A formalization of metric spaces in HOL Light

Marco Maggesi

DiMaI - Università degli Studi Firenze

GnCS - Geometry and Computer Sciences 2017
Pescara (Italy), February 8-10, 2017

Background

Geometry:

- **Metric spaces** are an indispensable tool in mathematics (geometry, analysis, algebra, ...).

Computer Science:

- Computer can be useful for **theorem proving**:
  - **Discover** new theorems (*automated theorem proving*);
  - **Check** proofs (*computer checked mathematics*).

This work:

- **Implement** metric spaces in the **HOL Light** theorem prover.

The tool

HOL Light theorem prover

- **Interactive** theorem prover.
- **Simple foundation** (typed lambda calculus, 10 rules, 3 axioms).
- Easy to **program and extend** (write your own *tactics*).
- Remarkable **standard library** (real and complex analysis, linear algebra, topology and geometry, . . .).

This work

Our main results:

- A **definition of metric spaces** (overcome technical issues related to the logical foundation).
- Computer **verification of some classical results** about (complete) metric spaces.
- Applications to Ordinary Differential Equations.
- (*Main topic of this talk*) Implementation of a **decision procedure** for the *elementary theory of metric spaces*.

Comparison with other work (in HOL)

- Euclidean Spaces in HOL Light [Harrison 2005]
  - decision procedure (`NORM_ARITH`)
  - only euclidean metric
- Metric spaces in Isabelle/HOL [Immler and Hölzl 2012]
  - Isar proof language (more readable)
  - *Total* metric spaces
    - axiomatic classes
    - adequate for most applications
    - some limitations in expressivity spaces (e.g., L^p spaces)
  - no specialized decision procedure
- Metric spaces in HOL Light (this work)
  - *Partial* Metric spaces
    - can reason subspaces and families of metric spaces
  - Decision procedure `METRIC_ARITH`

Elementary theory of Metric spaces

Structure

Carrier: M the domain (the *set* of points)

Distance: $d \colon M \times M \longrightarrow \mathbb{R}$

Axioms

Non-negativity: $d(x, y) \geq 0$

Indiscernibility: $d(x, y) = 0$ if and only if $x = y$

Symmetry: $d(x, y) = d(y, x)$

Triangle inequality: $d(x, z) \leq d(x, y) + d(y, z)$

Esempi di spazi metrici

- Standard metric of $\mathbb{R}^n$:

$$d(x,y) = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}$$

- L^∞ metric on $\mathbb{R}^n$:

$$d_\infty(x,y) = \max\left\{|x_1 - y_1|, \ldots, |x_n - y_n|\right\}$$

- *Manhattan* metric (L_1 metric) on $\mathbb{R}^n$:

$$d_1(x,y) = |x_1 - y_1| + \cdots + |x_n - y_n|$$

- Metric of a normed vector space:

$$d(u,v) = ||u - v||$$

- L^∞ metric on the space of continuous functions on $[0,1]$

$$d_\infty(f,g) = \max\left\{|f(x) - g(x)| : 0 \leq x \leq 1\right\}$$

Complete metric spaces

Cauchy sequences: The distance between its terms becomes arbitrary small after a certain index.

Easy result: Every convergent sequence is a Cauchy sequence.

Definition: A metric space is *complete* if the converse it is also true.

Some results proved:

- Baire category theorem.
- Banach fixed-point theorem.
- Proof of completeness of some notable spaces ($\mathbb{R}^n$, bounded functions, continuous bounded functions).

Example: the Banach Fixed Point Theorem

Theorem (Banach)

Every contraction $f : M \to M$ on a non empty complete metric space M has an unique fixed-point.

Formal statement in HOL Light:

```
⊢ ∀m f k.
    ¬(mspace m = ∅) ∧ mcomplete m ∧
    (∀x. x ∈ mspace m ⟹ f x ∈ mspace m) ∧
    k < &1 ∧
    (∀x y. x ∈ mspace m ∧ y ∈ mspace m
           ⟹ mdist m (f x,f y) ≤ k * mdist m (x,y))
    ⟹ (∃!x. x ∈ mspace m ∧ f x = x)
```

Example: the Banach Fixed Point Theorem

Theorem (Banach)

Every contraction $f : M \to M$ on a non empty complete metric space M has an unique fixed-point.

Formal statement in HOL Light:

$$
\begin{array}{l}
\vdash \forall M\ f\ k\,. \\
\quad \neg(M = \emptyset) \wedge \mathtt{complete}\ M \wedge \\
\quad (\forall x.\ x \in M \Longrightarrow f(x) \in M) \wedge \\
\quad k < 1 \wedge \\
\quad (\forall x\ y.\ x \in M \wedge y \in M \\
\qquad\qquad \Longrightarrow d(f(x), f(y)) \le k\ d(x, y)) \\
\quad \Longrightarrow (\exists! x.\ x \in M \wedge f(x) = x)
\end{array}
$$

Example: Continuous bounded functions

One key example is the space of continuous bounded functions with L^∞-metric.

