# 工学部専門科目「計算と論理」配布資料
# 自然演繹と Coq

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

December 3, 2013

**証明体系** (*proof system*) のひとつである**自然演繹** (*natural deduction*) によって，Coq で使われている論理の形式化 (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)

ここでは，命題の構成要素 (**論理結合子** (*logical connective*) という) として「ならば (->)」だけを考える**極小論理** (*minimal logic*) から始めて，`Induction.v` までの内容で扱われる論理 (だいたい，スコットの Logic of Computable Functions と呼ばれる体系に相当する) に拡張する．[1]

[1] 通常は，極小論理に「かつ」「または」といった「ならば」以外の論理結合子を導入した**命題論理** (*propositional logic*)，「任意の〜」「ある〜について」といった量化子を導入した**述語論理** (*predicate*)，自然数についての述語論理である**算術** (*arithmetic*) へと徐々にコマを進めるが，ここでは，算術を包摂する体系まで一気に進む．ただし，「ならば」以外の論理結合子は後で導入する．

# 1 極小論理

## 1.1 命題，文脈

これまでの Coq の演習で扱った命題は，`n + 2 = 3` や `n * m = m * n` といった，ふたつの式を等号で結んだものを最小の単位として，それらを `->` でつないだり，全称量化 `forall` をつけたりすることで，より複雑な命題を構成してきた．

極小論理や命題論理では「ならば」「かつ」「または」といった，命題をつなげてより大きな命題を作る論理結合子に着目するため，最小の命題 (これを**原子命題** (*atomic proposition*) という) としてどんなものを考えるかについては特に何も約束ごとがない．このため，以下しばらく，原子命題としては単に `A`, `B`, `C` などがあることとし，原子命題を指す記号としては $\boldsymbol{p}$ を使う．

まず，以下に極小論理における命題と文脈の定義を示す．

$$
\begin{array}{lcl}
\boldsymbol{H} \text{ (仮定名)} & \in & \{\texttt{H1}, \texttt{H2}, \texttt{IH}, \ldots, \} \\
\boldsymbol{p}, \boldsymbol{q} \text{ (原子命題)} & & \\
 & & \\
\boldsymbol{P}, \boldsymbol{Q} \text{ (命題)} & ::= & \boldsymbol{p} \\
 & | & \boldsymbol{P} \texttt{ -> } \boldsymbol{Q} \\
 & & \\
\boldsymbol{\Gamma}\text{(文脈)} & ::= & \bullet \\
 & | & \boldsymbol{\Gamma},\ \boldsymbol{H} : \boldsymbol{P}
\end{array}
$$

- 極小論理における命題は原子命題を「ならば」を意味する `->` でつないだものである．`->` は右結合である．
- 文脈は $\boldsymbol{H} : \boldsymbol{P}$ という形の列であり，$\boldsymbol{P}$ が (名前 $\boldsymbol{H}$ で) 仮定されていることを示している．列中の仮定の名前は相異なる．
- 文脈 $\boldsymbol{\Gamma}$ に現れる仮定の名前の集合を $dom(\boldsymbol{\Gamma})$ と書く．
- 文脈の先頭の $\bullet$ (と，それに続くコンマ) は省略する．

## 1.2 判断と導出規則

単純型付ラムダ計算などで，型付け関係 $\boldsymbol{\Gamma} \vdash \boldsymbol{M} : \boldsymbol{T}$ を規則を使って定義したのと同様に,「文脈 $\boldsymbol{\Gamma}$ のもとで命題 $\boldsymbol{P}$ が成立する」ということを示す関係 $\boldsymbol{\Gamma} \vdash \boldsymbol{P}$ (これを**判断** (*judgment*) とも呼ぶ) を規則を使って定義する．

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．

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

$$\frac{\Gamma,\ H : P \vdash Q \qquad H \notin dom(\Gamma)}{\Gamma \vdash P \texttt{->} Q} \quad (\texttt{->I})$$

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

### 1.3 判断の導出例

1. 判断 $\vdash$ `A -> B -> A` の導出:

$$\dfrac{\dfrac{\dfrac{}{\texttt{H1 : A, H2 : B} \vdash \texttt{A}}\ \textsc{Assumption}}{\texttt{H1 : A} \vdash \texttt{B -> A}}\ \texttt{->I}}{\vdash \texttt{A -> B -> A}}\ \texttt{->I}$$

