Department of Computer Science, Australian National University
COMP2600 / COMP6260 — Formal Methods in Software Engineering
Semester 2, 2015

Assignment 1

Structural Induction, FOL Specification and Natural Deduction

Due: 11am on Monday 24th August 2015

The submission of your assignment must be done via the assignment boxes in the student foyer. Failure to submit by the due date will result in late penalties as per the course page. Other arrangements that are required because of truly exceptional circumstances need to be negotiated before your deadline.

Your submission must be well-presented on clean A4 paper with a fully completed standard cover page, including your *tutor's name* and your *tutorial group*. The COMP2600 page has a link to an appropriate cover page.

1 Structural Induction [10 marks]

Consider the definition of binary trees given in the lectures

```
data Tree a = Nul | Node a (Tree a) (Tree a)
```

and the following three functions:

```
f :: Tree a -> Int
f Nul = 0                                      -- F1
f (Node x Nul Nul) = 1                         -- F2
f (Node x l r) = (f l) + (f r)                 -- F3

g :: Tree a -> Int
g t = h 0 t                                    -- G

h :: Int -> Tree a -> Int
h acc Nul = acc                                -- H1
h acc (Node x Nul Nul) = acc + 1               -- H2
h acc (Node x  l   r ) = h (h acc l) r         -- H3
```

Establish, using structural induction, that `f t` = `g t` for all trees `t` of type `Tree a`.

State clearly what property P is being proved by induction, including any quantifiers needed in the statement of P and in the inductive hypothesis.

Answer. We establish that the following

$$P(\mathtt{t}) = \forall \mathtt{acc}(\mathtt{acc} + \mathtt{f\ t} = \mathtt{h\ acc\ t})$$

holds for all trees `t` by structural induction.

Base case: `t = Nul`. We show that `acc + f Nul = h acc Null` by means of the following calculation:

```
  acc + f Nul
= acc + 0      -- by F1
= acc          -- by arithmetic
= h acc Nul    -- by H1
```

As `acc` was arbitrary, this shows that the equation holds for all values of `acc`.

Step case: `t = Node x l r`
We separate the induction hypothesis for the left and the right subtree:

$$\forall \mathtt{acc}(\mathtt{acc} + \mathtt{f\ l} = \mathtt{h\ acc\ l}) \quad -- \quad \mathtt{IH1}$$
$$\forall \mathtt{acc}(\mathtt{acc} + \mathtt{f\ r} = \mathtt{h\ acc\ r}) \quad -- \quad \mathtt{IH2}$$

and show that

$$\forall \mathtt{acc}(\mathtt{acc} + \mathtt{f}(\mathtt{Node\ x\ l\ r}) = \mathtt{h\ acc\ }(\mathtt{Node\ x\ l\ r})).$$

Let `acc` be arbitrary. We distinguish the following cases.

Case 1. Both `l = Nul` and `r = Nul`. We obtain:

```
  acc + f (Node x Nul Nul)
= acc + 1                  -- by F2
= h acc (Node x Nul Nul)   -- by H2
```

Case 2. Either `l` or `r` is distinct from `Nul`. We obtain:

```
  acc + f (Node x l r)
= acc + (f l) + (f r) -- by F3
= h (acc + (f l))  r   -- by IH1 instantiated with acc + (f l)
= h (h acc l) r        -- by IH2 instantiated with acc
= h acc (Node x l r)   -- by H3
```

As the statement holds in both cases, and one of the cases necessarily obtains, the property holds. To get that the equation `f t = h t` holds for all `t: Tree a` we argue that

```
  f t
= 0 + (f t)    -- arithmetic
= h 0 t        -- by the previous proof
= g t          -- by G
```

which finishes the proof.

Suggested marks: 2 for finding the right property, 1 for the idea of the case distinction, 1 for the base case, 1 for the simple case of both trees being empty, 2 for the case of both trees not being empty, 1 for putting everything back together and 2 for clarity of the proof (understanding what is being proved under which assumptions).

2 Propositional Natural Deduction [7 Marks]

Consider the following formulae of propositional logic:

i. $(q \to r) \to ((p \to q) \to (p \to r))$

ii. $(r \vee \neg(p \to q)) \iff (r \vee p \vee \neg q)$

iii. $(\neg p \vee (q \to r)) \wedge p \wedge q \wedge \neg r$

For each of the formulae, decide whether it is a contingency, a tautology or a contradiction. In case of a contingency, give an assignment of truth values to the atomic proposition under which the formula evaluates to `true` and an assignment under which it evaluates to `false`. For tautologies, give a proof of the formula using natural deduction. For contradictions, show that the negation of the formula is a tautology by giving a natural deduction proof (of the negation).

In the natural deduction proofs, you may only use the introduction and elimination rules discussed in lectures and given in the Appendix. Do not use algebraic laws, or any of the derived rules obtained in lectures.