For $f, g \colon X \longrightarrow M$ bounded functions define

$$d_\infty(f,g) = \sup_{x \in X} d_M(f(x), g(x)).$$

If M is complete, the function space is complete:

$\vdash$ ∀`top m. mcomplete m` $\Longrightarrow$ `mcomplete (cfunspace top m)`

We will use this fact in the proof of the Picard-Lindelöf theorem.

A decision procedure for metric space

We implemented a **decision procedure** `METRIC_ARITH` for general metric spaces (similar to Harrison's `NORM_ARITH`).

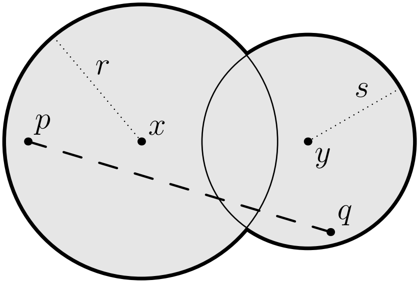
Based on a work of Solovay, Arthan and Harrison [2012].

Can automatically prove basic facts like **"triangle law"** lemmas.

Can handle a wider range of quantifiers (basically a $\forall\exists$ fragment of the theory).

A decision procedure for metric space (Example)

Given B_1, B_2 two intersecting open balls of radius r, s respectively, the diameter of their union $B_1 \cup B_2$ is less than $2(r+s)$.



$$
\begin{aligned}
\forall M\ \mathtt{x\ y\ r\ s.}\ \neg(\mathtt{DISJOINT}\ (B(\mathtt{x,r}))\ (B(\mathtt{y,s}))) \\
\Longrightarrow \forall \mathtt{p\ q.\ p} \in B(\mathtt{x,r}) \cup B(\mathtt{y,s}) \wedge \\
\mathtt{q} \in B(\mathtt{x,r}) \cup B(\mathtt{y,s}) \\
\Longrightarrow d(\mathtt{p,q}) < \mathtt{2\ (r\ +\ s)}
\end{aligned}
$$

Undecidability of the theory of metric spaces

The elementary theory of metric spaces is undecidable

- Early result due to Bondi [1973].
- A simple proof [Kutz 2003] can be obtained by considering metric spaces associated to graph and reducing the problem to the undecidability about problems on binary relations

Problem

Find a decidable class of valid formulas in the language of the metric spaces.

Decidable fragments $\forall\exists$ and $\exists\forall$

Definition

- A formula ϕ is $\forall\exists$ if
  - is in prenex form
  - no universal quantifier occurs in the scope of an existential one.
- In short:

$$\phi \equiv \forall \bar{x}.\, \exists \bar{y}.\, \psi$$

- $\exists\forall$ formulas are defined similarly:

$$\phi \equiv \exists \bar{x}.\, \forall \bar{y}.\, \psi$$

Theorem (Bernays-Schönfinkel)

(1) The class of valid $\forall\exists$ sentences without function symbols is decidable.

(2) The class of satisfiable $\exists\forall$ sentences without function symbols is decidable.

This results can extended to important cases where function symbols occur.

Theorem (Tarski)

The theory of real closed fields is decidable.

Putting the two results together we can obtain a decidability result for metric spaces.

$\forall\exists_p$ and $\exists\forall_p$ sentences

Definition

- A sentence in the language of metric spaces ϕ is $\forall\exists_p$ if
  1. is in prenex form;
  2. no universal quantifier over points is in the scope of an existential quantifier (of any sort);
- $\exists\forall_p$ sentences are defined analogously.

Remark

Since universal quantifiers commute up to logical equivalence, any $\forall\exists_p$ sentence ϕ can be assumed to be of the form

$$\phi \equiv \forall x_1, \ldots, x_n. \exists \bar{y} / Q\bar{z}. \psi$$

Idea

The validity of an $\forall\exists_p$ formula in the language of metric spaces can be reduced to the validity of a formula of real closed fields trough the following three steps:

$$\text{Metric spaces} \xrightarrow{(1)} \text{Finite metric spaces} \xrightarrow{(2)} (\mathbb{R}^n, d_\infty) \xrightarrow{(3)} \text{Real closed fields}$$

Theorem (Step 1: Reduction to finite metric spaces)

Given an $\forall\exists_p$ sentence in the language of metric spaces $\phi \equiv \forall x_1, \ldots, x_n.\, \exists\bar{y}/\mathrm{Q}\bar{z}.\, \psi$ TFAE:

(1) ϕ is valid in all (non empty) metric spaces;

(2) ϕ is valid in all finite metric spaces with no more than $\max\{n, 1\}$ points.

Proof (1) $\Longrightarrow$ (2).

Trivial. □

Proof (2) $\Longrightarrow$ (1).

Let ϕ be valid in all (non empty) finite metric spaces with at most n points.

Given n points $x_1, \ldots, x_n$, the formula $\rho :\equiv \exists\bar{y}/\mathrm{Q}\bar{z}.\, \psi$ is valid on the metric space $S := \{x_1, \ldots, x_n\} \subseteq M$.

