第3回の補足

情報工学科　篠埜 功

この資料では第 3 回の配布資料についていくつか補足を行う。

1　17ページの Hoare triple の導出

17 ページの Hoare triple **while** true **do** x:=1 の導出木を以下に示す。

$$\dfrac{\dfrac{\dfrac{\text{true} \Rightarrow \text{true} \wedge \text{true} \quad \overline{\{\text{true}\}\ x := 1\ \{\text{true}\}}\ (\text{assign})}{\{\text{true} \wedge \text{true}\}\ x := 1\ \{\text{true}\}}\ (\text{conseq})}{\{\text{true}\}\ \textbf{while}\ \text{true}\ \textbf{do}\ x := 1\ \{\text{true} \wedge \neg\text{true}\}}\ (\text{while}) \quad \text{true} \wedge \neg\text{true} \Rightarrow \text{false}}{\{\text{true}\}\ \textbf{while}\ \text{true}\ \textbf{do}\ x := 1\ \{\text{false}\}}\ (\text{conseq})$$

上記の導出木の $\{\text{true}\}\ x := 1\ \{\text{true}\}$ の部分は、

$$\text{true}[1/\text{x}] = \text{true}$$

であることにより、assignment axiom から成り立つ。

また、上記の導出木中で、assignment axiom を assign、conseqence rule を conseq、while rule を while と略記している。

2　置換の定義

assignment axiom で使われている、論理式の置換の定義を示す。まず、この講義の Hoare 論理で扱う論理式を以下のように定義する（配布資料ではスペースが足りないので論理式の定義を与えていない）。

$$\begin{array}{rcl}
P & := & \text{true} \mid \text{false} \\
 & \mid & P \wedge P \mid P \vee P \mid \neg P \mid P \Rightarrow P \\
 & \mid & E \leq E \mid E \geq E \mid E < E \mid E > E \mid E = E \\
E & := & N \\
 & \mid & V \\
 & \mid & E + E \\
 & \mid & E - E \\
N & := & \cdots \mid -2 \mid -1 \mid 0 \mid 1 \mid 2 \mid \cdots \\
V & := & x \mid y \mid z \mid \cdots
\end{array}$$

このような定義を帰納的定義 (inductive definition) という（これについては講義の範囲外)。上記で定義された論理式に対して置換を以下のように帰納的に定義する（これも講義の範囲外)。

$$
\begin{array}{rcll}
P[E/x] & = & \text{case } P \text{ of} & \\
 & & \text{true} & \rightarrow \quad \text{true} \\
 & & \text{false} & \rightarrow \quad \text{false} \\
 & & P_1 \wedge P_2 & \rightarrow \quad P_1[E/x] \wedge P_2[E/x] \\
 & & P_1 \vee P_2 & \rightarrow \quad P_1[E/x] \vee P_2[E/x] \\
 & & \neg P & \rightarrow \quad \neg P[E/x] \\
 & & P_1 \Rightarrow P_2 & \rightarrow \quad P_1[E/x] \Rightarrow P_2[E/x] \\
 & & E_1 \leq E_2 & \rightarrow \quad E_1[E/x] \leq E_2[E/x] \\
 & & E_1 \geq E_2 & \rightarrow \quad E_1[E/x] \geq E_2[E/x] \\
 & & E_1 < E_2 & \rightarrow \quad E_1[E/x] < E_2[E/x] \\
 & & E_1 > E_2 & \rightarrow \quad E_1[E/x] > E_2[E/x] \\
 & & E_1 = E_2 & \rightarrow \quad E_1[E/x] = E_2[E/x] \\
E[E_0/x] & = & \text{case } E \text{ of} & \\
 & & N & \rightarrow \quad N \\
 & & E_1 + E_2 & \rightarrow \quad E_1[E_0/x] + E_2[E_0/x] \\
 & & E_1 - E_2 & \rightarrow \quad E_1[E_0/x] - E_2[E_0/x] \\
 & & V & \rightarrow \quad \text{if } V = x \text{ then } E_0 \text{ else } V
\end{array}
$$

3 Hoare tripleの表記法について

Hoare triple の書き方はさまざまなものが使われる。講義資料では $\{P_1\}\ S\ \{P_2\}$ の形の表記法を用いたが、Hoare の論文 [1] では $P_1\ \{S\}\ P_2$ のようにプログラムの方を中括弧で囲んでいる。

参考文献

[1] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 12(10):576–580, 583, 1969.