Overview

The coursework is in 2 parts:

1. Natural Deduction proofs in Isabelle/HOL (40 marks)
2. Introduction to Quantifier Elimination (60 marks)
   2.1 Local axiomatic reasoning in Isabelle
   2.2 Quantifier Elimination for unbounded DLOs (48 marks)
   2.3 Quantifier Elimination for bounded DLOs (12 marks)

This coursework is worth 20% of your overall mark for the course.

The deadline is 2pm, Friday 27th February 2015.
Objectives of the Coursework

1. Experience in Natural Deduction proving
2. Introduction to the technique of *Quantifier Elimination*
3. Experience in reasoning with local axioms
4. Experience in completing a reasonably sized formalisation task in Isabelle/HOL
Part 1
Part 1 : Natural Deduction proofs in Isabelle/HOL

This part asks you to complete some proofs of propositional and first-order (and one second-order) proof in Isabelle/HOL.

They should be relatively straightforward if you have been through all the exercises.

All of these can be proved by Isabelle’s automated proof methods. Be careful to only use the proof methods and tactics listed in the coursework description.
Part 2
Quantifier elimination (QE) is a technique for constructing decision procedures for first-order formulas in certain restricted theories.

A QE procedure turns a formula $P$ that contains quantifiers into an equivalent formula $Q$ with no quantifiers and no extra variables. If $P$ had no free variables, then the validity of $Q$ in the theory is (usually) easy to decide. The validity (or not) of $P$ then follows.

This part of the coursework will introduce you to a quantifier elimination procedure for the theory of dense linear orders.

1. Local axiomatic reasoning in Isabelle/HOL
2. Quantifier Elimination for the theory of unbounded DLOs
3. Quantifier Elimination for the theory of bounded DLOs
In Lecture 6, I advocated **definitional** extension of Isabelle over **axiomatic** extension.

Sometimes, we want to reason from axioms *locally*. For example, to prove results about all groups, or all rings, or all vector spaces. We later instantiate the axioms with actual groups, rings, vector spaces.

Isabelle provides a facility for doing this called **locales**.

```isabelle
locale group = 
  fixes mult :: 'a ⇒ 'a ⇒ 'a and unit :: 'a 
  assumes left_unit : mult unit x = x 
  and associativity : mult x (mult y z) = mult (mult x y) z 
  and left_inverse : ∃y. mult y x = unit
```
We can now state lemmas (and theorems and definitions) that are “in” some locale:

```
lemma (in group) associativity_bw :  
  "mult (mult x y) z = mult x (mult y z)"
apply (subst associativity)
apply (rule refl)
done
```
Part 2.1 : Local axiomatic reasoning in Isabelle/HOL

For this coursework, we are interested in the theory of *dense linear orders*:

A dense linear order is some set with:

1. A *less than* relation \( x \sqsubseteq y \), that is transitive (if \( x \sqsubseteq y \) and \( y \sqsubseteq z \) then \( x \sqsubseteq z \)) and irreflexive (it is never the case that \( x \sqsubseteq x \)).
2. It is *linear*: all the elements of the set are arranged along a line. Formally, for any pair \( x, y \), either they are equal or \( x \sqsubseteq y \) or \( y \sqsubseteq x \).
3. It is *dense*: between every pair \( x, y \) such that \( x \sqsubseteq y \), there lies another element \( z \).

An *unbounded* dense linear order is a dense linear order that has no least element and no greatest element.

Examples: \( \mathbb{R}, \mathbb{Q} \). Non-example: \( \mathbb{Z} \).
Part 2.2 : Quantifier Elimination for the theory of DLOs

The first-order theory of unbounded Dense Linear Orders is **decidable** (and hence **complete**):

Given a first-order formula $P$ only containing the atomic predicates equality ($=$) and less than ($<$), there is an algorithm that can decide whether or not $DLO \models P$.

We can implement this procedure by using **quantifier elimination**.

If we can eliminate all the quantifiers from a formula with no free variables, then we have reduced the problem to checking a formula with only propositional connectives and no atomic propositions, which is trivial.
Part 2.2 : Quantifier Elimination for the theory of DLOs

To eliminate all quantifiers from a formula, it suffices to eliminate quantifiers from formulas of the form:

$$\exists x. \, P$$

where $P$ has no quantifiers.

If we can do this, we can work bottom-up through the formula eliminating quantifiers as we go, using the equivalence

$$\forall x. P \equiv \neg (\exists x. \neg P).$$
We can make the problem of QE for $\exists x. P$ even easier if we arrange things so that if is of the form (where each $a_{i,j}$ is an atomic predicate $y = z$ or $y < z$):

$$\exists x. (a_{1,1} \land \ldots \land a_{m_1,1}) \lor \ldots \lor (a_{1,n} \land \ldots \land a_{m,n,n})$$

because this is equivalent to:

$$(\exists x. a_{1,1} \land \ldots \land a_{m_1,1}) \lor \ldots \lor (\exists x. a_{1,n} \land \ldots \land a_{m,n,n})$$

The form $\bigvee_i \bigwedge_j a_{i,j}$ is called **Disjunctive Normal Form (DNF)**.
Part 2.2 : Quantifier Elimination for the theory of DLOs

Convert to Disjunctive Normal Form by bottom-up translation.

By assumption, there are no quantifiers, and $P \rightarrow Q \equiv \neg P \lor Q$.

