Automated Reasoning

Lecture 6: Representation

Jacques Fleuriot
jdf@inf.ed.ac.uk

Recap

- Last time: First-Order Logic
- This time: Representing mathematical concepts

Representing Knowledge

So far, we have:

- Seen the primitive rules of (first-order) logic
- Reasoned about abstract Ps, Qs, and Rs

But we usually want to reason in some mathematical theory. For example: number theory, real analysis, automata theory, euclidean geometry, ...

How do we **represent** this theory so we can prove theorems about it?

- **Which logic do we use?** — Propositional, FOL, Temporal, Hoare Logic, HOL?
- Do we **axiomatise** our theory, or **define** it in terms of more primitive concepts?
- What style do we use? *e.g.* **functions** vs. **relations**

Further Issues

What are the important theorems in our theory?

- Which formalisation is most useful?
- Is it **easy to understand**?
- Is it **natural**?
- How easy is it to **reason** with?

Often a matter of taste, or experience, or tradition, or efficiency of implementation, or following the idioms of the people you are working with. No single right way!

Granularity of the representation

- What primitives do we need? Consider geometry:
  - Define lines in terms of points? (Tarksi)
  - Or take points and lines as primitive? (Hilbert)
- Or computing; should we treat programs as:
  - State transition systems? (operational)
  - Functions mapping inputs to outputs? ($\sim$ denotational)

Axioms vs. Definitions

Let's say we want to reason using the natural numbers $\{0, 1, 2, 3, \ldots\}$

Axiomatise? Assume a collection of function symbols and *unproven axioms*. For instance, the Peano axioms:

$$\begin{array}{l} \forall x.\ \neg(0 = S(x)) \\ \forall x.\ x + 0 = x \\ \forall x.\ x + S(y) = S(x + y) \\ \ldots \end{array}$$

Define? If our logic has sets as a primitive (or are definable), then we can *define* the natural numbers via the von Neumann ordinals:

$$0 = \emptyset, 1 = \{\emptyset\}, 2 = \{\emptyset, \{\emptyset\}\}, \ldots$$

Then we can *prove* the Peano axioms for this definition.

Axioms vs. Definitions

Axiomatisation:

- (+) Sometimes less work – finding a good definition, and (formally) working with it can be hard.
- (-) How do we know that our axiomatisation is adequate for our purposes, or is complete?
- (-) How do we know that our axiomatisation is consistent? Can we prove $\bot$ from our axioms (and hence everything)?

Definition:

- (-) Can be a lot of work, sometimes needing some ingenuity.
- (+++) If the underlying logic is consistent, then we are *guaranteed* to be consistent (c.f., "Why should you believe Isabelle" from Lecture 4). We have **relative consistency**.

Axiomatisation, an example: Set Theory

Let's take FOL, a binary atomic predicate $\in$ and the following axiom for every formula P with one free variable x:

$$\exists y.\ \forall x.\ x \in y \leftrightarrow P(x)$$

"For every predicate P there is a set y such that its members are exactly those that satisfy P"

We can now define empty set, pairing, union, intersection...

Axiomatisation, an example: Set Theory

Let's take FOL, a binary atomic predicate $\in$ and the following axiom for every formula P with one free variable x:

$$\exists y.\ \forall x.\ x \in y \leftrightarrow P(x)$$

"For every predicate P there is a set y such that its members are exactly those that satisfy P"

We can now define empty set, pairing, union, intersection…

But it is **too powerful!** Let $P(x) \equiv \neg(x \in x)$. Then by the axiom there is a y such that:

$$y \in y \leftrightarrow y \notin y$$

This is **Russell's paradox**.

Axiomatisation, an example: Set Theory

Let's take FOL, a binary atomic predicate $\in$ and the following axiom for every formula P with one free variable x:

$$\exists y.\ \forall x.\ x \in y \leftrightarrow P(x)$$

"For every predicate P there is a set y such that its members are exactly those that satisfy P"

We can now define empty set, pairing, union, intersection...

But it is **too powerful!** Let $P(x) \equiv \neg(x \in x)$. Then by the axiom there is a y such that:

$$y \in y \leftrightarrow y \notin y$$

This is **Russell's paradox**.

Background: the axiom is called "unrestricted comprehension", it was replaced by:

$$\forall z.\ \exists y.\ \forall x.\ (x \in y \leftrightarrow (x \in z \wedge P(x)))$$

+ some other axioms to give ZF set theory.

Building up Definitions: Integers

Starting from the natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$, we can define:

- each integer $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ as an **equivalence class** of pairs of natural numbers under the relation $(a, b) \sim (c, d) \iff a + d = b + c$;
- For example, -2 is represented by the equivalence class $[(0, 2)] = [(1, 3)] = [(100, 102)] = \ldots$.
- we define the sum and product of two integers as

$$\begin{aligned} [(a, b)] + [(c, d)] &= [(a + c, b + d)] \\ [(a, b)] \times [(c, d)] &= [(ac + bd, ad + bc)]\,; \end{aligned}$$

- we define the set of **negative** integers as the set $\{[(a, b)] \mid b > a\}$.
- Exercise: show that the product of negative integers is non-negative.