2. 判断 $\vdash$ `(A -> B -> C) -> (A -> B) -> (A -> C)` の導出:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \texttt{A -> B -> C}}\ \textsc{Asm} \quad \dfrac{}{\Gamma \vdash \texttt{A}}\ \textsc{Asm}}{\Gamma \vdash \texttt{B -> C}}\ \texttt{->E} \quad \dfrac{}{\Gamma \vdash \texttt{A -> B}}\ \textsc{Asm} \quad \dfrac{}{\Gamma \vdash \texttt{A}}\ \textsc{Asm}}{\Gamma \vdash \texttt{B}}\ \texttt{->E}}{\Gamma \vdash \texttt{C}}\ \texttt{->I}}{\texttt{H1 : A -> B -> C, H2 : A -> B} \vdash \texttt{A -> C}}\ \texttt{->I}}{\texttt{H1 : A -> B -> C} \vdash \texttt{(A -> B) -> (A -> C)}}\ \texttt{->I}}{\vdash \texttt{(A -> B -> C) -> (A -> B) -> (A -> C)}}\ \texttt{->I}$$

   ただし $\Gamma$ は `H1 : A -> B -> C, H2 : A -> B, H3 : A` とする．Assumption は As と略している．また `A -> B -> C` は `A -> (B -> C)` のことであることに注意.

## 2 単純型付ラムダ計算に関する論理

極小論理を元に，だいたい `Induction.v` までで扱った範囲に相当する論理体系を与える．ここでの原子命題は，単純型付ラムダ計算の項を使って $\boldsymbol{M_1}$ `=` $\boldsymbol{M_2}$ という形で与えられる．同時に，全称量化子を導入する．

$$\begin{array}{lcl}
\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{H} & \in & \{\texttt{a}, \texttt{b}, \texttt{c}, \ldots, \} \\
\\
\boldsymbol{S}, \boldsymbol{T} & ::= & \texttt{nat} \\
& | & \texttt{bool} \\
& | & \boldsymbol{S} \texttt{ -> } \boldsymbol{T} \\
\\
\boldsymbol{P}, \boldsymbol{Q} & ::= & \boldsymbol{M_1} \texttt{ = } \boldsymbol{M_2} \\
& | & \boldsymbol{P} \texttt{ -> } \boldsymbol{Q} \\
& | & \forall \boldsymbol{x} : \boldsymbol{T}, \boldsymbol{P} \\
\\
\Gamma & ::= & \bullet \\
& | & \Gamma,\ \boldsymbol{x} : \boldsymbol{T} \\
& | & \Gamma,\ \boldsymbol{H} : \boldsymbol{P}
\end{array}$$

命題中に現れる項は型がついているものでないといけないことはもちろんだが，各項に型がついていても命題としては一貫性が取れていないこともある．例えば，

$$\texttt{∀b : bool,∀n : nat,b = n}$$

のような命題は，そもそも意味がないものとして排除する必要がある．そのためにまず命題に対する型付けを考える．

命題に対する型付け関係は

$$\Gamma \vdash P : \texttt{Prop}$$

と書く．$P$が正しい/証明できる，という意味の$\Gamma \vdash P$との区別に注意せよ．例えば，$\vdash$ `∀n : nat,n = S O` は導出でき (そうも) ないが，$\vdash$ `∀n : nat,n = S O : Prop` は成り立つ．命題の型付けは単に $P$ が**真偽を議論する対象になりうる**命題であることを示しているだけで，その内容が正しいかどうかとは関係がない．

## 2.1 命題の型付け規則

$$\frac{\Gamma \vdash M_1 : T \qquad \Gamma \vdash M_2 : T}{\Gamma \vdash M_1 \texttt{ = } M_2 : \texttt{Prop}} \quad (=\mathrm{P})$$

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

$$\frac{\Gamma, x : T \vdash P : \texttt{Prop}}{\Gamma \vdash \forall x : T, P : \texttt{Prop}} \quad (\forall\mathrm{P})$$

以下，$\Gamma \vdash P$ のための (極小論理に加える) 規則を与えるが，$\Gamma \vdash P : \texttt{Prop}$ であることを前提とする．

