Proving in the Isabelle Proof Assistant that the Set of Real Numbers is not Countable

Villadsen, Jørgen

Publication date: 2018

Document Version
Publisher's PDF, also known as Version of record

Link back to DTU Orbit

Citation (APA):

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.
Proving in the Isabelle Proof Assistant that the Set of Real Numbers is not Countable

Jørgen Villadsen
DTU Compute, AlgoLoG, Technical University of Denmark, 2800 Kongens Lyngby, Denmark
jovi@dtu.dk

Abstract
We present a new succinct proof of the uncountability of the real numbers – optimized for clarity – based on the proof by Benjamin Porter in the Isabelle Analysis theory.

1 Introduction
In 1874 Georg Cantor proved that set of real numbers is not countable – or, no surjective function from the natural numbers to the real numbers exists.

\textbf{theorem} \#f :: nat ⇒ real. surj f

We use the Isabelle proof assistant, more precisely Isabelle/HOL, and omit the so-called cartouches \(\langle...\rangle\) around formulas as is common in recent papers about formalizations in Isabelle. Since the notion of the real numbers in Isabelle is not grounded in decimal expansions, Cantor’s elegant diagonal argument from 1891 is not suitable. With some effort we have ordered by year the immediately known formalizations of the theorem.

<table>
<thead>
<tr>
<th>Formalization</th>
<th>Author</th>
<th>Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProofPower</td>
<td>Rob Arthan</td>
<td>2003</td>
</tr>
<tr>
<td>Metamath</td>
<td>Norman Megill</td>
<td>2004</td>
</tr>
<tr>
<td>Mizar</td>
<td>Grzegorz Bancerek</td>
<td>2004</td>
</tr>
<tr>
<td>HOL Light</td>
<td>John Harrison</td>
<td>2005</td>
</tr>
<tr>
<td>Isabelle</td>
<td>Benjamin Porter</td>
<td>2005</td>
</tr>
<tr>
<td>Coq</td>
<td>Nickolay Shmyrev</td>
<td>2006</td>
</tr>
</tbody>
</table>
Freek Wiedijk’s comprehensive list “Formalizing 100 Theorems” has been a valuable starting point:

http://www.cs.ru.nl/~freek/100/

We present a new succinct proof – optimized for clarity – based on the proof by Benjamin Porter in the Isabelle Analysis theory and inspired by the traditional proof (Hansen 1999, p. 45). The full proof is available in the appendix and also online here together with other results about countable and uncountable sets:

https://github.com/logic-tools/continuum

We note that the theorem can also be phrased as follows using quantifiers only.

\[ \exists f. \forall y :: \text{real}. \exists x :: \text{nat}. y = f x \]

We have not yet fully investigated if our approach can be generalized to other proofs except that we have recently considered a related proof, namely that the set of rational numbers is in fact countable, based on the rather scattered formalization in the Isabelle Library which incidentally differs in a number of ways from the traditional proof (Hansen 1999).

2 A Possible New Feature in Isabelle

As a possible new feature in Isabelle we use “...” to signify a proof found by Isabelle’s Sledgehammer tool (Blanchette 2017), possibly also using some more or less obvious proof methods.

We suggest to implement it like a kind of extended “sorry” proof methods that is a “fake proof pretending to solve the pending claim without further ado” (cf. the Isabelle/Isar Reference Manual in the Isabelle distribution).

But when the Sledgehammer tool finds a proof then the “...” should somehow change color and/or shape to indicate this.

In this way Isabelle proofs can still be replayed.

Perhaps the “...” notation is not ideal since it is used for other things in Isabelle.
3 The Proof Skeleton

We provide a proof skeleton and continue the proof in the following section.

The proof is by contradiction.

```plaintext
assume \( \exists f :: \text{nat} \Rightarrow \text{real. surj} \ f \)
show False
```

We first obtain a name for the surjective function.

```plaintext
from \( \exists f. \text{surj} \ f \) obtain \( f :: \text{nat} \Rightarrow \text{real where} \ \text{surj} \ f \) ..
then have assumption: \( \exists n. \ f \ n = z \) for \( z \) ...
```

Here “..” is a standard proof; it abbreviates “by standard” and performs elementary proof steps depending on the application environment. And the “...” proof is a resolution proof “by (metis surj_def)” which we for further transparency separate into two proof steps “unfolding surj_def by metis” as shown in the appendix.

