Lean Seminar Series

Getting Started: Proving with the Lean Interactive Theorem Prover

Session 1 UTSC

November 24, 2021

Welcome to the LEAN Seminar Series!

While you are getting settled, please enjoy

The “Surprise” Symphony
in G Major
By Franz Joseph Haydn

Our Research Team : Theorem Proving for Math Education

Gila Hanna
Mathematics Education
Professor
OISE/UT

Kitty Yan
Mathematics Education
Postdoc Fellow
OISE/UT

Japleen Kaur Anand
Mathematics Education
Master’s Student
OISE/UT

Logan Murphy
Computer Science
Master’s Student
CS/UT

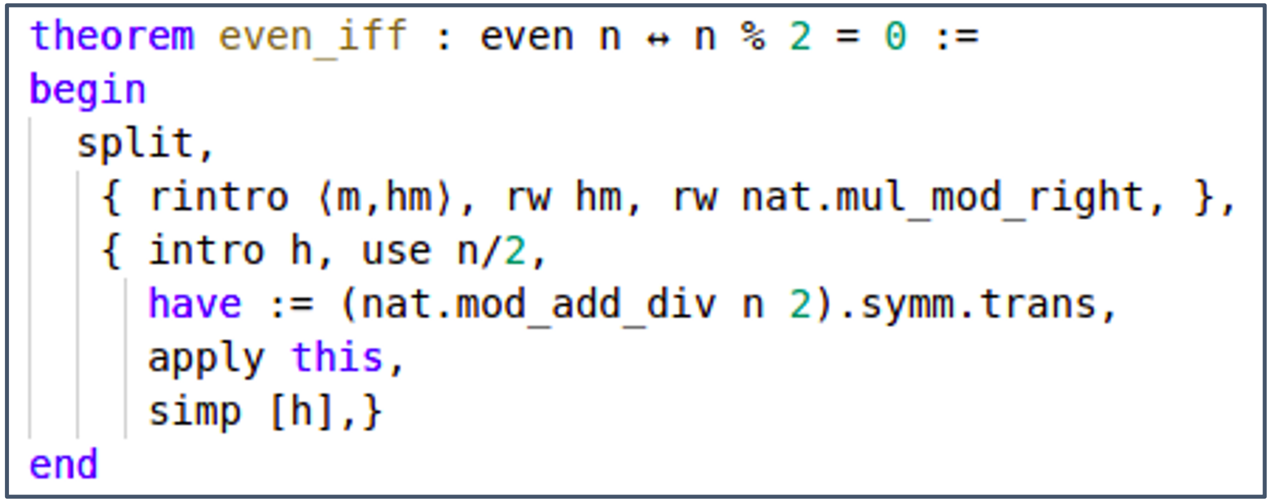
Overview

- A brief introduction to Lean
- Solving a logical puzzle
- Getting familiar with quantifiers
- Translating plain language to logical symbols
- A close look at Peano axioms
- Starting the natural number game

The LEAN Theorem Prover

Lean is a *proof assistant.*

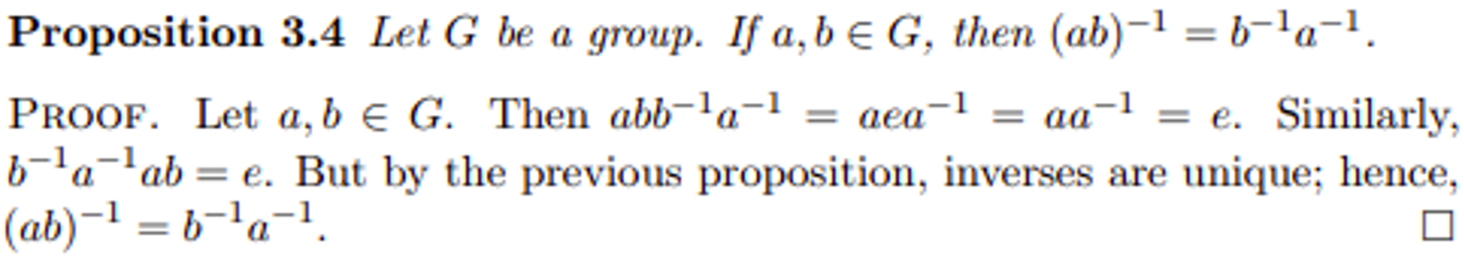
- Environment for writing formal proofs
- Checks whether a proof is correct
- Provides automation



```
theorem even_iff : even n ↔ n % 2 = 0 :=
begin
  split,
   { rintro ⟨m,hm⟩, rw hm, rw nat.mul_mod_right, },
   { intro h, use n/2,
     have := (nat.mod_add_div n 2).symm.trans,
     apply this,
     simp [h],}
end
```

