化

五十嵐 淳
京都大学 大学院情報学研究科 通信情報システム専攻
igarashi@kuis.kyoto-u.ac.jp

November 27, 2012

証明体系(proof system) のひとつである**自然演繹**(natural deduction) によって，**算術**(自然数を対象とした論理) における証明の形式化 (記号化) を行う.

- 証明体系 (proof system):
  - 「(判断・命題が) 証明できるとはどういうことか」「証明が違う・同じとはどういうことか」を考えるための道具
  - 構成要素:
    - 判断・命題の (形式的) 定義
    - 導出 (証明を形式化したもの) の定義
  - 自然演繹，シーケント計算，ヒルベルト流公理系，などの「流儀」の違う証明体系
- 自然演繹 (natural deduction):
  - ゲンツェン (Gentzen) によって作られた証明体系の (流儀の) ひとつ
  - 人間の推論過程を自然に表現することが狙い
  - 導出の定義に使われる規則に特徴: 導入規則と除去規則 (後述)

1　式，命題，文脈，判断の構文

- Backus–Naur Form (BNF) による構文定義とメタ変数

$$\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{H} \quad \in \quad \{\mathtt{a}, \mathtt{b}, \mathtt{c}, \ldots, \}$$

⟨式⟩	::=	⟨変数⟩	$\boldsymbol{e}$	::=	$\boldsymbol{x}$
	|	`0`		|	`0`
	|	`S(`⟨式⟩`)`		|	`S(`$\boldsymbol{e}$`)`
	|	⟨式⟩`+`⟨式⟩		|	$\boldsymbol{e_1}$ `+` $\boldsymbol{e_2}$
	|	⟨式⟩`*`⟨式⟩		|	$\boldsymbol{e_1}$ `*` $\boldsymbol{e_2}$
⟨型⟩	::=	`nat`	$\boldsymbol{T}$	::=	`nat`
⟨命題⟩	::=	⟨式⟩`=`⟨式⟩	$\boldsymbol{P}, \boldsymbol{Q}$	::=	$\boldsymbol{e_1}$ `=` $\boldsymbol{e_2}$
	|	⟨命題⟩`->`⟨命題⟩		|	$\boldsymbol{P}$ `->` $\boldsymbol{Q}$
	|	`∀`⟨変数⟩`:`⟨型⟩`,`⟨命題⟩		|	$\forall \boldsymbol{x} : \boldsymbol{T}, \boldsymbol{P}$
⟨文脈⟩	::=	$\bullet$	Γ	::=	$\bullet$
	|	⟨文脈⟩`,` ⟨変数⟩`:` `nat`		|	Γ, $\boldsymbol{x} : \boldsymbol{T}$
	|	⟨文脈⟩`,` ⟨変数⟩`:`⟨命題⟩		|	Γ, $\boldsymbol{H} : \boldsymbol{P}$
⟨判断⟩	::=	⟨文脈⟩$\vdash$⟨命題⟩	$\mathcal{J}$	::=	$\Gamma \vdash \boldsymbol{P}$

- `*` は `+` よりも結合が強く，いずれも左結合である．
- `->` は $\forall$ よりも結合が強く，`->` は右結合である．
- 式 $\boldsymbol{e}$ 中に現れる変数の集合を $FV(\boldsymbol{e})$ と書く．また，命題 $\boldsymbol{P}$ 中に**全称量化されずに現れる**変数の集合を $FV(\boldsymbol{P})$ と書く．これらの変数を式の/命題の**自由変数**(free variable) と呼ぶ．
- 文脈中でコロンの左側に並んだ変数を**宣言された変数**といい，宣言された変数の集合を $dom(\Gamma)$ と書く．
- Γ, $\boldsymbol{x} : \mathtt{nat}$ という形の文脈については，$\boldsymbol{x} \notin dom(\Gamma)$ が成り立っているものとする．
- Γ, $\boldsymbol{H} : \boldsymbol{P}$ という形の文脈については，
  1. $\boldsymbol{H} \notin dom(\Gamma)$
  2. $\boldsymbol{P}$ の自由変数は Γ で宣言されている，つまり，$FV(\boldsymbol{P}) \subseteq dom(\Gamma)$

