Automated Reasoning 2019/2020

Assignment: Theorem Proving in Isabelle

Jacques Fleuriot Imogen Morris

October 17, 2019

Introduction

The practical assignment for students on the Automated Reasoning course involves theorem proving in Isabelle. You will be required to formalise a few axioms about a *geometry of sections* and then combine these with the rules of logic to mechanically prove a number of geometric theorems.

Isabelle

Isabelle is a generic interactive theorem prover. This means that Isabelle can be used to formalise theorems in various logics. For this practical, you will be using Isabelle/HOL, which is the higher-order logic of Isabelle. To get started, download the file Practical.thy from:

`http://www.inf.ed.ac.uk/teaching/courses/ar`

Essential Reading

As you will be using Isabelle interactively, you will need to be familiar with the system before you start. Formal mathematics is not trivial! You will find this assignment much easier if you attend the lectures, attempt the various Isabelle exercises given on the course webpages, and ask questions about using Isabelle before you start. It is recommended that you read Chapter 5 of the Isabelle/HOL tutorial located at:

`http://www.cl.cam.ac.uk/research/hvg/Isabelle/documentation.html`

Some Useful Commands

Isabelle has many commands which will help you mechanise the theorems in this practical. You should refer to the Isabelle tutorial and lectures to discover the commands available. One of the built-in methods you should be aware of is called auto. It uses both the *classical reasoner* and simplifier of Isabelle. The command **apply** auto tells Isabelle to apply auto to all subgoals. You are only allowed to use this command in Parts 2 and 3 of the practical.

If you are struggling to mechanise a lemma or theorem in Isabelle, then the command sorry can be used. This allows the lemma or theorem to be asserted as true without completing the proof. It will enable you to make progress in the practical, however no marks will be allocated for the missing part of the proof. You should not use other people's proofs or formalisations.

Structure of this document

The tasks are divided into three parts: propositional and first order logic, formalisation of a geometry of sections and finally a more challenging set of proofs from the same geometry. All tasks that you are required to do are enclosed in boxes.

Part 1: Some propositional and first-order proofs [25%]

For the first part of this assignment, you should attempt to prove a number of simple propositional and first-order statements in Isabelle. You should keep your proofs as simple as possible e.g. avoid using classical if it is not necessary and avoid circular reasoning.

For this part of the assignment use only the following proof methods: rule, rule_tac, drule, drule_tac, erule, erule_tac, frule, frule_tac and assumption. You are also restricted to using only the following Natural Deduction rules: conjI, conjE, impI, impE, mp,notI, iffE, notI, notE, disjI1, disjI2, disjE, exI, exE, allI, allE and spec. You are also allowed to use classical and ccontr.

Attempt proofs of the following statements:

- $A \vee A \longrightarrow A$ (1 mark)
- $(P \longrightarrow R) \longrightarrow (\neg P \vee R)$ (1 mark)
- $(P \wedge Q \longrightarrow R) \longrightarrow P \longrightarrow Q \longrightarrow R$ (1 mark)
- $\neg\neg P \vee \neg P$ (3 marks)
- $(P \vee R) \longleftrightarrow (\neg(\neg P \wedge \neg R))$ (4 marks)
- $((\forall x.\ F\ x) \wedge (\forall x.\ G\ \mathrm{x})) \longrightarrow (\forall x.\ F\ x \wedge G\ x)$ (1 mark)
- $(\forall x\ y.\ R\ x\ y) \longrightarrow (\forall x.\ R\ x\ x)$ (1 mark)
- $(\forall x.\ P\ x) \vee (\exists x.\ \neg P\ x)$ (3 marks)
- $(\forall x.\ \neg(P\ x \longrightarrow Q\ x)) \longrightarrow \neg(\exists x.\ \neg P\ x \wedge Q\ x)$ (3 marks)
- $(\exists \mathrm{Bob}.\ (\mathrm{drunk\ Bob} \longrightarrow (\forall x.\ \mathrm{drunk}\ x))$ (3 marks)
- $\neg(\exists \mathrm{barber}.\ \mathrm{man\ barber} \wedge (\forall x.\ \mathrm{man}\ x \wedge \neg\ \mathrm{shaves}\ x\ x \leftrightarrow \mathrm{shaves\ barber}\ x))$ (4 marks)

Part 2: A Geometry of Sections [55%]

