Question 1 Prove that the question of whether an assignment to a variable is a flow down during program execution in Dennis model of security of class 12 is undecidable.

Consider the following program $P$ (assumed to compute with mathematical integers $\mathbb{Z}$).

\[
\begin{align*}
    s &= 0; \quad i = 0; \\
    \text{while } (i \neq N) \text{ do} \\
        &\quad s = s+i; \quad i = i+1; \\
    \text{od}; \\
    r &= N(N-1)/2 - s;
\end{align*}
\]

Question 2 Prove that any execution of program $P$ starting with $N \geq 0$ always terminates while any execution of program $P$ starting with $N < 0$ never terminates.

Question 3 Provide invariants in program $P$ characterizing the final value of $r$ upon termination, if ever.

Question 4 It is required that upon termination, $s$ be private and $r$ be public where private $< public$. Prove that program $P$ never leaks any private information to the result $r$.

Question 5 Can the confidentiality result of Question 4 be proved for program $P$ by Dennis’ flow analysis of class 12; or by the Volpano-Irvine-Smith type system of class 13? Can confidentiality be proved by static analysis of class 14 using interval analysis?