CS 103X: Discrete Structures
Homework Assignment 5 — Solutions

Exercise 1 (25 points)**.** Formulate each of the below as a *single* statement (proposition or predicate), using only mathematical and logical notation that has been defined in class. For example, the use of logical quantifiers and connectives, and arithmetic, number-theoretic, and set-theoretic operations is allowed, as is the use of operators like gcd or sets like $\mathbb{Q}$, $\mathbb{R}$, etc., but *not* the use of English-language words or informal shorthand like $\{1, 2, \ldots, n\}$.

(a) Every integer multiple of 4 can be expressed as the difference of two perfect squares.

(b) Bernoulli's inequality (see Homework 2) holds.

(c) Two integers are coprime if and only if every integer can be expressed as their linear combination.

(d) The principle of induction.

(e) Goldbach's conjecture. ("Every even integer greater than 2 can be written as the sum of two primes." You should *not* rely on an externally defined set $\mathbb{P}$ of primes.)

Solution

(a) $\forall x \in \mathbb{Z} : \big((4 \mid x) \to \exists y, z \in \mathbb{Z} : (x = y^2 - z^2)\big)$

(b) $\forall x \in \mathbb{R}\ \forall n \in \mathbb{N} : \big((x > -1) \to ((1+x)^n \geq 1 + nx)\big)$

(c) $\forall a, b \in \mathbb{Z} : \big(\gcd(a, b) = 1 \leftrightarrow \forall c \in \mathbb{Z}\ \exists u, v \in \mathbb{Z} : c = au + bv\big)$

(d) $\forall A \subseteq \mathbb{N}^+ : \big((1 \in A) \wedge (\forall k \in A : (k \in A) \to (k+1 \in A))\big) \to (A = \mathbb{N}^+)$

(e) $\forall n \in \mathbb{N} : \Big((n > 2) \wedge (2 \mid n)\Big) \to \Big(\exists p, q \in \mathbb{N}^+ \backslash \{1\} : \big(n = p + q\big) \wedge \big(\forall a \in \mathbb{N}^+ \backslash \{1\} : (a = p \vee a \nmid p) \wedge (a = q \vee a \nmid q)\big)\Big)$

Exercise 2 (25 points)**.** After completing the previous exercise, write the negation of each of your logical statements, such that the symbol $\neg$ does not appear in your statements. (That is, eliminate negated quantifiers and negated compounds as you have learned in class, and then replace statements such as $\neg(a \mid b)$ by statements like $a \nmid b$.) Read the negations out in natural language and check for yourself that you understand why these are the right negations for the statements in the previous exercise.

Solution

(a) We'll work this one out from scratch. Notice how we move the negation symbol progressively further into the expression, changing quantifiers as we go:

$$\begin{aligned}
&\neg(\forall x \in \mathbb{Z} : (4 \mid x \to \exists y, z \in \mathbb{Z} : (x = y^2 - z^2))) && \Leftrightarrow \\
&\exists x \in \mathbb{Z} : \neg(4 \mid x \to \exists y, z \in \mathbb{Z} : (x = y^2 - z^2)) && \Leftrightarrow \\
&\exists x \in \mathbb{Z} : (4 \mid x \wedge \neg(\exists y, z \in \mathbb{Z} : (x = y^2 - z^2))) && \Leftrightarrow \\
&\exists x \in \mathbb{Z} : (4 \mid x \wedge (\forall y, z \in \mathbb{Z} : \neg(x = y^2 - z^2))) && \Leftrightarrow \\
&\exists x \in \mathbb{Z} : (4 \mid x \wedge (\forall y, z \in \mathbb{Z} : x \neq y^2 - z^2))
\end{aligned}$$

This of course says that there is some integer x which is a multiple of 4 yet is not the difference of any two perfect squares, which is precisely what we want.