In Part 2, you can use Isabelle's automatic tools (such as simp, auto, blast) in your proofs. However, you may **not** use smt, metis, meson, presburger and moura

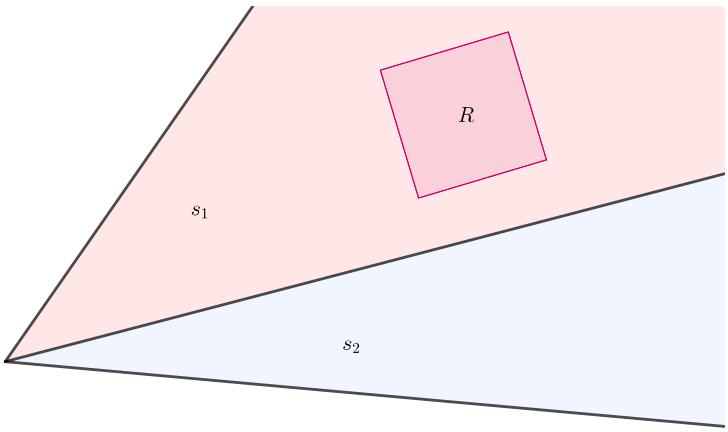

Figure 1: Here s_1 and s_2 represent sections which together could be said to form a bundle and R represents a region.

In some work on qualitative geometry, Kulik et al. present a formal *axiomatic* framework dealing with sections [1]. This work introduces points (denoted by P), regions (denoted by R, R'), sectors, sections (denoted by s, s') and bundles (denoted by σ by Kulik et al. and b by us) as primitive geometric entities (structures) and primitive relations, namely, *incidence* and *crossing*. A number of basic definitions and axioms are then given to characterise the relationships between these various primitive entities. The motivation for the work is being able to compare the positions of various objects without a coordinate system. Hence Kulik et al. define several pre-orders.

In this assignment, your task is to formalise part of this axiomatic framework and mechanically prove a number of theorems as given in the paper [1]. Your work will thus provide a rigorous, mechanical verification of some

of the claims made by Kulik et al.

Using your formalised definitions and axioms, you will mechanise (in your theory file) a number of resulting properties taken from Kulik et al.'s paper. You may be required (or find it helpful) to prove additional lemmas, not explicitly mentioned and/or named in the paper, to facilitate your mechanisation task. Express your lemmas in the style **assumes** $\cdots$ **shows**. You are expected to give readable, structured Isar proofs. It is acceptable to give one-line proofs of theorems (e.g. **by** auto) unless otherwise indicated. You should also not use the automatically generated Isar proofs.

Drawing pictures of some of the objects may help you to solve some of the problems. Kulik et al. depict regions as rectangles or ovals, sections as cone-shaped areas, and bundles of sections as cones with the same endpoint (see Figure 1). However, you are free to represent them as any objects which satisfy the axioms.

2.1 Mechanizing the incidence locale (12 marks)

We have split Kulik and Eschebach's theory into several locales, each of which imports the previous one. We begin with a locale which introduces sections and regions, as well as the incidence relation. Kulik et al. state that sections are either regions or sectors. In Isabelle, we use separate type variables for 'region and 'section which is why we need to introduce the coercion (or embedding) function region_to_section that allows us to use regions with functions which take sections as arguments. We found that Kulik et al. were inconsistent in their usage of section/sector, so we blend these two concepts into a single type 'section.

```
locale incidence =
  fixes incidence_points_on_sections :: "'point ⇒ 'section ⇒ bool"
  (infix "ι_point" 80)
  fixes region_to_section :: "'region ⇒ 'section"
  and section_nonempty:
  and section_uniqueness:
```

The binary incidence relation is also given in the locale. The predicate takes two arguments and represents the notion of a point being in a section. It has been declared as an *infix* predicate, so you can express that a point P is in the section s by P ι_{point} s. In the template file Practical.thy, you have

been provided with the declared, but not yet defined, predicates isPartOf (representing the $\subseteq$ given by Kulik et al.), isIncludedIn, overlaps. These are slightly more readable names – using infix notations whenever possible – for the predicates used by Kulik et al. (e.g. we can specify that a point R is included in a section s as R isIncludedIn s instead of i(R,s)).

