情報論理・プログラムの数理
第5回演習レポート（5月18日出題）解答

1.

For Σ-terms $\mathbf{t}, \mathbf{s}_1, \ldots, \mathbf{s}_n$ and mutually different variables $\mathbf{x}_1, \ldots, \mathbf{x}_n \in \mathbf{Var}$, the *simultaneous substitution* of $\mathbf{s}_1, \ldots, \mathbf{s}_n$ for $\mathbf{x}_1, \ldots, \mathbf{x}_n$ in $\mathbf{t}$ is denoted by $\mathbf{t}[\mathbf{s}_1, \ldots, \mathbf{s}_n/\mathbf{x}_1, \ldots, \mathbf{x}_n]$. It is defined as the Σ-term obtained by replacing free occurrences of $\mathbf{x}_1, \ldots, \mathbf{x}_n$ in $\mathbf{t}$ with $\mathbf{s}_1, \ldots, \mathbf{s}_n$ respectively. Note here that free occurrences of $\mathbf{x}_1, \ldots, \mathbf{x}_n$ in $\mathbf{s}_i$ are not replaced.

Then by induction on the construction of the term $\mathbf{t}$, we can prove the following proposition that is a generalization of Proposition 2.5.7.

Proposition 1. $[\![\mathbf{t}[\mathbf{s}_1, \ldots, \mathbf{s}_n/\mathbf{x}_1, \ldots, \mathbf{x}_n]]\!]_{\mathbb{X},J} = [\![\mathbf{t}]\!]_{\mathbb{X},J[\mathbf{x_1} \mapsto [\![\mathbf{s_1}]\!]_{\mathbb{X},J}, \ldots, \mathbf{x}_n \mapsto [\![\mathbf{s}_n]\!]_{\mathbb{X},J}]}$. □

Proof for Sublemma 2.6.9. By Definition 2.5.11, in order to prove that $\mathbb{X}$ is a (Σ, E)-algebra, it suffices to show that for all $(\mathbf{s} = \mathbf{t}) \in E$, we have $\mathbb{X} \models \mathbf{s} = \mathbf{t}$, i.e. $[\![\mathbf{s}]\!]_{\mathbb{X},J} = [\![\mathbf{t}]\!]_{\mathbb{X},J}$ for each valuation $J : \mathbf{Var} \to X$ on $\mathbb{X}$.

Let $(\mathbf{s} = \mathbf{t}) \in E$ and $J : \mathbf{Var} \to X$ be a valuation on $\mathbb{X}$. Moreover, as the numbers of variables in $\mathbf{s}$ and $\mathbf{t}$ are finite, let $\mathrm{FV}(\mathbf{s}) \cup \mathrm{FV}(\mathbf{t}) = \{\mathbf{x}_1, \ldots, \mathbf{x}_n\}$. For each $i \in \{1, \ldots, n\}$, let $J(\mathbf{x}_i) = [\mathbf{u}_i]_{\sim_E}$.

Then we have:

$$
\begin{aligned}
[\![\mathbf{s}]\!]_{\mathbb{X},J} &= [\![\mathbf{s}]\!]_{\mathbb{X},J_c[\mathbf{x_1} \mapsto J(\mathbf{x}_1), \ldots, \mathbf{x_n} \mapsto J(\mathbf{x}_n)]} && \text{(by Lemma 2.5.5)} \\
&= [\![\mathbf{s}]\!]_{\mathbb{X},J_c[\mathbf{x_1} \mapsto [\mathbf{u}_1]_{\sim_E}, \ldots, \mathbf{x_n} \mapsto [\mathbf{u}_n]_{\sim_E}]} && \text{(by definition)} \\
&= [\![\mathbf{s}]\!]_{\mathbb{X},J_c[\mathbf{x_1} \mapsto [\![\mathbf{u}_1]\!]_{\mathbb{X},J_c}, \ldots, \mathbf{x_n} \mapsto [\![\mathbf{u}_n]\!]_{\mathbb{X},J_c}]} && \text{(by Sublemma 2.6.8)} \\
&= [\![\mathbf{s}[\mathbf{u}_1, \ldots, \mathbf{u}_n/\mathbf{x}_1, \ldots, \mathbf{x}_n]]\!]_{\mathbb{X},J_c} && \text{(by Proposition 1 above)} \\
&= [\mathbf{s}[\mathbf{u}_1, \ldots, \mathbf{u}_n/\mathbf{x}_1, \ldots, \mathbf{x}_n]]_{\sim_E} && \text{(by Sublemma 2.6.8)}
\end{aligned}
$$

Here $J_c : \mathbf{Var} \to X$ denotes the canonical valuation introduced in the proof of Sublemma 2.6.7. Similarly, we have:

$$
[\![\mathbf{t}]\!]_{\mathbb{X},J} = [\mathbf{t}[\mathbf{u}_1, \ldots, \mathbf{u}_n/\mathbf{x}_1, \ldots, \mathbf{x}_n]]_{\sim_E}
$$

Let $\mathbf{y}_1, \ldots, \mathbf{y}_n \in \mathbf{Var}$ be mutually different variables such that $\mathbf{y}_1, \ldots, \mathbf{y}_n \notin \mathrm{FV}(\mathbf{s}) \cup \mathrm{FV}(\mathbf{t}) \cup \mathrm{FV}(\mathbf{u}_1) \cup \cdots \mathrm{FV}(\mathbf{u}_n)$ (as $\mathbf{Var}$ is an infinite set, such a family indeed exists). Then we have the following proof tree.

