A. Instructions

- You can work together in groups of \( \leq 4 \). Submit your work on Blackboard. Submit one copy, under the name of one person in the group (doesn't matter who). Include the names and A-IDs of everyone in the group (including the submitter) inside that copy.

B. Why?

- A formal proof describes the reasons for believing that something is valid.
- Proof outlines are easier to use than proofs but give the same information.

C. Outcomes

After this homework, you should be able to

- Convert between formal correctness proofs and full, partial, and minimal proof outlines.

D. Problems: Proofs and Proof Outlines [100 points total]

**Part 1: Complete Formal Proof**

1. [30 = 10*3 points] Consider the program below, which calculates the sum of the first \( n \) squares.

\[
\{ n \geq 0 \} \ S_0; \ \{ \text{inv} \} \ \textbf{while} \ k < n \ \textbf{do} \ S_1 \ \{ s = \text{sum}(n) \}
\]

where

- \( S_0 \equiv k := 0; \ s := k; \ r := s \)
- \( S_1 \equiv r := r+2^*k+1; \ k := k+1; \ s := s+r \)
- \( p \equiv 0 \leq k \leq n \land s = \text{sum}(k^2) \land r = k^2 \)
- \( \text{sum}(k^2) = \text{the sum of} \ 0^2 \ldots \ k^2. \) (Let \( \text{sum}(k^2) = 0 \) if \( k < 0 \).)

The formal proof of partial correctness for the program below is incomplete. For parts (a) – (f), give definitions for \( p_1 - p_6 \). Use substitution notation and (separately) list the results of carrying out the substitutions. For parts (g) – (j), give definitions for the rule references \( r_1 - r_4 \). Include the line numbers (e.g. Sequence 1, 2, not just Sequence).

(a) \( p_1 \)  (b) \( p_2 \)  (c) \( p_3 \)  (d) \( p_4 \)  (e) \( p_5 \)  (f) \( p_6 \)

(g) \( r_1 \)  (h) \( r_2 \)  (i) \( r_3 \)  (j) \( r_4 \)
1. \{n \geq 0\} k := 0 \{p_1\}  \\
2. \{p_1\} s := 0 \{p_2\}  \\
3. \{n \geq 0\} k := 0; s := 0 \{p_2\}  \\
4. \{p_2\} r := 0 \{p_3\}  \\
5. p_3 \rightarrow p  \\
6. \{n \geq 0\} S_0 \{p_3\}  \\
7. \{n \geq 0\} S_0 \{p\}  \\
8. \{p_4\} s := s + r \{p\}  \\
9. \{p_5\} k := k + 1 \{p_4\}  \\
10. \{p_5\} k := k + 1; s := s + r \{p\}  \\
11. \{p_6\} r := r + 2 * k + 1 \{p_5\}  \\
12. \{p_6\} S_1 \{p\}  \\
13. p \land k < n \rightarrow p_6  \\
14. \{p \land k < n\} S_1 \{p\}  \\
15. \{\text{inv } p\} W \{p \land k \geq n\}  \\
   \text{where } W \equiv \textbf{while } k < n \textbf{ do } S_1 \textbf{ od}  \\
16. p \land k \geq n \rightarrow s = \text{sum}(n)  \\
17. \{\text{inv } p\} W \{s = \text{sum}(n)\}  \\
18. \{n \geq 0\} S_0; W \{s = \text{sum}(n)\}  \\

\textbf{Part 2: Translate Formal Proof into Full Outline}  

2. [16 points] Give the full proof outline that corresponds to the proof in problem 1: Insert conditions \(p, p_1, p_2\), etc., as necessary.

\{n \geq 0\} k := 0; \ldots s := k; \ldots r := s; \ldots \{\text{inv } p\} \textbf{while } k < n \textbf{ do}  \\
   \ldots \{\text{inv } p\} \textbf{while } k < n \textbf{ do}  \\
   \ldots r := r + 2 * k + 1;  \\
   \ldots k := k + 1;  \\
   \ldots s := s + r \ldots \} \textbf{ od}  \\
\ldots \{s = \text{sum}(n)\}  \\

\textbf{Part 3: Expand Minimal Outline}  

3. [30 = 3*10 points] We will perform different expansions of the minimal outline below into full proof outlines for partial correctness.

\{T\} \textbf{if } y \geq 0 \textbf{ then } x := \text{sqrt}(y) \textbf{ fi} \{y \geq 0 \rightarrow x = \text{sqrt}(y)\}
a. Complete the full outline below, which uses \(wp\) everywhere to add internal conditions. Feel free to add or remove whitespace.

\[
\begin{align*}
&\{T\}\ldots \\
&\text{if } y \geq 0 \text{ then} \\
&\quad \{\ldots\} x := \sqrt{y} \{\ldots\} \\
&\text{else} \\
&\quad \{\ldots\} \text{ skip } \{\ldots\} \\
&\text{fi } \{y \geq 0 \rightarrow x = \sqrt{y}\}
\end{align*}
\]

b. Complete the full outline below, which uses \(sp\) everywhere.

\[
\begin{align*}
&\{T\}\text{ if } y \geq 0 \text{ then} \\
&\quad \{\ldots\} x := \sqrt{y} \{\ldots\} \\
&\text{else} \\
&\quad \{\ldots\} \text{ skip } \{\ldots\} \\
&\text{fi } \{y \geq 0 \rightarrow x = \sqrt{y}\}
\end{align*}
\]

c. Complete the full outline below, which uses a mix of \(wp\) and \(sp\).

\[
\begin{align*}
&\{T\}\text{ if } y \geq 0 \text{ then} \\
&\quad \{\ldots\} \{\ldots\} x := \sqrt{y} \{\ldots\} \\
&\text{else} \\
&\quad \{\ldots\} \{\ldots\} \text{ skip } \{\ldots\} \\
&\text{fi } \{y \geq 0 \rightarrow x = \sqrt{y}\}
\end{align*}
\]

4. [24 = 12 * 2 points] Expand the minimal outline below into a full proof outline for partial correctness by giving definitions for \(p_1 – p_7\) [11/12]. Also list the three predicate logic obligations. Use substitution notation in your definitions (\(predicate[expr/var]\)), and list the results of carrying out the substitutions.

[11/12: The calculations should be done symbolically. E.g., the answers for \(p_1\) and \(p_2\) are in terms of \(p_0\).]

Hint: It’s not necessarily the case that \(p_{i+1}\) is a function of \(p_i\].

\[
\begin{align*}
&\{p_0\} x := 1 ; p_1 ; k := 0 ; \{p_2\} \\
&\text{inv } p \equiv 1 \leq x = 2^k \leq b[j] \\
&\text{while } 2^x \leq b[j] \text{ do} \\
&\quad \{p_3\} \\
&\quad \{p_4\} k := k+1 \\
&\quad \{p_5\} x := 2^x \\
&\quad \{p_6\} \\
&\text{od } \{p_7\} \{q \equiv x = 2^k \leq b[j] < 2^{k+1}\}
\end{align*}
\]