Your tasks are to:

1. Formalise an axiom stating that every section has a point incident to it. This should go in the incidence locale. This is not given by Kulik et al. but we found it necessary for the proofs. (2 marks)

2. Formalise an axiom stating that two sections are the same if the same points are incident to each. This should go in the incidence locale. Again, this is not given by Kulik et al. but is necessary for certain proofs. (2 marks)

3. Formalise Definitions D1-D3 from Kulik et al.'s paper [1] in the locale context. (3 marks)

4. Give a structured proof of region_overlaps_itself which states that a region overlaps itself. Make sure your proof forms an explanation why the theorem is true. (2 marks)

5. Formalise and prove that isPartOf is a reflexive, transitive and anti-symmetric relation. (3 marks)

2.2 Mechanizing the section_bundles locale (5 marks)

The locale section_bundles imports the incidence locale. The structure of the locale has already been given, so you only need to add the axioms. Notice that we introduce another kind of incidence denoted by ι_{section}. Kulik et al. use the same notation for incidence of points on sections and incidence of sections on bundles, but as we use types, we separate these two kinds of incidence.

Your tasks are to:

1. Formalise the axioms SC1 and SI1 within the locale. (2 marks)

2. Kulik et al. introduce a new order relation 'at least as restrictive as' at the beginning of Section 2.2 in Definition D4:

   i) Add the definition of atLeastAsRestrictiveAs into the locale context. (1 mark)

   A convenient infix notation is provided below the definition:

   ```
   notation atLeastAsRestrictiveAs ("_ ≤_ _" [80, 80, 80] 80)
   ```

   Notice that the direction of $\leq$ is different from that given by Kulik et al. in their paper. This is because saying 'R is at least as restrictive as R'' implies that R is 'smaller' than R', not 'greater', as Kulik et al.'s notation would imply.

   ii) Use this notation to formalise and prove that the relation atLeastAsRestrictiveAs is reflexive, transitive and antisymmetric. Reflexivity is given for you. (2 marks)

2.3 Mechanising the comparison locale (4 marks)

Your tasks are to:

1. Formalise Axioms SB2 from Kulik et al.'s paper [1] within the locale. (1 marks)

2. Formalise and prove Theorems T1 and T2 in the locale context. (2 marks)

We formalise the definition of core as follows

```
definition isCore ( infix "isCoreOf" 80) where
"s isCoreOf b = (s ι_section b ∧(∀s'. s' ι_section b ⟹s ≤_b s'))"
```

Note that the property of being a core is defined using an = symbol by Kulik et al. in their article. Although this is a convenient notational device

for the paper, this is not advisable in our formalization as (among many other issues) = is already defined in Isabelle. So, we explicitly define a new relation isCoreOf such that s is the core of b, i.e. $s = core(b)$, is denoted by s isCoreOf b. Note also that one often has to make such representational choices (e.g. relational vs. functional) when dealing with the mechanization of a (pen-and-paper) framework.

3. Given the definition of core, now define hull, making an analogous representational choice. (1 mark)

2.4 Mechanising the crossing_sector locale (34 marks)

In this locale, we do not introduce any new relation. We have a separate locale only so that we could demonstrate that T1 and T2 do not depend for their proofs on Axiom SC2.

Your tasks are to:

1. Formalise Axiom SC2 in this locale. (1 mark)

2. Formalise and prove the following remarks given by Kulik et al. in this locale as three separate lemmas:

   Employing (T1), (T2), and the axiom (SC2), we obtain the following results for the core and the hull of a section bundle:

   - If a region overlaps the core of a section bundle then it overlaps every section of the section bundle. (4 marks)
   - If a region crosses the hull of a section bundle then it crosses every sector of the section bundle. (4 marks)
   - If a region does not overlap the hull of a section bundle, it does not overlap any of its sections. (4 marks)

Make sure your proofs are structured Isar proofs of more than one line so that the proofs form explanations for why the theorems are true.

We now introduce one of the partial orderings defined by Kulik et al. in their paper. In your theory file you will find overlapsAsMuchAs (and

eq_overlapsAsMuchAs and the strict version more_overlapsAsMuchAs). This relation corresponds to $\geq_o$ ('overlaps as much as') from the paper. Since it would be repetitive, we do not define all the partial orders mentioned in the paper. We also introduce abbreviations for the symmetric versions of all of these e.g. rev_overlapsAsMuchAs and its notation. But since these are simply pretty-printing, any lemmas involving rev_overlapsAsMuchAs can be proven using exclusively facts about overlapsAsMuchAs. Kulik et al. state that $\geq_o$ is a linear pre-order, i.e. it is reflexive, transitive and any two regions can be compared using it.