In our proof we now obtain a certain natural-numbers-indexed set \( D \) of real numbers with a kind of diagonalization property.

```plaintext
obtain \( D :: \text{nat} \Rightarrow \text{real set} \)
where
  \((\bigcap n. \ D \ n) \neq {}\)
  \(f \ n \not\in D \ n\)
  for \( n \)
```

We defer the proof of the existence of the indexed set \( D \) to the next section. From the indexed set \( D \) we easily obtain the contradiction.

```plaintext
then obtain \( e \) where \( \nexists n. \ f \ n = e \) ...
moreover from assumption have \( \exists n. \ f \ n = e \).
ultimately show ?thesis ..
```

Here “...” is the resolution proof “by (metis INT_E UNIV_I ex_in_conv)” as shown in the appendix.
4 The Indexed Set D

We need to fill the gap in the proof skeleton regarding the indexed set D.

We start by defining two functions of three arguments.

\[
\text{obtain } L \ R :: \text{real} \Rightarrow \text{real} \Rightarrow \text{real} \Rightarrow \text{real}
\]

where *

\[
L \ a \ b \ c < R \ a \ b \ c
\]

\[
\{L \ a \ b \ c .. R \ a \ b \ c\} \subseteq \{a .. b\}
\]

\[
c \not\in \{L \ a \ b \ c .. R \ a \ b \ c\}
\]

if \(a < b\) for \(a \ b \ c\)

We here include the complete proof of the existence of the two functions, except for the “...” proofs shown in the appendix.

\[
\text{proof -}
\]

\[
\text{have } \exists x \ y. \ a \leq x \land x < y \land y \leq b \land \neg (x \leq c \land c \leq y)
\]

\[
\text{if } a < b \text{ for } a \ b \ c :: \text{real} \ ... \ 
\]

\[
\text{then have } \exists x \ y. \ x < y \land \{x .. y\} \subseteq \{a .. b\} \land c \not\in \{x .. y\}
\]

\[
\text{if } a < b \text{ for } a \ b \ c :: \text{real} \ ... \ 
\]

\[
\text{then show } ?\text{thesis} \ ... \ 
\]

\[
\text{qed}
\]

We recursively define an indexed set of intervals given by pairs – the endpoints of the intervals.

\[
\text{define } P :: \text{nat} \Rightarrow \text{real} \times \text{real}
\]

where

\[
P \equiv \text{rec}_\text{nat}
\]

\[
(L \ 0 \ 1 \ (f \ 0), \ R \ 0 \ 1 \ (f \ 0))
\]

\[
(\lambda n \ (x, y). \ (L \ x \ y \ (f \ (\text{Suc} \ n)), \ R \ x \ y \ (f \ (\text{Suc} \ n))))
\]

We prove that the endpoints are ordered as expected; again the “...” proofs are shown in the appendix.

\[
\text{with } *(1) \text{ have } \theta: \text{fst} \ (P \ n) < \text{snd} \ (P \ n) \text{ for } n \ ...
\]
Finally we define the indexed set of intervals and prove the required properties.

\[
\text{define } I : : \text{n} \mapsto \text{real set}
\]
\[
\text{where}
\]
\[
I \equiv \lambda n. \{\text{fst (P n)} \ldots \text{snd (P n)}\}
\]
\[
\text{with } 0 \text{ have } I n \neq \{\} \text{ for } n \ldots
\]
\[
\text{moreover from } 0 \ast (2) \text{ have decseq } I \ldots
\]
\[
\text{ultimately have finite } S \mapsto (\bigcap n \in S. I n) \neq \{\} \text{ for } S \ldots
\]
\[
\text{moreover have closed } (I n) \text{ for } n \ldots
\]
\[
\text{moreover have compact } (I n) \text{ for } n \ldots
\]
\[
\text{ultimately have } (\bigcap n. I n) \neq \{\} \ldots
\]
\[
\text{moreover from } 0 \ast (3) \text{ have } f n \notin I n \text{ for } n \ldots
\]
\[
\text{ultimately show } ?\text{thesis }..
\]

5 Conclusion

We have with good results explained the proof to a group of mathematicians with little or no knowledge of formal methods. In particular the “…” notation is useful and might be relevant to implement, perhaps with the Proof Strategy Language available in the Isabelle Archive of Formal Proofs.

