Problem Set 2

Due: March 3

Reading:

- Chapter **??**. *Predicate Formulas*,
- Chapter **??**. *Mathematical Data Types* through **??**. *Binary Relations*,
- Chapter **??**. *Induction*.

These assigned readings do **not** include the Problem sections. (Many of the problems in the text will appear as class or homework problems.)

Reminder:

- Instructions for PSet submission are on the class Stellar page. Remember that each problem should prefaced with a *collaboration statement*.

Problem 1.
Express each of the following predicates and propositions in formal logic notation. The domain of discourse is the nonnegative integers $\mathbb{N}$. Moreover, in addition to the propositional operators, variables and quantifiers, you may define predicates using addition, multiplication, and equality symbols, but no *exponentiation* (like x^y) and no use of integer *constants* like $\texttt{0}$ or $\texttt{1}$ (until you justify using them in part (a)).

For example, the predicate "$x \geq y$" could be expressed by the following logical formula.

$$\exists w. (y + w = x).$$

Now that we can express $\geq$, it's OK to use it to express other predicates. For example, the predicate $x < y$ can now be expressed as

$$y \geq x \text{ AND NOT}(x = y).$$

For each of the predicates below, describe a logical formula to express it. It is OK to use in the logical formula any of the predicates previously expressed.

(a) $x = \texttt{1}$.

Solution. We could say there is only one number less than x:

$$\exists z. z < x \text{ AND } \forall y. y < x \text{ IMPLIES } y = z.$$

Alternatively, both

$$\forall y. x \cdot y = y,$$

and

$$x \cdot x = x \text{ AND } x + x \neq x$$

work nicely. ■

(b) m is a divisor of n (notation: $m \mid n$)

Solution.

$$m \mid n ::= \quad \exists k.\ k \cdot m = n$$

$\blacksquare$

(c) n is a prime number.

Solution.

$$\textsc{Prime}(n) ::= \quad (n \neq 1) \ \text{ AND } \ \forall m.\ (m \mid n) \text{ IMPLIES } (m = 1 \text{ OR } m = n).$$

Note that $n \neq 1$ is an abbreviation of the formula $\text{NOT}(n = 1)$. $\blacksquare$

(d) n is a power of a prime.

Solution. A number n is a power of a prime p iff its only prime factor is p. So,

$$\textsc{Prime-power}(n) ::= \quad \exists p.\ [\textsc{Prime}(p) \text{ AND } (\forall m.\ (m \mid n \text{ AND } \textsc{Prime}(m)) \text{ IMPLIES } m = p].$$

Notice that this correctly handles the fact that 1 is a zero power of a prime, because if $n = 1$, then no prime m divides n. $\blacksquare$

Problem 2.
Let A, B and C be sets. Prove that:

$$A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C). \tag{1}$$

Hint: P OR Q OR R is equivalent to

$$(P \text{ AND } \overline{Q}) \text{ OR } (Q \text{ AND } \overline{R}) \text{ OR } (R \text{ AND } \overline{P}) \text{ OR } (P \text{ AND } Q \text{ AND } R).$$

Solution. *Proof.* We prove that an element x is a member of the left-hand side of (1) iff it is a member of the right-hand side.

$$\begin{aligned}
& x \in A \cup B \cup C \\
& \quad \text{iff} \quad (x \in A) \text{ OR } (x \in B) \text{ OR } (x \in C) && \text{(by def of } \cup) \\
& \quad \text{iff} \quad ((x \in A) \text{ AND } \overline{(x \in B)}) \text{ OR } \\
& \qquad ((x \in B) \text{ AND } \overline{(x \in C)}) \text{ OR } \\
& \qquad ((x \in C) \text{ AND } \overline{(x \in A)}) \text{ OR } \\
& \qquad ((x \in A) \text{ AND } (x \in B) \text{ AND } (x \in C)) && \text{(by the equivalence in the Hint)} \\
& \quad \text{iff} \quad (x \in A - B) \text{ OR } (x \in B - C) \text{OR } \\
& \qquad\quad (x \in C - A) \text{ OR } (x \in A \cap B \cap C) && \text{(by def of } -, \cap) \\
& \quad \text{iff} \quad x \in (A - B) \cup (B - C) \cup (C - A) \cup \\
& \qquad\quad (A \cap B \cap C) && \text{(by def of } \cup)
\end{aligned}$$

$\blacksquare$

Alternative solution by cases:

We prove that the left-hand side is contained in the right-hand side, and that the right-hand side is contained in the left-hand side.