## 2.2 全称量化に関する規則

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

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

導入規則 ∀I は，$P$ 中に現れる変数 $x$ について，その型以外特に仮定を置かずに $P$ が成り立つ時,「任意の $x$ について $P$ が成り立つ」といってよいことを示している．また，除去規則は,「任意の $x$ について $P$ が成り立つ」ならば，実際，任意に選んだ具体的な項 $M$ について $P$ が成り立つことを示している．

## 2.3 「等しさ」に関する導出規則

$$\frac{M_1 \longleftrightarrow M_2 \qquad \Gamma \vdash M_1 : T \qquad \Gamma \vdash M_2 : T}{\Gamma \vdash M_1 \texttt{ = } M_2} \quad (=\mathrm{I})$$

$$\frac{\Gamma \vdash M_1 = M_2 \qquad \Gamma \vdash P[M_1]}{\Gamma \vdash P[M_2]} \tag{=E}$$

導入規則 =I は，簡約を通じて等しい，ということが (この論理での) 等しさの定義であることを示している．除去規則 =E は，命題中の項は等しい項で置き換えてよいことを示している．

### 2.4 自然数に関する導出規則

$$\frac{\Gamma \vdash \mathtt{S}(M_1) = \mathtt{S}(M_2)}{\Gamma \vdash M_1 = M_2} \tag{InjS}$$

$$\frac{\Gamma \vdash \mathtt{0} = \mathtt{S}(M) \qquad \Gamma \vdash P : \mathtt{Prop}}{\Gamma \vdash P} \tag{ContraNat}$$

$$\frac{\Gamma \vdash P[\mathtt{0}] \qquad \Gamma,\ y : \mathtt{nat},\ H : P[y] \vdash P[\mathtt{S}(y)]}{\Gamma \vdash \forall x : \mathtt{nat}, P[x]} \tag{IndNat}$$

規則 InjS は，S の injectivity (1-to-1 であること) を，規則 ContraNat は 0 が 1 以上の自然数とは決して等しくない (等しい，という結論が出てきたら矛盾なので，そこから何でも導ける) ことを示している．規則 IndNat は数学的帰納法の原理を推論規則で表したものである．

### 2.5 真偽値に関する導出規則

$$\frac{\Gamma \vdash \mathtt{true} = \mathtt{false} \qquad \Gamma \vdash P : \mathtt{Prop}}{\Gamma \vdash P} \tag{ContraBool}$$

$$\frac{\Gamma \vdash P[\mathtt{true}] \qquad \Gamma \vdash P[\mathtt{false}]}{\Gamma \vdash \forall x : \mathtt{bool}, P[x]} \tag{IndBool}$$

### 2.6 導出の例

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

1. 判断 $\vdash \forall \mathtt{x}, \mathtt{x} = \mathtt{S\ 0} \to \mathtt{x} + \mathtt{S(S\ 0)} = \mathtt{S(S(S\ 0))}$ の導出:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Gamma \vdash \mathtt{S\ 0} = \mathtt{x}}\ \textsc{Assumption} \quad \dfrac{\mathtt{S\ 0 + S(S\ 0)} \leftrightarrow \mathtt{S(S(S\ 0))} \quad \Gamma \vdash \mathtt{S\ 0} : \mathtt{nat} \quad \Gamma \vdash \mathtt{S(S\ 0)} : \mathtt{nat}}{\Gamma \vdash \mathtt{S\ 0 + S(S\ 0)} = \mathtt{S(S(S\ 0))}}\ =\!\mathrm{E}}{\mathtt{x : nat},\ \mathtt{H : S\ 0} = \mathtt{x} \vdash \mathtt{x + S(S\ 0)} = \mathtt{S(S(S\ 0))}}\ =\!\mathrm{I}}{\mathtt{x : nat} \vdash \mathtt{S\ 0} = \mathtt{x} \to \mathtt{x + S(S\ 0)} = \mathtt{S(S(S\ 0))}}\ \to\!\mathrm{I}}{\vdash \forall \mathtt{x}, \mathtt{S\ 0} = \mathtt{x} \to \mathtt{x + S(S\ 0)} = \mathtt{S(S(S\ 0))}}\ \forall\mathrm{I}$$