References


Appendix: Formalization in Isabelle

\begin{verbatim}
theory Scratch imports Complex_Main begin
  theorem \( \exists f :: \text{n} \mapsto \text{real. surj f} \):
    proof
      assume \( \exists f :: \text{n} \mapsto \text{real. surj f} \)
      show False
      proof
        from \( \exists f. \text{surj f} \) obtain f :: \( \text{n} \mapsto \text{real} \) where \( \text{surj f} \) ..

        then have assumption: \( \exists n. f n = z \) for z
          unfolding surj_def by metis
\end{verbatim}
obtain D :: {nat ⇒ real set} where \( \{\bigcap_n D_n \neq \emptyset\} \), \( \{f \in D_n \} \) for \( n \)
proof
obtain L R :: {real ⇒ real ⇒ real ⇒ real}
where
\(*\) \( L \ a \ b \ c < R \ a \ b \ c \) \( \langle L \ a \ b \ c .. R \ a \ b \ c \rangle \subseteq \langle a .. b \rangle \); \( c \notin \{L \ a \ b \ c .. R \ a \ b \ c\} \)
if \( (a < b) \) for \( a \ b \ c \)
proof
have \( \langle \exists x \ y \cdot a \leq x \land x < y \land y \leq b \land \neg (x \leq c \land c \leq y) \rangle \) if \( (a < b) \) for \( a \ b \ c \) :: real
using that dense less_le_trans not_le not_less_iff_gr_or_eq by (metis \{full_types\})
then have \( \langle \exists x \ y \cdot (x < y \land (x \ldots y) \subseteq \langle a \ldots b \rangle \land c \notin \langle x \ldots y \rangle \rangle \) if \( (a < b) \) for \( a \ b \ c \) :: real
using that by fastforce
then show \(?thesis\)
  using that by metis
qed

define P :: {nat ⇒ real × real}
where
\( \langle P = \text{rec}_\text{nat} \langle\langle L \ 0 \ 1 \ \emptyset\rangle, \\
\langle R \ 0 \ 1 \ \emptyset\rangle \rangle \rangle \ (\lambda n \ (x, y). \langle L \ x \ y \ (f \ (\text{Suc} n)), \\
\langle R \ x \ y \ (f \ (\text{Suc} n))\rangle \rangle \rangle \)

with \(*\{1\}\) have \( \emptyset \): \( \langle \text{fst} \ (P \ n) < \text{snd} \ (P \ n) \rangle \) for \( n \)
u refunding split_def by (induct \( n \)) simp_all

define I :: {nat ⇒ real set}
where
\( \langle I = \lambda n. \ (\text{fst} \ (P \ n)) \ldots \text{snd} \ (P \ n)\rangle \)

with \( 0 \) have \( \langle I \ n \neq \emptyset \rangle \) for \( n \)
using less_imp_le by fastforce

moreover from \( 0 \ \langle*\rangle \) have \( \langle \text{decseq} \ I \rangle \)
u refunding \( \text{I} \ \text{def} \ P \ \text{def} \ \text{split}_\text{def} \ \text{decseq}_\text{Suc}_\text{iff} \ \text{by} \ \text{simp} \)

ultimately have \( \langle \text{finite} \ S \longrightarrow (\bigcap_n S \ I \ n) \neq \emptyset \rangle \) for \( S \)
u using decseqO \ subset_empty \ INF_greatest \ Max.ge \ by \ metis

moreover have \( \langle \text{closed} \ (I \ n) \rangle \) for \( n \)
u refunding \( \text{I} \ \text{def} \ by \ \text{simp} \)

moreover have \( \langle \text{compact} \ (I \ n) \rangle \) for \( n \)
u refunding \( \text{I} \ \text{def} \ using \ \text{compact}_\text{lcc} \ \text{compact}_\text{Int} \text{closed} \ \text{decseqO} \ \text{inf.absorb_iff2} \ \text{le0} \ \text{by} \ \text{simp} \)

ultimately have \( \langle (\bigcap_n I \ n) \neq \emptyset \rangle \)
u using \( \text{INT.insert} \ \text{compact}_\text{Imp} \text{_image} \ \text{empty_subsetI} \ \text{finite.insert} \ \text{inf.absorb_iff2} \ \text{by} \ \text{metis} \)

moreover from \( 0 \ \langle*\rangle \) have \( \langle f \ n \notin I \ n \ \rangle \) for \( n \)
u refunding \( \text{I} \ \text{def} \ P \ \text{def} \ \text{split}_\text{def} \ \text{by} \ \langle \text{induct} \ n \rangle \ \text{simp}_\text{all} \)

ultimately show \(?thesis\)
qed

then obtain e where \( \langle \exists n. \ f \ n = e \rangle \)
using INT_E UNIV_I ex_in_conv by metis

moreover from assumption have \( \langle \exists n. \ f \ n = e \rangle \)

ultimately show \(?thesis\)
qed

end — Jørgen Villadsen, DTU Denmark - Based on work by Benjamin Porter, NICTA Australia