L21 Interactive Formal Verification
Michaelmas Term, Academic Year 2017–2018
Assessed Exercise 2: Metric Spaces

Dr. Dominic P. Mulligan

November 26, 2017

Contents

1 Introduction

This is the second assessed exercise for the L21 "Interactive Formal Verification" MPhil course in academic year 2017–2018. In this exercise you will prove some properties of structures called metric spaces and two closely associated concepts: continuity and open balls. The exercise will test your ability to write structured proofs, work with sets and quantifiers, and carefully select relevant auxiliary lemmas and introduction and elimination principles to make theorem proving easier. Indeed, all proofs should be written as Isar structured proofs, as far as possible. Concretely, the marking scheme for this exercise is as follows (out of a total of 100):

- **50 marks** for correct definitions, lemma statements and structured proofs, in accordance with the distribution of marks outlined in the body of this document,

- **30 marks** for extra proofs of properties about metric spaces, continuity and open balls presented in this exercise, more definitions related to metric spaces and properties about them, or the use of features of Isabelle not lectured in class, or similar along these lines. Any reasonable evidence that you have gone "above and beyond" in your use of Isabelle will be considered here, and obviously the more ambitious you are, the more marks you accrue,

- **20 marks** for a nice writeup detailing all decisions made in your choice of lemmas, proof strategies, and so on, and an explanation as to what extensions you have decided

to implement, or novel features of Isabelle that you have used, to merit some of the 30 marks mentioned above.

Your submissions should be submitted electronically on the L21 Moodle site before 4pm Cambridge local time on submission day. See the course website for submission dates for the two assessed exercises. Submissions should consist of an edited version of the theory file that this document is based on (also available from the course website) that includes your solutions to the exercises contained within, along with a PDF document containing your writeup. Your writeup need not be especially long—2 sides of A4 will suffice—but it should be detailed, describing auxilliary lemmas and definitions that you introduced, if any, design decisions, and so on. Late submissions will of course be penalised, and as always students should not confer with each other when answering the sheet.

Before beginning: for those who have not encountered metric spaces before it may be a good idea for you to skim-read the Wikipedia article on the subject to familiarise yourself with key concepts before beginning.[1] However, the exercises have been written in such a way that consulting any such background material on metric spaces is not strictly necessary, with enough background information embedded within this document to help you through.

---

[1]See https://en.wikipedia.org/wiki/Metric_space

2 Metric spaces, and some examples

As the definition of metric spaces relies crucially on the real numbers, we will be working with the Isabelle/HOL theory `Complex_Main`—rather than the more usual `Main`—for this exercise. This theory imports an implementation of the real and complex numbers, as well as associated definitions and theorems:

theory *Assessed-Exercise-Two-Questions*
  imports *Complex-Main*
begin

Consider the distance between any two points in $\mathbb{R}^3$, the absolute distance between two integers, or the Lehvenstein (edit) distance between a pair of strings. Many mathematical objects have a notion of distance associated with them—and some even have multiple different reasonable notions of distance. *Metric spaces* are intended as an abstraction of all of these notions of distance, and of our own informal understanding of this concept.

Formally, a metric space $\langle C, \delta \rangle$ is a carrier set C paired with a *metric* (or distance) function $\delta : C \times C \to \mathbb{R}$ that intuitively represents the distance between any two points of the carrier set, C. We can capture this structure in Isabelle/HOL using a record with two fields, one corresponding to the carrier, and the other to the metric function:

record $'a$ *metric-space* =
  carrier :: $'a$ *set*
  metric :: $'a \Rightarrow {}'a \Rightarrow real$

I note here that, differing slightly from the standard mathematical presentation, I have Curried the metric function in the Isabelle/HOL modelling of a metric space. This is a minor difference that has no impact on the theory. Also, I use Isabelle's type polymorphism to express an ambivalence in the type of the contents of the carrier set.

As a supposed generalisation of our intuitive notion of distance, a metric function must satisfy a number of important laws, or properties, in order for the pair $\langle C, \delta \rangle$ to be a valid metric space. These are as follows:

- It makes no sense to state that one object is a negative distance from some other object: distances are only ever zero or positive, and never negative. Therefore the real number returned by a metric space's metric function for any two points must be non-negative.