The LEAN Theorem Prover

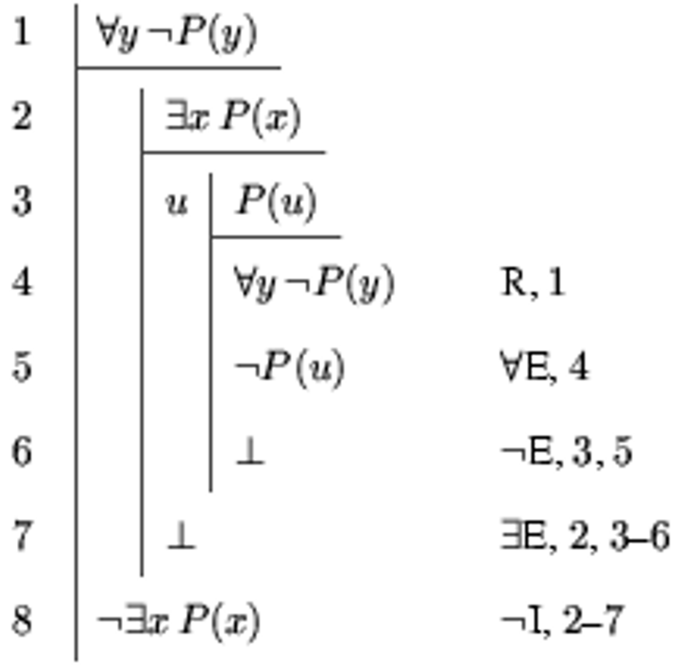
Informal Proof



Proposition 3.4 *Let G be a group. If $a, b \in G$, then $(ab)^{-1} = b^{-1}a^{-1}$.*

Proof. Let $a, b \in G$. Then $abb^{-1}a^{-1} = aea^{-1} = aa^{-1} = e$. Similarly, $b^{-1}a^{-1}ab = e$. But by the previous proposition, inverses are unique; hence, $(ab)^{-1} = b^{-1}a^{-1}$. □

Formal Proof



1	$\forall y \, \neg P(y)$	
2	$\quad \exists x \, P(x)$	
3	$\quad u \quad P(u)$	
4	$\qquad \forall y \, \neg P(y)$	R, 1
5	$\qquad \neg P(u)$	∀E, 4
6	$\qquad \bot$	¬E, 3, 5
7	$\quad \bot$	∃E, 2, 3–6
8	$\neg \exists x \, P(x)$	¬I, 2–7

The LEAN THEOREM PROVER Theorem Prover

Why use a proof assistant for mathematics?