(b) $\exists x \in \mathbb{R} \exists n \in \mathbb{N} : ((x > -1) \wedge ((1+x)^n < 1 + nx))$

(c) $\exists a, b \in \mathbb{Z} : (\gcd(a, b) \neq 1 \leftrightarrow \forall c \in \mathbb{Z}, \exists u, v \in \mathbb{Z} : c = au + bv)$ (The negation of $a \leftrightarrow b$ can be either of the equivalent statements $\neg a \leftrightarrow b$ and $a \leftrightarrow \neg b$. We avoid a lot of manipulations by using the first statement.)

(d) $\exists A \subseteq \mathbb{N}^+ : \big(1 \in A\big) \wedge \big(\forall k \in A : (k \in A) \rightarrow (k+1 \in A)\big) \wedge \big(A \neq \mathbb{N}^+\big)$

(e) $\exists n \in \mathbb{N} : \Big((n > 2) \wedge (2 \mid n)\Big) \wedge \Big(\forall p, q \in \mathbb{N}^+ \setminus \{1\} : \big(n \neq p+q\big) \vee \big(\exists a \in \mathbb{N}^+ \setminus \{1\} : (a \neq p \wedge a \mid p) \vee (a \neq q \wedge a \mid q)\big)\Big)$

Exercise 3 (10 points)**.** Let's formulate the famous "Barber of Seville" paradox in the notation of first-order logic (i.e. the sort of logic described in the lecture notes). In English, the paradox may be stated as:

> "The barber of Seville shaves precisely those residents of Seville who do not shave themselves."

(Convince yourself that this is indeed a paradox.) Assume S is the set of all residents of Seville, which includes the barber. We have the following predicates over elements of the set S:

- $\mathit{Shaves}(x, y)$: true if x shaves y, false otherwise.
- $\mathit{Barber}(x)$: true if x is the barber of Seville (you may assume that Seville has just one barber), false otherwise.

Rewrite the statement of the paradox using only these predicates, along with the notation of mathematical logic.

Solution The given statement doesn't look very easy to translate directly into logical formalism, so let's rephrase it in a more logic-friendly form:

> "The Barber of Seville shaves every resident of Seville if and only if the latter does not shave himself."

(We will prudently assume that Seville has only male residents.) This seems easier to translate. Here's a first attempt:

$$\forall x \in S : \big(\mathit{Shaves}(\text{Barber-of-Seville}, x) \leftrightarrow \neg \mathit{Shaves}(x, x)\big)$$

But what is this mysterious "Barber-of-Seville" object? We have no constants like this given to us, so we must think of a clever way to introduce the barber. We rephrase the statement again:

> "There is a barber of Seville, and he shaves every resident of Seville if and only if the latter does not shave himself."

This can be translated as:

$$\exists y \in S : \mathit{Barber}(y) \wedge \Big(\forall x \in S : \big(\mathit{Shaves}(y, x) \leftrightarrow \neg \mathit{Shaves}(x, x)\big)\Big)$$

Notice how the existential quantifier and the *Barber* predicate are used to identify the barber (the universal quantifier and an $\rightarrow$ instead of the $\wedge$ are not appropriate here — why?). The paradox occurs, of course, because we allow $x = y$, in which case we have $\mathit{Shaves}(y, y) \leftrightarrow \neg \mathit{Shaves}(y, y)$, which is patently false, so the condition on y can never be satisfied and this contradicts the existence of such a y. Note that the $\mathit{Barber}(y)$ term is actually completely unnecessary for the paradox itself.

Exercise 4 (20 points)**.** Assuming P, Q and R are logical propositions, which of the following statements are tautologies, which are contradictions, and which are neither? No proof is necessary, but for every statement that you think is neither a tautology nor a contradiction you should provide one set of truth assignments to its variables that makes it true, and another set that makes it false.