  が成立しているものとする．
- 文脈の先頭の $\bullet$ (それに続くコンマ) は省略する．
- 文脈を $\boldsymbol{x} : \mathtt{nat}$ や $\boldsymbol{H} : \boldsymbol{P}$ の形の集合と見て，$\boldsymbol{H} : \boldsymbol{P}$ が Γ に現れることを $\boldsymbol{H} : \boldsymbol{P} \in \Gamma$ と書くことがある．

- 判断 $\boldsymbol{\Gamma} \vdash \boldsymbol{P}$ は「文脈 $\boldsymbol{\Gamma}$ のもとで命題 $\boldsymbol{P}$ が成立する」と読み，$FV(\boldsymbol{P}) \subseteq dom(\boldsymbol{\Gamma})$ が成立しているものとする．

2 計算 (簡約)

計算による式の単純化を**簡約**(reduction) という．式の簡約を $\boldsymbol{e} \longrightarrow \boldsymbol{e'}$ と書き，以下のようなパターンで定義される．

$\boxed{\boldsymbol{e} \longrightarrow \boldsymbol{e'}}$

$$
\begin{array}{lcl}
\mathtt{O} + \boldsymbol{e} & \longrightarrow & \boldsymbol{e} \\
\mathtt{S}(\boldsymbol{e_1}) + \boldsymbol{e_2} & \longrightarrow & \mathtt{S}(\boldsymbol{e_1} + \boldsymbol{e_2}) \\
\mathtt{O} * \boldsymbol{e} & \longrightarrow & \mathtt{O} \\
\mathtt{S}(\boldsymbol{e_1}) * \boldsymbol{e_2} & \longrightarrow & \boldsymbol{e_2} + \boldsymbol{e_1} * \boldsymbol{e_2}
\end{array}
$$

厳密には，上のパターンを部分式に当てはめたものについても $\boldsymbol{e} \longrightarrow \boldsymbol{e'}$ と書く．例えば

$$
\begin{array}{lcl}
\mathtt{S(O)} + \mathtt{S(O)} + \mathtt{S(S(O))} & \longrightarrow & \mathtt{S(O} + \mathtt{S(O))} + \mathtt{S(S(O))} \\
\mathtt{S(O} + \mathtt{S(O))} + \mathtt{S(S(O))} & \longrightarrow & \mathtt{S(O} + \mathtt{S(O)} + \mathtt{S(S(O)))} \\
\mathtt{S(O} + \mathtt{S(O))} + \mathtt{S(S(O))} & \longrightarrow & \mathtt{S(S(O))} + \mathtt{S(S(O))}
\end{array}
$$

である．簡約の対象になった + を網かけで明示してある．2，3 番目の例のように，ひとつの式に対して簡約結果が複数ある場合もある．簡約によって変形の対象になった部分式を**簡約基**(redex) という．

また，+ は左結合なので，

$$\mathtt{S(O)} + \mathtt{S(O)} + \mathtt{S(S(O))} \longrightarrow \mathtt{S(O)} + \mathtt{S(O} + \mathtt{S(S(O)))}$$

とは簡約されないことに注意．

0 ステップ以上の簡約，すなわち，

$$\boldsymbol{e} \longrightarrow \cdots \longrightarrow \boldsymbol{e'}$$

を

$$\boldsymbol{e} \longrightarrow^{*} \boldsymbol{e'}$$

と書く．(「0 ステップ以上」なので $\boldsymbol{e}$ と $\boldsymbol{e'}$ が同じ式の場合もある．)

3 導出と導出規則

- 導出 … 判断の「証明」に相当する．木構造．
- 導出規則 … 導出を定める規則．

導出規則は一般に

$$\frac{\boldsymbol{\mathcal{J}_1} \qquad \cdots \qquad \boldsymbol{\mathcal{J}_n}}{\boldsymbol{\mathcal{J}_0}} \quad \text{(規則名)}$$