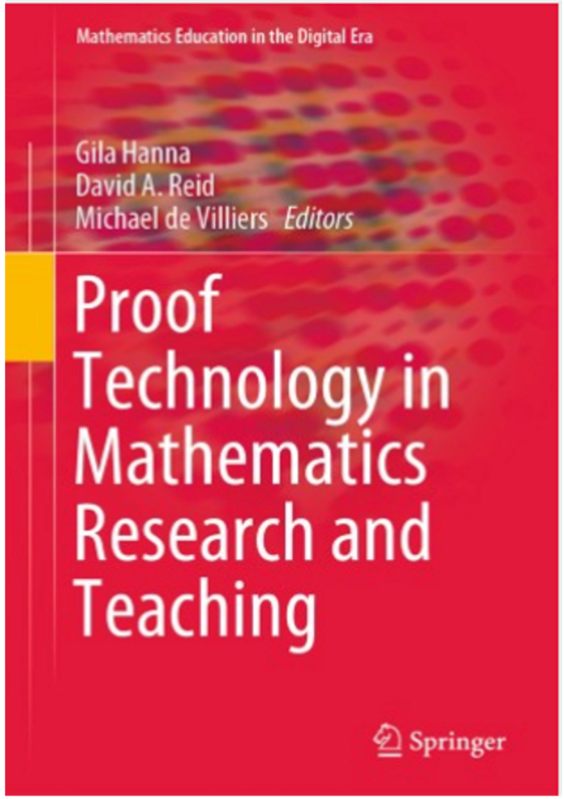
“I think there is a non-zero chance that some of our great castles are built on sand.”

- Kevin Buzzard, Imperial College London (See: Xena Project)

The LEAN THEOREM PROVER Theorem Prover

Universities where mathematics is taught or assessed with computerized tools:

- Imperial College London, UK
- Loughborough University, UK
- Université Paris Sud, France
- Carnegie Mellon University, USA
- University of South Carolina, USA
- University of Hawaii, USA



Mathematics Education in the Digital Era

Gila Hanna
David A. Reid
Michael de Villiers *Editors*

Proof Technology in Mathematics Research and Teaching

Springer

The LEAN Theorem Prover

Why Lean?

- Relatively new
- Interest from mathematicians
- Active community

LEAN Community

The LEAN Theorem Prover

Before we spend more time with Lean…

A Logic Puzzle - Malice and Alice

Alice's family was involved in a murder.

Who was the victim?

A Logic Puzzle - Malice and Alice

- Who was the victim? Who was the murderer?
- How did you arrive at your solution?
- Which given condition(s) are most critical?

Quantifiers

- In normal use, quantifiers are determiners:
  - "all", "each", "some", "many", "most", and "few"
- In mathematics, they refer to the two extremes:
  - for all
  - there is at least one
- Universal quantifier denoted by ∀x

→ for all x it is the case that…

$$\forall x[x^2 \geq 0]$$

"Every leopard has spots." $\boxed{\forall x\ [\mathrm{L}(x) \Rightarrow \mathrm{S}(x)]}$

Quantifiers

- Existential quantifier denoted by ∃x

  → there exists an object *x* having property *p*.

  $$\exists x[x^2 + 2x + 1 = 0]$$

  "Some birds cannot fly." $\boxed{\exists x\ [B(x)\ \wedge\ \neg F(x)]}$

- "*You may fool all of the people some of the time, you can even fool some of the people all the time, but you cannot fool all of the people all the time.*"

- If let F(*p*, *t*) mean that you can fool person *p* at time *t*, then

  → $\boxed{\exists t \forall p F(p,t) \wedge \exists p \forall t F(p,t) \wedge \neg \forall p \forall t F(p,t)}$

Minds On

Natural Numbers: 0, 1, 2, 3, 4, 5,…

Try describing the natural numbers without mentioning properties of numbers.

Peano Axioms

- What is an axiom?
- Peano axioms

Published in 1889 by Giuseppe Peano

9 axioms of arithmetic, including

  - Four axioms of equality
  - Five axioms of number theory

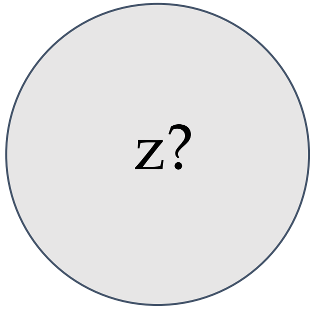
The five Peano Axioms of Number Theory

1. Zero is a natural number.
2. Every natural number has a successor in the natural numbers.
3. Zero is not the successor of any natural number.
4. The successors of two natural numbers are same iff the two original numbers are the same.*
5. If a set contains zero and the successor of every number is in the set, then the set contains the natural numbers.**

Axiom 1: Zero is a natural number

The first axiom asserts the existence of at least one member of the set N.

