Problem 3

Problem 1. $\forall X \in \texttt{PNat}, \mathrm{fact}(X) = \mathrm{fold}*(\mathrm{mkl2}(X))$.

Proof. By direct proof.
What to show: $\mathrm{fact}(x) = \mathrm{fold}*(\mathrm{mkl2}(x))$
where $x \in \texttt{PNat}$. Note that x is a fresh constant[1].

$$\begin{aligned} \underline{\mathrm{fact}(x)} &\longrightarrow \underline{\mathrm{fold}*(\mathrm{mkl1}(x))} && \text{(by Lemma 1)} \\ &\longrightarrow \mathrm{fold}*(\underline{\mathrm{rev}(\mathrm{mkl1}(x))}) && \text{(by Problem 1)} \\ &\longrightarrow \mathrm{fold}*(\mathrm{mkl2}(x)) && \text{(by Problem 2)} \end{aligned}$$

□

Lemma 1. $\forall X \in \texttt{PNat}, \mathrm{fact}(X) = \mathrm{fold}*(\mathrm{mkl1}(X))$.

Proof. By structural induction on X.

(1) Base case
What to show: $\mathrm{fact}(0) = \mathrm{fold}*(\mathrm{mkl1}(0))$.

$$\begin{aligned} \underline{\mathrm{fact}(0)} &\longrightarrow \mathrm{s}(0) && \text{(by fact1)} \\ \mathrm{fold}*(\underline{\mathrm{mkl1}(0)}) &\longrightarrow \underline{\mathrm{fold}*(\mathit{nil})} && \text{(by mkl1-1)} \\ &\longrightarrow \mathrm{s}(0) && \text{(by fold*-1)} \end{aligned}$$

(2) Induction case
What to show: $\mathrm{fact}(\mathrm{s}(x)) = \mathrm{fold}*(\mathrm{mkl1}(\mathrm{s}(x)))$
Induction hypothesis: $\mathrm{fact}(x) = \mathrm{fold}*(\mathrm{mkl1}(x))$
where $x \in \texttt{PNat}$. Note that x is a fresh constant.

$$\begin{aligned} \underline{\mathrm{fact}(\mathrm{s}(x))} &\longrightarrow \underline{\mathrm{s}(x) * \mathrm{fact}(x)} && \text{(by fact2)} \\ &\longrightarrow (x * \underline{\mathrm{fact}(x)}) + \mathrm{fact}(x) && \text{(by *2)} \\ &\longrightarrow (x * \mathrm{fold}*(\mathrm{mkl1}(x))) + \underline{\mathrm{fact}(x)}) && \text{(by IH)} \end{aligned}$$

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

$$
\begin{aligned}
&\longrightarrow (x * \mathrm{fold}*(\mathrm{mkl1}(x))) + \mathrm{fold}*(\mathrm{mkl1}(x)) && \text{(by IH)}\\
\mathrm{fold}*(\underline{\mathrm{mkl1}(\mathrm{s}(x))}) &\longrightarrow \underline{\mathrm{fold}*(\mathrm{s}(x) \mid \mathrm{mkl1}(x))} && \text{(by mkl1-2)}\\
&\longrightarrow \underline{\mathrm{s}(x) * \mathrm{fold}*(\mathrm{mkl1}(x))} && \text{(by fold*-2)}\\
&\longrightarrow (x * \mathrm{fold}*(\mathrm{mkl1}(x))) + \mathrm{fold}*(\mathrm{mkl1}(x)) && \text{(by *2)}
\end{aligned}
$$

□