Propositions

A proposition is either True or False

- may be easy or difficult to assign truth value to proposition
- prop itself should always be precise; unambiguous

connectors

$$\text{NOT: } \neg p \equiv \text{ it is not the case that p} \tag{1}$$
$$\text{AND: } p \wedge q \equiv \text{ p and q} \tag{2}$$
$$\text{OR: } p \vee q \equiv \text{ p or q} \tag{3}$$
$$\text{IF THEN: } p \to q \equiv \text{ if p then q / p implies q} \tag{4}$$

implication

p	q	$p \implies q$
T	T	T
T	F	F
F	T	T
F	F	T

alright guess we'll just expand the table a bit

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \implies q$
T	T	F	T	T	T
T	F	F	F	T	F
F	T	T	F	T	T
F	F	T	F	F	T

POP QUIZ WOO

$$p \equiv x > 0$$
$$q \equiv y > 1$$
$$r \equiv x < y$$

p	q	r	$q \wedge r$	$p \vee (q \wedge r)$	$p \vee q$
T	T	T	T	T	T
T	T	F	F	T	T
F	T	T	T	T	T
T	F	T	F	T	T
T	F	F	F	T	T
F	F	T	F	F	F
F	T	F	F	F	T
F	F	F	F	F	F

Table 1: Note that row 7 is not actually possible.

Quantifiers

e.g.,

EVERY; A; SOME; ANY; ALL; THERE EXISTS

define *predicate* $P(c)$ where

$$C = \{c \mid c \text{ is a car}\}$$

$$P(c) = \text{"car c has four wheels"}$$

we write the statement "for all c in C, P(c) is true" as

$$\forall c \in C : P(c)$$

e.g., for the function $f(x) = x^2$, we can write

$$\forall x \in \mathbb{R} : f(x) \geq 0$$

More on Proofs.

Direct Proof Template for proving $p \implies q$

Proof.

1. Start by assuming that the statement claimed in p is **T**
2. Restate your assumption in mathematical terms
3. Use mathematical and logical derivations to relate your assumption to q
4. Argue that you have shown that q must be **T**
5. End by concluding that q is **T**

Example.

Thm. If $x, y \in \mathbb{Q}$, then $x + y \in \mathbb{Q}$

Proof.

1. Assume that $x, y \in \mathbb{Q}$
2. Then there are integers a, c and natural numbers b, d such that $x = \frac{a}{b}$ and $y = \frac{c}{d}$
3. Then $x + y = (ad + bc)/bd$
4. Since $ad + bc \in \mathbb{Z}$ and $bd \in \mathbb{N}$, $x + y$ is rational.

Another example.

Thm. If $4^x - 1$ is divisible by 3, then 4^{x+1} is divisible by 3 for $x \in \mathbb{R}$.

Proof.

1. Assume that $4^x - 1$ is divisible by 3.
2. So $4^x - 1 = 3k$ for an integer k, i.e. $4^x = 3k + 1$
3. Observe: $4^{x+1} = 4 \cdot 4^x$. So
$$4^{x+1} = 4(3k + 1) = 12k + 4$$
Then $4^{x+1} - 1 = 12k + 3 = 3(4k + 1)$ is a multiple of 3.
4. Since it's a multiple of 3, it must be divisible by 3.
5. ayooo q is **T** ***

*** Note that we don't actually know that $4^x - 1$ is divisible by 3.

Exercise.

Theorem. For all pairs of odd integers m, n, the sume $m + n$ is an even integer.

Proof.

1. Assume m and n are both odd.
2. aighty this means that $m = 2k + 1$ and $n = 2l + 1$.
3. adding these together, we have
$$m + n = 2k + 1 + 2l + 1 = 2 + 2k + 2l = 2(k + l + 1)$$
4. since $m + n$ is a multiple of 2, it is divisible by 2 and thus an even number
5. **QED**

Contraposition Template for $p \implies q$

Proof.

1. Start by assuming that the statement claimed in q is **F**
2. Restate your assumption in mathematical terms
3. Use mathematical and logical derivations to relate your assumption to p
4. Argue that you have shown that p must be **F**
5. End by concluding that p is **F**

Example
Theorem. If x^2 is even, then x is even.
Proof.