For the other connectives:

1. Atoms $(y = z)$ and $(y < z)$ are already in DNF
2. If $P$ and $Q$ are in DNF, then $P \lor Q$ is in DNF
3. If $P$ and $Q$ are in DNF, then:

   \[ P \land Q \equiv \left( \bigvee_{i} C_{i} \right) \land \left( \bigvee_{j} D_{j} \right) \equiv \bigvee_{i} \left( C_{i} \land \bigvee_{j} D_{j} \right) \equiv \bigvee_{i,j} \left( C_{i} \land D_{j} \right) \]

4. If $P$ is in DNF, then

   \[ \neg P \equiv \neg \left( \bigvee_{i \ j} a_{i,j} \right) \equiv \bigwedge_{i} \neg \left( \bigwedge_{j_{i}} a_{i,j} \right) \equiv \bigwedge_{i} \bigvee_{j_{i}} \neg a_{i,j} \]

which is not in DNF (it is CNF), so use previous three points to convert to DNF. But we also need to negate atoms...
Part 2.2: Quantifier Elimination for the theory of DLOs

To translate negation into DNF, we needed to negate atoms:

\[ \neg(y = z) \qquad \neg(y < z) \]

But to be in DNF, we are not allowed negation, only atoms!

Fortunately, in the theory of DLOs, we have the following equivalences:

1. \[ \neg(y = z) \iff (y < z \lor z < y) \]
2. \[ \neg(y < z) \iff (y = z \lor z < y) \]

**Question:** prove these statements in the theory of DLOs, in Isabelle/HOL. (8 marks)
Part 2.2 : Quantifier Elimination for the theory of DLOs

We have reduced QE to formulas of the form:

$$\exists x. a_1 \land \ldots \land a_m$$

Divide the $a_i$ into those which contain $x$ and those that don’t:

$$(b_1 \land \ldots \land b_{n_1}) \land (\exists x. c_1 \land \ldots \land c_{n_2})$$

If $x = x$ occurs in the $c_i$, then just remove it.

If $x < x$ occurs in the $c_i$, then $P \equiv \bot$, so we are done.

If $x = y$ or $y = x$ occurs in the $c_i$, then we can eliminate $x$ by replacing it with $y$:

$$(\exists x. (x = y) \land c_1 \land \ldots \land c_{n_2}) \equiv (c_1[y/x] \land \ldots \land c_{n_2}[y/x])$$
If $x < x$ does not occur, and there are no equalities involving $x$, we have reduced the problem to eliminating the quantifier from formulas of the following form:

$$\exists x. \left( \bigwedge_i s_i < x \right) \wedge \left( \bigwedge_j x < t_j \right)$$

where none of the $s_i$ or $t_j$ are $x$.

In the theory of DLOs, this formula is equivalent to:

$$\bigwedge_{i,j} s_i < t_j$$

And the quantifier vanishes!
Question: Prove this equivalence:

\[
\left( \exists x. \left( \bigwedge_i s_i < x \right) \land \left( \bigwedge_j x < t_j \right) \right) \equiv \bigwedge_{i,j} s_i < t_j
\]

This proceeds in three stages, reasoning in the theory of DLOs:

1. Every finite set has a minimum element;
2. Every finite set has a maximum element;
3. If there are two sets \( L \) and \( U \), then: every element of \( L \) is less than every element of \( U \) if and only if there exists an \( x \) that is greater than all of \( L \) and less than all of \( U \).
Part 2.3 : Quantifier Elimination for bounded DLOs (12 marks)

The final question asks you to describe the adaptation of the quantifier elimination procedure to *bounded* DLOs.

1. Describe, in English, what needs to be changed from the procedure for unbounded DLOs.
2. State and prove the relevant lemmas in Isabelle/HOL.

*Hint*: look through your proofs, and make a note of where the assumptions of unboundedness are used.
Some notes on Quantifier Elimination

You are not asked to implement the QE procedure. Though you can if you want to.

The quantifier elimination procedure described here has appalling complexity. Each negation in the original formula produces an exponential blow-up in the size of the formula, leading to a complexity of

\[ O\left(2^{2^2 \ldots 2^n}\right) \]

where \( n \) is the size of the original formula, and \( m \) is the number of negations. Treating \( \forall x. P \) as \( \neg \exists x. \neg P \) makes this even worse.

Decidability for DLOs is known to be PSPACE-complete (Kozen, 2006).

As far as I know, the best quantifier elimination procedure for DLO is \( O(n!) \), by Nipkow.
Some Hints on Proving in Isabelle/HOL
Hints and tips on Proving in Isabelle/HOL

1. Before attempting a complex proof, try a proof on paper first

2. A general heuristic for natural deduction proofs:
   ▶ Look at the goal. Is there an introduction rule that applies?
   ▶ Look at the assumptions. Would it be useful to use an elimination rule?
   ▶ Use the _tac variants of rules to specify how to instantiate the variables to avoid too many meta-variables.
   ▶ Is there another lemma or theorem that might be useful? use cut_tac or insert.
   ▶ Is there another formula $P$ that you can prove from the current assumptions that might be useful in proving the final goal? use subgoal_tac.

3. Use oops or sorry if you are stuck, to move on. (sorry treats the lemma as an axiom for the rest of the file, oops does not)
If you get stuck

1. Demonstrator hours (AT5.05):
   - 2pm to 4pm Thursdays
   - 2pm to 4pm Fridays

2. Ask me directly bob.atkey@ed.ac.uk

3. Ask on the course mailing list ar-students@inf.ed.ac.uk
Good luck!