Software Verification – Exam

ETH Zürich

20 December 2010

Surname, first name: ........................................................................................................

Student number: ...........................................................................................................

I confirm with my signature that I was able to take this exam under regular circumstances and that I have read and understood the directions below.

Signature: ..............................................................................................................

Directions:

• Exam duration: 1 hour 45 minutes.

• Except for a dictionary you are not allowed to use any supplementary material.

• All solutions can be written directly on the exam sheets. If you need more space for your solution ask the supervisors for a sheet of official paper. You are not allowed to use other paper. Please write your student number on each additional sheet.

• Only one solution can be handed in per question. Invalid solutions need to be crossed out clearly.

• Please write legibly! We will only correct solutions that we can read.

• Manage your time carefully (take into account the number of points for each question).

• Please immediately tell the exam supervisors if you feel disturbed during the exam.

Good luck!
<table>
<thead>
<tr>
<th>Question</th>
<th>Available points</th>
<th>Your points</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Axiomatic semantics</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>2) Separation logic</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>3) Data flow analysis</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>4) Model checking</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>5) Software model checking</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>6) Termination proofs</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>70</strong></td>
<td></td>
</tr>
</tbody>
</table>
1 Axiomatic semantics (9 points)

Consider the following Hoare triple (all variables of type \textit{NATURAL}, assumed to describe mathematical natural numbers):

\begin{verbatim}
{ y = n }
1 from
2 z := 1
3 until y = 0 loop
4 y := y - 1
5 z := z * x
6 end
{ z = x^n }
\end{verbatim}

Prove that this triple is a theorem of Hoare’s axiomatic system for partial correctness.
2 Separation Logic (13 points)

Consider the definition of the list binary predicate:

\[
\begin{align*}
\text{list } i &\equiv \text{empty} \land i = \text{nil} \\
\text{list } i (a : \sigma) &\equiv \exists j \cdot (i \mapsto a, j) \ast (\text{list } j \sigma)
\end{align*}
\]

where \(\sigma \equiv [\ ] \mid a : \sigma\) defines a sequence of integers.

2.1 States and semantics (7 points)

Consider the separation logic predicate \(P\), where

\[
P \equiv 3 \mapsto 5, 8 \ast 8 \mapsto 7, 11 \ast 11 \mapsto 6, 1 \ast 1 \mapsto 3, \text{nil}
\]

and answer the following questions:

(1) For every state \((s, h)\) that satisfies \(P\), the heap component \(h\) will be the same. Write such a function \(h\) explicitly as a set of pairs.

(2) If \((s, h) \models P\), then \((s, h) \models \text{list } i \sigma \ast \text{true}\) for several values of \(i\) and \(\sigma\). Provide all such pairs \((i, \sigma)\).
2.2 Separation logic and verification (6 points)

Consider the signature and separation logic specification for a routine that adds a value to the front of a linked list. It returns a pointer to the new head node by storing it in the Result variable:

\[
\text{add}
\begin{array}{ll}
\text{front} & (\text{list},\text{pointer} : \text{INTEGER}; \text{value} : \text{INTEGER}) : \text{INTEGER} \\
\text{require} & \text{list list} \sigma \\
\text{ensure} & \text{list Result} (\text{value} : \sigma)
\end{array}
\]

(1) Write a body for the routine. Use the \texttt{cons} command, whose semantics is given by the axiom:

\[
\text{ConsAxiom} \quad \{\emptyset\}x := \text{cons}(e_1, \ldots, e_n)\{x \mapsto e_1, \ldots, e_n\}
\]

provided that \(1 \leq n\) and \(x\) is not free in any of \(e_1, \ldots, e_n\).