という形をしており，各判断には通常メタ変数 (これを規則のパラメータと呼ぶ) が現れる．$\boldsymbol{\mathcal{J}_1}, \ldots, \boldsymbol{\mathcal{J}_n}$ (ただし $n = 0$ の場合もある) を規則の前提，$\boldsymbol{\mathcal{J}_0}$ を規則の結論と呼ぶ．導出規則の直観的な意味は「前提の判断が全て成立する時結論も成立する」である．

導出規則のインスタンス　規則のパラメータを具体的な式や命題などで具体化したものを**規則のインスタンス**と呼ぶ．例えば，以下は，次節の規則 (->I) のインスタンスである．

$$\frac{\texttt{x : nat, H : 0 = x} \vdash \texttt{S(0) = x + S(0)}}{\texttt{x : nat} \vdash \texttt{0 = x -> S(0) = x + S(0)}}\ (\texttt{->I})$$

導出規則の前提の () で囲まれた部分は**付帯条件**といって，規則のインスタンスを作るにあたってパラメータが満たさなければいけない条件を書いたものである．例えば規則 (Assumption) では，パラメータ $\boldsymbol{P}$ は $\boldsymbol{\Gamma}$ 中に現れるものでなければならない．

また，導出規則中で $\boldsymbol{P}[\boldsymbol{x}]$ や $\boldsymbol{P}[\boldsymbol{e}]$ のような形が現れることがある．これは (0 個以上の)「穴ボコ」が空いた命題 $\boldsymbol{P}$ を考え，その穴ボコに $\boldsymbol{x}$ や $\boldsymbol{P}$ を入れたものを表す．例えば，規則 (∀E) のインスタンスとして，

$$\frac{\vdash \forall \texttt{x : nat,x = x}}{\vdash \texttt{0 = 0}}\ (\forall\text{E})$$

が考えられる．この時 $\boldsymbol{P}$ は [ ] = [ ] ([ ] が穴ボコ) であると考えられる．穴ボコの空いた命題についても，$FV(\boldsymbol{P}) \subseteq dom(\boldsymbol{\Gamma})$ の条件が課されるので，以下は，$\boldsymbol{P}$ として [ ] = x を考えると，

$$\frac{\vdash \forall \texttt{x : nat,x = x}}{\vdash \texttt{0 = x}}\ (\forall\text{E})$$

となりそうだが，$\{\texttt{x}\} \not\subseteq dom(\bullet) = \emptyset$ なので，規則 (∀E) のインスタンス**ではない**．

導出　規則のインスタンスを使って導出可能な判断とその導出を定義する．

1. 判断 $\boldsymbol{\mathcal{J}}$ が前提の数が 0 の規則のインスタンス

   $$\frac{}{\boldsymbol{\mathcal{J}}}\ (\text{規則名})$$

   である時，$\boldsymbol{\mathcal{J}}$ は導出可能であるといい，その導出はこのインスタンスである．

2. 導出可能な判断 $\boldsymbol{\mathcal{J}_1}, \ldots, \boldsymbol{\mathcal{J}_n}$ の導出がそれぞれ $\boldsymbol{\mathcal{D}_1}, \ldots, \boldsymbol{\mathcal{D}_n}$ であり，また，ある規則のインスタンスが

   $$\frac{\boldsymbol{\mathcal{J}_1} \quad \cdots \quad \boldsymbol{\mathcal{J}_n}}{\boldsymbol{\mathcal{J}_0}}\ (\text{規則名})$$

   である時，判断 $\boldsymbol{\mathcal{J}_0}$ は導出可能であり，その導出は

   $$\frac{\boldsymbol{\mathcal{D}_1} \quad \cdots \quad \boldsymbol{\mathcal{D}_n}}{\boldsymbol{\mathcal{J}_0}}\ (\text{規則名})$$

   である．

つまり，導出とは，判断をノードのラベルとした木構造であり，親子のノードのラベル間の関係は導出規則のいずれかに従ったものになっている．

4　算術の導出規則

自然演繹の特徴は，命題の構成要素 (今の場合「ならば」，全称量化，等号) ひとつにつき，それが結論に現れる規則 (導入規則と呼び規則名が I (introduction の頭文字) で終わる)・前提に現れる規則 (除去規則と呼び規則名が E (elimination の頭文字) で終わる) がひとつずつあるところである．導入規則は，論理結合子によって構成される命題が成立する一般的な条件を示しており，除去規則はその命題からどんな結論が導けるかを示している．

