Transition:- DS + Algorithms

Proofs

Last time:

$\neg(P(x) \wedge \neg P(y)) =$

deMorgans $\neg P(x) \vee \underbrace{\neg\neg P(y)}$

$= \neg P(x) \vee P(y)$

Implications + quantifiers

Let $P(x) =$ "$x > 0$"

and $Q(x,y) =$ "$xy \leq 0$"

translate:

all $\mathbb{R}$

$\underbrace{\boxed{\forall x \forall y}}_{\text{lazy: universe or set?}} \in \mathbb{R} \underbrace{(P(x) \wedge \neg P(y))}_{p} \rightarrow \underbrace{Q(x,y)}_{q}$

For every pair of real #s, $x + y$, if $x > 0$ and $y \leq 0$, then $xy \leq 0$.

Contrapositive: "$\forall x, y \in \mathbb{R}$, if $xy > 0$ then either $x \leq 0$ or $y > 0$".

Proofs

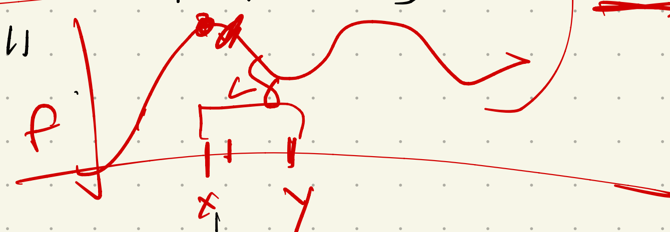
A theorem (or lemma, proposition, etc.) is a statement that can rigorously be shown to hold true.

Generally in math, something like:

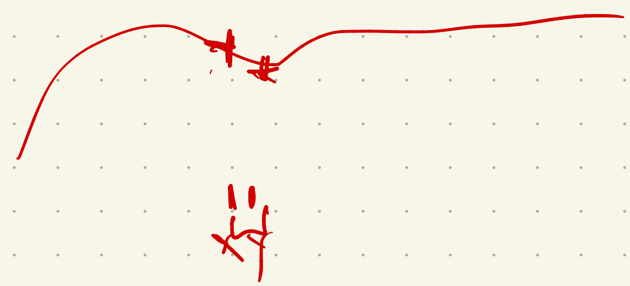
→ "If n is even, then it is divisible by 2."

"$\forall \varepsilon > 0$ $\exists \delta > 0$ ~~s.t.~~ if $|f(x) - f(y)| < \varepsilon$, then $|x - y| < \delta$" cts

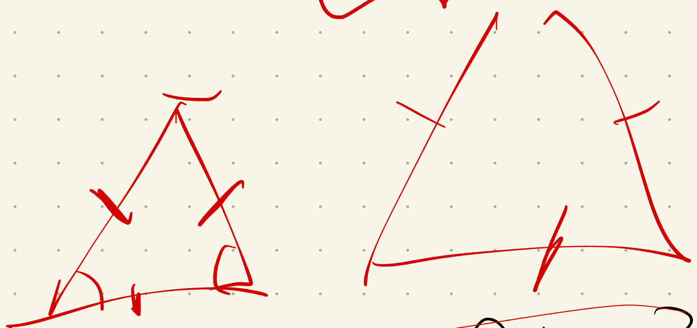
$\in \mathbb{R}$ $\mathbb{R}$



The sequence of statements giving the argument is a proof.



Consider $p \to q$:



p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	T	T

When is it false?

So: to justify $p \to q$, need to show **not** in row 2.

In other words:
if $p = T$, q cannot be F.

"inference"

First, some base assumptions & dfns:

← exists or existential!

x even: $\iff \exists k \in \mathbb{Z}$ s.t. $2k = x$

x odd $\iff \exists k \in \mathbb{Z}$ s.t. $x = 2k+1$

8 even: $\iff$ b/c $2 \cdot \underline{4} = 8$

parity: whether even or odd

x divides y, or $x \mid y$, if & only if
$\exists k \in \mathbb{Z}$ s.t. $k \cdot x = y$

Other good background:

x rational: $\exists p, q \in \mathbb{Z}$ s.t. $x = p/q$

x composite/prime: only 1 and x are divisors of x,

not prime, or $\exists$ at least one divisor $y \neq 1$ or x

Some other background assumptions!

The rules of algebra.

For example if x, y, and z are real numbers and $x = y$, then $x + z = y + z$.

The set of integers is closed under addition, multiplication, and subtraction.

In other words, sums, products, and differences of integers are also integers.

Every integer is either even or odd.

This fact is proven elsewhere in the material.

If x is an integer, there is no integer between x and $x + 1$.

In particular, there is no integer between 0 and 1.

The relative order of any two real numbers.

For example, $\frac{1}{2} < 1$ or $4.2 \geq 3.7$.

The square of any real number is greater than or equal to 0.

This fact is proven in a later exercise.

