ETH zürich

Discrete Mathematics **2024**

Student: Jeferson Morales Mariciano <jmorale@ethz.ch>

Assignment 3 **Due date:** Thursday, 10 October 2024, 23:59

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

Consider the universe $U = \mathbb{N} \setminus \{0\}$. Express each of the following statements with a formula in predicate logic, in which the only predicates appearing are $divides(x, y)$, $equals(x, y)$ and $prime(x)$ (instead of divides(x, y) and equals(x, y) you can write $x|y$ 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, . . .). You can also use $\leftrightarrow$. 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.

i)

$$\forall x\, \forall y\, \forall z\ \left(((x \,|\, y) \land (x \,|\, z)) \longrightarrow (x \,|\, (y + z))\right) \tag{1}$$

ii)

$$\forall x\, \forall y\ \left((prime(x) \land (y \,|\, x)) \longrightarrow ((y = 1) \lor (y = x))\right) \tag{2}$$

iii)

$$\forall x\, \forall y\ \left((x \cdot y = 1) \longrightarrow ((x = 1) \land (y = 1))\right) \tag{3}$$

iv)

$$\forall x\ \left(prime(x) \longrightarrow \forall y\, \forall z\ ((x \,|\, (y \cdot z)) \longleftrightarrow ((x \,|\, y) \lor (x \,|\, z)))\right) \tag{4}$$

Exercise 3.8, Proof by Contradiction ($\star$) (4 Points)

Let $n, m \in \mathbb{N}$ be arbitrary. We say "n divides m" and write $n|m$ 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:

$$n|m \ \text{ and } \ n|(m + 1) \Longrightarrow n = 1.$$

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.

Proof. From Definition 2.17, a proof by contradiction of a statement S proceeds in 3 steps:

1. Find a suitable mathematical statement T.

2. Prove that T is false.

3. Assume that S is false and prove (from this assumption) that T is true (a contradiction).

The general informal overview of the proof is to use the statement 3.2 **iii)** 3 i.e. the only natural number which has an inverse is 1. It will be used to prove that statement T is false, namely that there exist some pair(s) of number belonging to $\mathbb{N}$ such that their product is 1 and at least one of them is not 1, meaning that 1 is not the only natural number with an inverse. Then, from assuming that $\neg S$ is true, we will prove that T is true through composition of implications, which will lead to a contradiction. The statement provided to be proved will be our statement S, namely that if a number n divides two other consecutive numbers, then it must be equal to 1.

The interpretation is fixed by remarking that the universe is $U = \mathbb{N}$ of natural numbers, the predicates will be $divides(x, y)$, $equals(x, y)$, $sum(x, y)$, $multiplication(x, y)$. Finally, the function symbols used will be $\,|\,, =, +, \cdot$ for divisibility, equality, addition and multiplication, respectively. Nevertheless, we stick to make mathematical statements about formulas.

From the statement 3.2 **iii)** 3:

$$\forall x\, \forall y\ \ ((x \cdot y = 1) \longrightarrow ((x = 1) \wedge (y = 1)))$$

its negation leads to state that there exists some pair of numbers which product is 1 and at least one of these numbers is not 1, meaning 1 is not the only natural number with an inverse as shown below:

$$\begin{aligned}
& \neg\forall x\, \forall y\ \ ((x \cdot y = 1) \longrightarrow ((x = 1) \wedge (y = 1))) & \\
\Longrightarrow\ & \exists x\, \neg\forall y\ \ ((x \cdot y = 1) \longrightarrow ((x = 1) \wedge (y = 1))) & (\text{from 2.4.8, } \neg\forall x P(x) \equiv \exists x \neg P(x)) \\
\Longrightarrow\ & \exists x\, \exists y\, \neg\, ((x \cdot y = 1) \longrightarrow ((x = 1) \wedge (y = 1))) & (\text{idem}) \\
\Longrightarrow\ & \exists x\, \exists y\, \neg\, (\neg\, (x \cdot y = 1) \vee ((x = 1) \wedge (y = 1))) & (A \to B \equiv \neg A \vee B) \\
\Longrightarrow\ & \exists x\, \exists y\ \ (\neg\neg\, (x \cdot y = 1) \wedge \neg\, ((x = 1) \wedge (y = 1))) & (\text{De Morgan}) \\
\Longrightarrow\ & \exists x\, \exists y\ \ ((x \cdot y = 1) \wedge \neg\, ((x = 1) \wedge (y = 1))) & (\text{double negation}) \\
\Longrightarrow\ & \exists x\, \exists y\ \ ((x \cdot y = 1) \wedge (\neg\, (x = 1) \vee \neg\, (y = 1))) & (\text{De Morgan})
\end{aligned}$$

