Problem 14

Problem 1. $\forall X \in \texttt{PNat}, \forall L1, L2 \in \texttt{NatList}, \text{diff}(L1, X \mid L2) = \text{drop}(\text{diff}(L1, L2), X)$.

Proof. By structural induction on L.

(1) Base case

What to show: $\text{diff}(nil, x \mid l2) = \text{drop}(\text{diff}(nil, l2), x)$
where $x \in \texttt{PNat}$ and $l2 \in \texttt{NatList}$. Note that $x, l2$ are fresh constants[1].

$$\begin{aligned}
\underline{\text{diff}(nil, x \mid l2)} &\longrightarrow nil && \text{(by diff1)} \\
\text{drop}(\underline{\text{diff}(nil, l2)}, x) &\longrightarrow \underline{\text{drop}(nil, x)} && \text{(by diff1)} \\
&\longrightarrow nil && \text{(by drop1)}
\end{aligned}$$

(2) Induction case

What to show: $\text{diff}(y \mid l1, x \mid l2) = \text{drop}(\text{diff}(y \mid l1, l2), x)$
Induction hypothesis: $\text{diff}(l1, x \mid l2) = \text{drop}(\text{diff}(l1, l2), x)$
where $x, y \in \texttt{PNat}$ and $l1, l2 \in \texttt{NatList}$. Note that $x, y, l1, l2$ are fresh constants.

We use case splitting for our proofs as follows:
Case 1: $\text{has}(l2, y) = true$

$$\begin{aligned}
\underline{\text{diff}(y \mid l1, x \mid l2)} &\longrightarrow \text{if } \underline{\text{has}(x \mid l2, y)} \text{ then } \text{diff}(l1, x \mid l2) \\
&\quad \text{else } (y \mid \text{diff}(l1, x \mid l2)) \text{ fi} && \text{(by diff2)} \\
&\longrightarrow \text{if } ((y = x) \mathit{ or } \underline{\text{has}(l2, y)}) \text{ then } \text{diff}(l1, x \mid l2) \\
&\quad \text{else } (y \mid \text{diff}(l1, x \mid l2)) \text{ fi} && \text{(by has2)} \\
&\longrightarrow \text{if } \underline{((y = x) \mathit{ or } true)} \text{ then } \text{diff}(l1, x \mid l2) \\
&\quad \text{else } (y \mid \text{diff}(l1, x \mid l2)) \text{ fi} \\
& && \text{(by case splitting)} \\
&\longrightarrow \underline{\text{if } true \text{ then } \text{diff}(l1, x \mid l2)} \\
&\quad \underline{\text{else } (y \mid \text{diff}(l1, x \mid l2)) \text{ fi}} && \text{(by or)}
\end{aligned}$$

[1] A fresh constant of a sort denotes an arbitrary value of the sort, and has never been used before.

$$\begin{aligned}
&\longrightarrow \underline{\text{diff}(l1, x \mid l2)} && \text{(by if1)}\\
&\longrightarrow \text{drop}(\text{diff}(l1, l2), x) && \text{(by IH)}\\
\text{drop}(\underline{\text{diff}(y \mid l1, l2)}, x) &\longrightarrow \text{drop}(\text{if } \underline{\text{has}(l2, y)} \text{ then diff}(l1, l2)\\
&\quad \text{else } (y \mid \text{diff}(l1, l2) \text{ fi}, x) && \text{(by diff2)}\\
&\longrightarrow \text{drop}(\underline{\text{if } true \text{ then diff}(l1, l2)}\\
&\quad \underline{\text{else } (y \mid \text{diff}(l1, l2) \text{ fi}}, x)\\
& && \text{(by case splitting)}\\
&\longrightarrow \text{drop}(\text{diff}(l1, l2), x) && \text{(by if1)}
\end{aligned}$$

Case 2: $\text{has}(l2, y) = false$

$$\begin{aligned}
\underline{\text{diff}(y \mid l1, x \mid l2)} &\longrightarrow \text{if } \underline{\text{has}(x \mid l2, y)} \text{ then diff}(l1, x \mid l2)\\
&\quad \text{else } (y \mid \text{diff}(l1, x \mid l2)) \text{ fi} && \text{(by diff2)}\\
&\longrightarrow \text{if } ((y = x) \textit{ or } \underline{\text{has}(l2, y)}) \text{ then diff}(l1, x \mid l2)\\
&\quad \text{else } (y \mid \text{diff}(l1, x \mid l2)) \text{ fi} && \text{(by has2)}\\
&\longrightarrow \text{if } \underline{((y = x) \textit{ or } false)} \text{ then diff}(l1, x \mid l2)\\
&\quad \text{else } (y \mid \text{diff}(l1, x \mid l2)) \text{ fi}\\
& && \text{(by case splitting)}\\
&\longrightarrow \text{if } (y = x) \text{ then } \underline{\text{diff}(l1, x \mid l2)}\\
&\quad \text{else } (y \mid \text{diff}(l1, x \mid l2)) \text{ fi} && \text{(by or)}\\
&\longrightarrow \text{if } (y = x) \text{ then drop}(\text{diff}(l1, l2), x)\\
&\quad \text{else } (y \mid \underline{\text{diff}(l1, x \mid l2)}) \text{ fi} && \text{(by IH)}\\
&\longrightarrow \text{if } (y = x) \text{ then drop}(\text{diff}(l1, l2), x)\\
&\quad \text{else } (y \mid \text{drop}(\text{diff}(l1, l2), x)) \text{ fi} && \text{(by IH)}\\
\text{drop}(\underline{\text{diff}(y \mid l1, l2)}, x) &\longrightarrow \text{drop}(\text{if } \underline{\text{has}(l2, y)} \text{ then diff}(l1, l2)\\
&\quad \text{else } (y \mid \text{diff}(l1, l2)) \text{ fi}, x) && \text{(by diff2)}\\
&\longrightarrow \text{drop}(\underline{\text{if } false \text{ then diff}(l1, l2)}\\
&\quad \underline{\text{else } (y \mid \text{diff}(l1, l2)) \text{ fi}}, x)\\
& && \text{(by case splitting)}\\
&\longrightarrow \underline{\text{drop}(y \mid \text{diff}(l1, l2), x)} && \text{(by if2)}\\
&\longrightarrow \text{if } (y = x) \text{ then drop}(\text{diff}(l1, l2), x)\\
&\quad \text{else } (y \mid \text{drop}(\text{diff}(l1, l2), x)) \text{ fi} && \text{(by drop2)}
\end{aligned}$$

□