Automated Reasoning 2020/2021

Assignment: Theorem Proving in Isabelle

Jake Palmer Imogen Morris Jacques Fleuriot

March 8, 2021

Introduction

The practical assignment for students on the Automated Reasoning course involves theorem proving in Isabelle. You will be required to formalise some axioms and definitions about a *geometry of regions* 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:

`Learn` → `Assessment` → `Assignment: Theorem Proving in Isabelle`

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 regions and finally a more challenging set of tasks 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 if it is not necessary and avoid circular reasoning. You should not prove any additional helper lemmas, though you may make use of the earlier lemmas to help prove the later ones.

For this part of the assignment use only the following proof methods: rule, rule_tac, drule, drule_tac, erule, erule_tac, frule, frule_tac, cut_tac and assumption.

You are also restricted to using only the following Natural Deduction (ND) rules: conjI, conjE, impI, impE, mp, iffI, iffE, notI, notE, disjI1, disjI2, disjE, exI, exE, allI, allE and spec.

Attempt proofs of the following statements, without using ccontr, classical, notnotD nor excluded_middle.

- $A \vee A \longleftrightarrow A$ (1 mark)
- $A \wedge A \longleftrightarrow A$ (1 mark)
- $(\neg\ P \vee R) \longrightarrow (P \longrightarrow R)$ (1 mark)
- $(\exists x.\ P\ x \wedge Q\ x) \longrightarrow (\exists x.\ P\ x) \wedge (\exists x.\ Q\ x)$ (1 mark)
- $(\neg\ (\exists x.\ \neg\ P\ x) \vee R) \longrightarrow ((\exists x.\ \neg\ P\ x) \longrightarrow R)$ (1 mark)
- $(\forall x.\ P\ x) \longrightarrow \neg\ (\exists x.\ \neg\ P\ x)$ (2 marks)

Prove the following, using any of the ND rules mentioned above, but only one of the classical rules given next to the statement in square brackets:

- $P \vee \neg\ P$ [only ccontr] (3 marks)
- $\neg\neg\ P \Longrightarrow P$ [only excluded_middle] (3 marks)
- $(\neg\ P \Longrightarrow P) \Longrightarrow P$ [only notnotD] (3 marks)
- $(\neg\ P \Longrightarrow \bot) \Longrightarrow P$ [only classical] (3 marks)

You may use any of the previously proven rules including excluded_middle, classical, notnotD and ccontr in the following proofs:

- $(\neg\ (\forall x.\ P\ x \vee R\ x)) = (\exists x.\ \neg\ P\ x \wedge \neg\ R\ x)$ (3 marks)
- $(\exists x.\ P\ x \vee R\ x) = (\neg\ ((\forall x.\ \neg\ P\ x) \wedge \neg\ (\exists x.\ R\ x)))$ (3 marks)

Part 2: A Geometry of Regions [55%]

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

In some work on qualitative geometry, Bennett et al. present a formal *axiomatic* framework dealing with regions [3, 2, 1]. This work introduces regions as primitive geometric entities and primitive relations, namely, *parthood* and *sphere*. A number of basic definitions and axioms are 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 and without taking the traditional entities of points, lines, etc. as primitive. They also provide a description of qualitative kinematics in this framework, which is outside the scope of this coursework.

In this assignment, your task is to formalise part of this axiomatic framework and mechanically prove a number of theorems as given in the handout and the companion document – Summary Description of Region Based Geometry – to this assignment. Your work will thus provide a rigorous, mechanical verification of some of the claims made by Bennett et al. in their papers.

As part of your mechanisation, you may be required (or find it helpful) to prove additional lemmas, not explicitly mentioned and/or named in the theory file. Express your lemmas in the style **assumes** ... **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. Ensure that none of your structured Isar proofs starts with any applications of apply[1], and that they are not solved by a single command. This is to ensure that the proofs form explanations for why the theorems are true.

2.1 Mechanizing the mereology locale (7 marks)

Please see the Summary Description document at `Learn` → `Assessment` → `Assignment: Theorem Proving in Isabelle` for a description of the mereological and region based geometry definitions and axioms.

We have split Bennett et al.'s theory into several locales. We begin with one that introduces *parthood* as well as a set of regions represented simply by the type variable 'region. We will use this to define our basic mereological notions.