- The distance travelled when walking from Cambridge to St. Neots is the same as the distance travelled when walking from St. Neots to Cambridge. Generalising, the distance between a point x and a point y must be the same as the distance between the point y and the point x. That is: a metric space's metric function is *symmetric*,

- The distance between any two points is zero if and only if the two points are identical. This law is a little harder to justify intuitively, as in natural language we often say that the distance between two touching objects is zero. However, if we think of the elements of the carrier set as "points" with no internal volume then the axiom asserts that any two co-located points are identical,

- There are no shortcuts: a metric function must capture the *shortest* distance between any two points. The distance travelled when travelling from point x to z via an interme-

diary point y must be at least as long as the distance travelled simply moving between points x and z directly.

The third law above is sometimes known as the "identity of indiscernibles", whilst the last law is sometimes referred to as the "triangular inequality". These laws can be easily captured as a HOL predicate on `metric_space` records, asserting that a carrier set and metric function pairing constitute a valid metric space:

definition *metric-space* :: $'a$ *metric-space* $\Rightarrow$ *bool* **where**
  metric-space $M \equiv$
    $(\forall\, x {\in} carrier\ M.\ \forall\, y {\in} carrier\ M.\ metric\ M\ x\ y \geq 0) \wedge$
    $(\forall\, x {\in} carrier\ M.\ \forall\, y {\in} carrier\ M.\ metric\ M\ x\ y = metric\ M\ y\ x) \wedge$
    $(\forall\, x {\in} carrier\ M.\ \forall\, y {\in} carrier\ M.\ metric\ M\ x\ y = 0 \longleftrightarrow x = y) \wedge$
    $(\forall\, x {\in} carrier\ M.\ \forall\, y {\in} carrier\ M.\ \forall\, z {\in} carrier\ M.$
      $metric\ M\ x\ z \leq metric\ M\ x\ y + metric\ M\ y\ z)$

Note here that I use the same name, `metric_space`, to denote both the underlying type of metric space records as well as the predicate asserting that those records correctly model a metric space. This does not matter—the two names live in different namespaces. Now that we have a suitable set of definitions for modelling metric spaces in Isabelle/HOL we can begin showing that some concrete carrier set and metric function pairings are indeed valid metric spaces. As a first example, a metric space can be constructed from the set of real numbers by taking the distance between any two reals, j and k, to be their absolute difference, $|\, j - k\, |$. We can capture this by defining a suitable instance of the `metric_space` record:

definition *real-abs-metric-space* :: *real metric-space* **where**
  real-abs-metric-space $\equiv (\!|\ carrier = UNIV,\ metric = \lambda x\ y.\ abs\ (x - y)\ |\!)$

Note here that the carrier set of the metric space is `UNIV`, the universal set. Isabelle correctly infers that this has type `real set` as the type of `real_abs_metric_space` has been constrained to the type `real metric_space`. Now that we have a pairing of a carrier set and metric function, we must show that this pairing is indeed a valid metric space. We do this by proving that the `metric_space` predicate holds of this record.

Exercise (4 marks): prove that the predicate `metric_space` holds of `real_abs_metric_space` by proving the following theorem. That is, replace the `oops` command below with a complete structured proof.

theorem
  shows *metric-space real-abs-metric-space*
  oops

The set of real numbers can be lifted into a metric space in another way, using the so-called *British Rail metric* which models the tendency of all rail journeys between any two points in the United Kingdom to proceed by first travelling to London, and then travelling onwards. (The French call this the *SNCF metric* due to a similar tendency in Metropolitan France.) This metric space can again be captured quite easily in Isabelle/HOL, by following the same pattern as before.

Exercise (4 marks): prove that the predicate `metric_space` holds of `br_metric_space` by proving the following theorem. That is, replace the `oops` command below with a complete structured proof.

definition *br-metric-space* :: *real metric-space* **where**
  br-metric-space ≡ ⦇ *carrier = UNIV, metric = λx y. if x = y then 0 else abs x + abs y* ⦈

theorem
  shows *metric-space br-metric-space*
  oops

As a final example, we consider endowing pairs of integers with a metric. For pairs of integers (i_1, j_1) and (i_2, j_2) one can use $| i_1 - i_2 | + | j_1 - j_2 |$ as a metric—sometimes called the taxicab metric. Proving that this is a valid metric space is a little more involved than the other two examples, due to fiddling with pairs, but still fairly straightforward.

