ETH Zürich, D-INFK
HS 2023, 13. October 2023

Prof. Ueli Maurer
Giovanni Deligios

Diskrete Mathematik

Solution 3

Part 1: Predicate Logic

3.1 Expressing Relationship of Humans in Predicate Logic

a) $\exists u\ \exists v\ \ (\texttt{par}(x,u) \wedge \texttt{par}(u,v) \wedge \texttt{par}(v,y))$.

b) $\exists u\ \exists v\ \exists w\ (\texttt{par}(u,v) \wedge \texttt{par}(u,w) \wedge \texttt{par}(v,x) \wedge \texttt{par}(w,y) \wedge \neg\texttt{par}(v,y) \wedge \neg\texttt{par}(w,x))$.

3.2 From Natural Language to a Formula

a) $\exists x\, \exists y\, \big(\texttt{integer}(x) \wedge \texttt{integer}(y) \wedge \texttt{less}(0,x) \wedge \texttt{less}(0,y) \wedge \texttt{less}(x+y,0)\big)$.

b) $\forall x\, \neg\Big(\forall y\, \big(\exists p\, \exists q\, (\texttt{integer}(p) \wedge \texttt{integer}(q) \wedge \neg\texttt{equals}(q,0) \wedge \texttt{equals}(q\cdot y, p)) \rightarrow \texttt{less}(y,x)\big)\Big)$.

c) $\Big(\forall x\, \forall y\, \exists z \big(\texttt{integer}(z) \wedge ((\texttt{less}(x,z) \wedge \texttt{less}(z,y)) \vee (\texttt{less}(y,z) \wedge \texttt{less}(z,x)))\big)\Big) \rightarrow \forall x\, \texttt{less}(0,x)$.

d) $\forall x\, \forall y\, \Big(\texttt{integer}(x) \wedge \texttt{integer}(y) \wedge \big(\exists k\, (\texttt{integer}(k) \wedge \texttt{equals}(x+y, 2\cdot k+1))\big)\Big) \rightarrow \Big(\big((\exists k\, (\texttt{integer}(k) \wedge \texttt{equals}(x, 2\cdot k))) \wedge (\exists k\, (\texttt{integer}(k) \wedge \texttt{equals}(y, 2\cdot k+1)))\big) \vee \big((\exists k\, (\texttt{integer}(k) \wedge \texttt{equals}(y, 2\cdot k))) \wedge (\exists k\, (\texttt{integer}(k) \wedge \texttt{equals}(x, 2\cdot k+1)))\big)\Big)$.

3.3 Winning Strategy

a) The numbers announced by Alice cannot depend on Bob's choice for b_1 and b_2. Therefore, the statement can be described by the following formula:

$$\exists a_1 \exists a_2 \forall b_1 \forall b_2\ \ \big(a_1 + (a_2+b_1)^{|b_2|+1} = 1\big).$$

The above statement is false, because for each tuple (a_1, a_2), there exists a tuple $(b_1, b_2) := (2 - a_2 - a_1, 0)$ such that

$$a_1 + (a_2+b_1)^{|b_2|+1} = a_1 + (a_2 + 2 - a_2 - a_1) = 2.$$

Therefore, Alice does not have a winning strategy.

b) In this case, Alice's choice for a_2 can depend on b_1. Therefore, the statement can be described by the following formula:

$$\exists a_1 \forall b_1 \exists a_2 \forall b_2 \ \big(a_1 + (a_2 + b_1)^{|b_2|+1} = 1\big).$$

This statement is true. A possible winning strategy for Alice is to choose $a_1 = 1$ and $a_2 = -b_1$. For such choice, we have

$$a_1 + (a_2 + b_1)^{|b_2|+1} = 1 + 0^{|b_2|+1} = 1.$$

Part 2: Proof Patterns

3.4 Indirect Proof of an Implication (2.6.3)

a) Assume that n is even. Then, $n = 2k$ for some $k \in \mathbb{N}$. We have therefore $n^2 = n \cdot n = 2k \cdot 2k = 2 \cdot 2k^2$. Hence, n^2 is even.

Detailed solution:

Statement S: n^2 is odd.

Statement T: n is odd.