[1] Using rule applications to begin a proof like so is fine: proof (rule allI, rule impI)

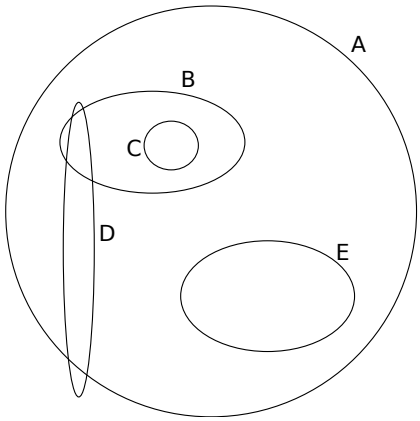

Figure 1: Consider what mereological relations the regions A, B, C, D, and E are in with respect to parthood and the following definitions.

locale partof =
  fixes partof :: "'region ⇒ 'region ⇒ bool" (infix "⊑" 100)

The binary parthood relation takes two arguments and represents the notion of one region being a part of another. It has been declared as an *infix* predicate, so you can express that a region r is a part of the region s by $r \sqsubseteq s$. In the template file Practical.thy, you have been provided with the declared, but not yet defined, predicates properpartof, overlaps, partialoverlap, sumregions.

Your tasks are to:

1. Formalise the four primary mereological relations: properpartof, overlaps, partialoverlap, and sumregions. You may consult the companion document for these definitions. (4 mark)

2. Formalise the axiom A1, the transitivity of the parthood relation. (1 mark)

3. Formalise the axiom A2, which states that for every non-empty set of regions, combining (or "summing") these regions gives you another region. (1 mark)

4. Formalise the axiom A2', which states that only one region can be the outcome of a combination of regions.
(1 mark)

Your formalization should give your axioms in sequent form by separating the premises and conclusion, wherever appropriate, using Isabelle's meta implication $\Longrightarrow$.

2.2 Mechanizing some mereology proofs (32 marks)

The axioms and definitions you have provided are enough to prove all the standard theorems of mereology. For the rest of this part, we will be:

- Proving that parthood is a partial order.
- Proving other miscellaneous theorems.

In Isabelle/HOL, if one proves that a relation is a partial order, all of the theorems proven about partial orders generally will become available for later proofs, and automated tools like auto will be able to leverage this. If the theorem is not already stated you must translate the description into assumes ... shows style in Isabelle.

First, as a warm-up:

Using an apply-style proof and any of the rules from Part 1, prove:

The relation overlaps is a symmetric relation. (2 marks)

Next:

Your tasks are to state and prove, using structured proof style:

1. A member of a set of regions is part of the region the set sums to.
(1 mark)

2. The relation overlaps is a reflexive relation. Use a structured proof style. For full marks, you should make use of sumregions.
(3 marks)

3. Every region has some part. (1 mark)

4. A region's parts also overlap it. Your mechanised proof should follow the same argument as that given in Section 4 of the companion document. (2 marks)

5. The sum of all parts of a region x is x. (1 mark)

6. If a given relation r satisfies certain relationships to mereological notions, and summing the single region y gives x, one can also sum over the relation r y to produce x. This statement has already been formalised for you in the Isabelle file. (2 marks)

7. If e overlaps f, there is a region which is part of e and overlaps f. (1 mark)

8. Summing a single region is the same as summing its parts. Prove this by instantiating the relation in sum_relation_is_same with an appropriate lambda expression. (1 mark)

9. If two regions are part of each other, they are equal. Your mechanised proof should follow the same argument as that given in Section 4 of the companion document. (5 marks)

10. Summing each region z where all parts of z overlap y is the same thing as summing y alone. Your mechanised proof should follow the same argument as that given in Section 4 of the companion document. (4 marks)

11. Summing a single region x is x. Start your structured proof by obtaining some y which is the sum of x. (2 marks)

12. Summing every region z where all parts of z overlap x is x. (2 marks)

13. If a region s is a proper part of a region r, there is a proper part of r which does not overlap s. (4 marks)

14. Prove that parthood is a partial order by using sledgehammer on each goal of the sublocale parthood_partial_order. (1 mark)

2.3 Mechanizing some region based geometry proofs (16 marks)

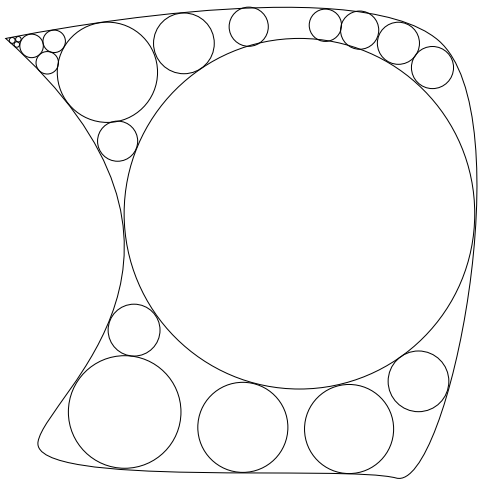

Figure 2: A partial covering of a region using its spherical parts.

