ETH Zürich, D-INFK
HS 2023, 30. September 2023

Prof. Ueli Maurer
David Lanzenberger

Diskrete Mathematik

Exercise 2

Exercise 2.3 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/`.

2.1 Logical Consequence

Prove or disprove the following statements about formulas.

a) ($\star$) $A \wedge (A \rightarrow B) \models B$

b) ($\star$) $A \rightarrow B \models \neg A \rightarrow \neg B$

c) ($\star$) $\models (A \rightarrow B) \vee (B \rightarrow A)$

d) ($\star\,\star$) $(A \rightarrow B) \wedge (B \rightarrow C) \models (A \rightarrow C)$

2.2 Satisfiability and Tautologies ($\star$)

For each of the formulas below, determine whether it is satisfiable or unsatisfiable and whether it is a tautology or not. Prove your answers.

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

b) $\big((A \rightarrow B) \wedge (B \rightarrow C)\big) \wedge \neg(A \rightarrow C)$

2.3 Simplifying a Formula ($\star$) *(8 Points)*

Consider the propositional formula

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

Give a formula G that is equivalent to F, but in which each atomic formula A, B, and C appears at most once. *Prove* that $F \equiv G$ by providing a sequence of equivalence transformations with *at most* 9 steps.

Expectation. Your proof should be in the form of a sequence of steps, where each step consists of applying the definition of $\rightarrow$ (that is $F \rightarrow G \equiv \neg F \vee G$), one of the rules given in Lemma 2.1 of the lecture notes[1], or one of the following rules: $F \wedge \neg F \equiv \bot$, $F \wedge \bot \equiv \bot$, $F \vee \bot \equiv F$, $F \vee \neg F \equiv \top$, $F \wedge \top \equiv F$, and $F \vee \top \equiv \top$. For this exercise, associativity is to be applied as in Lemma 2.1 *3)*. Each step of your proof should apply a *single* rule *once* and state *which* rule was applied.

[1] Lemma 2.1 states rules involving propositional symbols, but you may apply those rules at the level of formulas (see Section 2.3.5 of the lecture notes).

2.4 Knights and Knaves ($\star\star\star$)

We find ourselves on a strange island with only two types of inhabitants: knights and knaves. The knights always tell the truth, while the knaves always lie. From the outside, both groups look exactly the same and we cannot distinguish one from the other.

We have lost our way and come to a fork in the road. We know that one of the roads leads to a deadly jungle, while the other will take us to a friendly village. We see an islander standing at the fork. He is willing to answer only one question and his answer can only be "Yes" or "No". What question do we ask?

We want to use propositional logic to solve this problem. Let A be the proposition "The left road leads to the village." and let B be the proposition "The islander is a knight." We phrase our question as a formula F in A and B, asking the islander about the truth value of F. How do we choose F such that we are guaranteed to learn which road leads to the village?

2.5 Quantifiers and Predicates

In this exercise the universe is fixed to the set $\mathbb{Z}$ of integers.

a) For each of the following statements, write a formula, in which the only predicates are `less`, `equals` and `prime` (instead of `less`(n, m) and `equals`(n, m) you can write $n < m$ and $n = m$ accordingly).[2] You can also use the symbols $+$ and $\cdot$ to denote addition and multiplication.

- **i)** ($\star$) If the product of two integer numbers is positive, then at least one of these numbers is positive.
- **ii)** ($\star$) For every natural number, one can find a strictly greater natural number that is divisible by 3.
- **iii)** ($\star\star$) Every even integer greater than 2 is a sum of two primes.

Which of the above statements are true? (You do not need to justify this.)

b) Consider the following predicates $P(x)$ and $Q(x, y)$:

$$P(x) = \begin{cases} 1, & x > 0 \\ 0, & \text{otherwise} \end{cases} \qquad Q(x, y) = \begin{cases} 1, & xy = 1 \\ 0, & \text{otherwise} \end{cases}$$

In this context, describe the following statements in words. Also, for each statement, decide whether it is true or false.

- **i)** ($\star$) $\forall x\, \exists y\, Q(x, y)$
- **ii)** ($\star$) $\exists x \big(\forall y\, \neg Q(x, y) \;\wedge\; \exists y\, P(y)\big)$

[2]Note that `less`(n, m) is true if n is *strictly* smaller than m, so it is false for $n = m$.

2.6 Finding an Interpretation for a Formula ($\star\star$)

Consider the formula

$$F = \forall x\ \exists y\ \exists z\ \left(\neg(x = y) \land \neg P(x, y) \land \neg(x = z) \land P(x, z)\right).$$

For the following two subtasks, no justification is required.

a) Find an *infinite* universe U and a predicate $P : U^2 \to \{0, 1\}$ such that F is true.

b) Let $n \geq 3$ be a natural number. Find a universe U with n elements (i.e., $|U| = n$) and a predicate $P : U^2 \to \{0, 1\}$ such that F is true.

Note: The universe U and the predicate P have to be defined in terms of n, such that F is true for *all* $n \geq 3$. In particular, no fixed choice of n (say, $n = 3$) is allowed.

Due by 5. October 2022, 23:59.
Exercise 2.3 will be graded.