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.

Answer 1 Assume by reductio ad absurdum that the question is decidable that is can be answered statically (at compile time). Then termination of program P would be decidable by considering the following program Q such that

\[ P; \text{public := secret;} \]

(where public and secret are fresh variables not in P) since P terminates if and only if there is no flow down which is the case if and only if the assignment public := secret is never executed, so that termination would be decidable, a contradiction.

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.

Answer 2 If initially \( N \geq 0 \), the program P terminates since \( i \) strictly increases from 0 in the loop and eventually reaches \( N \) (which is never modified) by successive increments by 1.

Else \( N < 0 \) initially and then the test \( (i != N) \) is initially false and remains false after any iteration in the loop which increments \( i \) and leaves \( N \) unmodified.
Question 3  Provide invariants in program P characterizing the final value of r upon termination, if ever.

Answer 3  The following invariants prove that upon termination $r = 0$.

\begin{verbatim}
{ N>=0, by hypothesis }
s=0; i=0;
{ N>=i>=0 & s = i(i-1)/2 }
while (i != N) do
    { N>i>=0 & s = i(i-1)/2 }
    s = s+i;
    { N>=i>=0 & s = i(i-1)/2 + i = (i^2-i+2i)/2 =
        (i^2+2i)/2 = (i+1)i/2 = (i+1)(i+1-1)/2 }
    i = i+1;
    { N>=i>0 & s = 1(i-1)/2 }
od;
{ i=N & s=N(N-1)/2 }
r = N(N-1)/2 - s;
{ r=0 }
\end{verbatim}

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 $r$.

Answer 4  This is obviously true in case of non-termination. Else, upon termination $r = 0$, a constant, so no private information is leaked to $r$.

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?

Answer 5  Confidentiality cannot be proved for P with a security type system which does not take values into account and so cannot conclude that $r$ is constant upon termination. Since $s$ apparently flows to $r$ in the last assignment, the program is untypable hence rejected. For static analysis of class 14, interval/octagon/polyhedral analysis cannot prove that $s = \frac{N(N-1)}{2}$ and so will also fail to prove confidentiality.