Cantor's Diagonalization Argument

Ludovico Deponte

Coq Project 2022

January 28, 2022

Overview

1. Objectives
2. Planning
3. Formalization
4. Evaluation

Cantor's Diagonalization Argument

Goal: show that the set $S := \{A\}$ is uncountable.
By contradiction,
Suppose S is countable, i.e. you have a surjection from $\mathbb{N}$ to S, then

	$g_n(1)$	$g_n(2)$	$g_n(3)$	$g_n(4)$	$g_n(5)$	$g_n(6)$	$g_n(7)$	$g_n(8)$	$g_n(9)$	$g_n(10)$	$\dots$
$g_1(i)$	a_1^1	a_1^2	a_1^3	a_1^4	a_1^5	a_1^6	a_1^7	a_1^8	a_1^9	a_1^{10}	$\dots$
$g_2(i)$	a_2^1	a_2^2	a_2^3	a_2^4	a_2^5	a_2^6	a_2^7	a_2^8	a_2^9	a_2^{10}	$\dots$
$g_3(i)$	a_3^1	a_3^2	a_3^3	a_3^4	a_3^5	a_3^6	a_3^7	a_3^8	a_3^9	a_3^{10}	$\dots$
$g_4(i)$	a_4^1	a_4^2	a_4^3	a_4^4	a_4^5	a_4^6	a_4^7	a_4^8	a_4^9	a_4^{10}	$\dots$
$g_5(i)$	a_5^1	a_5^2	a_5^3	a_5^4	a_5^5	a_5^6	a_5^7	a_5^8	a_5^9	a_5^{10}	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

$$A^* = g'(a_1^1)\, g'(a_2^2)\, g'(a_3^3)\, g'(a_4^4)\, g'(a_5^5)\ \dots$$

Initial Plan

- Minimal Goal: diagonalization on infinite sequences of $\mathbb{N}$.

Initial Plan

- Minimal Goal: diagonalization on infinite sequences of $\mathbb{N}$.
- Realistic Goal: define $\mathbb{R}$ with Dedekin cuts and diagonalization on $\mathbb{R}$.

Initial Plan

- Minimal Goal: diagonalization on infinite sequences of $\mathbb{N}$.
- Realistic Goal: define $\mathbb{R}$ with Dedekin cuts and diagonalization on $\mathbb{R}$.
- Extended Goal: general diagonalization theorem.

Updated Plan

- Minimal Goal: diagonalization on infinite sequences of $\mathbb{N}$.

Updated Plan

- Minimal Goal: diagonalization on infinite sequences of $\mathbb{N}$.
- Realistic Goal: diagonalization on $\mathcal{P}(\mathbb{N})$.

Updated Plan

- Minimal Goal: diagonalization on infinite sequences of $\mathbb{N}$.
- Realistic Goal: diagonalization on $\mathcal{P}(\mathbb{N})$.
- Extended Goal: countability of $\mathbb{Q}_r$.

Formalization

- How to formalize S?
- How to build the new element A^*

Minimal Goal

- Infinite sequences of $\mathbb{N}$ as functions `nat -> nat`.

Minimal Goal

- Infinite sequences of $\mathbb{N}$ as functions `nat -> nat`.
- Create an element not in the enumeration defining:

$$g'(i) = \mathtt{S}(f_n(i))$$

Realistic Goal

- Subsets of $\mathbb{N}$ as functions `nat -> bool`.

$$g_n(i) = \top \text{ iff } i \in S$$

Realistic Goal

- Subsets of $\mathbb{N}$ as functions `nat -> bool`.

$$g_n(i) = \top \text{ iff } i \in S$$

- Create an element not in the enumeration defining:

$$g'(n) = \neg(g_n(i))$$

Extended Goal

- Formalization of divisibility and greatest common divisor.

Extended Goal

- Formalization of divisibility and greatest common divisor.
- Formalize reduced rationaals by defining each $q \in \mathbb{Q}_r$ as a tuple $(num, den, proof)$.

Extended Goal

- Formalization of divisibility and greatest common divisor.
- Formalize reduced rationaals by defining each $q \in \mathbb{Q}_r$ as a tuple $(num, den, proof)$.
- Define a function from $\mathbb{N}$ to $\mathbb{Q}_r$.

$$\texttt{f\_N\_to\_Q}(n) = \frac{n}{1}$$

- Show that `f_N_to_Q` is injective

Extended Goal

- Formalization of divisibility and greatest common divisor.
- Formalize reduced rationaals by defining each $q \in \mathbb{Q}_r$ as a tuple $(num, den, proof)$.
- Define a function from $\mathbb{N}$ to $\mathbb{Q}_r$.

$$\texttt{f\_N\_to\_Q}(n) = \frac{n}{1}$$

- Show that `f_N_to_Q` is injective
- Define a function from $\mathbb{Q}_r$ to $\mathbb{N}$.

$$\texttt{f\_Q\_to\_N}(\frac{a}{b}) = 2^a \cdot 3^{sgn(a)} \cdot 5^b \cdot 7^{sgn(b)}$$

where $sgn(z) = \begin{cases} 1 & \text{if } z > 0 \\ 0 & \text{otherwise} \end{cases}$

- Show that `f_Q_to_N` is injective.

Extended Goal: assumptions

- `proofIrrelevance`

Extended Goal: assumptions

- `proofIrrelevance`
- `Z_one_GCD`:
  greatest common divisor between 1 and $q \in \mathbb{Q}_r$ is 1.

Extended Goal: assumptions

- `proofIrrelevance`
- `Z_one_GCD`:
  greatest common divisor between 1 and $q \in \mathbb{Q}_r$ is 1.
- `small_Godel`:
  asserts that if we have $2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4} = 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3} \cdot 7^{b_4}$ then $a_i = b_i$.

Extended Goal: assumptions

- `proofIrrelevance`
- `Z_one_GCD`:
  greatest common divisor between 1 and $q \in \mathbb{Q}_r$ is 1.
- `small_Godel`:
  asserts that if we have $2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdot 7^{a_4} = 2^{b_1} \cdot 3^{b_2} \cdot 5^{b_3} \cdot 7^{b_4}$ then $a_i = b_i$.
- `Z_abs_sgn_eq`:
  if two rationals r_1, r_2 have the same absolute value and the same sign, then $r_1 = r_2$.
- `C_B_S_Thm`: the Cantor Bernstein Schroder Theorem
  if there is a injection from A to B and there is an injection from B to A, then there is a bijection between A and B.

My Progress

✓ Minimal Goal

My Progress

- ✓ Minimal Goal
- ✓ Realistic Goal

My Progress

- ✓ Minimal Goal
- ✓ Realistic Goal
- Extended Goal
  - ✓ define $\mathbb{Q}_r$
  - ✓ define `f_N_to_Q`
  - show `f_N_to_Q` is injective
  - ✓ define `f_Q_to_N`
  - ✓ show `f_Q_to_N` is injective
  - ✓ apply `C_B_S_Thm` to `f_N_to_Q` and `f_Q_to_N`

Difficulties encountered & the Coq experience

- deciding how to define the objects used
- working with libraries and converting between different types
- working with `Record`

- proofs that look trivial are sometimes hard to formalize
- knowing Type Theory would have helped