ETH Zürich, D-INFK
HS 2018, 28. September 2018

Prof. Ueli Maurer
Marta Mularczyk

Diskrete Mathematik

Exercise 3

Exercises 3.1 and 3.7 a) give **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://www.crypto.ethz.ch/teaching/lectures/DM18`.

3.1 Propositional Logic

($\star\star$) Consider the following formulas *(4 Points)*

$$F := (A \lor \neg C) \land (A \lor B \lor C) \land (\neg A \lor \neg B) \qquad G := B \to (\neg C \land \neg A)$$

Is it true that $F \models G$? Prove your answer.

3.2 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). [1] You can also use the symbols $+$ and $\cdot$ to denote addition and multiplication.

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

Do you know which of the above statements are true? (You do not need to justify.)

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

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

3.3 Transitivity of Quantifiers

Argue why the statement **a)** is *true*, and why the statement **b)** is *false*.[2]

a) $(\star\star)$ $\exists y\, \forall x\, P(x,y) \models \forall x\, \exists y\, P(x,y)$.

b) $(\star\star)$ $\forall x\, \exists y\, P(x,y) \models \exists y\, \forall x\, P(x,y)$.

3.4 Winning Strategy $(\star\star)$

Alice and Bob play a game in which the stake is a chocolate bear. Rules of the game are the following: Alice chooses two integers a_1, a_2 and Bob chooses two integers b_1, b_2. Alice wins whenever $a_1 + (a_2 + b_1)^{|b_2|+1} = 1$ and Bob wins otherwise.

a) First, consider the case when Alice and Bob announce all their numbers at the same time. Give a formula that describes the statement "Alice has a winning strategy." Is this statement true?

b) In the second case, Alice and Bob announce their numbers one by one. That is, first Alice announces a_1, then Bob announces b_1, then Alice announces a_2, and at the end Bob replies with b_2. Once again, give a formula that describes the statement "Alice has a winning strategy.". Is this statement true in this case?

3.5 Direct Proof of an Implication (2.4.3) $(\star)$

Prove directly that the product of two even natural numbers is even.

3.6 Indirect Proof of an Implication (2.4.4)

Prove indirectly that for all natural numbers $n > 0$, we have:

a) $(\star\star)$ If $42^n - 1$ is a prime, then n is odd.

b) $(\star\star)$ If n^2 is odd, then n is also odd.

3.7 Case Distinction (2.4.7)

Prove by case distinction that:

a) $(\star\star)$ $n^3 + 2n + 6$ is divisible by 3 for all natural numbers $n \geq 0$. *(4 Points)*

b) $(\star\star\star)$ If p and $p^2 + 2$ are primes, then $p^3 + 2$ is also a prime.

Due on 9. October 2018.
Exercises 3.1. and 3.7. a) are graded.

---

[2] At this point you should only give an intuitive argument. To turn this argument into a proof, we would need the formal definitions from Chapter 6.