(2) Prove your routine body correct.
(3) Write down the schemas of all the inference rules that you used in the proof above.
[This page is intentionally left blank.]
### 3 Data flow analysis (12 points)

An arithmetic expression is called *trivial* if it consists only of a single variable or constant; it is called *non-trivial* otherwise. Let $\text{AExp}_a$ denote the set of all non-trivial arithmetic expressions that occur in a given program fragment, and let $\text{AExp}(a)$ denote the set of all non-trivial arithmetic subexpressions of an expression $a$. Furthermore, let $\text{Vars}(a)$ denote the set of variables occurring in $a$.

With this terminology, recall the definition of the *available expressions analysis* from the lecture:

$$
\begin{align*}
\AE_{\text{entry}}(\ell') &= \begin{cases} 
\emptyset & \text{if } \ell' \text{ is the initial label} \\
\bigcap_{(\ell,\ell') \in \text{CFG}} \AE_{\text{exit}}(\ell) & \text{otherwise}
\end{cases} \\
\AE_{\text{exit}}(\ell) &= (\AE_{\text{entry}}(\ell) \setminus \text{kill}_{\AE}(B')) \cup \text{gen}_{\AE}(B')
\end{align*}
$$

where $B$ is an elementary block of the form $[x := a]$ or $[b]$, and the $\text{kill}$ and $\text{gen}$ functions are given by

$$
\begin{align*}
\text{kill}_{\AE}([x := a]) &= \{ a' \in \text{AExp}_a \mid x \in \text{Vars}(a') \} \\
\text{kill}_{\AE}([b]) &= \emptyset \\
\text{gen}_{\AE}([x := a]) &= \{ a' \in \text{AExp}(a) \mid x \notin \text{Vars}(a') \} \\
\text{gen}_{\AE}([b]) &= \text{AExp}(b)
\end{align*}
$$

Now consider the following program fragment:

1. $a := b \ast c$
2. $d := e + f$
3. $f := a - d$
4. if $f > 0$ then
5.   $f := b \ast c$
6. else
7.   from
8.   $g := 1$
9.   until $a \ast g > 10$ loop
10. $a := a \ast f$
11. $g := g + 1$
12. end
13. end
14. $b := a + b \ast c$

(1) Draw the control flow graph of the program fragment and label each elementary block. (3 points)

(2) Annotate your control flow graph with the analysis result of an available expressions analysis of the program fragment. (7 points)
(3) How can you use your analysis result to optimize the program fragment? (2 points)

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................

.................................................................
4 Model Checking (10 points)

Recall the semantics of LTL over finite words with alphabet $P$. For a word $w = w(1)w(2)\cdots w(n) \in P^*$ with $n \geq 0$ and a position $1 \leq i \leq n$ the satisfaction relation $\models$ is defined recursively as follows for $p, q \in P$.

\[
\begin{align*}
  w, i \models p & \quad \text{iff} \quad p = w(i) \\
  w, i \models \neg \phi & \quad \text{iff} \quad w, i \not\models \phi \\
  w, i \models \phi_1 \land \phi_2 & \quad \text{iff} \quad w, i \models \phi_1 \quad \text{and} \quad w, i \models \phi_2 \\
  w, i \models X\phi & \quad \text{iff} \quad i < n \quad \text{and} \quad w, i + 1 \models \phi \\
  w, i \models \phi_1 U \phi_2 & \quad \text{iff} \quad \text{there exists } i \leq j \leq n \text{ such that: } w, j \models \phi_2 \\
    & \quad \text{and for all } i \leq k < j \text{ it is the case that: } w, k \models \phi_1 \\
  w, i \models \Diamond \phi & \quad \text{iff} \quad \text{there exists } i \leq j \leq n \text{ such that: } w, j \models \phi \\
  w, i \models \Box \phi & \quad \text{iff} \quad \text{for all } i \leq j \leq n \text{ it is the case that: } w, j \models \phi \\
  w \models \phi & \quad \text{iff} \quad w, 1 \models \phi
\end{align*}
\]

4.1 Automata and LTL formulas (6 points)

Consider the automata $T_A$ (with states $A, B, C$) and $T_X$ (with states $X, Y, Z$) in Figure 1 over the alphabet $\{p, q\}$. Notice that $T_A$ is nondeterministic but $T_X$ is deterministic.