(a) $(P \vee Q) \rightarrow (P \wedge Q)$

(b) $(P \vee \neg Q) \wedge (\neg P \wedge Q)$

(c) $((P \vee Q) \wedge R) \leftrightarrow ((P \wedge R) \vee (Q \wedge R))$

(d) $(P \leftrightarrow Q) \wedge (Q \leftrightarrow R) \wedge \neg(P \leftrightarrow R)$

Solution

(a) Neither. If P and Q are both true, both sides are true and the implication holds. If P is true and Q false, the left side is true and the right side false, then the implication fails.

(b) Contradiction. $(\neg P \wedge Q)$ holds only when P is false and Q true. With these values, $(P \vee \neg Q)$ is false, so there are no values of P and Q that satisfy the whole statement.

(c) Tautology. For the left side to hold, at least one of P or Q is true and R must be true. For the right side, either $(P \wedge R)$ or $(Q \wedge R)$ must hold; in either case R must be true and then at least one of P or Q must be true. Thus both sides will always have the same truth value and the bidirectional implication holds.

(d) Contradiction. For $(P \leftrightarrow Q)$ to hold P and Q must have the same truth values. Thus the statement implies that P and Q have the same value, and Q and R have the same value (together these mean P and R have the same truth value), while the last part of the conjunction means that P and R have different truth values. Thus no values of P, Q, R will satisfy the statement.

Exercise 5 (20 points)**.** You are given the following (all letters are logical propositions):

$$(t \rightarrow (r \vee p)) \rightarrow ((\neg r \vee k) \wedge \neg k).$$

Prove that this implies $\neg r$. Write down a proof using inference rules like we did in class. Manufacture inference rules from tautologies as needed.

Solution We proceed as follows:

$$\begin{aligned}
(t \rightarrow (r \vee p)) \rightarrow ((\neg r \vee k) \wedge \neg k) &\Leftrightarrow \\
\neg(t \rightarrow (r \vee p)) \vee ((\neg r \vee k) \wedge \neg k) &\Leftrightarrow \\
\neg(t \rightarrow (r \vee p)) \vee ((\neg r \wedge \neg k) \vee (k \wedge \neg k)) &\Leftrightarrow \\
\neg(t \rightarrow (r \vee p)) \vee ((\neg r \wedge \neg k) \vee \mathcal{F}) &\Leftrightarrow \\
\neg(t \rightarrow (r \vee p)) \vee (\neg r \wedge \neg k) &\Leftrightarrow \\
(t \wedge \neg(r \vee p)) \vee (\neg r \wedge \neg k) &\Leftrightarrow \\
(t \wedge (\neg r \wedge \neg p)) \vee (\neg r \wedge \neg k) &\Leftrightarrow \\
(t \wedge (\neg p \wedge \neg r)) \vee (\neg r \wedge \neg k) &\Leftrightarrow \\
((t \wedge \neg p) \wedge \neg r) \vee (\neg r \wedge \neg k) &\Leftrightarrow \\
((t \wedge \neg p) \wedge \neg r) \vee (\neg k \wedge \neg r) &\Leftrightarrow \\
((t \wedge \neg p) \vee \neg k) \wedge \neg r &\Rightarrow \\
\neg r &
\end{aligned}$$

The inference rules we use are, in order:

$$\begin{aligned}
a \rightarrow b &\Leftrightarrow \neg a \vee b \\
(a \vee b) \wedge c &\Leftrightarrow (a \wedge c) \vee (b \wedge c) \\
a \wedge \neg a &\Leftrightarrow \mathcal{F} \\
a \vee \mathcal{F} &\Leftrightarrow a \\
\neg(a \rightarrow b) &\Leftrightarrow a \wedge \neg b \\
\neg(a \vee b) &\Leftrightarrow \neg a \wedge \neg b \\
a \wedge b &\Leftrightarrow b \wedge a \\
a \wedge (b \wedge c) &\Leftrightarrow (a \wedge b) \wedge c \\
a \wedge b &\Leftrightarrow b \wedge a \\
(a \vee b) \wedge c &\Leftrightarrow (a \wedge c) \vee (b \wedge c) \\
a \wedge b &\Rightarrow b
\end{aligned}$$

These should all be familiar to you.