Indirect proof:
n is not odd.
$\stackrel{.}{\Longrightarrow}$ n is even.
$\stackrel{.}{\Longrightarrow}$ $n = 2k$ for some $k \in \mathbb{N}$.
$\stackrel{.}{\Longrightarrow}$ $n \cdot n = 2k \cdot 2k$ for some $k \in \mathbb{N}$.
$\stackrel{.}{\Longrightarrow}$ $n \cdot n = 2 \cdot 2k^2$ for some $k \in \mathbb{N}$.
$\stackrel{.}{\Longrightarrow}$ $n \cdot n = 2l$ for some $l \in \mathbb{N}$.
$\stackrel{.}{\Longrightarrow}$ $n^2 = 2l$ for some $l \in \mathbb{N}$.
$\stackrel{.}{\Longrightarrow}$ n^2 is even.

b) Assume that n is even. We show that in such case $42^n - 1$ is not a prime. To this end, notice that, since n is even, there must exist a natural number $k > 0$, such that $n = 2k$. It follows that $42^n - 1 = 42^{2k} - 1 = (42^k + 1)(42^k - 1)$. Therefore, we found two non-trivial divisors of $42^n - 1$, namely $(42^k + 1)$ and $(42^k - 1)$ (they are greater than 1, because $k > 0$). Thus, $42^n - 1$ cannot be a prime.

Detailed solution:
We consider two statements S and T. We have to show that $S \Longrightarrow T$ is true. To this end, we use an indirect direct proof, that is, we assume that T is false and show that, under this assumption S, must also be false.

Statement S: $42^n - 1$ is a prime.

Statement T: n is odd.

Indirect proof:
n is not odd.
$\stackrel{.}{\Longrightarrow}$ n is even.
$\stackrel{.}{\Longrightarrow}$ There exists a natural number, call it k, such that $k > 0$ and $n = 2k$.
$\stackrel{.}{\Longrightarrow}$ We have $42^n - 1 = 42^{2k} - 1 = (42^k + 1)(42^k - 1)$ for $k > 0$.
$\stackrel{.}{\Longrightarrow}$ There exist two non-trivial divisors of $42^n - 1$, namely $(42^k + 1)$ and $(42^k - 1)$.
$\stackrel{.}{\Longrightarrow}$ $42^n - 1$ is not a prime.

3.5 Case Distinction (2.6.5)

a) Let n be any natural number greater or equal 0. Let $n = 3k + c$, where $0 \leq c \leq 2$ and $k \in \mathbb{N}$. We have

$$\begin{aligned} n^3 + 2n + 6 &= (3k + c)^3 + 2(3k + c) + 6 \\ &= c^3 + 9c^2k + 27ck^2 + 2c + 27k^3 + 6k + 6. \end{aligned}$$

Each summand is divisible by 3, except the term $c^3 + 2c$. Hence, we only need to show that $c^3 + 2c$ is divisible by 3 for $0 \leq c \leq 2$.

Case $c = 0$**:** $c^3 + 2c = 0$, which is divisible by 3.

Case $c = 1$**:** $c^3 + 2c = 3$, which is divisible by 3.

Case $c = 2$**:** $c^3 + 2c = 12$, which is divisible by 3.

Since the above cases cover all possibilities for c, we can conclude the proof.

b) In the following, we let $R_3(x)$ denote the remainder of the division of x by 3 (for example, $R_3(5) = 2$). For any prime number p, we can distinguish the following three cases:

$p = 2$**:** If $p = 2$, then $p^2 + 2 = 6$ is not a prime. Thus, the claim holds for $p = 2$.

$p = 3$**:** If $p = 3$, then $p^2 + 2 = 11$ is a prime. However, we now have $p^3 + 2 = 29$, which is also a prime. Thus, the claim also holds for $p = 3$.

$p > 3$**:** If $p > 3$ is a prime, then 3 cannot divide p. Therefore, we have $R_3(p) \in \{1, 2\}$. Thus, it holds that

$$R_3(p^2) = R_3(R_3(p) \cdot R_3(p)) = 1.$$

It follows that

$$R_3(p^2 + 2) = R_3(R_3(p^2) + R_3(2)) = R_3(1 + 2) = 0$$

Therefore, $p^2 + 2$ must be divisible by 3 and so it is not a prime. Thus, the claim holds also for $p > 3$.

