CS615 Autumn 2004 Quiz 1

Time: 60 mins Total marks: 20

- ***The exam is open book and notes.***
- ***Results/proofs covered in class/problem sessions/assignments may simply be cited, unless specifically asked for.***
- ***Unnecessarily lengthy solutions will be penalized.***
- ***If you need to make any assumptions, state them clearly.***
- ***Do not copy solutions from others or indulge in unfair means.***

1. Consider the following annotated program (command) written by a student. Given a positive natural number `n`, the student claims that her program can be used to set i to the value of n in atmost $2.\lceil \log_2 n \rceil$ iterations of the `while` loops. All variables in the program are assumed to be of type `natural_number`.

   The student has provided underlined assertions in the program as annotations to aid formal verification.

```
# command C

# Assert (n > 0)
# --------------
i := 1;
iter_count1 := 0;
iter_count2 := 0;

# Assert (i < 2*n)
# ----------------
# Assert (iter_count1 = log2 i)
# -----------------------------
while (i < n)
   iter_count1 := iter_count1 + 1;
   i := i * 2;


# Assert (iter_count1 <= ceil(log2 n))
# ------------------------------------

if (i <> n) then
  lbound := i div 2;
  ubound := i;
  i := (lbound + ubound) div 2;
```

```
# Assert (lbound <= n <= ubound)
# ------------------------------
# Assert (lbound <= i <= ubound)
# ------------------------------
# Assert (0 <= ubound - lbound <= n)
# ----------------------------------
# Assert ((ubound - lbound) * 2 ^ iter_count2 <=  n)
# --------------------------------------------------

while (i <> n)
    iter_count2 := iter_count2 + 1;

    if (i > n) then
      ubound := i;
    else
      lbound := i;

    i := (ubound + lbound) div 2;

# Assert (iter_count2 <= ceil(log2 n))
# ------------------------------------
```

Using the provided annotations as proof outline, give a Hoare deductive proof for the Hoare Logic formula $\{P\}\ C\ \{Q\}$ where $P = (\mathtt{n} > 0)$ and $Q = (\mathtt{i} = \mathtt{n}) \wedge (\mathtt{iter\_count1} \leq \lceil \log_2 \mathtt{n} \rceil) \wedge (\mathtt{iter\_count2} \leq \lceil \log_2 \mathtt{n} \rceil)$.

You must clearly indicate any additional domain-specific axioms that you use in your proof, and you must *minimize* the use of such additional axioms.

At each step of your proof, you MUST indicate which axiom or inference rule you are using.