Formal Methods and Functional Programming

Solutions of Exercise Sheet 9: Induction

Assignment 1

Task 1.1: We define $P(n) \equiv U_n = 3^n - 2^{n+1}$, we prove $\forall n \geq 0.\, P(n)$ by strong induction.

Let $n \geq 0$ be arbitrary, and let us assume $P(j)$ for all j such that $0 \leq j < n$. Our goal is to prove $P(n)$. We distinguish three cases:

Case 1: $n = 0$. In this case, $U_0 = -1 = 1-2 = 3^0 - 2^{0+1}$, which concludes the case.

Case 2: $n = 1$. In this case, $U_1 = -1 = 3-4 = 3^1 - 2^{1+1}$, which concludes the case.

Case 3: $n \geq 2$. In this case, $U_n = 5U_{n-1} - 6U_{n-2}$. Since $n-1 < n$ and $n-2 < n$, we know that $P(n-1)$ and $P(n-2)$ hold. Thus,

$$\begin{aligned} U_n &= 5U_{n-1} - 6U_{n-2} \\ &= 5(3^{n-1} - 2^n) - 6(3^{n-2} - 2^{n-1}) \\ &= (15-6) \times 3^{n-2} - (10-6) \times 2^{n-1} \\ &= 3^n - 2^{n+1} \end{aligned}$$

which concludes the proof.

Task 1.2: We define $Q(n) \equiv \forall k.\, 0 \leq k \leq n \Rightarrow P(k)$, and we prove $Q(n)$ for all $n \geq 1$ by *weak induction*.

Base case: To prove $Q(1)$, we take k arbitrary, and we assume $0 \leq k \leq 1$. We thus have two cases:

Case 1: $k = 0$. We need to prove $P(0)$, which holds by definition: $U_0 = -1 = 3^0 - 2^1$.

Case 2: $k = 1$. $P(1)$ holds by definition: $U_1 = -1 = 3^1 - 2^2$.

Induction step: Let $n \geq 1$ be arbitrary. We assume $Q(n)$, and prove $Q(n+1)$. To prove $Q(n{+}1)$, we need to prove $P(k)$ for all k such that $0 \leq k \leq n{+}1$. If $0 \leq k \leq n$, we get $P(k)$ from $Q(n)$. Thus, to prove $Q(n{+}1)$, we simply need to prove $P(n{+}1)$.

We do the same proof as in the induction step in the proof by strong induction (with n shifted by 1). In this case, $U_{n+1} = 5U_n - 6U_{n-1}$. Since $n \leq n$ and $n-1 \leq n$, we know that $P(n)$ and $P(n-1)$ hold, from $Q(n)$. Thus,

$$\begin{aligned} U_{n+1} &= 5U_n - 6U_{n-1} \\ &= 5(3^n - 2^{n+1}) - 6(3^{n-1} - 2^n) \\ &= (15-6) \times 3^{n-1} - (10-6) \times 2^n \\ &= 3^{n+1} - 2^{n+2} \end{aligned}$$

which concludes the proof.

Assignment 2 (Run-Length Encoding)

Task 2.1: We define

$$\begin{aligned} P(xs) \equiv \forall n, v :: \texttt{Nat} \cdot \forall ys :: \texttt{[Nat]} \cdot \texttt{length}\ ys\ \texttt{\% 2 = 0} \implies \\ \texttt{srclen (aux (dec}\ xs\texttt{)}\ n\ v\ ys\texttt{) = srclen}\ xs\ \texttt{+}\ n\ \texttt{+ srclen}\ ys \end{aligned}$$

and prove $\forall xs :: \texttt{[Nat]} \cdot P(xs)$ by strong structural induction on xs: We have to show $P(xs)$ for some arbitrary $xs :: \texttt{[Nat]}$ and may assume that the proposition holds for all proper subterms of xs, i.e., our induction hypothesis (IH) is $\forall ys \sqsubset xs \cdot P(ys)$.

Let $n, v :: \texttt{Nat}$ and $ys :: \texttt{[Nat]}$ be arbitrary. We prove that the implication holds by assuming its left-hand side and then showing that its right-hand side holds. That is, we assume `length` ys `% 2 = 0` (in the elaborations below, we will refer to this assumption as (A)) and have to show `srclen (aux (dec` xs`)` n v ys`) = srclen` xs `+ n + srclen` ys. We proceed by a case analysis on xs.