1. Assume that x is odd.
2. Then $\exists k \in \mathbb{Z} : x = 2k + 1$
3. Then $x^2 = 2(2k^2 + 2k) + 1$
4. This means x^2 is 1 added to a multiple of 2, so it's odd.
5. x^2 is odd so the proof is over lol

Exercise
Theorem. If r is irrational, then $\sqrt{r}$ is irrational.
Proof.

1. Let's assume $\sqrt{r}$ is rational.
2. So $\exists a, b \in Z : \sqrt{r} = \frac{a}{b}$
3. What happens when we square it?

$$\sqrt{r}^2 = (\frac{a}{b})^2$$

$$r = \frac{a^2}{b^2}$$

   a and b are both integers, so r must be rational
4. So it's clear that r is not irrational in this case (it is rational).
5. unnecessary restatement of concluding p is **F**

Equivalence: sort of a sidenote

IF AND ONLY IF

$$p \iff q$$

This just means you have to prove the implication **both ways**.

Contradictions

e.g.,

$$1 = 2;\ n^2 < n \text{ for } n \in \mathbb{N};\ |x| < x;\ p \wedge \neg p$$

Wowie these look **FISHY** don't they?

Proof Template

1. To derive a contradiction, assume that p is **F**
2. Restate your assumption in mathematical terms
3. Derive a **FISHY** statement?a contradiction that must be false
4. Thus, the assumption in step 1 is false, and p is **T**

Exercise

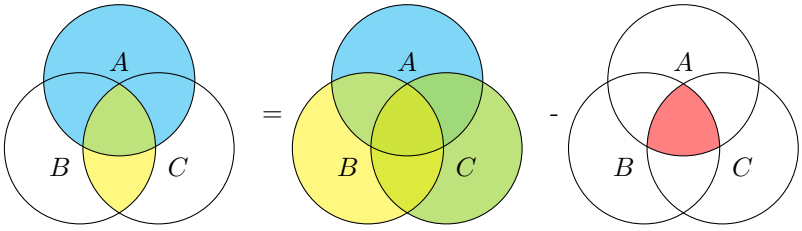
Theorem. Let a, b be integers. Then $a^2 - 4b \neq 2$

Proof.

1. Say $a^2 - 4b = 2$
2. Then
$$a^2 = 2 + 4b = 2(1 + 2b)$$
$$a = \sqrt{2}\sqrt{1 + 2b}$$
3. $\sqrt{2}$ is irrational, so a must be irrational, so it's not an integer. but a is an integer. **FISHY.**
4. alright so we must have
$$a^2 - 4b \neq 2$$

Proofs about Sets

Let's look at $A \cup (B \cap C) = (A \cup C) \cap (A \cup C)$



Induction

Template

1. Show $P(1)$
2. Assume $P(n)$
3. Show $P(n) \implies P(n+1)$

More Proof-y Things

Well-Ordering Principle

Any non-empty set of natural numbers has a minimum element.

This is important because induction follows form well ordering. e.g.

Take some predicate $P(n)$. If $P(1)$, and $P(n) \implies P(n+1)$, then $P(n)$ for $n \geq 1$.

Proof. Suppose $P(1)$ and $P(n) \implies P(n+1)$ for $n \geq 1$.

Assume $P(n)$ false for some values of n, with $n*$ representing the smallest counterexample for $P(n)$. Here, $n* > 1$ because $P(1)$ is true.

Given this assumption, $n * -1$ is not a counterexample because $n*$ is the smallest counterexample, so $P(n * -1)$ is true.

But since $P(n * -1)$ is true, we must have $P(n * -1) \implies P(n*)$. So we have a contradiction. Therefore $P(n)$ is true for all $n \geq 1$.

An example

$$n < 2^n \text{ for } n \geq 1$$

Proof.

Induction.

$P(1)$ is true because $1 < 2$. Assume $P(n)$ true. Then

$$n + 1 \leq n + n = 2n \leq 2 \cdot 2^n = 2^{n+1}$$

So $P(n+1)$ is true and therefore $P(n)$ is true.

Well-ordering

Assume that there is an $n \geq 1$ such that $n \geq 2^n$. Let $n*$ be the minimum example of this, so $n* \geq 2^n$.

