ETH Zürich, D-INFK
HS 2017, 4. December 2017

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik

Solution 12

Part 1: Propositional logic

12.1 Syntax and semantic of XOR

To the definition of syntax (Definition 6.22) we add the following statement:

If F and G are formulas, then also $(F \oplus G)$ is a formula.

To the definition of semantics (Definition 6.23) we add the following:

$\mathcal{A}((F \oplus G)) = 1$ *if and only if* $\mathcal{A}(F) = 1$ *or* $\mathcal{A}(G) = 1$*, but not both.*

12.2 Satisfiability

a) We give a counterexample. Let $F := A$ and $G := A \wedge \neg A$. Then F adn $F \to G$ are both satisfiable (for $A = 1$ and $A = 0$, accordingly). However, G is not satisfiable.

b) i. The set M is not satisfiable. To show this, assume that all formulas in M are true. Since $\neg A \in M$, A must be false. Thus, since $\neg A \to \neg C \in M$, C must be false as well. But this implies that $B \wedge C \in M$ is false, which is a contradiction.

ii. A model for N is, for example, the truth assignment, in which A_1 is true and A_i is false for all $i > 1$. For example, one could interpret the statement A_i as "i is less or equal to 1", for $i \in \mathbb{N}$.

12.3 Normal forms

a) The function table of $F = (\neg A \to B \wedge C) \leftrightarrow \neg C$ is

A	B	C	$(\neg A \to B \wedge C)$	$\neg C$	$(\neg A \to B \wedge C) \leftrightarrow \neg C$
0	0	0	0	1	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	1	0	0
1	0	0	1	1	1
1	0	1	1	0	0
1	1	0	1	1	1
1	1	1	1	0	0

Using the technique from the proof of Theorem 6.4, we can find an equivalent formula in conjunctive normal form:

$$(A \vee B \vee C) \wedge (A \vee \neg B \vee C) \wedge (A \vee \neg B \vee \neg C) \wedge (\neg A \vee B \vee \neg C) \wedge (\neg A \vee \neg B \vee \neg C)$$

and an equivalent formula in disjunctive normal form:

$$(\neg A \wedge \neg B \wedge C) \vee (A \wedge \neg B \wedge \neg C) \vee (A \wedge B \wedge \neg C)$$

b)

$$\begin{aligned}
& (A \wedge \neg B) \vee (\neg A \wedge (C \wedge D)) & \\
\equiv\ & \big((A \wedge \neg B) \vee \neg A\big) \wedge \big((A \wedge \neg B) \vee (C \wedge D)\big) & \mid 6) \\
\equiv\ & \big(\neg A \vee (A \wedge \neg B)\big) \wedge \big((A \wedge \neg B) \vee (C \wedge D)\big) & \mid 2) \\
\equiv\ & \big((\neg A \vee A) \wedge (\neg A \vee \neg B)\big) \wedge \big((A \wedge \neg B) \vee (C \wedge D)\big) & \mid 6) \\
\equiv\ & \big((\neg A \vee A) \wedge (\neg A \vee \neg B)\big) \wedge \big(((A \wedge \neg B) \vee C) \wedge ((A \wedge \neg B) \vee D)\big) & \mid 6) \\
\equiv\ & \big((\neg A \vee A) \wedge (\neg A \vee \neg B)\big) \wedge \big((C \vee (A \wedge \neg B)) \wedge (D \vee (A \wedge \neg B))\big) & \mid 2), 2) \\
\equiv\ & (\neg A \vee A) \wedge (\neg A \vee \neg B) \wedge (C \vee A) \wedge (C \vee \neg B) \wedge (D \vee A) \wedge (D \vee \neg B) & \mid 6), 6)
\end{aligned}$$

This formula is in conjunctive normal form. Using equivalences 2), 11), 2) and 9), one can find a simpler formula equivalent to G, also in conjunctive normal form:

$$(\neg A \vee \neg B) \wedge (C \vee A) \wedge (C \vee \neg B) \wedge (D \vee A) \wedge (D \vee \neg B).$$

However, finding a simple formula was not required.