- **Case** $xs \equiv$ `[]`:

$$\begin{aligned} & \texttt{srclen (aux (dec [])}\ n\ v\ ys\texttt{)} & \\ = {} & \texttt{srclen (aux []}\ n\ v\ ys\texttt{)} & \text{(D1)} \\ = {} & \texttt{srclen (}ys\ \texttt{++ [}n\texttt{,}v\texttt{])} & \text{(A1)} \\ = {} & \texttt{srclen}\ ys\ \texttt{+}\ n & \text{(L3)} \\ = {} & \texttt{0 +}\ n\ \texttt{+ srclen}\ ys & \text{(arith)} \\ = {} & \texttt{srclen [] +}\ n\ \texttt{+ srclen}\ ys & \text{(S1)} \end{aligned}$$

- **Case** $xs \equiv [m]$, for some $m :: \texttt{Nat}$: Analogous to the previous case.
- **Case** $xs \equiv (m{:}u{:}zs)$, for some $m, u :: \texttt{Nat}$ and $zs :: \texttt{[Nat]}$: We perform a further case distinction on the values of m and u:

– **Subcase** $u = v$:

$$\begin{aligned}
&\texttt{srclen (aux (dec (}m\texttt{:}v\texttt{:}zs\texttt{)) }n\ v\ ys\texttt{)} \\
&= \texttt{srclen (aux (rep }m\ v\texttt{ ++ dec }zs\texttt{) }n\ v\ ys\texttt{)} && \text{(D3)} \\
&= \texttt{srclen (aux (dec }zs\texttt{) (}n\texttt{+}m\texttt{) }v\ ys\texttt{)} && \text{(L2)} \\
&= \texttt{srclen }zs\texttt{ + (}n\texttt{+}m\texttt{) + srclen }ys && \text{(IH,A)} \\
&= m\texttt{ + srclen }zs\texttt{ + }n\texttt{ + srclen }ys && \text{(arith)} \\
&= \texttt{srclen (}m\texttt{:}u\texttt{:}zs\texttt{) + }n\texttt{ + srclen }ys && \text{(S3)}
\end{aligned}$$

– **Subcase** $u \neq v$ and $m = 0$:

$$\begin{aligned}
&\texttt{srclen (aux (dec (0:}u\texttt{:}zs\texttt{)) }n\ v\ ys\texttt{)} \\
&= \texttt{srclen (aux (rep 0 }u\texttt{ ++ dec }zs\texttt{) }n\ v\ ys\texttt{)} && \text{(D3)} \\
&= \texttt{srclen (aux ([] ++ dec }zs\texttt{) }n\ v\ ys\texttt{)} && \text{(R1)} \\
&= \texttt{srclen (aux (dec }zs\texttt{) }n\ v\ ys\texttt{)} && \text{(++)} \\
&= \texttt{srclen }zs\texttt{ + }n\texttt{ + srclen }ys && \text{(IH,A)} \\
&= \texttt{0 + srclen }zs\texttt{ + }n\texttt{ + srclen }ys && \text{(arith)} \\
&= \texttt{srclen (}0\texttt{:}u\texttt{:}zs\texttt{) + }n\texttt{ + srclen }ys && \text{(S3)}
\end{aligned}$$

– **Subcase** $u \neq v$ and $m > 0$:

$$\begin{aligned}
&\texttt{srclen (aux (dec (}m\texttt{:}u\texttt{:}zs\texttt{)) }n\ v\ ys\texttt{)} \\
&= \texttt{srclen (aux (rep }m\ u\texttt{ ++ dec }zs\texttt{) }n\ v\ ys\texttt{)} && \text{(D3)} \\
&= \texttt{srclen (aux ((}u\texttt{:(rep (}m\texttt{-1) }u\texttt{)) ++ dec }zs\texttt{) }n\ v\ ys\texttt{)} && \text{(R2)} \\
&= \texttt{srclen (aux (}u\texttt{:(rep (}m\texttt{-1) }u\texttt{ ++ dec }zs\texttt{)) }n\ v\ ys\texttt{)} && \text{(L1)} \\
&= \texttt{srclen (aux (rep (}m\texttt{-1) }u\texttt{ ++ dec }zs\texttt{) 1 }u\texttt{ (}ys\texttt{ ++ [}n\texttt{,}v\texttt{])} && \text{(A3)} \\
&= \texttt{srclen (aux (dec }zs\texttt{) ((}m\texttt{-1)+1) }u\texttt{ (}ys\texttt{ ++ [}n\texttt{,}v\texttt{]))} && \text{(L2)} \\
&= \texttt{srclen (aux (dec }zs\texttt{) }m\ u\texttt{ (}ys\texttt{ ++ [}n\texttt{,}v\texttt{]))} && \text{(arith)} \\
&= \texttt{srclen }zs\texttt{ + }m\texttt{ + srclen (}ys\texttt{ ++ [}n\texttt{,}v\texttt{])} && \text{(*)} \\
&= \texttt{srclen }zs\texttt{ + }m\texttt{ + srclen }ys\texttt{ + }n && \text{(A,L3)} \\
&= m\texttt{ + srclen }zs\texttt{ + }n\texttt{ + srclen }ys && \text{(arith)} \\
&= \texttt{srclen (}m\texttt{:}u\texttt{:}zs\texttt{) + }n\texttt{ + srclen }ys && \text{(S3)}
\end{aligned}$$