Let z be in N.



How can we construct N further?

Just keep including the next element!

Axiom 2: Every natural number has a successor in the natural numbers

For every n in N, S(n) is also in N, i.e. N is closed under S, **where S is the successor function**.

Or if n ∈ N, then S(n) ∈ N

What if S(z) = z?

Does it look like the set of natural numbers?

Here comes the third axiom.

Axiom 3: Zero is not the successor of any natural number.

For every n ∈ N, S(n) ≠ z where S denotes successor function
i.e. there is no natural number whose successor is zero.

Let's see what we have so far..
z ∈ N (First axiom)
S(z) ∈ N (Second axiom)
S(z) ≠ z (Third axiom)

Now consider S(S(z))
S(S(z)) ∈ N; S(S(z)) ≠ z

What if S(S(z)) = S(z)?
There will be only two elements in N: z and S(z).

Axiom 4 (Axiom of Injection)

For all m and $n \in$ N, $m = n$ if and only if $S(m) = S(n)$. That is, S is an **injection**.

So S(S(z))≠S(z) (why?)

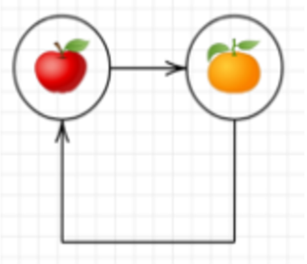
Now we have:
z, S(z), S(S(z)) in N
S(z)≠z, S(S(z))≠z, S(S(z))≠S(z)

Using the four axioms, can we now identify N with the set of our natural numbers:
0 → 1 → 2 → 3 → …?

There’s more...

Consider the following example and check if the four axioms are satisfied:

$$0 \to 1 \to 2 \to 3 \to \ldots$$



1. There is a “z”, 0.
2. Every element has a successor in the set.
3. 0 is not a successor of any element.
4. No two elements have the same successor.

Do we want apple and orange, or any other random elements, to be natural numbers?

Here comes the fifth axiom...

Axiom 5 (Axiom of Induction)

If M is a subset of N s.t.

1. $z \in M$
2. $n \in M \Rightarrow S(n) \in M$

Then $N \subseteq M$.

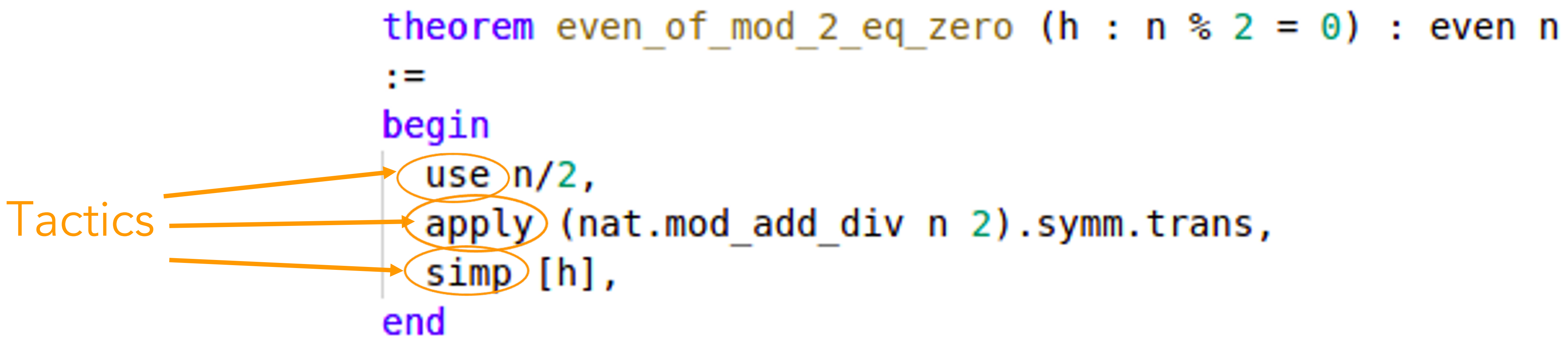
i.e. N is the minimal set that satisfies the previous axioms.