Since the above cases cover all prime numbers, the claim holds.

3.6 Proof by Contradiction (2.6.6)

a) Let x be any irrational number and let r be any rational number. Assume that $s = x + r$ is rational. To reach a contradiction, we show that in such case x must be rational. Indeed, we have $x = s - r$. Therefore, we have that x is a difference of two rational numbers and thus, by the fact from the hint, it must also be rational. This is a contradiction with the assumption that x is irrational.

Detailed solution:
Consider a statement S. To show that S is true, we will state a false statement T, and show that if S is false, then T is true.

Fix any irrational number x and any rational number r.

Statement S**:** The sum $x + r$ is irrational.

Statement T**:** x is rational.

Proof by contradiction:

We show that if S is false, then T is true:

S is false.
$\overset{\cdot}{\Longrightarrow}$ It is not true that the sum $x + r$ is irrational.
$\overset{\cdot}{\Longrightarrow}$ The sum $s = x + r$ is rational.
$\overset{\cdot}{\Longrightarrow}$ $x = s - r$, where s and r are some rational numbers.
$\overset{\cdot}{\Longrightarrow}$ x is rational. (by the fact from the hint)
$\overset{\cdot}{\Longrightarrow}$ T is true.

The statement T is trivially false.

b) Assume for contradiction that $2^{\frac{1}{n}}$ is rational for some $n > 2$. That is, assume that there exist two positive integers, call them p and q, such that $2^{\frac{1}{n}} = \frac{p}{q}$. This implies that $2 = \frac{p^n}{q^n}$. Hence, we have $q^n + q^n = p^n$, which is a contradiction with Fermat's Last Theorem.

The contradiction with Fermat's Last Theorem follows from the counterexample $q^n + q^n = p^n$.

Detailed solution:

Fix any integer $n > 2$.

Statement S**:** $2^{\frac{1}{n}}$ is irrational.

Statement T**:** There exist positive integers p, q such that $q^n + q^n = p^n$.

Proof by contradiction:

We show that if S is false, then T is true:

S is false.
$\overset{\cdot}{\Longrightarrow}$ It is not true that $2^{\frac{1}{n}}$ is irrational.
$\overset{\cdot}{\Longrightarrow}$ $2^{\frac{1}{n}}$ is rational.
$\overset{\cdot}{\Longrightarrow}$ There exist positive integers p and q such that $2^{\frac{1}{n}} = \frac{p}{q}$.
$\overset{\cdot}{\Longrightarrow}$ There exist positive integers p and q such that $2 = \frac{p^n}{q^n}$.
$\overset{\cdot}{\Longrightarrow}$ There exist positive integers p and q such that $q^n + q^n = p^n$.
$\overset{\cdot}{\Longrightarrow}$ T is true.

The statement T is false, since it is a counterexample to Fermat's Last Theorem.

3.7 New Proof Patterns

a) The proof pattern described corresponds to the following statement about formulas:

$$(\neg A \to (B_1 \vee B_2)) \wedge (\neg B_1 \vee \neg B_2) \models A.$$

We show that the proof pattern is not sound by showing that the statement is false. Consider a truth assignment for which A is false, B_1 is true, and B_2 is false. Computing the function table of $(\neg A \to (B_1 \vee B_2)) \wedge (\neg B_1 \vee \neg B_2)$ shows that the formula is true under this truth assignment. Since A is false, the logical consequence does not hold.

b) The proof pattern described corresponds to the following statement about formulas:

$$((A \wedge \neg B) \to C) \wedge \neg C \models A \to B.$$

We show that the proof pattern is sound by showing that the statement is true. To do so, we compute the function tables of the formulas involved.

A	B	C	$((A \wedge \neg B) \to C) \wedge \neg C$	$A \to B$
0	0	0	1	1
0	0	1	0	1
0	1	0	1	1
0	1	1	0	1
1	0	0	0	0
1	0	1	0	0
1	1	0	1	1
1	1	1	0	1

The table shows that if under a certain truth assignment of the propositional symbols A, B, and C the formula $((A \wedge \neg B) \to C) \wedge \neg C$ is true, then the formula $A \to B$ is also true. Therefore, the logical consequence holds, and the proof pattern is sound.