4.1　論理 (「ならば」・全称量化) に関する導出規則

$$\frac{(\boldsymbol{H} : \boldsymbol{P} \in \boldsymbol{\Gamma})}{\boldsymbol{\Gamma} \vdash \boldsymbol{P}} \quad (\textsc{Assumption})$$

$$\frac{\boldsymbol{\Gamma},\ \boldsymbol{H} : \boldsymbol{P} \vdash \boldsymbol{Q}}{\boldsymbol{\Gamma} \vdash \boldsymbol{P}\ \texttt{->}\ \boldsymbol{Q}} \quad (\texttt{->}\mathrm{I})$$

$$\frac{\boldsymbol{\Gamma} \vdash \boldsymbol{P}\ \texttt{->}\ \boldsymbol{Q} \qquad \boldsymbol{\Gamma} \vdash \boldsymbol{P}}{\boldsymbol{\Gamma} \vdash \boldsymbol{Q}} \quad (\texttt{->}\mathrm{E})$$

$$\frac{\boldsymbol{\Gamma},\ \boldsymbol{x} : \boldsymbol{T} \vdash \boldsymbol{P}}{\boldsymbol{\Gamma} \vdash \forall \boldsymbol{x} : \boldsymbol{T}, \boldsymbol{P}[\boldsymbol{x}]} \quad (\forall\mathrm{I})$$

$$\frac{\boldsymbol{\Gamma} \vdash \forall \boldsymbol{x} : \boldsymbol{T}, \boldsymbol{P}[\boldsymbol{x}]}{\boldsymbol{\Gamma} \vdash \boldsymbol{P}[\boldsymbol{e}]} \quad (\forall\mathrm{E})$$

4.2　「等しさ」に関する導出規則

$$\frac{(\boldsymbol{e} \longrightarrow^{*} \boldsymbol{e'})}{\boldsymbol{\Gamma} \vdash \boldsymbol{e} = \boldsymbol{e'}} \quad (=\mathrm{I})$$

$$\frac{\boldsymbol{\Gamma} \vdash \boldsymbol{e} = \boldsymbol{e'} \qquad \boldsymbol{\Gamma} \vdash \boldsymbol{P}[\boldsymbol{e}]}{\boldsymbol{\Gamma} \vdash \boldsymbol{P}[\boldsymbol{e'}]} \quad (=\mathrm{E})$$

4.3　自然数に関する導出規則

$$\frac{\boldsymbol{\Gamma} \vdash \texttt{S}(\boldsymbol{e_1}) = \texttt{S}(\boldsymbol{e_2})}{\boldsymbol{\Gamma} \vdash \boldsymbol{e_1} = \boldsymbol{e_2}} \quad (\textsc{InjS})$$

$$\frac{\boldsymbol{\Gamma} \vdash \texttt{0} = \texttt{S}(\boldsymbol{e})}{\boldsymbol{\Gamma} \vdash \boldsymbol{P}} \quad (\textsc{ContraNat})$$

$$\frac{\boldsymbol{\Gamma} \vdash \boldsymbol{P}[\texttt{0}] \qquad \boldsymbol{\Gamma},\ \boldsymbol{y} : \texttt{nat},\ \boldsymbol{H} : \boldsymbol{P}[\boldsymbol{y}] \vdash \boldsymbol{P}[\texttt{S}(\boldsymbol{y})]}{\boldsymbol{\Gamma} \vdash \forall \boldsymbol{x} : \texttt{nat}, \boldsymbol{P}[\boldsymbol{x}]} \quad (\textsc{IndNat})$$