Answer.

i. is a tautology.

1	$q \to r$	
2	$p \to q$	
3	p	
4	q	$\to$-E, 2, 3
5	r	$\to$-E, 1, 4
6	$p \to r$	$\to$-I, 3, 5
7	$(p \to q) \to (p \to r)$	$\to$-I, 2, 6
8	$(q \to r) \to ((p \to q) \to (p \to r))$	$\to$-I, 1, 7

ii. is a contingency. It evaluates to `true` under the any assignment for which $r =$ `true` and to `false` for $p = q = r =$ `false`.

iii. $(\neg p \vee (q \to r)) \wedge p \wedge q \wedge \neg r$ is a contradiction. We prove the negation by natural deduction:

1	$\neg p \vee (q \to r)) \wedge p \wedge q \wedge \neg r$	
2	$\neg p \vee (q \to r)$	$\wedge$-E, 1
3	$p \wedge q \wedge \neg r$	$\wedge$-E, 1
4	$p \wedge q$	$\wedge$-E, 3
5	$\neg r$	$\wedge$-E, 3
6	p	$\wedge$-E, 4
7	q	$\wedge$-E, 4
8	$\neg p$	
9	$p \wedge \neg p$	$\wedge$-I, 6, 8
10	$q \to r$	
11	r	$\to$-E, 7, 10
12	$r \wedge \neg r$	$\wedge$-I, 5, 11
13	$\neg(p \wedge \neg p)$	
14	$r \wedge \neg r$	R, 12
15	$p \wedge \neg p$	$\neg$E, 13, 14
16	$p \wedge \neg p$	$\vee$-E, 2, 8–9, 10–15
17	$\neg(\neg p \vee (q \to r)) \wedge p \wedge q \wedge \neg r)$	$\neg$I, 1, 16

Suggested marks: 1 for the contingency, 2 for the natural deduction proof of the tautology and 4 for the natural deduction proof of the negated contradiction.

3 First Order Natural Deduction [3 Marks]

Give a natural deduction proof of the following derived rule, where y is not free in A.

$$\frac{\exists y.(A \to P(y))}{A \to \exists y.P(y)}$$

You may only use the introduction and elimination rules discussed in lectures and given in the Appendix. Do not use algebraic laws, or any of the derived rules obtained in lectures.

Answer. We have the following natural deduction proof:

1		$\exists y.(A \to P(y))$	
2	a	$A \to P(a)$	
3		A	
4		$P(a)$	$\to$-E, 2, 3
5		$\exists y.P(y)$	=-I, 4
6		$A \to \exists y.P(y)$	$\to$-I, 3–5
$*$7		$A \to \exists y.P(y)$	=-E, 1, 2–6

Here $(*)$ indicates that y is not free in A as per the problem statement.

Appendix 1 — Natural Deduction Rules

$$(\wedge I) \quad \frac{p \qquad q}{p \wedge q} \qquad\qquad (\wedge E) \quad \frac{p \wedge q}{p} \qquad \frac{p \wedge q}{q}$$

$$(\vee I) \quad \frac{p}{p \vee q} \qquad \frac{p}{q \vee p} \qquad\qquad (\vee E) \quad \frac{p \vee q \qquad \begin{matrix}[p]\\ \vdots \\ r\end{matrix} \qquad \begin{matrix}[q]\\ \vdots \\ r\end{matrix}}{r}$$

$$(\to I) \quad \frac{\begin{matrix}[p]\\ \vdots \\ q\end{matrix}}{p \to q} \qquad\qquad (\to E) \quad \frac{p \qquad p \to q}{q}$$

$$(\neg I) \quad \frac{\begin{matrix}[p]\\ \vdots \\ q \wedge \neg q\end{matrix}}{\neg p} \qquad\qquad (\neg E) \quad \frac{\begin{matrix}[\neg p]\\ \vdots \\ q \wedge \neg q\end{matrix}}{p}$$

$$(\forall I) \quad \frac{P(a) \qquad (a \text{ arbitrary})}{\forall x.\ P(x)}$$

$$(\forall E) \quad \frac{\forall x.\ P(x)}{P(a)}$$

$$(\exists I) \quad \frac{P(a)}{\exists x. P(x)}$$

$$(\exists E) \quad \frac{\exists x. P(x) \qquad \begin{matrix}[P(a)]\\ \vdots \\ q\end{matrix} \qquad (a \text{ arbitrary})}{q \quad (a \text{ is not free in } q)}$$

Appendix 2 — Truth Table Values

p	q	$p \vee q$	$p \wedge q$	$p \rightarrow q$	$\neg p$	$p \leftrightarrow q$
T	T	T	T	T	F	T
T	F	T	F	F	F	F
F	T	T	F	T	T	F
F	F	F	F	T	T	T