Part 2: Predicate logic

12.4 Structures and models

a) **i)** $\mathcal{A}$ is a model for F, because for all positive natural numbers x, y, z we have:

$$x \mid xy \quad \wedge \quad y \mid xy \quad \wedge \quad (y \nmid x \rightarrow yz \nmid x).$$

(1 Point)

ii) $\mathcal{A}$ is not a model for F, because there exist positive natural numbers x, y, z, for which the following does not hold:

$$x \mid x^y \quad \wedge \quad y \mid x^y \quad \wedge \quad (y \nmid x \rightarrow y^z \nmid x).$$

The counterexample is $x = 2, y = 3$ (note that $y \nmid x^y$). *(1 Point)*

iii) $\mathcal{A}$ is a model for F, because for all subsets A, B, C of $\mathbb{N}$ we have: *(1 Point)*

$$A \cap B \subseteq A \quad \wedge \quad A \cap B \subseteq B \quad \wedge \quad (A \not\subseteq B \rightarrow A \not\subseteq B \cap C).$$

b) **i)** A model for G is, for example, the following suitable structure $\mathcal{A}$:

$$U^{\mathcal{A}} = \mathbb{R}^+;\; f^{\mathcal{A}}(x) = 2x;\; P^{\mathcal{A}}(x, y) = 1 \iff x \leq y;\; Q^{\mathcal{A}}(x, y) = 1;\; z^{\mathcal{A}} = 1.$$

The structure $\mathcal{A}$ is a model for G, because for every positive real number x, there exists a positive real number y, for example $y = 1.5x$, such that $x \leq y < 2x$ and $Q^{\mathcal{A}}(y, 1) = 1$. *(1 Point)*

ii) For example, the following structure is suitable but is not a model for G:

$$U^{\mathcal{A}} = \mathbb{R}^+;\; f^{\mathcal{A}}(x) = x;\; P^{\mathcal{A}}(x, y) = 0;\; Q^{\mathcal{A}}(x, y) = 0;\; z^{\mathcal{A}} = 1.$$

$\mathcal{A}$ is not a model, because $Q^{\mathcal{A}}(x, y) = 0$ for all $x, y \in \mathbb{R}^+$. *(1 Point)*

iii) For example, the following structure is not suitable for G: *(1 Point)*

$$U^{\mathcal{A}} = \mathbb{R}^+;\; z^{\mathcal{A}} = 42.$$

12.5 Free variables

i) $\forall x \forall y\ (P(x, y) \vee P(x, \underline{\mathbf{z}}))$

ii) $\big(\forall x\ (\exists x\ P(x) \wedge P(x)) \vee P(\underline{\mathbf{x}})\big)$
In the first occurence of $P(x)$, x is bound by $\exists x$ and the second is bound by $\forall x$.

iii) $\forall x\ \big(\exists y\ P(y, x) \vee \exists z\ Q(x, f(z))\big)$
There are no free variables in this formula.

12.6 Tautologies

For any interpretation $\mathcal{A} = (U, \phi, \psi, \xi)$, let $\mathcal{A}_{[u_1,\dots,u_n]}$ denote the same structure $\mathcal{A}$, except that ξ is overwritten so that $\xi(x_i) = u_i$ for all $i \in \{1, \dots, n\}$ (note that ξ always defines the free variables $x_1, \dots, x_n$). We have the following:

$G := \forall x_1 \dots \forall x_n\ F$ is valid.
$\iff$ For all structures $\mathcal{A}$ suitable for G, we have $\mathcal{A}(G) = 1$.
$\iff$ For all structures $\mathcal{A}$ suitable for G and all $u_1, \dots, u_n \in U$, we have $\mathcal{A}_{[u_1,\dots,u_n]}(F) = 1$.
$\iff$ For all structures $\mathcal{A}$ suitable for F, we have $\mathcal{A}(F) = 1$.
$\iff$ F is valid.

The first and last step follow from Definition 6.11, while the second transition holds by Definition 6.35. The third step follows from the fact that any structure $\mathcal{A}$ is suitable for F if and only if it is suitable for G and assigns to all the free variables $x_1, \dots x_n$ some values $u_1, \dots, u_n \in U$.