4.4 導出の例

ここでは，$\forall$x : nat,$\boldsymbol{P}$ は $\forall$x,$\boldsymbol{P}$ と省略する．

1. 判断 $\vdash \forall$x,x = S(O) -> x + S(S(O)) = S(S(S(O))) の導出:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\boldsymbol{\Gamma} \vdash \mathtt{S(O) = x}}\ \textsc{Assumption} \quad \dfrac{}{\boldsymbol{\Gamma} \vdash \mathtt{S(O) + S(S(O)) = S(S(S(O)))}}\ =\!\mathrm{I}}{\mathtt{x : nat,\ H : S(O) = x} \vdash \mathtt{x + S(S(O)) = S(S(S(O)))}}\ =\!\mathrm{E}}{\mathtt{x : nat} \vdash \mathtt{S(O) = x -> x + S(S(O)) = S(S(S(O)))}}\ \mathtt{->}\mathrm{I}}{\vdash \mathtt{\forall x,S(O) = x -> x + S(S(O)) = S(S(S(O)))}}\ \forall\mathrm{I}$$

   ただし $\boldsymbol{\Gamma}$ は x : nat, H : S(O) = x である．

2. 判断 $\vdash \forall$x,x + O = x の導出:

$$\dfrac{\dfrac{}{\vdash \mathtt{O + O = O}}\ =\!\mathrm{I} \quad \dfrac{\dfrac{}{\boldsymbol{\Gamma} \vdash \mathtt{x + O = x}}\ \textsc{Assumption} \quad \dfrac{}{\boldsymbol{\Gamma} \vdash \mathtt{S(x) + O = S(x+O)}}\ =\!\mathrm{I}}{\boldsymbol{\Gamma} \vdash \mathtt{S(x) + O = S(x)}}\ =\!\mathrm{E}}{\vdash \mathtt{\forall x,x + O = x}}\ \textsc{IndNat}$$

   ただし $\boldsymbol{\Gamma}$ は x : nat, IH : x + O = x である．

3. 命題 $\boldsymbol{P}$ を $\forall$x,$\forall$y,x = y -> y = x，文脈 $\boldsymbol{\Gamma}$ を sym : $\boldsymbol{P}$, z : nat, H : S(S(O)) = S(S(O)) * z とする．この時，判断 $\boldsymbol{\Gamma} \vdash$ S(S(O)) * z = S(S(O)) の導出:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\boldsymbol{\Gamma} \vdash \mathtt{\forall x,\forall y,x = y -> y = x}}\ \textsc{Assumption}}{\boldsymbol{\Gamma} \vdash \mathtt{\forall y,S(S(O)) = y -> y = S(S(O))}}\ \forall\mathrm{E}}{\boldsymbol{\Gamma} \vdash \mathtt{S(S(O)) = S(S(O)) * z -> S(S(O)) * z = S(S(O))}}\ \forall\mathrm{E} \quad \dfrac{}{\boldsymbol{\Gamma} \vdash \mathtt{S(S(O)) = S(S(O)) * z}}\ \textsc{Assumption}}{\boldsymbol{\Gamma} \vdash \mathtt{S(S(O)) * z = S(S(O))}}\ \mathtt{->}\mathrm{E}$$

4. 判断 $\vdash \forall$x,x + O = O -> x = O の導出:

$$\dfrac{\dfrac{}{\vdash \mathtt{O + O = O -> O = O}}\ \mathtt{->}\mathrm{I} \quad \dfrac{\dfrac{\dfrac{\dfrac{}{\boldsymbol{\Gamma},\ \mathtt{H' : S(x) + O = O} \vdash \mathtt{S(x) + O = O}}\ \textsc{Assumption} \quad \dfrac{}{\boldsymbol{\Gamma},\ \mathtt{H' : S(x) + O = O} \vdash \mathtt{S(x) + O = S(x+O)}}\ =\!\mathrm{I}}{\boldsymbol{\Gamma},\ \mathtt{H' : S(x) + O = O} \vdash \mathtt{O = S(x+O)}}\ =\!\mathrm{E}}{\boldsymbol{\Gamma},\ \mathtt{H' : S(x) + O = O} \vdash \mathtt{S(x) = O}}\ \textsc{ContraNat}}{\boldsymbol{\Gamma} \vdash \mathtt{S(x) + O = O -> S(x) = O}}\ \mathtt{->}\mathrm{I}}{\vdash \mathtt{\forall x,x + O = O -> x = O}}\ \textsc{IndNat}$$

   ただし $\boldsymbol{\Gamma}$ は x : nat, IH : x + O = O -> x = O である．