CSC 165
more proof
Danny Heap
heap@cs.toronto.edu
http://www.cdf.toronto.edu/~heap/165/W10/

\[
\begin{align*}
\text{AT} & \rightarrow \text{tomorrow} \\
\text{T1} & \rightarrow \text{(later) tonight}
\end{align*}
\]
proving existence

To prove the a set is non-empty, it’s enough to exhibit one element. How do you prove:

$$\exists x \in \mathbb{R}, x^3 + 3x^2 - 4x = 12$$

Set $$x = 2$$. Then $$x \in \mathbb{R} \neq 2 \in \mathbb{R}$$ is well-known.

Then $$x^3 + 3x^2 - 4x = 2^3 + 3 \cdot 2^2 - 4 \cdot 2$$ # sub $$x = 2$$

$$= 8 + 12 - 8$$ # algebra

$$= 12$$

Conclude $$\exists x \in \mathbb{R}, x^3 + 3x^2 - 4x = 12$$ # introduced $$\exists$$
prove a claim about a sequence

Define sequence \( a_n \) by:

\[
\forall n \in \mathbb{N} \quad a_n = n^2
\]

Now prove:

\[
\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i
\]

Let \( i = 2 \). Then \( i \in \mathbb{N} \) and \( 2 \in \mathbb{N} \).

Assume \( j \in \mathbb{N} \) is arbitrary, generic.

Assume \( a_j \leq i \) and assumption on \( i \).

Then \( j^2 \leq i = 2 \) defines \( a_j \), and assumption on \( i \).

Then \( j \leq \sqrt{2} \) since \( \sqrt{ } \) is monotonic.

\( j < 2 \) since \( \sqrt{2} < 2 \).

Then \( j < 2 \) and consequent follows from assumption.

Then \( j \leq i \) and introduced.

Then \( \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i \) and introduced.

Conclude \( \exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i \) and introduced.
infinitely many primes

Define the prime natural numbers as \( P = \{ p \in \mathbb{N} \mid p \) has exactly two distinct divisors in \( \mathbb{N} \} \).

How do you prove:

\[ S : \forall n \in \mathbb{N}, |P| > n \quad \neg S \quad \exists n \in \mathbb{N}, |P| \leq n \]

It would be nice to have some result \( R \) that leads to \( S \). If you could show \( R \Rightarrow S \), and that \( R \) is true, then you'd be done. But, out of many elementary results, how do you choose an \( R \)?

Contradiction will often lead you there.

\( F_1 \land F_2 \land F_3 \land \ldots \land F_n \Rightarrow S \)

\( \neg S \Rightarrow \neg F_1 \lor \neg F_2 \lor \neg F_3 \lor \ldots \lor \neg F_n \)
Proof

Assume $\exists n \in \mathbb{N}, \mid p \mid \leq n$

Then $\exists k \in \mathbb{N}, \mid p \mid = n$ # assumption.

Then $p = \sqrt[3]{p_0 \cdot p_1 \cdots p_{k-1}}$

Let $r = p_0 \cdot p_1 \cdots p_{k-1} \in \mathbb{N}$ # $\mathbb{N}$ closed under $*$

Then $r \geq 6$ # since $2, 3 \in p$ and all other factors $\geq 1$

Then $r+1 > 1$ # $r \geq 6$

Then $\exists p \in p$, $p \mid r+1$ # every nat num $>1$ has prime divisor

Also $p \mid r$ # since $p$ is one of the factors $p_0 \cdots p_{k-1}$

Then $p \mid (r - (r+1))$ # divide 2 ints $\Rightarrow$ divide difference

So $p \mid 1 \Rightarrow p = 1$ # only divisor of 1

# contradiction! $1 \notin p$

Conclude $S$ # since assuming $\exists n$ leads to $\rightarrow \leftarrow$ contradiction.
Take care when expressing a proof about a function that returns a non-boolean value, such as a number:

\[ [x] \text{ is the largest integer } \leq x. \]

Now prove the following statement (notice that we quantify over \( x \in \mathbb{R} \), not \( [x] \in \mathbb{R} \):

\[ \forall x \in \mathbb{R}, [x] < x + 1 \]

Assume \( x \in \mathbb{R} \) is arbitrary real.

Then \( [x] \leq x \) # from definition

Then \( [x] < x + 1 \) # add \( x \) to both sides of \( 0 < 1 \)

Then \( [x] < x + 1 \) # transitivity

Conclude \( \forall x \in \mathbb{R}, [x] < x + 1 \)
You may have been disappointed that the last proof used only part of the definition of floor. Here's a symbolic re-writing of the definition of floor:

\[
\forall x \in \mathbb{R}, \ y = \lfloor x \rfloor \iff y \in \mathbb{Z} \land y \leq x \land (\forall z \in \mathbb{Z}, z \leq x \Rightarrow z \leq y)
\]

The full version of the definition should prove useful to prove:

\[
\forall x \in \mathbb{R}, \lfloor x \rfloor > x - 1
\]

Assume \( x \in \mathbb{R} \) # generic

Let \( y = \lfloor x \rfloor \) # into a variable

Then \( y \in \mathbb{Z} \) # from defn.