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{\mathbf{s}=\mathbf{t}}\ (\textsc{Axiom}),\ (\mathbf{s}=\mathbf{t})\in E}{\mathbf{s}[\mathbf{y}_1/\mathbf{x}_1]=\mathbf{t}[\mathbf{y}_1/\mathbf{x}_1]}\ (\textsc{Subst})}{\vdots}\ (\textsc{Subst})}{\mathbf{s}[\mathbf{y}_1/\mathbf{x}_1]\ldots[\mathbf{y}_n/\mathbf{x}_n]=\mathbf{t}[\mathbf{y}_1/\mathbf{x}_1]\ldots[\mathbf{y}_n/\mathbf{x}_n]}\ (\textsc{Subst})}{\mathbf{s}[\mathbf{y}_1/\mathbf{x}_1]\ldots[\mathbf{y}_n/\mathbf{x}_n][\mathbf{u}_1/\mathbf{y}_1]=\mathbf{t}[\mathbf{y}_1/\mathbf{x}_1]\ldots[\mathbf{y}_n/\mathbf{x}_n][\mathbf{u}_1/\mathbf{y}_1]}\ (\textsc{Subst})}{\vdots}\ (\textsc{Subst})}{\mathbf{s}[\mathbf{y}_1/\mathbf{x}_1]\ldots[\mathbf{y}_n/\mathbf{x}_n][\mathbf{u}_1/\mathbf{y}_1]\ldots[\mathbf{u}_n/\mathbf{y}_n]=\mathbf{t}[\mathbf{y}_1/\mathbf{x}_1]\ldots[\mathbf{y}_n/\mathbf{x}_n][\mathbf{u}_1/\mathbf{y}_1]\ldots[\mathbf{u}_n/\mathbf{y}_n]}\ (\textsc{Subst})
$$

Note here that

$$\mathbf{s}[\mathbf{y}_1/\mathbf{x}_1]\ldots[\mathbf{y}_n/\mathbf{x}_n][\mathbf{u}_1/\mathbf{y}_1]\ldots[\mathbf{u}_n/\mathbf{y}_n] \equiv \mathbf{s}[\mathbf{u}_1,\ldots,\mathbf{u}_n/\mathbf{x}_1,\ldots,\mathbf{x}_n]$$

and

$$\mathbf{t}[\mathbf{y}_1/\mathbf{x}_1]\ldots[\mathbf{y}_n/\mathbf{x}_n][\mathbf{u}_1/\mathbf{y}_1]\ldots[\mathbf{u}_n/\mathbf{y}_n] \equiv \mathbf{t}[\mathbf{u}_1,\ldots,\mathbf{u}_n/\mathbf{x}_1,\ldots,\mathbf{x}_n]\,.$$

Hence by the definition of $\sim_E$ (equation (2.18)), we have

$$[\mathbf{s}[\mathbf{u}_1,\ldots,\mathbf{u}_n/\mathbf{x}_1,\ldots,\mathbf{x}_n]]_{\sim_E} = [\mathbf{t}[\mathbf{u}_1,\ldots,\mathbf{u}_n/\mathbf{x}_1,\ldots,\mathbf{x}_n]]_{\sim_E}\,.$$

Hence we have $[\![\mathbf{s}]\!]_{\mathbb{X},J} = [\![\mathbf{t}]\!]_{\mathbb{X},J}$ and this concludes the proof. □

2 (Exercise 3.2).

1.

$$\cfrac{\cfrac{\cfrac{}{A\Rightarrow A}\ (\textsc{Init})}{\neg A, A\Rightarrow}\ (\neg\text{-L})}{A\Rightarrow\neg\neg A}\ (\neg\text{-R})$$

2.

$$\cfrac{\cfrac{\cfrac{}{A\Rightarrow A}\ (\textsc{Init})}{\Rightarrow A,\neg A}\ (\neg\text{-R})}{\neg\neg A\Rightarrow A}\ (\neg\text{-L})$$

3.

$$\cfrac{\cfrac{\cfrac{\cfrac{}{A\Rightarrow A}\ (\textsc{Init})}{B, A\Rightarrow A}\ (\textsc{Weakening-L})}{A\Rightarrow B\supset A}\ (\supset\text{-R})}{\Rightarrow A\supset(B\supset A)}\ (\supset\text{-R})$$

