ETH Zürich, D-INFK
HS 2023, 8. December 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Exercise 12

Exercise 12.5 gives **bonus points**, which can increase the final grade. The solution to this exercise must be your own work. You may not share your solutions with anyone else. See also the note on dishonest behavior on the course website: `https://crypto.ethz.ch/teaching/DM23/`.

12.1 CNF and DNF ($\star$)

a) Let $F = (\neg(A \to C)) \leftrightarrow (A \to B)$. Using the method of function tables, construct a formula in CNF that is equivalent to F and a formula in DNF that is equivalent to F.

b) Let $G = (A \wedge \neg B) \vee (\neg A \wedge (C \wedge D))$. Using the equivalences from Lemma 6.1, construct a formula in CNF that is equivalent to G. In each step write which equivalence you use.

12.2 Free Variables ($\star$)

Determine all occurrences of free variables in the following formulas:

i) $\forall x \forall y\ (P(x,y) \vee P(x,z))$

ii) $\forall x\ (\exists x\ P(x) \wedge P(x)) \vee P(x)$

iii) $\forall x\ \big(\exists y\ P(y,x) \vee \exists z\ Q(x, f(z))\big)$

12.3 Interpretations ($\star$)

a) Which of the interpretations **i)**, **ii)** and **iii)** are models for the following formula? Justify your answers. (The symbol $\mid$ denotes the divisibility relation.)

$$F = \forall x \forall y \forall z\ \big(P(f(x,y),x)\ \wedge\ P(f(x,y),y)\ \wedge\ \big(\neg P(x,y) \to \neg P(x, f(y,z))\big)\big)$$

i)	$U^{\mathcal{A}} = \mathbb{N} \setminus \{0\}$,	$f^{\mathcal{A}}(x,y) = x \cdot y$,	$P^{\mathcal{A}}(x,y) = 1 \iff y \mid x$
ii)	$U^{\mathcal{A}} = \mathbb{N} \setminus \{0\}$,	$f^{\mathcal{A}}(x,y) = x^y$,	$P^{\mathcal{A}}(x,y) = 1 \iff y \mid x$
iii)	$U^{\mathcal{A}} = \mathcal{P}(\mathbb{N})$,	$f^{\mathcal{A}}(A,B) = A \cap B$,	$P^{\mathcal{A}}(A,B) = 1 \iff A \subseteq B$

b) Let $G = \big(\forall x\ \exists y\ P(x,y)\big)\ \wedge\ \big(\forall y\ \exists x\ P(x,y)\big)\ \wedge\ \big(\forall x\ \forall y\ (P(x,y) \to \neg P(y,x))\big)$. Find an interpretation with *a finite universe* that is

i) not suitable for G.

ii) suitable but not a model for G.

iii) suitable and a model for G.

12.4 Predicate Logic with Equality ($\star$)

We extend the syntax and the semantics of predicate logic as follows:

Syntax: If t_1 and t_2 are terms, then $(t_1 = t_2)$ is a formula.

Semantics: If F is of the form $(t_1 = t_2)$ for terms t_1 and t_2, then $\mathcal{A}(F) = 1$ if and only if $\mathcal{A}(t_1) = \mathcal{A}(t_2)$.

a) Let $F = \forall x \forall y\ (x = y)$. Find the necessary and sufficient conditions for an interpretation $\mathcal{A}$ to be a model for F. Justify your answer.

b) Let $G = \exists x \exists y\ \neg(x = y)$. Find the necessary and sufficient conditions for an interpretation $\mathcal{A}$ to be a model for G. Justify your answer.

c) Find a formula with equality H, such that for any interpretation $\mathcal{A}$ suitable for H, we have $\mathcal{A}(H) = 1 \iff |U^{\mathcal{A}}| \geq 3$.

12.5 A New Quantifier $\bigcirc$ ($\star$) *(8 Points)*

We extend predicate logic with a new quantifier $\bigcirc$ (read: *for many*) as follows:

Syntax: If F is a formula, then for any variable symbol x_i, $\bigcirc x_i\, F$ is a formula.

Semantics: $\mathcal{A}(\bigcirc x_i\, F) = 1$ if and only if $\left\{u \in U^{\mathcal{A}} \mid \mathcal{A}_{[x_i \to u]}(F) = 1\right\} \sim U^{\mathcal{A}}$.[1]

Using the semantics of predicate logic extended in this way, prove or disprove the following statements, where F is an arbitrary formula.

a) The formula $(\bigcirc x\, F) \wedge (\bigcirc x\, \neg F)$ is unsatisfiable.

b) $\bigcirc x\, F \models \exists x\, F$.

c) $\forall x \bigcirc y F \models \bigcirc y \forall x F$.

Expectation: If the statement is true, your proof should use the definitions of the semantics. In each step, at most one definition (e.g., the semantics of $\bigcirc$) should be applied. If the statement is not true, you should provide a counterexample: make sure to define everything needed for a suitable interpretation.

12.6 Statements About Formulas ($\star\star$)

Prove or disprove each of the following statements. Do not use any theorems or lemmas from the lecture notes. Note that x may appear free in F, G or both.

a) For any formulas F and G, we have

$$\forall x\ (F \wedge G)\ \models\ (\forall x\ F) \wedge G.$$

b) For any formulas F and G, we have

$$\exists x\ (F \wedge G)\ \models\ (\exists x\ F) \wedge G.$$

[1] The symbol $\sim$ for *equinumerous* was introduced in Definition 3.42-(i). For sets A and B we have $A \sim B$ if and only if there exists a bijection $f : A \to B$.

Due by 14. December 2023.
Exercise 12.5 is graded.