Then \( y \leq x \) #

Then \( y + 1 \in \mathbb{Z} \) # \( y \in \mathbb{Z} \land \mathbb{Z} \) closed under +

Then \( y + 1 > y \) # add 1 to both sides \( \Downarrow \)

So \( y + 1 > x \) # contrapositive of 3rd clause of defn

So \( y > x - 1 \) # move 1 \( \Rightarrow \)

So \( \lfloor x \rfloor > x - 1 \) #

Conclude \( \forall x \in \mathbb{R}, \lfloor x \rfloor > x - 1 \)
scratch
Define a sequence:

\[ \forall n \in \mathbb{N} \quad a_n = \lfloor n/2 \rfloor \]

(of course, if you treat "/" as integer division, there's no need to take the floor. Now consider the claim:

\[ \neg \left( \exists i \in \mathbb{N} , \forall j \in \mathbb{N} , j > i \Rightarrow a_j = a_i \right) \]

The claim is false. Disprove it.
Prove \( \forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \land a_j \neq a_i \).

Assume \( i \in \mathbb{N} \) generic. Set \( j = i + 2 \). Then \( j \in \mathbb{N} \neq i, 2 \in \mathbb{N} \), and \( \mathbb{N} \) closed under addition.

Then \( j = i + 2 > i \) add \( i \) to both sides \( j \geq 2 > 0 \).

Then \( a_j = \left\lfloor \frac{j}{2} \right\rfloor = \left\lfloor \frac{i + 2}{2} \right\rfloor = \left\lfloor \frac{i}{2} + 1 \right\rfloor > \left\lfloor \frac{i}{2} \right\rfloor \).

\( \neq \) since \( \left\lfloor \frac{i}{2} + 1 \right\rfloor > \frac{i}{2} \neq \) since \( \left\lfloor x \right\rfloor > x - 1 \)

\( \geq \left\lfloor \frac{i}{2} \right\rfloor \neq \) def \( \lfloor \cdot \rfloor \)

Then \( j > i \land a_j \neq a_i \) show both.

Then \( \exists j \in \mathbb{N}, j > i \land a_j \neq a_i \) introduced \( \exists \).

Conclude \( \forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \land a_j \neq a_i \) introduced \( \forall \).
cases

Sometimes your argument has to split to take into account possible properties of your generic element:

\[ \forall n \in \mathbb{N}, n^2 + n \text{ is odd} \]

A natural approach is to factor \( n^2 + n \) as \( n(n + 1) \), and then consider the case where \( n \) is odd, then the case where \( n \) is even.

**Case 1** Assume \( \exists k \in \mathbb{N}, n = 2k \)

- Pick \( k \in \mathbb{N}, n = 2k \) \( \# \) since it exists.
- Then \( n^2 + n = n(n + 1) = 2k(2k + 1) \) \( \# \) sub \( n = 2k \).
- Then \( \exists j \in \mathbb{N}, n^2 + n = 2j \) \( \# j = 2k(2k + 1) \in \mathbb{N} \) \( \# \) \( 2, k, 1 \in \mathbb{N} \) and \( \mathbb{N} \) closed under +.

**Case 2** Assume \( \exists k \in \mathbb{N}, n = 2k + 1 \)

- Pick \( k \in \mathbb{N}, n = 2k + 1 \) \( \# \) since it exists.
- Then \( n^2 + n = n(n + 1) = (2k + 1)(2k + 2) \) \( \# \) algebra
  \[ = 2(2k + 1)(k + 1) \in \mathbb{N}, 2, k, 1 \in \mathbb{N} \]
- Then \( \exists j \in \mathbb{N}, n^2 + n = 2j \) \( \# j \)
- Then \( \exists j \in \mathbb{N}, n^2 + n = 2j \) \( \# j \) true in both possible cases.

Conclude \( \forall n \in \mathbb{N}, n^2 + n \) is even \( \# \) introduced +
Assume \( j \geq i = 2 \)
Then \( j - 2 \geq 0 \)
Then \( j^2 - 2j \geq 0 \)
Then \( j^2 \geq 4 > 2 \)

\[
\begin{align*}
  j & \geq 2 \\
  j^2 & \geq 4 \\
\end{align*}
\]

# mult by \( j \)

\[
\begin{align*}
  j^2 + 2j & \geq 2j + 4 \\
\end{align*}
\]

# mult by \( j + 2 \)