Your tasks are to:

1. Formalise and prove that the relation $\geq_o$ is reflexive and transitive. This shows that $\geq_o$ is a pre-order. (2 marks)
2. Formalise and prove Theorem T4. (1 mark)
3. Formalise T5 and write a structured proof using Theorem T4 in the proof. Theorem T5 shows that $\geq_o$ is linear. (3 marks)

Kulik et al. give only one proof in their paper, namely that of Theorem T3.

You are now required to formalise and prove Theorem T3.

4. Give a structured proof of both directions of the if-and-only-if. For the direction "$\Leftarrow$", make sure that you follow the proof given by Kulik et al. (11 marks)
5. In under 200 words, compare and contrast the mechanical proof that you produced with Kulik et al.'s pen-and-paper proof. In particular, indicate any reasoning, proof parts, and/or useful lemmas that you had to make explicit during the mechanisation but may have been glossed over or assumed by the pen-and-paper proof. Also highlight any inaccuracies in their language or notation. Note any parts where you had to diverge from their reasoning, and why.

   (4 marks)

Part 3: Challenge Problem [20%]

In Section 2.4 of their paper, Kulik et al. prove some facts about the relations $\geq_{\mathsf{ci}}$ and $\geq$ (i.e. 'crosses or is included as much as' and 'belongs as much as') given certain simplifying assumptions. For this part you are allowed to use any proof method including those which may appear by the invocation of sledgehammer, apart from smt.

Your tasks are to:

1. Formalise the relation ci between regions and sections, which Kulik et al. state as 'a region crosses or is included in a section'. This is mentioned at the end of the first paragraph of Section 2.1 of their paper. (2 marks)

2. Formalise the relation $\geq_{\mathsf{ci}}$ ('crosses or is included as much as') which Kulik et al. tell us is defined analogously to $\geq_{\mathsf{o}}$ ('overlaps as much as'). This is described just after Definition D7. Define suitable infix notation. (2 marks)

3. Formalise the relation $\geq$ ('belongs as much as') given in Definition D8 of Kulik et al.'s paper. Define suitable infix notation. (2 marks)

4. Formalise and prove Theorems T6-T8 for both the relation $\geq_{\mathsf{ci}}$ and the relation $\geq$. Give structured proofs which serve as an explanation for why the theorems are true. (14 marks)

You can put all of this into the context of the final locale crossing_sector.

Demonstrator Hours and Help

The demonstrator, Imogen Morris (s1402592@ed.ac.uk), will be available to give advice on Mondays, 9am-11am in 4.12, Appleton Tower.

You are strongly encouraged to make use of the Piazza forum for discussion of general problems and for sharing any queries that you may have.

Important. Note that, although we encourage discussions about the assignment, you must **not** discuss or share actual proof scripts (i.e. solutions) for any of the problems with fellow students.

Submission

By 4pm on 18th November 2019 you must submit your solution in electronic form. This should consist of your theory file Practical.thy and can be submitted using the command:

```
submit ar cw1 Practical.thy
```

Late coursework will be penalised in accordance with the Informatics standard policy (see `http://edin.ac/1LRblYG`). Please consult your course guide for specific information about this. Also note that, while we encourage students to discuss the practical among themselves, we take plagarism **seriously** and any suspected case will be treated appropriately. Please remember the University requirements as regards all assessed work. Details about this can be found at:

`http://web.inf.ed.ac.uk/infweb/admin/policies/academic-misconduct`

Furthermore, you are required to take reasonable measures to protect your assessed work from unauthorised access. For example, if you put any such work on a public repository then you must set access permissions appropriately (permitting access only to yourself).

References

[1] Lars Kulik, Carola Eschenbach, Christopher Habel, and Hedda Rahel Schmidtke. A graded approach to directions between extended objects. In Max J. Egenhofer and David M. Mark, editors, *Geographic Information Science*, pages 119–131, Berlin, Heidelberg, 2002. Springer Berlin Heidelberg. `http://www.inf.ed.ac.uk/teaching/courses/ar/SectionGeometry.pdf`.