We know $1 < 2^1$, so $n* \geq 2$, which gives $\frac{1}{2}n* \geq 1$. So

$$n * -1 \geq n * -\frac{1}{2}n* = \frac{1}{2}n* \geq \frac{1}{2} \cdot 2^{n*} = 2^{n*-1}$$

which means that $n * -1$ is a smaller counterexample! ooOOoOOOO.

Harder

Prove $\sum_{i=1}^{n} \frac{1}{\sqrt{i}} \leq 2n$.

Proof.

$P(1)$: $1 \leq 2 \cdot \sqrt{1}$ is true.

Assume $P(n)$. Then for $P(n+1)$ we have

$$\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} \leq 2\sqrt{n+1}$$

We can use the assumption of $P(n)$ to rewrite this

$$\begin{aligned} \sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} &= \sum_{i=1}^{n} \frac{1}{\sqrt{i}} + \frac{1}{\sqrt{n+1}} \\ &\leq 2\sqrt{n} + \frac{1}{\sqrt{n+1}} \end{aligned}$$

And here we use a *Lemma.* $2\sqrt{n} + \frac{1}{\sqrt{n+1}} \leq 2\sqrt{n+1}$

Which we prove by contradiction:

$$2\sqrt{n} + \frac{1}{\sqrt{n+1}} > 2\sqrt{n+1}$$
$$2\sqrt{n(n+1)} + 1 > 2(n+1)$$
$$4n(n+1) > 4(n+1)^2$$
$$4n > 4n + 4$$

Wow fishy.
Back to the proof:

$$\sum_{i=1}^{n+1} \frac{1}{\sqrt{i}} \leq 2\sqrt{n} + \frac{1}{\sqrt{n+1}}$$
$$\leq 2\sqrt{n+1}$$

So $P(n)$ is true for all $n \geq 1$.

Prove $n^2 \leq 2^n$ for $n \geq 4$

$$4^2 = 16 \leq 2^4 = 16$$

Assume that $n^2 \leq 2^n$ and that $2n + 1 \leq 2^n$. Then

$$(n+1)^2 = n^2 + 2n + 1 \leq 2^n + 2n + 1 \leq 2^n + 2^n = 2^n + 1$$

the tile problem

Can you tile a $2^n \times 2^n$ patio missing one of the center squares, using only the corner shaped tile?
let $P(n) :=$ the $2^n \times 2^n$ grid minus a center square can be L-tiled.
Suppose $P(n)$ is **T**. WELL. The $2^{n+1} \times 2^{n+1}$ patio can be separated into four $2^n \times 2^n$ patios.
Think about adding the center L to this first. Then all four of the subtiles were/are missing a corner square. Thus we can revise the original claim to be
$Q(n)$:
(i) the $2^n \times 2^n$ grid missing a center square can be L-tiled.
(ii) the $2^n \times 2^n$ grid missing a corner square can be L-tiled.
So add base cases and complete the proof.

Different Problem

$P(n) : n^3 < 2^n$ for $n \geq 10$
Suppose $P(n)$ is true. Consider $P(n+1) : (n+1)^3 < 2^{n+2}$??

$$(n+2)^3 = n^3 + 6n^2 + 12n + 8$$
$$< n^3 + nn^2 + n^2 n + n^3$$
$$< 4n^3 < 4 \cdot 2^n = 2^{n+2}$$

so

$$P(n) \implies P(n+2)$$

We can have two base cases to cover all cases—$P(10)$ and $P(11)$ are both true.

THE FUNDAMENTAL THEOREM OF ARITHMETIC

SUPPOSE $n \geq 2$. Then (i) n can be written as a product of prime factors, and (2) the representation of n as a product of primes is unique.

We could use $P(n)$: n is a product of primes. But this is hard. So let's use

$$Q(n) : P(2) \wedge P(3) \wedge P(4) \wedge \cdots P(n)$$

Proof. Q(1) claims 2 is a product of primes, which is true.

Assume that $Q(n)$ is true, so each of $2, 3, \ldots, n$ are prime products. Since we know $Q(n)$, to prove $Q(n+1)$, we just need to show that $n+1$ is a product of primes. There are some possible cases here:

- $n+1$ is prime. Fin.
- $n+1$ not prime, so $n+1 = kl$ where $2 \leq k, l \leq n$

In the second case, we know that $P(k)$ and $P(l)$ are both true, so k and l are both products of primes. Thus kl is a product of primes, so $n+1$ is a product of primes. $Q(n+1)$ is true for all $n \geq 2$.

