软件分析与验证 **截止时间: 2024 年 3 月 28 日**

作业 1

授课老师: 贺飞 Johnson 许霆康 (2019080126)

助教: 韩志磊、黄碧婷

在开始完成作业前，请仔细阅读以下说明：

- 我们提供作业的 LaTeX 源码，你可以在其中直接填充你的答案并编译 PDF（请使用 xelatex）。当然，你也可以使用别的方式完成作业（例如撰写纸质作业后扫描到 PDF 文件之中）。但是请注意，最终的提交一定只是 PDF 文件。提交时请务必再次核对，防止提交错误。
- 在你的作业中，请务必填写你的姓名和学号，并检查是否有题目遗漏。请重点注意每次作业的截止时间。截止时间之后你仍可以联系助教补交作业，但是我们会按照如下公式进行分数的折扣：

$$\text{作业分数} = \text{满分} \times (1 - 10\% \times \min(\lceil \text{迟交周数} \rceil, 10)) \times \text{正确率}.$$

- 本次作业为独立作业，禁止抄袭等一切不诚信行为。作业中，如果涉及参考资料，请引用注明。

Problem 1: 判断题

给定下列陈述，请判断其是否正确。如果错误，请给出反例或解释原因。

1-1 给定任意的命题逻辑公式，它是否为永假式一定是可判定的。

Solution True. ■

1-2 给定命题逻辑公式 F 和 G，如果 F 是有效的且 G 不是有效的，则 $F \to G$ 一定不可满足。

Solution False. F is always true since it is valid and G contains some outcome which can be true since it is not valid. Therefore $F \to G$ is satisfiable. ■

1-3 给定命题逻辑公式 F 和 G，如果 F 是可满足的且 $\neg G$ 是不可满足的，则 $F \wedge G$ 一定可满足。

Solution True. F is satisfiable and G is valid. ■

1-4 任意给定一个一阶逻辑公式，一定可以在有限时间内判定其是否有效。

Solution True. ■

Problem 2: 解答题

2-1 考虑下列公式（记作 F）:

$$(P \vee Q \to R) \to (\neg R \vee \neg P) \to (Q \to R)$$

请列出它的真值表，并判断它是否有效. 若有效，请使用 $\mathcal{S}_{PL}$ 证明其有效性，即给出 $\vdash F$ 的证明.

Solution

P	Q	R	$(P \vee Q \to R)$	$(\neg R \vee \neg P)$	$(Q \to R)$	$(P \vee Q \to R) \to (\neg R \vee \neg P) \to (Q \to R)$
T	T	T	T	F	T	T
T	T	F	F	T	F	T
T	F	T	T	F	T	T
T	F	F	F	T	T	T
F	T	T	T	T	T	T
F	T	F	F	T	F	T
F	F	T	T	T	T	T
F	F	F	T	T	T	T

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{P \vee Q \to R, Q, R \vdash R}\ (Ax)}{P \vee Q \to R, Q \vdash \neg R, R}\ (\neg R) \qquad \dfrac{\dfrac{\dfrac{}{\neg P, P, Q \vdash Q, R}\ (Ax)}{\neg P, Q \vdash P \vee Q, R}\ (\to R) \qquad \dfrac{}{\neg P, Q, R \vdash R}\ (Ax)}{P \vee Q \to R, \neg P, Q \vdash R}\ (\to L)}{P \vee Q \to R, \neg R \vee \neg P, Q \vdash R}\ (\to L)}{P \vee Q \to R, \neg R \vee \neg P \vdash Q \to R}\ (\to R)}{P \vee Q \to R \vdash (\neg R \vee \neg P) \to (Q \to R)}\ (\to R)}{\vdash (P \vee Q \to R) \to (\neg R \vee \neg P) \to (Q \to R)}\ (\to R)$$

■

2-2 证明 $\mathcal{S}_{PL}$ 的切规则是可靠的:

$$\dfrac{\Gamma \vdash C, \Delta \qquad \Gamma, C \vdash \Delta}{\Gamma \vdash \Delta}\ (\text{切})$$

Solution Proof by Induction such that from height 1 to n where there is an instance where there exists an Axiom which shows it is satisfiable.

Assuming we have the following:

$$\dfrac{\Gamma, A \vdash A, \Delta \qquad \Gamma, A \vdash \Delta}{\Gamma, A \vdash \Delta}\ (\text{cut})$$

$$\downarrow$$

$$\dfrac{\dfrac{}{\Gamma, A \vdash A, \Delta}\ (\text{Axiom}) \dfrac{\nabla}{\Gamma, A \vdash \Delta}}{\Gamma, A \vdash \Delta}\ (\text{cut})$$

Since from this get an Axiom it means that it would be satisfiable as long as we can reach an instance of $\Gamma, A \vdash \Delta$

Assuming the previous as Part 1, now returning to the initial equation:

$$\dfrac{\Gamma \vdash B, \Delta \qquad \Gamma, B \vdash \Delta}{\Gamma \vdash \Delta}\ (\text{cut})$$

$$\downarrow$$

$$\dfrac{\dfrac{\nabla}{\Gamma, \vdash B, \Delta} \qquad \dfrac{\text{Part 1}}{\Gamma, B \vdash \Delta}\ (\text{cut})}{\Gamma \vdash \Delta}\ (\text{cut})$$

We can see that cut would give us Part 1 which means there exists an Axiom and therefore for any $\Gamma \vdash \Delta,$ there exists a cut which results in a solution therefore proving it is satisfiable.