Then ϕ is valid on M. □

Construction (Step 2: from finite metric spaces to $\mathbb{R}^n_\infty$)

Le (M, d) be a finite metric space with n points $p_1, \dots, p_n$. Consider $\mathbb{R}^n_\infty = (\mathbb{R}^n, d_\infty)$, where

$$d_\infty(x, y) = \max\{|x_1 - y_1|, \dots, |x_n - y_n|\}$$

Then the application

$$f_M \colon M \to \mathbb{R}^n$$

given by

$$f_M(p) = (d(p, p_1), \dots, d(p, p_n))$$

is an isometric embedding.

Theorem

The class of logically valid $\forall\exists_p$ sentences in the language of metric space is decidable.

Proof: Taking the negation we look for a decision procedure for the satisfiability of $\exists\forall_p$ sentences.
Let $\phi \equiv \exists x_1, \ldots, x_n . \forall \bar{y} / Q\bar{z} . \psi$.
Thanks to previous theorem, ϕ is satisfiable iff exists an interpretation of $x_1, \ldots, x_n$ in a metric space M with at most $\max(n, 1)$ points satisfying $\forall \bar{y} / Q\bar{z} . \psi$.
By replacing every subformula of ϕ of the form $\forall y . \psi$ with the conjunction $\psi[x_1/y] \wedge \cdots \wedge \psi[x_n/y]$ we obtain a sentence which is equisatisfiable with ϕ without universal quantifiers over points.
Therefore, we can assume that ϕ has the form $\exists x_1 \ldots x_n . \psi$ where only quantifiers over scalars occurs in ϕ.

To be continued . . .

Proof (second part)

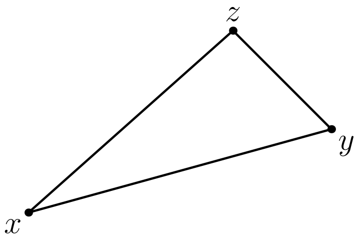
By using $f : M \to \mathbb{R}^n_\infty$, we have that ϕ is satisfiable iff it is so on $\mathbb{R}^n_\infty = (\mathbb{R}^n, d_\infty)$.
Let x_{ij}, $1 \leq i, j \leq n$ be new scalar variables ($f_M(x_i) = (x_{i1}, \ldots, x_{in})$ and ψ' the formula obtained by replacing in ψ

- every subterm of the form $x_s = x_t$ with $x_{s1} = x_{t1} \wedge \cdots \wedge x_{sn} = x_{tn}$ and
- every subterm of the form $d(x_s, x_t)$ with $d_\infty(f_M(x_s), f_M(x_t)) = \max\{|x_{s1} - x_{t1}|, \ldots, |x_{sn} - x_{tn}|\}$

$\exists x_1 \ldots x_n . \psi$ is satisfiable iff $\phi' :\equiv \exists x_{11}, x_{12} \ldots x_{nn} . \psi'$ is satisfiable.
Now, ϕ' is a formula without variables on points, the we can apply a decision procedure for real closed fields.

QED

Example: Reverse triangle inequality



Triangle inequality:

$$d(x, y) \leq d(x, z) + d(z, y)$$

<u>Reverse</u> triangle inequality:

$$\left| d(x, z) - d(z, y) \right| \leq d(x, y)$$

Reverse triangle inequalitiy

"Human" proof of the reverse triangle inequality

$$|d(x,y) - d(y,z)| \leq d(x,z)$$

1. Use $|a-b| \leq c \iff a \leq c + b \wedge b \leq c + a$. We get

$$d(x,y) \leq d(x,z) + d(y,z)$$
$$d(y,z) \leq d(x,z) + d(x,y)$$

2. both inequalities are instances of the triangle inequality. QED

Reverse triangle inequalitiy

Machine proof of the reverse triangle inequality

$$|d(x,y) - d(y,z)| \le d(x,z)$$

1. Define
   - $S \stackrel{\text{def}}{=} \{x, y, z\} \subseteq M$ metric space with just 3 points;
   - Isometry $f\colon S \to \mathbb{R}^3_\infty$

$$f(p) \stackrel{def}{=} (d(p,x), d(p,y), d(p,z)).$$

2. Obtain the equivalent analytical problem

$$\Big| max\big(d(x,y), |d(x,z) - d(y,z)|\big) - max\big(d(y,z), |d(x,y) - d(x,z)|\big) \Big| \le max(d(x,z), |d(x,y) - d(y,z)|)$$

3. Prove the above inequality using Fourier-Motkin elimination.

Thank you for your attention!

Bibliography

- R.M. Solovay, R.D. Arthan, and J. Harrison. *Some new results on decidability for elementary algebra and geometry*. Annals of Pure and App Logic, 163(12):1765 1802, 2012.
- Marco Maggesi, *A formalization of metric spaces in HOL Light*. (to appear on J. of Automated Reasoning)