ETH Zürich, D-INFK
HS 2024, 4. October 2024

Prof. Ueli Maurer
Giovanni Deligios, Dr. Karen Klein

Diskrete Mathematik

Exercise 3

Exercises 3.2 and 3.8 give **bonus points**, which can increase the final grade. The solution to these exercises 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/DM24/`.

Part 1: Predicate Logic

3.1 Expressing Relationship of Humans in Predicate Logic ($\star$)

Consider, as in the lecture, the universe of all humans (including those who died) and the following predicate:

$$\texttt{par}(x, y) = 1 \iff \text{“}x \text{ is parent of } y.\text{”}$$

Express the following statements as a formula in predicate logic, using only the above predicates (in particular, do *not* use the predicate `equals`, often also written as $=$).

a) x is great-grandparent of y.

b) x and y are (first) cousins.

3.2 From Natural Language to a Formula ($\star$) *(4 Points)*

Consider the universe $U = \mathbb{N}\backslash\{0\}$. Express each of the following statements with a formula in predicate logic, in which the only predicates appearing are $\texttt{divides}(x, y)$, $\texttt{equals}(x, y)$ and $\texttt{prime}(x)$ (instead of $\texttt{divides}(x, y)$ and $\texttt{equals}(x, y)$ you can write $x \mid y$ and $x = y$ accordingly). You can also use the symbols $+$ and $\cdot$ to denote the addition and multiplication functions, and you can use constants (e.g., $0, 1, \ldots$). You can also use $\longleftrightarrow$. No justification is required.

i) ($\star$) If a number divides two numbers, then it also divides their sum.

ii) ($\star$) The only divisors of a prime number are 1 and the number itself.

iii) ($\star$) 1 is the only natural number which has an inverse.

iv) ($\star$) A prime number divides the product of two natural numbers if and only if it divides at least one of them.

3.3 Winning Strategy ($\star\star$)

Alice and Bob play a game in which the stake is a chocolate bar. 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?

Part 2: Proof Patterns

3.4 Indirect Proof of an Implication (2.6.3)

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

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

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

3.5 Case Distinction (2.6.5)

Prove by case distinction that:

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

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

3.6 Proof by Contradiction (2.6.6)

a) ($\star\star$) Show by contradiction that the sum of a rational number and an irrational number is irrational.

Hint: Use the fact that the difference of two rational numbers is rational.

b) ($\star\star\star$) Show that the number $2^{\frac{1}{n}}$ is irrational for $n > 2$, by reaching a contradiction with Fermat's Last Theorem.

Hint: Fermat's Last Theorem states that no positive integers a, b, c satisfy the equation $a^n + b^n = c^n$ for $n > 2$.

3.7 New Proof Patterns ($\star$)

For each of the following proof patterns, **prove** or **disprove** that it is sound.

a) ($\star$) To prove a statement S, find two appropriate statements T_1 and T_2. Assume that S is false and show (from this assumption) that one between the statements T_1 and T_2 is true. Then show that one statement between T_1 and T_2 is false.

b) ($\star$) To prove an implication $S \Rightarrow T$, find an appropriate statement R. Assume that S is true and T is false, and prove that (from these assumptions) R is true. Then show that R is false.

3.8 Proof by Contradiction ($\star$) *(4 Points)*

Let $n, m \in \mathbb{N}$ be arbitrary. We say "n divides m" and write $n \mid m$ if there exists a $k \in \mathbb{N}$ such that $k \cdot n = m$. Prove that the following statement is true, using a proof by contradiction:

$$n \mid m \text{ and } n \mid (m+1) \implies n = 1.$$

You are allowed to invoke the statement 3.2 **iii)** from above to justify one step.

You must use the same notation as in the lecture notes, i.e. precisely state what your statements S and T are, and justify each of your proof steps.

Due on 10. October 2024, 23:59.
Exercises 3.2 and 3.8 are graded.