CSC 165
more proof
Danny Heap
heap@cs.toronto.edu

http://www.cdf.toronto.edu/~heap/165/W10/
proving existence

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

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

Define sequence $a_n$ by:

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

Now prove:

$$\exists i \in \mathbb{N}, \forall j \in \mathbb{N}, a_j \leq i \Rightarrow j < i$$
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:

$$S : \quad \forall n \in \mathbb{N}, |P| > n$$

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.
scratch
non-boolean functions

Take care when expressing a proof about a function that returns a non-boolean value, such as a number:

\( \lfloor x \rfloor \) is the largest integer \( \leq x \).

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

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

Assume \( x \) is real \# generic element of \( \mathbb{R} \)

Then \( \lfloor x \rfloor \leq x \) \# from def

Then \( x \) \# just add \( x \) to both

\( x < x + 1 \)

Then \( \lfloor x \rfloor < x + 1 \) \# transitivity of \( < \), math pre-reqs.

Then \( \forall x \in \mathbb{R}, \lfloor x \rfloor < x + 1 \) \# introduced \( \forall \).
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:

$$\forall x \in \mathbb{R} \quad y = \lfloor x \rfloor \Leftrightarrow y \in \mathbb{Z} \land y \leq x \land (\forall z \in \mathbb{Z}, z \leq x \Rightarrow z \leq y)$$

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
Set \( y = \lfloor x \rfloor \) # convenience variable.
Then \( y \in \mathbb{Z} \). # defn of \( \lfloor x \rfloor = y \).
Then \( y + 1 \in \mathbb{Z} \). # \( y, 1 \in \mathbb{Z} \), \( \mathbb{Z} \) closed under +.
Then \( y + 1 > y \) # add \( y \) to \( 1 > 0 \).
Then \( y + 1 > x \) # contrapositive of 3rd clause of defn.
Then \( y > x - 1 \) # algebra.
Then \( \lfloor x \rfloor > x - 1 \) # \( y = \lfloor x \rfloor \). \( x = \tfrac{1}{2} + 1 \)

\[ \text{for sent}! \]

Conclude \( \forall x \in \mathbb{R}, \lfloor x \rfloor > x - 1 \). # introduced A
prove something is false

Define a sequence:
\[ a_n = \lfloor n/2 \rfloor \]

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

\[ \forall i \in \mathbb{N}, \forall j \in \mathbb{N}, j > i \Rightarrow a_j = a_i \]

The claim is false. Disprove it.

Assume \( i \in \mathbb{N} \). # generic natural number

Let \( j = i + 2 \). Then \( j \in \mathbb{N} \). # \( i, j \in \mathbb{N} \) and \( \mathbb{N} \) closed under +

Then \( j = i + 2 > i \). # add i to \( a > 0 \)

Then \( a_j = \lfloor \frac{i+2}{2} \rfloor = \lfloor \frac{i^2+1}{2} \rfloor > \frac{i}{2} \) # \( \lfloor x \rfloor > x-1 \)

\[ \geq \lfloor i/2 \rfloor \] # def \( \lfloor \) floor.

Then \( a_j = a_i \)

Then \( \exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i \) # shown above.

Then \( \forall i \in \mathbb{N}, \exists j \in \mathbb{N}, j > i \wedge a_j \neq a_i \) # introduced \( \forall \).
scratch
Sometimes your argument has to split to take into account possible properties of your generic element:

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

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 \( n = 2k \).

Pick \( n = 2k \).

Then \( n(n+1) = 2k(2k+1) = 2(k)(2k+1) \).

Then \( \exists j \in \mathbb{N} \) such that \( n(n+1) = 2j \) # \( j = k(2k+1) \in \mathbb{N} \).

**Case 2:** Assume \( n = 2k + 1 \).


scratch