Hence, w.r.t. interpretation the clearly **false statement T is "1 is not the only natural number which has an inverse"**. Let $n, k \in U$

$$T \Longrightarrow\ \ \exists n\, \exists k\ \ ((n \cdot k = 1) \wedge (\neg\, (n = 1) \vee \neg\, (k = 1)))$$

Now, the **statement to be proved S is "given n dividing two consecutive numbers, then it must be equal to 1"**:

$$S \Longrightarrow \forall n\, \forall m\ \ (((n \,|\, m) \wedge (n \,|\, (m + 1))) \longrightarrow n = 1)$$

Assuming that the statement S is false, i.e. $\neg S$, meaning that there exist some n, m such that n divides m and n divides $m + 1$, and n is not equal to 1:

$$\begin{aligned}
\neg S \Longrightarrow\ & \neg\forall n\, \forall m\ \ (((n \,|\, m) \wedge (n \,|\, (m + 1))) \longrightarrow n = 1) \\
\Longrightarrow\ & \exists n\, \neg\forall m\ \ (((n \,|\, m) \wedge (n \,|\, (m + 1))) \longrightarrow n = 1) \\
\Longrightarrow\ & \exists n\, \exists m\, \neg\, (((n \,|\, m) \wedge (n \,|\, (m + 1))) \longrightarrow n = 1) \\
\Longrightarrow\ & \exists n\, \exists m\, \neg\, (\neg\, ((n \,|\, m) \wedge (n \,|\, (m + 1))) \vee (n = 1)) \\
\Longrightarrow\ & \exists n\, \exists m\ \ (\neg\neg\, ((n \,|\, m) \wedge (n \,|\, (m + 1))) \wedge \neg\, (n = 1)) \\
\Longrightarrow\ & \exists n\, \exists m\ \ (((n \,|\, m) \wedge (n \,|\, (m + 1))) \wedge \neg\, (n = 1))
\end{aligned}$$

from definition of divisibility we have that:

$$n \,|\, m \overset{\text{def}}{\Longleftrightarrow} \exists k\ \ (k \cdot n = m)$$

so we can rewrite the statements $n \,|\, m$ and $n \,|\; (m+1)$ as:

$$\begin{cases} n \,|\, m & \overset{\cdot}{\Longrightarrow} \quad k_1 \cdot n = m \\ n \,|\, (m+1) & \overset{\cdot}{\Longrightarrow} \quad k_2 \cdot n = m+1 \overset{\cdot}{\Longrightarrow} (k_2 \cdot n) - 1 = m \end{cases}$$

since $m = m$, we can inject the first equation into the second one:

$$\begin{aligned} & k_1 \cdot n = (k_2 \cdot n) - 1 \\ \overset{\cdot}{\Longrightarrow} \quad & (k_1 \cdot n) - (k_2 \cdot n) = -1 \\ \overset{\cdot}{\Longrightarrow} \quad & n \cdot (k_1 - k_2) = -1 \\ \overset{\cdot}{\Longrightarrow} \quad & n \cdot (k_2 - k_1) = 1 \\ \overset{\cdot}{\Longrightarrow} \quad & n \cdot k = 1 \end{aligned}$$

By plugging all back into the formula derived from assumption of $\neg S$, using composition of implications, we get a contradiction that n times k gives 1, meaning it has an inverse, but n is not equal to 1, meaning that there exists a number that has an inverse and is not 1. It corresponds to the form of the statement T already proved to be false, as shown below:

$$\exists n \, \exists m \, \exists k \left(((n \,|\, m) \wedge (n \,|\, (m+1))) \wedge \underbrace{\neg\, (n = 1) \wedge ((k \cdot n) = 1)}_{T \text{ false for arbitrary k and n}} \right)$$

Therefore, the statement S must be true, it is satisfiable and holds for our interpretation, concluding the proof. $\square$