Your tasks are to state and prove:

1. Concentricity of spheres is an equivalence relation. (2 marks)
2. Every region x is the sum of its spherical parts. See Figure 2. [a] (5 marks)
3. A sphere s is centred on an interior point of r if and only if there exists a sphere s' in r on which s is also centred. (1 marks)
4. If x and y have equal interiors, they are the same regions. The lemma parthood_partial_order.antisym and the axiom A8 makes this proof simple. Give a one sentence explanation in a comment above the theorem why, out of all the axioms of mereology and region based geometry, only Axiom A8 is needed for the proof. (2 marks)
5. If s is a proper part of r, there is a sphere which is a proper part of r that does not overlap s. Make sure to give a structured proof that

shows your reasoning. (2 marks)

6. If a region is not a sphere, then it contains at least two spherical parts. Make sure to give a structured proof that shows your reasoning.

(4 marks)

[a] Hint: you may approach this by obtaining a region which the spherical parts of x sum to, and then prove the goal by contradiction.

Part 3: Challenge Problems [20%]

With the definitions and axioms presented by Bennett et al. we cannot yet leverage a standard points-based axiom system for geometry as doing so introduces an *inconsistency*. Your task is to investigate this inconsistency. You may **not** use method smt.

1. Derive a contradiction using Axiom A9 and the Tarskian axiom T4. The statement of the lemma has been provided for you. You should produce a readable structured proof with no supurfluous variables. Consider starting by making use of A9. The issue arises due to the definition of equidistant3, so this will need to be involved in your proof.[a] (3 marks)

2. Fix the definition of equidistant3, ensuring that one can still conclude that if the predicates are true, then all the arguments are spheres. Briefly explain in 2-3 sentences in a comment above one of the definitions what the issue was and how your change fixes it.

(3 marks)

[a] Reflexivity of parthood may be used to derive the contradiction (i.e. False) though its invocation may be hidden by the automated proof tools because we have already proven parthood is a partial order in the previous part.

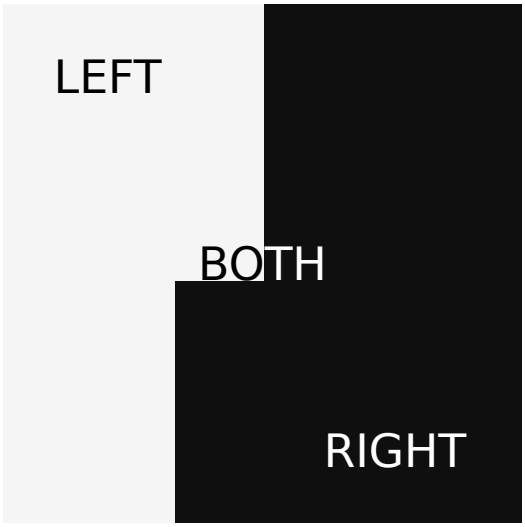

Figure 3: The smallest non-trivial mereology, consisting of the regions LEFT and RIGHT, as well as BOTH, the "universal region", as every other region is a part of it.

Finally, you will be constructing the smallest non-trivial mereology (see Figure 3), which consists of two regions and their sum, and proving that it satisfies the mereological axioms.

Your tasks are:

1. Implement the parthood relation tworeg_partof for the datatype two_reg. The datatype has been provided for you. (2 marks)
2. Prove that the type two_reg along with the parthood relation defined on it satisfy the axioms of mereology by using Isabelle's interpretation mechanism. (12 marks)

You will find information on working with datatypes and interpretations in the coursework lecture (and other AR lectures).

Demonstrator Hours and Help

The demonstrators, Imogen Morris (s1402592@sms.ed.ac.uk) and Jake Palmer (jake.palmer@ed.ac.uk), will be available to give advice on Teams on **Mondays, 9am-11am**, and **Tuesdays, 16:10pm-18:00pm** respectively.

You are also 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 22nd March 2021 you must submit your solution in electronic form. This should consist of your theory file Practical.thy and can be submitted under `Learn` → `Assessment`.

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.

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] Brandon Bennett. A categorical axiomatisation of region-based geometry. *Fundamenta Informaticae*, 46(1-2):145–158, 2001.

[2] Brandon Bennett, Anthony G Cohn, Paolo Torrini, and Shyamanta M Hazarika. A foundation for region-based qualitative geometry. In *ECAI*, pages 204–208, 2000.

[3] Brandon Bennett, Anthony G Cohn, Paolo Torrini, and Shyamanta M Hazarika. Region-based qualitative geometry. *University of Leeds, School of Computer Studies, Research Report Series, Report*, 2000.