Note that in the step marked with a (*), we combined (L4) and (A) to derive the fact `length (ys ++ [n,v]) % 2 = 0` so that we could then use the induction hypothesis to get the desired equality.

Task 2.2: We define

$$P(xs) \equiv \texttt{srclen (enc (dec }xs\texttt{)) = srclen }xs$$

and prove $\forall xs :: \texttt{[Nat]} \cdot P(xs)$ by strong structural induction on xs. Again, we have to show $P(xs)$ for some arbitrary $x :: \texttt{[Nat]}$ and may assume $\forall ys \sqsubset xs \cdot P(ys)$. We proceed by a case analysis on xs:

- **Case** $xs \equiv$ `[]`:

$$
\begin{aligned}
& \texttt{srclen (enc (dec []))} & \\
&= \texttt{srclen (enc [])} & \text{(D1)} \\
&= \texttt{srclen []} & \text{(E1)}
\end{aligned}
$$

- **Case** $xs \equiv$ `[`n`]`, for some n :: `Nat`:

$$
\begin{aligned}
& \texttt{srclen (enc (dec [}n\texttt{]))} & \\
&= \texttt{srclen (enc [])} & \text{(D2)} \\
&= \texttt{srclen []} & \text{(E1)} \\
&= \texttt{0} & \text{(S1)} \\
&= \texttt{srclen [}n\texttt{]} & \text{(S2)}
\end{aligned}
$$

- **Case**: $xs \equiv$ `(`n`:`v`:`ys`)`, for some n, v :: `Nat` and ys :: `[Nat]`: We perform a further case distinction on the value of n:

  - **Subcase** $n = 0$:

$$
\begin{aligned}
& \texttt{srclen (enc (0:}v\texttt{:}ys\texttt{))} & \\
&= \texttt{srclen (enc (rep 0 } v \texttt{ ++ dec } ys\texttt{))} & \text{(D3)} \\
&= \texttt{srclen (enc ([] ++ dec } ys\texttt{))} & \text{(R1)} \\
&= \texttt{srclen (enc (dec } ys\texttt{))} & \text{(++)} \\
&= \texttt{srclen } ys & \text{(IH)} \\
&= \texttt{0 + srclen } ys & \text{(arith)} \\
&= \texttt{srclen (0:}v\texttt{:}ys\texttt{)} & \text{(S3)}
\end{aligned}
$$

  - **Subcase** $n > 0$:

$$
\begin{aligned}
& \texttt{srclen (enc (dec (}n\texttt{:}v\texttt{:}ys\texttt{)))} & \\
&= \texttt{srclen (enc (rep } n\ v \texttt{ ++ dec } ys\texttt{))} & \text{(D3)} \\
&= \texttt{srclen (enc ((v:(rep (}n\texttt{-1) } v\texttt{)) ++ dec } ys\texttt{))} & \text{(R2)} \\
&= \texttt{srclen (enc (v:(rep (}n\texttt{-1) } v \texttt{ ++ dec } ys\texttt{)))} & \text{(L1)} \\
&= \texttt{srclen (aux (rep (}n\texttt{-1) } v \texttt{ ++ dec } ys\texttt{) 1 } v \texttt{ [])} & \text{(E2)} \\
&= \texttt{srclen (aux (dec } ys\texttt{) (1+(}n\texttt{-1)) } v \texttt{ [])} & \text{(L2)} \\
&= \texttt{srclen (aux (dec } ys\texttt{) } n\ v \texttt{ [])} & \text{(arith)} \\
&= \texttt{srclen } ys \texttt{ + } n \texttt{ + srclen []} & \text{(Task 2.1)} \\
&= \texttt{srclen } ys \texttt{ + } n \texttt{ + 0} & \text{(S1)} \\
&= n \texttt{ + srclen } ys & \text{(arith)} \\
&= \texttt{srclen (}n\texttt{:}v\texttt{:}ys\texttt{)} & \text{(S3)}
\end{aligned}
$$

  Note that we can apply the result of Task 2.1 because `length [] % 2 = 0`.