CS 360
Fall 2021
Our Three Basic Tools

Jeffrey Shallit
School of Computer Science
University of Waterloo
shallit@uwaterloo.ca
https://cs.uwaterloo.ca/~shallit
Tools for proofs

One of the main activities in this course is proving things. But what tools do we have to carry out proofs?

In this course, there are just three basic tools. (Of course, you are free to use any technique you know about.)

- Proof by contradiction.
- Showing two sets are equal.
- Proof by induction.
Let’s assume we have some proposition $P$ that we want to prove. In \textit{proof by contradiction}, we assume that $P$ is false, and get a contradiction somehow.

A typical example of this is Euclid’s proof that there are infinitely many prime numbers.
We assume, contrary to what we want to prove, that there are only finitely many primes, and \( p_1, p_2, \ldots, p_n \) is a complete list of them.

We then consider the number \( N = (p_1 p_2 \cdots p_n) + 1 \).

But when we divide \( N \) by each \( p_i \), we get a remainder of 1. So \( N \) must be divisible by some prime not on our list. So our list was not complete, a contradiction.

(A common mistake is to conclude that \( N \) itself must be prime, but this is not true in general: consider \( 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 \).)
This proof technique is used over and over in the course.

Typically we have two different descriptions of the same set, $A$ and $B$, and we want to prove they are equal.

To do so we prove that $A \subseteq B$ and $B \subseteq A$.

In order to do that, we assume $x \in A$ and somehow conclude that $x \in B$. Then we assume $y \in B$ and somehow conclude that $y \in A$. 
For example, suppose

$$A = \{n : n = x + y \text{ and } x, y \text{ both odd and positive}\}$$

and

$$B = \{2m : m \geq 1\}.$$

We want to show $A = B$.

$A \subseteq B$: Let $n \in A$. Then there are odd positive integers $x, y$ such that $n = x + y$. Write $x = 2j + 1$, $y = 2k + 1$, for $j, k \geq 0$. Then $n = 2j + 2k + 2 = 2(j + k + 1)$. So $n \in B$.

$B \subseteq A$: Let $n \in B$. Then $n = 2m$ for some $m \geq 1$. Take $x = 1$ and $y = 2m - 1$, and notice that both $x$ and $y$ are odd and positive. So $n \in A$. 
In proof by induction, we want to prove that some proposition $P(n)$ is true for all $n \geq 0$ (or $n \geq 1$ or ...).

To do so we first prove that $P(0)$ holds. This is the \textit{base case}.

Next we prove that \textit{if} $P(n)$ holds for some $n \geq 0$, then $P(n + 1)$ also holds.

So $P(0)$ holds, which proves that $P(1)$ holds, which proves that $P(2)$ holds, and so forth. So $P(n)$ is true for all $n \geq 0$. 
Example: let’s prove that $1 + 2 + \cdots + 2^n = 2^{n+1} - 1$ by induction.

The base case is $n = 0$. Then $2^0 = 1 = 2^1 - 1$.

Now assume the claim is true for $n - 1$; we prove it for $n$.

By the induction hypothesis, we have $1 + 2 + \cdots + 2^{n-1} = 2^n - 1$.

Add $2^n$ to both sides. Then

$$1 + 2 + \cdots + 2^n = 2^n + 2^n - 1 = 2^{n+1} - 1,$$

and the desired result is proved.