Interactive Formal Verification (L21)

1 Power, Sum

Power

▷ Define a (primitive recursive) function \(\text{pow} \ x \ n\) that computes \(x^n\) on natural numbers.

\[
\text{pow} :: \text{nat} \Rightarrow \text{nat} \Rightarrow \text{nat}
\]

▷ Prove the well known equation \(x^m \cdot n = (x^m)^n\):

\[
\text{theorem pow_mult: "pow} x (m \ast n) = \text{pow} (\text{pow} x m) n"
\]

Hint: prove a suitable lemma first. If you need to appeal to associativity and commutativity of multiplication: the corresponding simplification rules are named \textit{mult_ac}.

Summation

▷ Define a (primitive recursive) function \(\text{sum} \ ns\) that sums a list of natural numbers:

\[
\text{sum} [n_1, \ldots, n_k] = n_1 + \cdots + n_k.
\]

\[
\text{sum} :: \text{nat list} \Rightarrow \text{nat}
\]

▷ Show that \(\text{sum}\) is compatible with \textit{rev}. You may need a lemma.

\[
\text{theorem sum_rev: "sum} (\text{rev} \ ns) = \text{sum} \ ns"
\]

▷ Define a function \(\text{Sum} \ f \ k\) that sums \(f\) from 0 up to \(k-1\): \(\text{Sum} \ f \ k = f \ 0 + \cdots + f(k-1)\).

\[
\text{Sum} :: (\text{nat} \Rightarrow \text{nat}) \Rightarrow \text{nat} \Rightarrow \text{nat}
\]

▷ Show the following equations for the pointwise summation of functions. Determine first what the expression \textit{whatever} should be.

\[
\text{theorem "Sum} (\lambda i. f \ i + g \ i) \ k = \text{Sum} \ f \ k + \text{Sum} \ g \ k"
\]

\[
\text{theorem "Sum} f (k + 1) = \text{Sum} f \ k + \text{Sum} \textit{whatever} \ 1"
\]
What is the relationship between \texttt{sum} and \texttt{Sum}? Prove the following equation, suitably instantiated.

\textbf{theorem} \ "\texttt{Sum f k = sum whatever}"

Hint: familiarize yourself with the predefined functions \texttt{map} and \texttt{[i..<j]} on lists in theory \texttt{List}.