Exercise (5 marks): prove that the predicate `metric_space` holds of `taxicab_metric_space` by proving the following theorem. That is, replace the **oops** command below with a complete structured proof.

definition *taxicab-metric-space* :: (*int × int*) *metric-space* **where**
  taxicab-metric-space ≡
    ⦇ *carrier = UNIV, metric = λp1 p2. abs (fst p1 − fst p2) + abs (snd p1 − snd p2)* ⦈

theorem
  shows *metric-space taxicab-metric-space*
  oops

3 Making new metric spaces from old

We now have a handful of concrete metric spaces. Given such a collection of existing metric spaces, can we produce new metric spaces using generic constructions? That is, are there operations that take an arbitrary metric space and can produce new ones? In this section, we explore three different ways of building new metric spaces from old: restricting a metric space to a subset of the carrier, shifting a metric via a non-zero constant, and finally taking the product of two metric spaces. The first two are relatively straightforward:

Exercise (3 marks): Suppose $\langle C, \delta \rangle$ is a metric space and suppose $S \subseteq C$. Show that $\langle S, \delta \rangle$ is also a metric space by stating and proving (with a structured proof) a relevant lemma.

Exercise (3 marks): Suppose $\langle C, \delta \rangle$ is a metric space. Suppose also that $k > 0$ and that $\delta'(x, y) = k \cdot \delta(x, y)$. Show that $\langle C, \delta' \rangle$ is a metric space by stating and proving (with a structured proof) a relevant lemma.

Lastly, we consider taking the product of two metric spaces. Recall that mathematically $S \times T$ denotes the *Cartesian product* of two sets, consisting of all ordered pairs (s, t) where $s \in S$ and $t \in T$.

Exercise (5 marks): Suppose $\langle S, \delta_1 \rangle$ and $\langle T, \delta_2 \rangle$ are metric spaces. Show that the set $S \times T$ can be lifted into a metric space by first finding a suitable metric and thereafter proving (with a strucured proof) a relevant lemma. Your metric on $S \times T$ must make use of both δ_1 and δ_2.

4 Continuous functions, and some examples

One reason why metric spaces are mathematically interesting is because they provide an abstract venue within which one can define the important notion of *continuous function*, a core concept in topology and analysis. Indeed, metric spaces can be seen as a precursor to topology.

Suppose that $\langle S, \delta_1 \rangle$ and $\langle T, \delta_2 \rangle$ are metric spaces, and $f : S \to T$ is a function mapping elements of S to T. Suppose also that $s \in S$ is a point in S. We say that the function f is *continuous at the point s* if for every $\epsilon > 0$ there exists $d > 0$ such that $\delta_1(x, s) < d$ then $\delta_2(fx, fs) < \epsilon$ for all $x \in S$. Further, call the function $f : S \to T$ *continuous* if f is continuous at every point $s \in S$. These two definitions can be captured in Isabelle/HOL as follows:

context fixes *M1* :: $'a$ *metric-space* **and** *M2* :: $'b$ *metric-space* **begin**

definition *continuous-at* :: $('a \Rightarrow 'b) \Rightarrow 'a \Rightarrow bool$ **where**
  continuous-at f a $\equiv \forall \varepsilon > 0.$
    $(\exists d > 0. \ \forall x \in carrier \ M1. \ metric \ M1 \ x \ a \ < \ d \ \longrightarrow \ metric \ M2 \ (f \ x) \ (f \ a) \ < \ \varepsilon)$

definition *continuous* :: $('a \Rightarrow 'b) \Rightarrow bool$ **where**
  continuous f $\equiv \forall x \in carrier \ M1. \ continuous\text{-}at \ f \ x$

end

As an aside, here I use a `context` block to fix two arbitrary metric spaces—M1 and M2—of the correct type for the duration of my definitions. This means that I do not need to add the two metric spaces as explicit parameters to the `continuous_at` and `continuous` functions but can declare them as parameters "up front". Inspect the type of the definitions to see what `context` does:

term *continuous-at*
term *continuous*

Which functions are continuous? One obvious contender is the identity function. Suppose $\langle S, \delta \rangle$ is a metric space. Then the identity function $id : S \to S$ maps elements of the carrier S onto elements of the carrier S—that is, the identity function can be seen as a map from a metric space back onto itself.

Exercise (3 marks): show that the identity function id is a continuous function between a metric space and itself by stating and proving (with a strucured proof) a relevant lemma.

