Software Verification
Exercise Solution: Hoare & Separation logic

Solutions:

1) We introduce the helper variable z. The loop invariant \( y = z! \) is crucial for the proof, and can be found by executing the loop for a couple of iterations with test values.

\[
\begin{align*}
\{ & \text{true} \} \\
\{ & 1 = 0! \} \\
y & := 1; \\
\{ & y = 0! \} \\
z & := 0; \\
\{ & y = z! \} \\
\text{while (} z \neq x \text{) } \{ \\
& \{ y = z! \land z \neq x \} \\
& \{ y.(z + 1) = (z + 1)! \} \\
& z := z + 1; \\
& \{ y.z = z! \} \\
y & := y \ast z; \\
\{ & y = z! \} \\
\} \\
\{ & y = z! \land \neg(z \neq x) \} \\
\{ & y = x! \} 
\end{align*}
\]
2) The algorithm employs a helper variable k. The proof uses the definition of the list predicate from the slides (see slide 18). We first give a rather detailed proof outline. You can use fewer assertions in the exam - the second outline is a good example.

\[
\{ \text{list (a::as) i} \} \\
\{ \exists j. \text{i} \mapsto \text{a}, j \} * \text{list as j} \}
\]

\[
\{ \exists j. \text{i} \mapsto \text{a}, j \} * \text{list as j} \}
\]

\[
\{ \text{i} \mapsto \text{a} \}
\]

\[
\text{dispose(i)}; \\
\{ \text{empty} \}
\]

\[
\{ \text{i+1} \mapsto \text{j} \} * \text{list as j} \}
\]

\[
\{ \text{i+1} \mapsto \text{j} \}
\]

\[
k := [\text{i+1}]; \\
\{ \text{i+1} \mapsto \text{j} \land k=j \}
\]

\[
\{ \text{i+1} \mapsto \text{j} \} * \text{list as j} \land k=j \}
\]

\[
\{ \exists j. \text{j} \land k=j \}
\]

\[
\{ \exists j. \text{list as j} \land k=j \}
\]

\[
\{ \text{list as k} \}
\]

\[
i := k \\
\{ \text{list as k} \}
\]

\[
\{ \text{list as i} \}
\]

\[
\{ \text{list (a::as) i} \}
\]

\[
\{ \exists j. \text{i} \mapsto \text{a}, j \} * \text{list as j} \}
\]

\[
\{ \exists j. \text{i} \mapsto \text{a}, j \} * \text{list as j} \}
\]

\[
\text{dispose(i)}; \\
\{ \text{empty} \}
\]

\[
\{ \text{i+1} \mapsto \text{j} \} * \text{list as j} \}
\]

\[
\{ \text{i+1} \mapsto \text{j} \}
\]

\[
k := [\text{i+1}]; \\
\{ \text{i+1} \mapsto \text{j} \land k=j \}
\]

\[
\{ \exists j. \text{j} \land k=j \}
\]

\[
\{ \exists j. \text{list as j} \land k=j \}
\]

\[
\{ \text{list as k} \}
\]

\[
i := k \\
\{ \text{list as k} \}
\]

\[
\{ \text{list as i} \}
\]