![Figure 1: Automata $T_A$ (top) and $T_X$ (bottom).](image)

For each of the following LTL formulas say whether every run of $T_A$ or $T_X$ satisfies the formula. If it does, argue informally (but precisely) why this is the case; if it does not, provide a counterexample.
(1) $T_A \models \Box(\Diamond p)$

(2) $T_X \models \Box(\Diamond p)$

(3) $T_A \models \Diamond(p \land \Xi(p \lor q))$
4.2 Automata-based model checking (4 points)

Let \( \langle T_A \rangle \) and \( \langle T_X \rangle \) respectively denote the set of all words accepted by \( T_A \) and \( T_X \). Show that \( \langle T_A \rangle \not\subseteq \langle T_X \rangle \) by constructing the intersection automaton \( T_A \cap \neg T_X \) of \( T_A \) and the complement of \( T_X \), and by showing that the intersection automaton accepts some word.

(Remember that the complement automaton of \( T_X \) is identical to \( T_X \) except for the accepting states which are \( X \) and \( Y \) in the complement, with \( Z \) becoming a rejecting state in the complement).
5 Software model checking (13 points)

Consider the following code snippet $C$, where $x$, $y$ are integer variables.

1. \textbf{assume} $x + y > 0$ \textbf{end}
2. $x := x + y$

Remember that the Boolean abstraction of an \textbf{assume c end} statement is \textbf{assume not Pred (not c) end} followed by a parallel conditional assignment updating the predicates with respect to the original \textbf{assume} statement. \textit{Pred (f)} denotes the weakest under-approximation of the expression $f$ in terms of the given predicates.

5.1 Boolean abstractions (10 points)

Build the Boolean abstraction $A$ of the code snippet $C$ with respect to the following predicates:

\[
\begin{align*}
    p &= x > 0 \\
    q &= y > 0
\end{align*}
\]

.. note::
5.2 Abstract and concrete traces (3 points)

Provide an annotated trace for the Boolean abstraction $A$, and a corresponding annotated trace for the concrete program $C$ which is feasible. Note that in general there are multiple traces of $C$ corresponding to the same trace of $A$: you must select one which is feasible.

The trace of $A$ should be in the form of a valid sequence of statements and branch conditions in $A$ which reaches the bottom of $A$. Each statement in the sequence must be preceded and followed by a complete description of the abstract program state in terms of values of the Boolean predicates $p$, $q$. Similarly, the trace of $C$ should be in the form of a valid sequence of statements and branch conditions in $C$ which reaches the bottom of $C$ without violating any assertion. Each statement in the sequence must be preceded and followed by a concrete value for the variables $x$, $y$ which satisfies the corresponding state in the abstract trace of $A$. 

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................

........................................................................................................
6 Termination proofs (13 points)

Consider the following implementation of binary search, where \( \div \) denotes integer division.

```plaintext
binary_search (v : G; list : LIST [G]; n: INTEGER): BOOLEAN
-- Is 'v' contained in 'list' in the range [1..n]?
require n > 0 and list.is_sorted

do
from
  l := 1
  u := n
Result := False
until l > u
loop
  m := (l + u) \div 2
  if list [m] = v then
  -- Element found
  Result := True
  l := u + 1
  elseif list [m] > v then
  -- Continue search on left side
  u := m - 1
  else
  -- Continue search on right side
  l := m + 1
end
end

(1) Consider the loop invariant

\[ I \triangleq u - l + 1 \geq 0 \]

Find a suitable variant function \( V \) which decreases along all branches of the loop body, and describe how \( V \) and \( I \) can be combined to prove that the loop always terminates. You do not have to provide a formal proof, but only to outline a termination argument for the given program with a suitable variant \( V \). (7 points)
```
(2) Provide a proof that $I$ is an invariant of the loop. For full credit, it is enough if you consider only the else branch of the conditional and prove invariance (consecution) along it. (6 points)