ただし $M_1 + M_2$ は足し算を表すラムダ項 *plus* を使った *plus* $M_1\ M_2$ の略記であり，$\Gamma$ は $\mathtt{x : nat},\ \mathtt{H : S\ 0} = \mathtt{x}$ である．

2. 判断 $\vdash$ `∀x,x + 0 = x` の導出:

$$\dfrac{\dfrac{\vdots}{\vdash \texttt{0 + 0 = 0}}\ =\text{I} \qquad \dfrac{\dfrac{}{\boldsymbol{\Gamma} \vdash \texttt{x + 0 = x}}\ \textsc{Assumption} \qquad \dfrac{\vdots}{\boldsymbol{\Gamma} \vdash \texttt{S x + 0 = S(x+0)}}\ =\text{I}}{\boldsymbol{\Gamma} \vdash \texttt{S x + 0 = S x}}\ =\text{E}}{\vdash \texttt{∀x,x + 0 = x}}\ \textsc{IndNat}$$

ただし，$\boldsymbol{\Gamma}$ は `x : nat`, `IH : x + 0 = x` である．

3. 命題 $\boldsymbol{P}$ を `∀x,∀y,x = y -> y = x`，文脈 $\boldsymbol{\Gamma}$ を `sym :` $\boldsymbol{P}$, `z : nat`, `H : S(S(0)) = S(S(0)) * z` とする．この時，判断 $\boldsymbol{\Gamma} \vdash$ `S(S(0)) * z = S(S(0))` の導出:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\boldsymbol{\Gamma} \vdash \texttt{∀x,∀y,x = y -> y = x}}\ \textsc{Assumption}}{\boldsymbol{\Gamma} \vdash \texttt{∀y,S(S(0)) = y -> y = S(S(0))}}\ \forall\text{E}}{\boldsymbol{\Gamma} \vdash \texttt{S(S(0)) = S(S(0)) * z -> S(S(0)) * z = S(S(0))}}\ \forall\text{E} \qquad \dfrac{}{\boldsymbol{\Gamma} \vdash \texttt{S(S(0)) = S(S(0)) * z}}\ \textsc{Assumption}}{\boldsymbol{\Gamma} \vdash \texttt{S(S(0)) * z = S(S(0))}}\ \text{->E}$$

4. 判断 $\vdash$ `∀x,x + 0 = 0 -> x = 0` の導出:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\boldsymbol{\Gamma},\ \texttt{H' : S(x) + 0 = 0} \vdash \texttt{S(x) + 0 = 0}}\ \textsc{Assumption} \qquad \dfrac{\vdots}{\boldsymbol{\Gamma},\ \texttt{H' : S(x) + 0 = 0} \vdash \texttt{S(x) + 0 = S(x+0)}}\ =\text{I}}{\boldsymbol{\Gamma},\ \texttt{H' : S(x) + 0 = 0} \vdash \texttt{0 = S(x+0)}}\ =\text{E}}{\boldsymbol{\Gamma},\ \texttt{H' : S x + 0 = 0} \vdash \texttt{S x = 0}}\ \textsc{ContraNat}}{\boldsymbol{\Gamma} \vdash \texttt{S x + 0 = 0 -> S x = 0}}\ \text{->I} \qquad \dfrac{\dfrac{\vdots}{\texttt{H : 0 + 0 = 0} \vdash \texttt{0 = 0}}\ =\text{I}}{\vdash \texttt{0 + 0 = 0 -> 0 = 0}}\ \text{->I}}{\vdash \texttt{∀x,x + 0 = 0 -> x = 0}}\ \textsc{IndNat}$$

ただし $\boldsymbol{\Gamma}$ は `x : nat`, `IH : x + 0 = 0 -> x = 0` である．

## 3 Coq と自然演繹

Coq で行う証明は，ゴールとなる命題 $\boldsymbol{P}$ が与えられた時，$\boldsymbol{\Gamma} \vdash \boldsymbol{P}$ (ただし，$\boldsymbol{\Gamma}$ はそれまでに証明をした定理の集まり) を結論とする導出木を構成するプロセスに他ならない．例えば，上の $\vdash$ `∀x,x = S(0) -> x + S(S(0)) = S(S(S(0)))` の導出を考えてみよう．Coq で

```
Theorem foo : forall x:nat, x = 1 -> x + 2 = 3.
```

