CMPUT 272 Winter 2001: Section B1
Final Exam
Wednesday, April 25
Time: 120 minutes
Weight: 50%
Total Points: 75

Last Name:	
First Name:	
Unix ID:	

- This exam is **open book**
- This exam should have 9 pages and 8 questions. You are responsible for checking that your exam is complete.
- Unless otherwise specified, you may use whichever of HR or GT notation you prefer.
- If you need additional paper it is available from a proctor.

Question	Mark	
1		10
2		10
3		3
4		13
5		6
6		10
7		10
8		13
Σ		75

Question 1 [10 points]
Recall that for $a, b \in \mathbb{Z}$ we write $a|b$ to mean that a evenly divides b (or more precisely, $\exists i \in \mathbb{Z} : b = a \cdot i$).

Use induction to prove that $6|n^3 + 5n$ for all $n \in \mathbb{N}$. Clearly indicate the base case, induction step, and induction hypothesis. Also indicate where the induction hypothesis is used.

Question 2 [10 points]
Using the predicates:

H(x): x is a hero.
Brv(x): x is brave.
Bfl(x): x is beautiful.
A(x,y): x admires y.

translate the following sentences into predicate logic.

The universe of discourse consists of people, including the constants **Xena** and **Ares**.

1. Ares does not admire brave Xena.

2. Everybody admires a hero.

3. Heros are brave and beautiful.

4. Some people are brave, yet they are not heros.

5. Xena doesn't admire everone who admires her.

Question 3 [3 points]
Give a brief, informal argument that the composition of two total functions is total. Use diagrams, if they support your argument.

Question 4 [13 points]
A palindrome is a string whose spelling is the same forwards as backwards. For example "otto" and "able was I ere I saw elba" are palindromes. The code below tests whether an array holds a palindrome.

Palindrome Detector

Nat n; Char A[1..*n*]
Boolean pal;
Preconditions: (none)
Nat k;
$k, pal := 1, true;$
do
    Variant: ?
    Invariant: $(\forall i : 1 \leq i < k : A[i] = A[n+1-i]) \wedge (\neg pal \Rightarrow A[k] \neq A[n+1-k])$
  $[]\ (k = \lfloor \frac{n}{2} \rfloor + 1) \vee \neg pal \xrightarrow{exit}$
  $[]\ (k \leq \lfloor \frac{n}{2} \rfloor) \wedge pal \longrightarrow$
    if
      $[]\ A[k] = A[n+1-k] \longrightarrow k := k+1;$
      $[]\ A[k] \neq A[n+1-k] \longrightarrow pal := false;$
    fi
od
Postconditions: $pal \Rightarrow (\forall i : 1 \leq i \leq \lfloor \frac{n}{2} \rfloor : A[i] = A[n+1-i])$

4.a [2 pts]: State a variant for the loop. (without proof)

In the following you may assume that the loop terminates and that one of the guards always evaluates to true.

4.b [9 pts]: Prove that the invariant is true at the beginning of <u>each</u> iteration of the loop.
(there is more space on the next page)

4.c [2 pts]: Prove that the postcondition is true when the loop exits.

Question 5 [6 points]

Consider the following functions mapping $\mathbb{R}$ to $\mathbb{R}$. For each, determine which of the following properties it exhibits. In the table below, write a "$\surd$" if the function satisfies the property, and leave the entry blank otherwise.

function	total?	injective?	surjective?	bijective?
$\lambda x.e^x$				
$\lambda x.\ln(x)$				
$\lambda x.e^{\ln(x)}$				
$\lambda x.\ln(e^x)$				
$\{\langle x,y\rangle \mid xy = 1\}$				
$\{\langle x,y\rangle \mid x^2 = y\}$				

Question 6 [10 points]
This question requires you to do a `mizar` derivation. For this derivation:

- Use only the basic rules of inference, namely NE, NI, CE, CI, DE, DI, IE, II, EqE, EqI, RE, ContrI.
- Each step requires a justification (i.e. a reference to the formulas it is inferred from) and an annotation (i.e. the name of the inference rule used).
- You may use GT connectives, and omit writing the "[]" after propositions,

```
environ
  pr1: A[] implies B[];
  pr2: D[] implies not (A[] implies (B[] or C[]));

begin
  claim: not D[]
  proof
```

Question 7 [10 points]
Let $R \subseteq A \times A$ be a relation. Prove that if R is transitive then $R \circ R \subseteq R$. Note that:

- you may use GT notation, in particular
  - you may abbreviate the composition of R with itself by $R \circ R$
  - you may abbreviate `In[x,y,R]` as either $\langle x, y \rangle \in R$ or xRy
  - you may abbreviate `Subset[S,T]` as $S \subseteq T$
- you are not restricted to basic rules of inference.

```
environ
  reserve r,s,t for RELATION; reserve x,y,z for ELEMENT;
  CompositionDef: for r,s,t holds Composition[r,s,t] iff
    (for x,z holds In[x,z,t] iff (ex y st In[x,y,r] & In[y,z,s]));
  TransitivityDef: for r holds Transitive[r] iff
    (for x,y,z st In[x,y,r] & In[y,z,r] holds In[x,z,r]);
  SubsetDef: for r,s holds Subset[r,s] iff (for x,y st In[x,y,r] holds In[x,y,s]);
  Given R being RELATION;

begin
  claim: Transitive[R] implies Subset[RoR,R]
  proof
```

Question 8 [13 points]
Recall the definitions:

union: $\forall Y, Z\ (\forall x\ (x \in Y \cup Z \Leftrightarrow x \in Y \vee x \in Z))$
intersection: $\forall Y, Z\ (\forall x\ (x \in Y \cap Z \Leftrightarrow x \in Y \wedge x \in Z))$
subset: $\forall Y, Z\ (Y \subseteq Z \Leftrightarrow \forall x\ (x \in Y \Rightarrow x \in Z))$
set equality: $\forall Y, Z\ (Y = Z \Leftrightarrow \forall x\ (x \in Y \Leftrightarrow x \in Z))$

For the two statements below, determine whether each is true or false. Provide a formal proof for each true statement. Provide a counter-example for each false statement.

1. $\forall A, B\ (A \cap B = A \cup C \quad \Rightarrow \quad C \subseteq B)$
2. $\forall A, B\ (C \subseteq B \quad \Rightarrow \quad A \cap B = A \cup C)$