So by axiom 5:

0, 1, 2, 3, 4, … is the set of natural numbers. (minimal set satisfying axioms 1 and 2)

A word about “proving” in Lean:

“Tactic” : a kind of instruction to Lean on how to progress a proof.



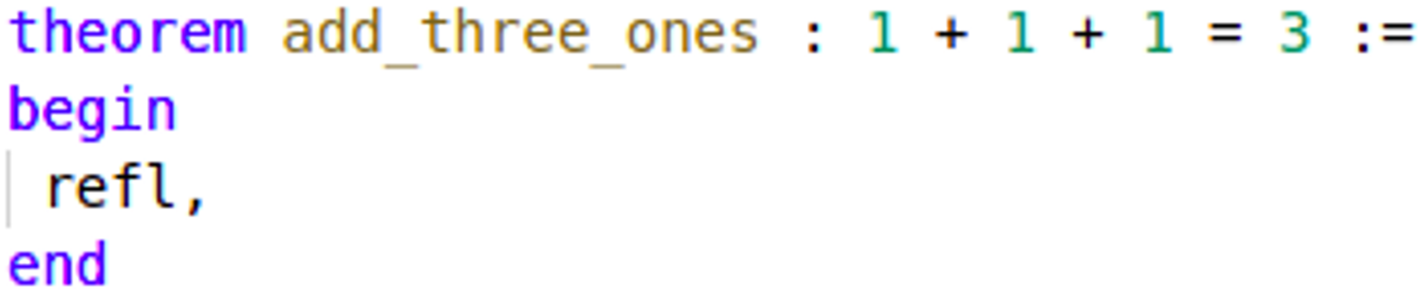
```
theorem even_of_mod_2_eq_zero (h : n % 2 = 0) : even n
:=
begin
  use n/2,
  apply (nat.mod_add_div n 2).symm.trans,
  simp [h],
end
```

Tactics

Tactic : Reflexivity

Abbreviation: `refl`

Used to close a goal of the form “P = Q”,
where P and Q can be “reduced” to the same value

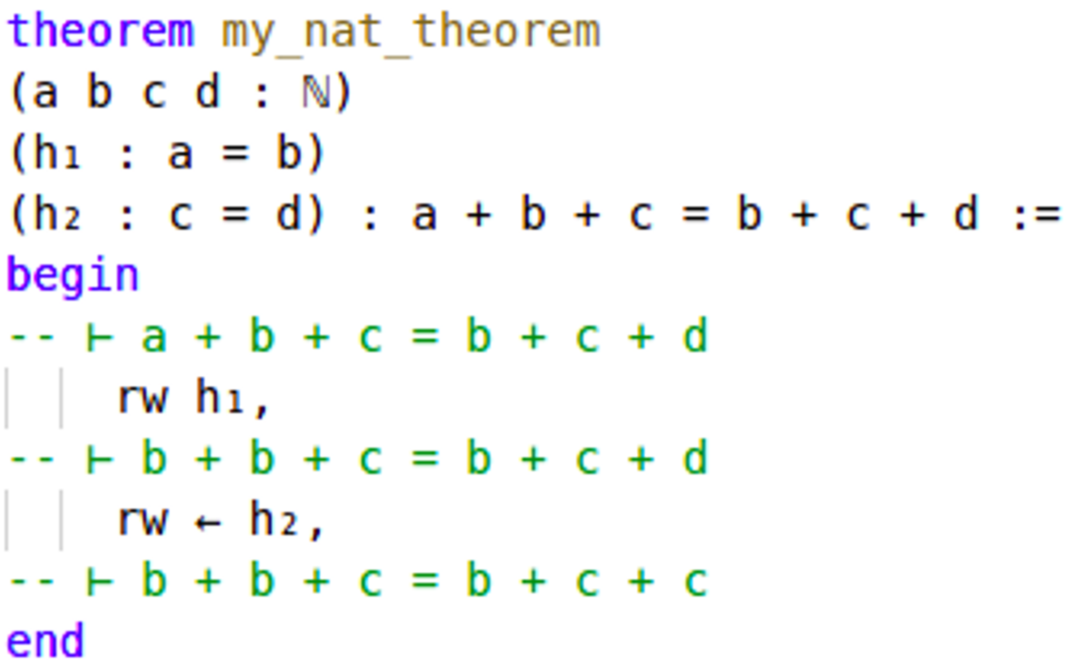


```
theorem add_three_ones : 1 + 1 + 1 = 3 :=
begin
 refl,
end
```