と打った場合，人間に課せられたのは，

$$\dfrac{?}{\vdash \texttt{∀x,x = S(0) -> x + S(S(0)) = S(S(S(0)))}}\ ??$$

という (根しかない) 木の ? 部分を埋めて導出木を完成させることである．

タクティックは，規則を組み合わせて (それまでに部分的に構成された) 木を「成長させる」働きをしている．例えば，`intros` タクティックは ∀I 規則や `->I` 規則に対応しており，上の木に対して，`intros x.` を実行すると木は成長して

$$\dfrac{\dfrac{?}{\texttt{x : nat} \vdash \texttt{S(0) = x -> x + S(S(0)) = S(S(S(0)))}}\ ??}{\vdash \texttt{∀x,S(0) = x -> x + S(S(0)) = S(S(S(0)))}}\ \forall\text{I}$$

になる．まだ未完成の部分にある命題 (と文脈) が新しいゴールである．

タクティックは複数の規則を組み合わせを表現していることもある．例えば，文脈に H : $\boldsymbol{M_1}$ = $\boldsymbol{M_2}$ が含まれており，ゴールが $\vdash P[\boldsymbol{M_2}]$ だった時に `rewrite <- H.` を実行すると，

$$\dfrac{\dfrac{}{\boldsymbol{\Gamma} \vdash \boldsymbol{M_1} = \boldsymbol{M_2}}\ \textsc{Assumption} \quad \dfrac{?}{\boldsymbol{\Gamma} \vdash \boldsymbol{P}[\boldsymbol{M_1}]}\ ??}{\boldsymbol{\Gamma} \vdash P[\boldsymbol{M_2}]}\ {=}\mathrm{E}$$

と木を成長させ，新しいゴールは $\boldsymbol{P}$ 中の $\boldsymbol{M_2}$ を $\boldsymbol{M_1}$ に書き換えた $\boldsymbol{P}[\boldsymbol{M_1}]$ になる．

大体，以下のような対応関係がある．

| タクティック | 規則 |
|---|---|
| `intros` | ->I または ∀I |
| `reflexivity` | =I |
| `apply` | Assumption, ∀E, ->E の組合せ |
| `rewrite` | Assumption と =E の組合せ |
| `induction`, `destruct` | IndNat または IndBool |
| `inversion` | InjS, ContraNat, ContraBool (と =E の組合せ) |

最後に `apply` タクティックについて見てみよう．$\boldsymbol{P}$ を

$$\forall \texttt{q : nat,} \forall \texttt{r : nat,q = r -> plus q q = mult r 2}$$

とし，H : $\boldsymbol{P}$ が文脈にあり，ゴールが

$$\texttt{plus 2 2 = mult x 2}$$

だったとする．ここで `apply H.` を実行するのは，以下のように導出木を成長させることと考えられる．

$$\dfrac{\dfrac{\dfrac{}{\boldsymbol{\Gamma} \vdash \boldsymbol{P}}\ \textsc{Assumption} \quad \dfrac{\dfrac{\dfrac{}{\boldsymbol{\Gamma} \vdash \texttt{0 : nat}}\ \text{T-Zero}}{\boldsymbol{\Gamma} \vdash \texttt{S 0 : nat}}\ \text{T-Succ}}{\boldsymbol{\Gamma} \vdash \texttt{2 : nat}}\ \text{T-Succ}}{\boldsymbol{\Gamma} \vdash \texttt{(2 = r) -> plus 2 2 = mult r 2}}\ \forall\mathrm{E} \quad \dfrac{}{\boldsymbol{\Gamma} \vdash \texttt{x : nat}}\ \text{T-Var}}{\boldsymbol{\Gamma} \vdash \texttt{(2 = x) -> plus 2 2 = mult x 2}}\ \forall\mathrm{E} \quad \dfrac{?}{\boldsymbol{\Gamma} \vdash \texttt{2 = x}}\ ??}{\boldsymbol{\Gamma} \vdash \texttt{plus 2 2 = mult x 2}}\ \texttt{->}\mathrm{E}$$