Constant functions are also continuous. Suppose $\langle S, \delta_1 \rangle$ and $\langle T, \delta_2 \rangle$ are metric spaces and $t \in T$ is a point in T. Suppose also that $f : S \to T$ maps all s to t (i.e. it is a constant function that always returns t). Then f is continuous.

Exercise (4 marks): show that constant functions are continuous by proving the following lemma. That is, replace the `oops` command below with a complete structured proof.

lemma *continuous-const*:
  assumes *metric-space M1* **and** *metric-space M2*
    and $y \in carrier \ M2$
  shows *continuous M1 M2* $(\lambda x. \ y)$
  oops

Lastly, suppose $\langle S, \delta_1 \rangle$, $\langle T, \delta_2 \rangle$, and $\langle U, \delta_3 \rangle$ are metric spaces. Suppose also that $f : S \to T$ and $g : T \to U$ are continuous functions between relevant metric spaces. Then, providing that for every $s \in S$ we have $f\,s \in T$ holds, the composition $(g \circ f) : S \to U$ is also a continuous function between the metric spaces $\langle S, \delta_1 \rangle$ and $\langle U, \delta_3 \rangle$.

Exercise (6 marks): show that the composition of two continuous functions is continuous by proving the following lemma. That is, replace the `oops` command below with a complete structured proof.

lemma *continuous-comp*:
  assumes *metric-space M1* **and** *metric-space M2* **and** *metric-space M3*
    and *continuous M1 M2 f* **and** *continuous M2 M3 g*
    and $\bigwedge x.\ x \in$ *carrier M1* $\implies f\,x \in$ *carrier M2*
  shows *continuous M1 M3* $(g\ o\ f)$
oops

5 Open balls

Suppose $\langle S, \delta \rangle$ is a metric space and $c \in S$ is a point in S. Suppose also that $r > 0$ is some strictly positive real number. Define the *open ball of radius r around the point c* as the set of all points in S that are strictly less than r distance away from the point c when measured using the metric δ. Where the underlying metric space is obvious, I will write $\mathcal{B}(c, r)$ for the open ball around point c of radius r.

Exercise (2 marks): Suppose $\langle S, \delta \rangle$ is a metric space. Define the open ball $\mathcal{B}(c, r)$ in this metric space by completing the definition of `open_ball`. That is, replace the `consts` declaration below with a complete definition.

consts *open-ball* :: $'a$ *metric-space* $\Rightarrow$ $'a$ $\Rightarrow$ *real* $\Rightarrow$ $'a$ *set*

For any open ball $\mathcal{B}(c, r)$ in a metric space $\langle S, \delta \rangle$ we have that $\mathcal{B}(c, r) \subseteq S$, i.e. open balls are always subsets of the underlying metric space's carrier set. This fact holds for any ball of any radius.

Exercise (2 marks): show that an arbitrary open ball in a fixed metric space is a subset of that metric space's carrier set by stating and proving (with a structured proof) a relevant lemma.

Moreover, we have that in a fixed metric space, the open ball $\mathcal{B}(c, 0) = \{\}$. That is, open balls of zero radius are the empty set.

Exercise (2 marks): show that an open ball in a fixed metric space with radius 0 is the empty set.

Additionally, it should be intuitively obvious that for any open ball in a fixed metric space $\mathcal{B}(c, r)$ where $r > 0$ we have the property that $c \in \mathcal{B}(c, r)$, i.e. the open ball contains its own centre as a point.

Exercise (3 marks): show that any open ball in a fixed metric space with strictly positive radius contains its centre as a point by proving the following lemma. That is, replace the `oops` command below with a complete structured proof.

lemma *centre-in-open-ball*:
  assumes *metric-space M* **and** $c \in$ *carrier M*

and *0 < r*
  shows *c ∈ open-ball M c r*
  oops

Lastly, suppose we have two open balls around the same centre point—$\mathcal{B}(c, r)$ and $\mathcal{B}(c, s)$—such that $r \leq s$ where c is contained within some ambient fixed metric space. Then it should be obvious that the open ball with smaller radius is a subset of the open ball with the larger radius.

Exercise (4 marks): show that an open ball around a fixed centre point with a smaller radius than another open ball around the same fixed centre point is a subset of the latter open ball by proving the following theorem. That is, replace the `oops` command below with a complete structured proof.

lemma *open-ball-le-subset*:
  assumes *metric-space M*
    and *c ∈ carrier M* **and** *r ≤ s*
  shows *open-ball M c r ⊆ open-ball M c s*
  oops

end

The end. . .