4.

$$
\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{\cfrac{}{B\Rightarrow B}\ (\textsc{Init})}{A,B\Rightarrow B}\ (\textsc{Weakening-L})}{B\Rightarrow A\supset B}\ (\supset\text{-R}) \qquad \cfrac{\cfrac{}{B\Rightarrow B}\ (\textsc{Init}) \qquad \cfrac{}{C\Rightarrow C}\ (\textsc{Init})}{B\supset C, B\Rightarrow C}\ (\supset\text{-L})}{(A\supset B)\supset(B\supset C), B, B\Rightarrow C}\ (\supset\text{-L})}{B,(A\supset B)\supset(B\supset C), B\Rightarrow C}\ (\textsc{Exchange-L})}{B,B,(A\supset B)\supset(B\supset C)\Rightarrow C}\ (\textsc{Exchange-L})}{B,(A\supset B)\supset(B\supset C)\Rightarrow C}\ (\textsc{Contraction-L})}{(A\supset B)\supset(B\supset C)\Rightarrow B\supset C}\ (\supset\text{-R})}{A,(A\supset B)\supset(B\supset C)\Rightarrow B\supset C}\ (\textsc{Weakening-L})}{(A\supset B)\supset(B\supset C)\Rightarrow A\supset(B\supset C)}\ (\supset\text{-R})
$$

5.

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{(Init)}
\UnaryInfC{$A \Rightarrow A$}
\RightLabel{($\wedge$-L1)}
\UnaryInfC{$A \wedge B \Rightarrow A$}
\RightLabel{($\neg$-L)}
\UnaryInfC{$\neg A, A \wedge B \Rightarrow$}
\AxiomC{}
\RightLabel{(Init)}
\UnaryInfC{$B \Rightarrow B$}
\RightLabel{($\wedge$-L2)}
\UnaryInfC{$A \wedge B \Rightarrow B$}
\RightLabel{($\neg$-L)}
\UnaryInfC{$\neg B, A \wedge B \Rightarrow$}
\RightLabel{($\vee$-L)}
\BinaryInfC{$\neg A \vee \neg B, A \wedge B \Rightarrow$}
\RightLabel{($\neg$-R)}
\UnaryInfC{$A \wedge B \Rightarrow \neg(\neg A \vee \neg B)$}
\RightLabel{($\supset$-R)}
\UnaryInfC{$\Rightarrow (A \wedge B) \supset \neg(\neg A \vee \neg B)$}
\end{prooftree}
$$

3 (Exercise 3.9).

An expression $\models A$ denotes that the formula A is a tautology.

For $\not\models A$, we have:

$$
\begin{aligned}
\not\models A &\Leftrightarrow A \text{ is not a tautology} && \text{(by definition)}\\
&\Leftrightarrow (\forall J : \mathbf{PVar} \to \{\mathrm{tt}, \mathrm{ff}\}.\ [\![A]\!]_J = \mathrm{tt}) \text{ does not hold} && \text{(by Definition 3.3.3)}\\
&\Leftrightarrow \exists J : \mathbf{PVar} \to \{\mathrm{tt}, \mathrm{ff}\}.\ [\![A]\!]_J = \mathrm{ff}\,.
\end{aligned}
$$

In contrast, for $\models \neg A$, we have:

$$
\begin{aligned}
\models \neg A &\Leftrightarrow \neg A \text{ is a tautology} && \text{(by definition)}\\
&\Leftrightarrow \forall J : \mathbf{PVar} \to \{\mathrm{tt}, \mathrm{ff}\}.[\![\neg A]\!]_J = \mathrm{tt} && \text{(by Definition 3.3.3)}\\
&\Leftrightarrow \forall J : \mathbf{PVar} \to \{\mathrm{tt}, \mathrm{ff}\}.[\![A]\!]_J = \mathrm{ff} && \text{(by Definition 3.3.2)}\,.
\end{aligned}
$$

Therefore $\not\models A$ and $\models \neg A$ are different. Indeed, if $A \equiv P \supset Q$ where $P, Q \in \mathbf{PVar}$ and $P \neq Q$, then $\not\models A$ holds as $[\![A]\!]_{J[P \mapsto \mathrm{tt}, Q \mapsto \mathrm{ff}]} = \mathrm{ff}$ while $\models \neg A$ does not hold as $[\![A]\!]_{J[P \mapsto \mathrm{tt}, Q \mapsto \mathrm{tt}]} = \mathrm{tt}$.

Moreover, by Definition 3.2.3, $\nvdash A$ iff there does not exist a proof tree whose root is $\Rightarrow A$. In contrast, $\vdash \neg A$ iff there exists a proof tree whose root is $\Rightarrow \neg A$. Indeed, if $A \equiv P \supset Q$ where $P, Q \in \mathbf{PVar}$ and $P \neq Q$, then $\nvdash A$ holds while $\vdash \neg A$ does not hold.