Question 1 (8 marks).
Consider the following specification:
\[\{ (y = y_0) \land (y \geq 0) \} \Downarrow\]
z = 0;
while (y > 0) {
    z = z + x;
    y = y - 1;
}
\[\{ z = x \cdot y_0 \} \Downarrow\]

(a) Prove that this specification is satisfied under partial correctness. Show all the needed details of your program annotation, and explicitly prove any implications required by your annotation.
(b) Prove that this specification is satisfied under total correctness. You may assume the partial correctness from part (a), whether or not you solved it.
Question 2 (6 marks).

[Learning Goal: Prove that a specification of a program using arrays is satisfied under partial correctness.]

Consider the following specification:
\[
\preceq \left( (x_1 = A[1] \land x_2 = A[2]) \land x_3 = A[3] \right) \preceq
\]
\[
\]
\[
\]
\[
\]
\[
A[1] = t ;
\]
\[
\preceq \left( (x_1 = A[2] \land x_2 = A[3]) \land x_3 = A[1] \right) \preceq
\]
Prove that this specification is satisfied under partial correctness. Show all the needed details of your program annotation, and explicitly prove any implications required by your annotation.
Question 3 (19 marks).

[Learning Goal: Prove that a specification of a program using arrays is satisfied under total correctness.]

The code below might be used as part of a “selection sort”. It scans an array $A$ and performs at most one swap to put the smallest element in the array at the beginning (i.e. in position 1). The array $A$ contains integer values. The domain for the values of all other variables is the positive integers.

The relations in the pre- and post-condition are
\begin{itemize}
  \item $Perm(X,Y)$: Arrays $X$ and $Y$ are permutations of one another.
  \item $Min(X,a,m)$: In array $X$, the smallest of the first $m$ elements is at position $a$.
\end{itemize}

\begin{verbatim}
\{ ((A = A_0) \land (n > 0)) \}\nminidx = 1;
    i = 1;
while (i < n) {
    i = i+1;
        minidx = i;
    }
}
if (minidx > 1) {
    t = A[1] ;
    A[minidx] = t ;
}
\{ (Perm(A,A_0) \land Min(A,1,n)) \}
\end{verbatim}

Use the formula
\[ (\forall j((1 \leq j \leq m) \rightarrow (X[a] \leq X[j]))) \]
as the definition of $Min(X,a,m)$.

Use the following axioms for $Perm$: for all arrays $B$, $C$ and $D$, and all positive integers $x$ and $y$,
\begin{itemize}
  \item P1: $Perm(B,B)$
  \item P2: $(Perm(B,C) \rightarrow Perm(C,B))$.
  \item P3: $((Perm(B,C) \land Perm(C,D)) \rightarrow Perm(B,D))$.
  \item P4: $Perm(B, B\{x \leftarrow B[y]\}\{y \leftarrow B[x]\})$.
\end{itemize}

For the first part of the question (on the next two pages), fill in the blanks with suitable annotations. N.B. the loop invariant has been filled in for you.
Q3 (a)

\[ ((A = A_0) \land (n > 0)) \]

<table>
<thead>
<tr>
<th>precondition</th>
</tr>
</thead>
<tbody>
<tr>
<td>minidx = 1 ;</td>
</tr>
<tr>
<td>i = 1 ;</td>
</tr>
<tr>
<td>( (Perm(A, A_0) \land Min(A, minidx, i) \land i \leq n) )</td>
</tr>
</tbody>
</table>

while ( i < n ) {

i = i + 1 ;


minidx = i ;

}

}
N.B. For your convenience, make the first assertion on this page a copy of the last assertion on the previous page. Only the assertion at the bottom of the previous page will be marked.

```c
if ( minidx > 1 ) {
    t = A[1] ;
    A[minidx] = t ;
}

(Perm(A, A_0) ∧ Min(A, 1, n))
```
Q3 (b) Justify each of the “implied” conditions from your annotation.
Formal proofs are NOT required; the markers will assume that you know basic arithmetic.
Do, however, mention the key points.
Q3 (c) Prove that the specification is satisfied under total correctness.
You may assume the results for the previous parts of this question, whether you solved them or not.