Other Representation Examples

- The rationals $\mathbb{Q}$ can be defined as pairs of integers. Reasoning about the rationals therefore reduces to reasoning about the integers.
- The reals $\mathbb{R}$ can be defined as sets of rationals. Reasoning about the reals therefore reduces to reasoning about the rationals.
- The complex numbers $\mathbb{C}$ can be defined as pairs of reals. Reasoning about the complex numbers therefore reduces to reasoning about the reals.
- In this way, we have **relative consistency**.
    - If the theory of natural numbers is consistent, so is the theory of complex numbers.

Functions or Predicates?

We can represent some property r holding between two objects x and y as:

a function with equality	$r(x) = y$
a predicate	$r(x, y)$

Is it better to use functions or predicates to represent properties?

It is not always clear which is best!

Functional Representation

For example, suppose we represent division of real numbers $(/)$ by a function $div : real \times real \Rightarrow real$.

- We define $div(x, y)$ when $y \neq 0$ in normal way
- What about division-by-zero? What is the value of $div(x, 0)$?
- In first-order logic, functions are assumed to be **total**, so we have to pick a value!
- We could *choose* a convenient element: say 0. That way:

$$0 \leq x \rightarrow 0 \leq 1/x.$$

Predicate Representation

Q) Can we represent division of real numbers $(/)$ by a relation $Div : real \times real \times real \Rightarrow bool$ such that $Div(x, y, z)$ is

- $x/y = z$ when $y \neq 0$, and
- $\bot$ when $y = 0$?

A) Yes: $Div(x, y, z) \;\equiv\; x = y * z \wedge \forall w.\ x = y * w \rightarrow z = w$
That is, z is that *unique* value such that $x = y * z$.

But now formulas are more complicated.

$$x, y \neq 0 \rightarrow \frac{1}{((x/y)\,/x)} = y$$

becomes

$$Div(x, y, u) \wedge Div(u, x, v) \wedge Div(1, v, w) \wedge x, y \neq 0 \rightarrow w = y$$

Functional Representation

Can we represent the concept of *square roots* with a function $\sqrt{} : \mathit{real} \Rightarrow \mathit{real}$?

- All positive real numbers have *two* square roots, and yet a function maps points to *single* values.
- We can pick one of the values arbitrarily: say, the *positive* (*principal*) square root.
- **Or** we can have the function map every real to a *set* $\sqrt{} : \mathit{real} \Rightarrow \mathit{real\ set}$:
$$\sqrt{x} \equiv \left\{ y \mid x = y^2 \right\}.$$
- But now we have two kinds of object: reals and sets of reals, and we cannot conveniently express:
$$(\sqrt{x})^2 = x$$
- Our representation of reals is no longer **self-contained**.

Predicate Representation

Q) Can we represent the concept of *square roots* with a relation $Sqrt : real \times real \Rightarrow bool$?

A) Yes. E.g. $Sqrt(x, y) \equiv x = y^2$.

Again drawback of formulas being more complicated

Functions, Predicates and Sets

We can translate back and forth. **But too much translation makes a formalisation hard to use!**

Any function $f : \alpha \to \beta$ can be represented as a relation $R : \alpha \times \beta \to bool$ or a set $S : (\alpha \times \beta) set$ by defining:

$$R(x, y) \equiv f(x) = y$$
$$S \equiv \{(x, y) \mid f(x) = y\}.$$

Any predicate P can be represented by a function f or a set S by defining:

$$f(x) \equiv \begin{cases} True & : \quad P(x) \\ False & : \quad \text{otherwise} \end{cases}$$
$$S \equiv \{x \mid P(x)\}.$$

Any set S can be represented by a function f or a predicate P by defining:

$$f(x) \equiv \begin{cases} True & : \quad x \in S \\ False & : \quad \text{otherwise} \end{cases}$$
$$P(x) \equiv x \in S$$

Set Theory, Functions, and HOL

In **pure** (without axioms) **FOL**, we **cannot directly represent** the statement:

> *there is a function that is larger on all arguments than the log function.*

To formalise it, we would need to quantify over functions:

$$\exists f.\ \forall x.\ f(x) > \log x.$$

Likewise we cannot quantify over predicates.

Solutions in FOL:

- Represent all functions and predicates by **sets**, and quantify over these. This is the approach of first-order set theories such as *ZF*.
- Introduce sorts for predicates and functions. Not so elegant now having 2 kinds of each.

Summary

- This time:
  - Issues involved in representing mathematical theories
  - Axioms vs. Definitions
  - Functions vs. Predicates
  - Introduction to Higher-Order Logic
  - Reading: Bundy, Chapter 4 (contains further discussion of issues in representation, e.g. variadic functions).
- On the course web-page: some more exercises, asking you to "prove" `False` from the axioms of Naive Set Theory.