Strong Induction

To prove $P(n) \forall n \geq 1$ by strong induction, use induction to prove the *stronger* claim that $Q(n)$: each of $P(1), P(2), \ldots, P(n)$ are true.

	Ordinary Induction	Strong Induction
Base Case	Prove $P(1)$	Prove $Q(1) = P(1)$
Induction Step	$P(n) \implies P(n+1)$	$Q(n) = P(1) \wedge \cdots \wedge P(n) \implies P(n+1)$

Induction is Important

Applications of Inudction

- Tournament rankings
- Greedy or recursive algorithms
- Games of strategy

Equal Pile Nim.
$P(n)$: Player 2 can win the ame that starts with n pennies in each row.

Player 2 can always return the game ot smaller equal piles. If player 2 wins the smaller game, Player 2 wins the larger game. Strong Induction!

In General

Recursive functions must have some base case, and a recursive progression that leads to the base case.p

TREES

Exercise 7.12 **Give recursive definition**

(a) $S = \{3^0, 3^1, 3^2, \dots\}$

$$1 \in \mathbb{S}$$
$$x \in \mathbb{S} \to 3 \cdot x \in \mathbb{S}$$

(b) $S = \{\text{all binary strings that are palindromes}\}$

$$\{\}, 0, 1 \in S$$
$$x \in S \implies 0x0 \in S \land x \in S \implies 1x1 \in S$$

(c) $S = \{\text{all strings of matched parentheses}\}$

$$\{\} \in S$$
$$x, y \in S \implies [x]y \in S$$

Rooted Binary Tree

Definition.

The empty tree ϵ is an RBT

If T_1, T_2 are disjoint RBTs with roots r_1 and r_2, then linking r_1 and r_2 to a *new* RBT with root r

Structural Induction

- Base Cases are True
- For every constructor rule, show: if P is T for the known parents, THen P is T for children
- By structural induction, conclude that P(s) is T for all s in S

Number Theory Stuff.

Some Basics

GCD

Euclid's algorithm

Bezout's Identity

Theorem. $\gcd(m, n)$ is the smallest positive integer linear combiantion of m and n:

$$\gcd(m, n) = mx + ny \qquad \text{for } x, y \in \mathbb{Z}$$

Crazy Facts about the GCD

(i) $\gcd(m, n) = \gcd(m, \text{rem}(n, m))$

(ii) Every common divisor of m, n divides $\gcd(m, n)$

(iii) For $k \in \mathbb{N}$, $\gcd(km, kn) = k \cdot \gcd(m, n)$

(iv) If $\gcd(l, m) = 1$ and $\gcd(l, n) = 1$, then $\gcd(l, mn) = 1$

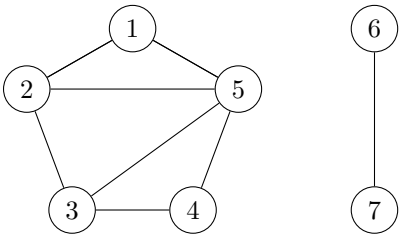
(v) If $d \mid mn$ and $\gcd(d, m) = 1$, then $d \mid n$

$$\begin{aligned} 5^2 &\equiv 1 \mod 3 \\ (5^2)^{1007} &\equiv 1 \mod 3 \\ 5 \cdot (5^2)^{1007} &\equiv 5 \equiv 2 \mod 3 \end{aligned}$$

Modular Division things

Suppose $ac \equiv bc \mod d$. Then $a \equiv b \mod d$ if $\gcd(c, d) = 1$.

GRAPHS



COUNTING

This is what discrete math is all about.

Say you have three kinds of things and you organize them into groups of three. how many possible groups? There are 10. But what happens when you scale up? gets a lot harder.

Sum Rule. N objects of two types: N_1 of type 1 and N_2 of type 2. Then $N = N_1 + N_2$.

$$|\{A_1 A_2 \dots A_n\}| = |A_1||A_2| \cdots |A_n|$$

Example: 10 runners; how many possible top 3 finishes? $|\{FST\}| = 10 \times 9 \times 8 = 720$