Tactic : Rewrite

Abbreviation: `rw`

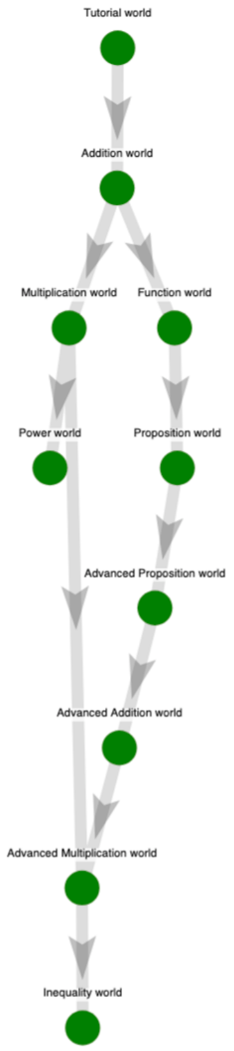
Given a hypothesis of the form “A = B”,
Replaces occurrences of A with B,
or vice versa.



```
theorem my_nat_theorem
(a b c d : ℕ)
(h₁ : a = b)
(h₂ : c = d) : a + b + c = b + c + d :=
begin
-- ⊢ a + b + c = b + c + d
    rw h₁,
-- ⊢ b + b + c = b + c + d
    rw ← h₂,
-- ⊢ b + b + c = b + c + c
end
```

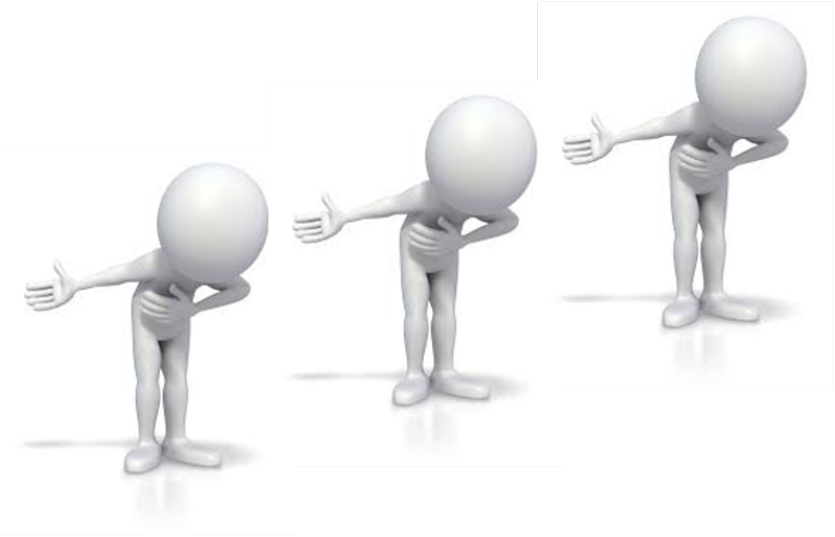
The Natural Number Game in Lean

- 10 worlds: Tutorial, addition, multiplication…
- 4-17 levels in each world
- Blue, grey, green nodes
- Use of Peano axioms
- Use of the principle of mathematical induction
- Use of tactics



The LEAN Seminar Series

Session 2 is on December 1, 2021.
See you all in a week!



Thank You!