■

2-3 考虑论域 $\mathcal{D} = \{\circ, \bullet\}$ 以及下面的解释函数

- $\mathcal{I}(f) = \{(\circ, \circ) \mapsto \bullet, (\circ, \bullet) \mapsto \circ, (\bullet, \circ) \mapsto \bullet, (\bullet, \bullet) \mapsto \circ\}$
- $\mathcal{I}(g) = \{\circ \mapsto \bullet, \bullet \mapsto \circ\}$
- $\mathcal{I}(p) = \{(\bullet, \circ), (\circ, \bullet)\}$

求公式 $\forall x.p(f(g(x), x), x)$ 的取值。

Solution

- $Let [\![x]\!]_{\mathcal{M},\rho} = \circ$
- $[\![g(x)]\!]_{\mathcal{M},\rho} = \mathcal{I}(g)([\![x]\!]_{\mathcal{M},\rho}) = \mathcal{I}(g)(\circ) = \bullet$
- $[\![f(g(x), x)]\!]_{\mathcal{M},\rho} = \mathcal{I}(f)(\bullet, \circ) = \bullet$
- $[\![p(f(g(x), x), x)]\!]_{\mathcal{M},\rho} = \mathcal{I}(p)(\bullet, \circ) = true$
- $Let [\![x]\!]_{\mathcal{M},\rho} = \bullet$
- $[\![g(x)]\!]_{\mathcal{M},\rho} = \mathcal{I}(g)([\![x]\!]_{\mathcal{M},\rho}) = \mathcal{I}(g)(\bullet) = \circ$
- $[\![f(g(x), x)]\!]_{\mathcal{M},\rho} = \mathcal{I}(f)(\circ, \bullet) = \circ$
- $[\![p(f(g(x), x), x)]\!]_{\mathcal{M},\rho} = \mathcal{I}(p)(\circ, \bullet) = true$
- For all of $x = \{\circ, \bullet\}$ is True therefore $\forall x.p(f(g(x), x), x)$ is True.

■

2-4 请使用 $\mathcal{S}_{FOL}$（包含命题逻辑中的 10 条规则和 4 条量词消去规则）构建推导树证明下列两个相继式：

1. $\exists x.(p(x) \to q(x)) \vdash \forall y.p(y) \to \exists z.q(z)$
2. $\forall y.p(y) \to \exists z.q(z) \vdash \exists x.(p(x) \to q(x))$

Solution $\exists x.(p(x) \to q(x)) \vdash \forall y.p(y) \to \exists z.q(z)$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{(Ax)}
\UnaryInfC{$p(c) \vdash p(c), q(c)$}
\RightLabel{$(\neg L)$}
\UnaryInfC{$\vdash p(c) \neg p(c), q(c)$}
\AxiomC{}
\RightLabel{(Ax)}
\UnaryInfC{$q(c) \vdash q(c), \neg p(c)$}
\RightLabel{$(\to L)$}
\BinaryInfC{$p(c) \to q(c)) \vdash \neg p(c), q(c)$}
\RightLabel{$(\exists L)$}
\UnaryInfC{$\exists x.(p(x) \to q(x)) \vdash \neg p(c), q(c)$}
\RightLabel{$(\forall R)$}
\UnaryInfC{$\exists x.(p(x) \to q(x)) \vdash \neg \forall y.\neg p(y), q(c)$}
\RightLabel{$(\neg L)$}
\UnaryInfC{$\exists x.(p(x) \to q(x)), \forall y.p(y), \vdash q(c)$}
\RightLabel{$(\neg L)$}
\UnaryInfC{$\exists x.(p(x) \to q(x)), \forall y.p(y), \neg q(c) \vdash \perp$}
\RightLabel{$(\exists L)$}
\UnaryInfC{$\exists x.(p(x) \to q(x)), \forall y.p(y), \neg \exists z.\neg q(z) \vdash \perp$}
\RightLabel{$(\neg R)$}
\UnaryInfC{$\exists x.(p(x) \to q(x)), \forall y.p(y) \vdash \exists z.q(z)$}
\RightLabel{$(\to R)$}
\UnaryInfC{$\exists x.(p(x) \to q(x)) \vdash \forall y.p(y) \to \exists z.q(z)$}
\end{prooftree}
$$

$\forall y.p(y) \to \exists z.q(z) \vdash \exists x.(p(x) \to q(x))$

$$
\begin{prooftree}
\AxiomC{}
\RightLabel{(Ax)}
\UnaryInfC{$p(c) \vdash p(c), q(c)$}
\RightLabel{$(\forall R)$}
\UnaryInfC{$p(c) \vdash \forall y.p(y), q(c)$}
\AxiomC{}
\RightLabel{(Ax)}
\UnaryInfC{$p(c), q(c) \vdash q(c)$}
\RightLabel{$(\exists L)$}
\UnaryInfC{$p(c), \exists z.q(z) \vdash q(c)$}
\RightLabel{$(\to L)$}
\BinaryInfC{$\forall y.p(y) \to \exists z.q(z), p(c) \vdash q(c)$}
\RightLabel{$(\to R)$}
\UnaryInfC{$\forall y.p(y) \to \exists z.q(z) \vdash p(c) \to q(c)$}
\RightLabel{$(\neg L)$}
\UnaryInfC{$\forall y.p(y) \to \exists z.q(z), \neg(p(c) \to q(c)) \vdash \perp$}
\RightLabel{$(\exists L)$}
\UnaryInfC{$\forall y.p(y) \to \exists z.q(z) \neg \exists x.\neg(p(x) \to q(x)) \vdash \perp$}
\RightLabel{$(\neg R)$}
\UnaryInfC{$\forall y.p(y) \to \exists z.q(z) \vdash \exists x.(p(x) \to q(x))$}
\end{prooftree}
$$

■