Software Architecture

ADT solution: BANK_ACCOUNT

Stephan van Staden
1. Balance non-negative

We prove this by induction over the structure of correct bank accounts:

**Base case:** The bank account is of the form \( \text{new\_account}(o) \), and we know \( \text{balance}(\text{new\_account}(o)) = 0 \) and that \( 0 \geq 0 \).

**Step case:** The bank account can have one of two forms, where \( a \) is a correct bank account with balance(\( a \)) \( \geq 0 \):

- Form \( \text{deposit}(a,i) \) where \( i \geq 0 \). By axiom A3, we know that \( \text{balance}(\text{deposit}(a,i)) = \text{balance}(a) + i \) which is non-negative because of the induction hypothesis and \( i \geq 0 \).
- Form \( \text{withdraw}(a,i) \) where \( \text{balance}(a) \geq i \geq 0 \). From axiom A4 it follows that \( \text{balance}(\text{withdraw}(a,i)) \geq 0 \).
2. Sufficient completeness (1)

The ADT is not sufficiently complete, since we cannot determine the owner of an account if a deposit or withdrawal was made.

To make it sufficiently complete, we have to add the axioms:

\[
\begin{align*}
A5: \text{owner}(\text{deposit}(a,v)) &= \text{owner}(a) \\
A6: \text{owner}(\text{withdraw}(a,v)) &= \text{owner}(a)
\end{align*}
\]
Let $P(n)$ be the property “for all terms $a$ of type \texttt{BANK\_ACCOUNT} with at most $n$ applications of deposit and withdraw, it can be proven 1) whether $a$ is correct or not and 2) whether $\text{balance}(a)$ and $\text{owner}(a)$ are correct or not and if correct, whether they can be reduced to terms not involving \texttt{new\_account}, \texttt{owner}, \texttt{balance}, \texttt{deposit} and \texttt{withdraw}”

\textbf{Base case $n=0$:} $a$ is \texttt{new\_account}(o), which is correct, and $\text{balance}(a) = 0$ and $\text{owner}(a) = o$. Thus $P(0)$ holds.
2. Sufficient completeness (3)

**Step case:** We assume the induction hypothesis (IH) $P(n-1)$ and have to prove $P(n)$.

**First case:** $a$ is deposit($b,i$) and the IH applies to terms $b$ and $i$.

1. Term $a$ is correct iff $b$ and $i$ are correct, which we can determine by IH, and $i > 0$, which we can determine (since we can reduce $i$ to a term not using functions of BANK_ACCOUNT by IH).

2. * balance($a$) is correct iff $a$ is correct, which we can determine (see 1). If balance($a$) is correct, then balance($a$) = balance($b$) + $i$, which can be reduced to a term not using functions of BANK_ACCOUNT by IH. * owner($a$) is correct iff $a$ is correct, which we can determine (see 1). If owner($a$) is correct, then owner($a$) = owner($b$), which can be reduced to a term not using functions of BANK_ACCOUNT by IH.
2. Sufficient completeness (4)

Step case (continued)
Second case: \( a \) is withdraw(\( b, i \)) and the IH applies to terms \( b \) and \( i \).

1. Term \( a \) is correct iff \( b \) and \( i \) are correct, which we can determine by IH, and balance(\( b \)) \( \geq i \geq 0 \), which we can determine (since we can reduce balance(\( b \)) and \( i \) to terms not using functions of BANK_ACCOUNT by IH).

2. * balance(\( a \)) is correct iff \( a \) is correct, which we can determine (see 1). If balance(\( a \)) is correct, then balance(\( a \)) = balance(\( b \)) - \( i \), which can be reduced to a term not using functions of BANK_ACCOUNT by IH.

* owner(\( a \)) is correct iff \( a \) is correct, which we can determine (see 1). If owner(\( a \)) is correct, then owner(\( a \)) = owner(\( b \)), which can be reduced to a term not using functions of BANK_ACCOUNT by IH.

QED