First, we show that the left-hand side is contained in the right-hand on the right.

Next, we show that the right-hand side is contained in the left-hand. This is easier. Let x belong to the right side. Then it belongs to one of $A - B$, $B - C$, $C - A$ or $A \cap B \cap C$. In the first case, we clearly know $x \in A$. In the second case, $x \in B$. In the third case, $x \in C$. In the last case, $x \in A$ again. So, in all cases, x belongs to one of A, B or C. So x belongs to the left-hand side. Therefore, the set on the right is contained in the set on the left.

Since each set is contained in the other, they are equal.

■

Problem 3. (a) Write predicates that express the following assertions.

- R is a surjection [>= 1 in].

  Solution. $\forall b.\, \exists a.\, a \; R \; b.$ ■

- R is a function [<= 1 out].

  Solution. $\forall b_1, b_2, a.\, (a \; R \; b_1 \text{ AND } a \; R \; b_2) \text{ IMPLIES } b_1 = b_2.$
  $\forall a_1, a_2, b_1, b_2.\, (a_1 \; R \; b_1 \text{ AND } a_2 \; R \; b_2 \text{ AND } b_1 \neq b_2) \text{ IMPLIES } a_1 \neq a_2.$ ■

- $x = y - z$.

  Solution. $\forall w.\, w \in x \text{ IFF } (w \in y \text{ AND } \text{NOT}(w \in z)).$ ■

- $x = \{\}$.

  Solution. $\forall z.\, \text{NOT}(z \in x)$ ■

Problem 4.

The Fibonacci numbers $F(0), F(1), F(2), \ldots$ are defined as follows:

$$
\begin{aligned}
F(0) &::= 0, \\
F(1) &::= 1, \\
F(n) &::= F(n-1) + F(n-2) && \text{for } n \geq 2.
\end{aligned}
$$

Thus, the first few Fibonacci numbers are 0, 1, 1, 2, 3, 5, 8, 13, and 21. Prove by induction that for all $n \geq 1$,

$$F(n-1) \cdot F(n+1) - F(n)^2 = (-1)^n. \tag{2}$$

Solution. *Proof.* The proof is by induction on n with equation (2) as induction hypothesis $P(n)$.

base case: $n = 1$. $P(1)$ holds because

$$F(1-1) \cdot F(1+1) - F(1)^2 = 0 \cdot 1 - 1^2 = -1^1.$$

inductive step: We show that $P(n+1)$ is true, assuming that $n \geq 1$ and $P(n)$ is true. To do this, we consider equation (2) with n replaced by $n+1$ and then transform the left-hand side of this new equation into the right-hand side, namely, $(-1)^{n+1}$. So starting with $n+1$ for n in left side of (2), we have

$$
\begin{aligned}
&F((n+1)-1) \cdot F((n+1)+1) - F(n+1)^2 \\
&= F(n) \cdot F(n+2) - F(n+1)^2 && \text{(simplify } (n+1) \pm 1\text{)} \\
&= F(n) \cdot (F(n+1) + F(n)) \\
&\qquad - F(n+1) \cdot (F(n) + F(n-1)) && \text{(def. of } F(n+2) \text{ \& } F(n+1)\text{)} \\
&= F(n) \cdot F(n+1) + F(n) \cdot F(n) \\
&\qquad - F(n+1) \cdot F(n) - F(n+1) \cdot F(n-1) && \text{(distribute multipliers)} \\
&= F(n) \cdot F(n) - F(n+1) \cdot F(n-1) && \text{(cancel } F(n) \cdot F(n+1)\text{)} \\
&= -(-1)^n && \text{(induction hypothesis (2))} \\
&= (-1)^{n+1}.
\end{aligned}
$$

This proves $P(n+1)$, completing the inductive step.

We conclude by induction that equation (2) holds for all $n \geq 1$. ■