Also: addition & mult are commutative:

$\forall x, y,\ x + y = y + x$! work for any x & y

Division & subtraction are not:

$\exists x, y$ s.t. $x - y \neq y - x$

Prove: $x = 3$ $y = 1$

$3 - 1 = 2 \neq 1 - 3 = -2$

Example:

If n is an odd integer, then n^2 is even.

"$\forall n \in \mathbb{Z}$, if n is odd, then n^2 is even"

hidden

True or false?

No: Find some n:

1 : $1^2 = 1$ odd, not even.

Example:

If $\overbrace{n \text{ is an even integer,}}^{p}$ then $\underbrace{n^2 \text{ is even.}}_{q}$ $\to n^2 = 2(\underbrace{\quad}_{\text{integer}})$

Proof:

(Assume p is true, and show that q cannot be false.)

must be T

Pick any n even $\overset{\text{dfn}}{\Longrightarrow} \exists k \in \mathbb{Z}$ s.t. $2k = n$.

then $n^2 = (2k)^2 = 4k^2$

$= 2(2k^2) = 2\ell$

where $\ell = 2k^2 = 2 \cdot k \cdot k \to$ this is in $\mathbb{Z}$

$\Rightarrow n^2$ is even

Example: (direct proof)

If $\underbrace{x \text{ is even}}_{}$ and $\underbrace{y \text{ is odd}}_{}$, then

$\underbrace{x+y \text{ is}}_{}$ odd

Proof: (assume first part, & directly reason to get conclusion)

p $\boxed{\begin{array}{l} x \text{ is even} \\ \text{and } y \text{ is odd} \end{array}}$ $\begin{array}{l} \Rightarrow \exists i \text{ s.t. } 2i = x \\ \Rightarrow \exists j \text{ s.t. } 2j+1 = y \end{array}$

then $x+y = 2i + 2j + 1$

$= 2\underbrace{(i+j)}_{\in \mathbb{Z}} + 1$

$\Rightarrow x+y$ is odd $\blacksquare$

Proof by cases

The book shows some basic proof by cases, but these can get more interesting:

For all $n \in \mathbb{Z}$, n^2+n is even.

Proof:

By cases:

n even: $n = 2k$ for $k \in \mathbb{Z}$

$$n^2+n = \underbrace{(2k)^2}_{4k^2} + 2k = 2\underbrace{(2k^2+k)}_{\in \mathbb{Z}}$$ ✓

n odd: $n = 2k+1$ for $k \in \mathbb{Z}$

$$n^2+n = (2k+1)^2 + 2k+1 = 4k^2+4k+1 + 2k+1$$

$$= 4k^2+6k+2 = 2(\underset{\in \mathbb{Z}}{\quad})$$

Assumptions

Proofs written for publication can assume a lot of background:

Theorem 3.2. *Let (X, f) be a generic Reeb graph with vertex set $V(X) = \{v_1, v_2, \ldots, v_n\}$. We denote the critical set $S = \{a_1 < a_2 < \ldots < a_n\}$ and assume that the vertices are sorted so that $f(v_i) = a_i$. Let $\varepsilon > 0$ be a value such that $2\varepsilon \neq |a_i - a_j|$ for any i, j. Let $W \subseteq V$ be the subset of vertices where each $w \in W$ contributes to a point in Rel_1 which has lifetime at most 2ε. Then there is a bijection*

$$\Phi : V(X) \setminus W \to V(S_\varepsilon(X)),$$

and $S_\varepsilon(X, f)$ is generic.

Even some later in class can be intense!

Theorem 4.1 (Master theorem)
Let $a \geq 1$ and $b > 1$ be constants, let $f(n)$ be a function, and let $T(n)$ be defined on the nonnegative integers by the recurrence

$T(n) = aT(n/b) + f(n)$,

where we interpret n/b to mean either $\lfloor n/b \rfloor$ or $\lceil n/b \rceil$. Then $T(n)$ has the following asymptotic bounds:

1. If $f(n) = O(n^{\log_b a - \epsilon})$ for some constant $\epsilon > 0$, then $T(n) = \Theta(n^{\log_b a})$.
2. If $f(n) = \Theta(n^{\log_b a})$, then $T(n) = \Theta(n^{\log_b a} \lg n)$.
3. If $f(n) = \Omega(n^{\log_b a + \epsilon})$ for some constant $\epsilon > 0$, and if $af(n/b) \leq cf(n)$ for some constant $c < 1$ and all sufficiently large n, then $T(n) = \Theta(f(n))$. ∎

Indirect proofs

or "proof by contrapositive"

Recall: $p \to q$ is logically equivalent to $\neg q \to \neg p$

So: if $p \to q$ seems difficult, we can instead consider showing $\neg q \to \neg p$ is true

Ex: If $3n+2$ is odd, then n is odd.

Try direct:

$3n+2$ odd $\Rightarrow \exists k \in \mathbb{Z}$ s.t.

$$3n+2 = 2k+1$$

$$\Rightarrow 3n = 2k-1$$

$$\Rightarrow n = \frac{2k+1}{3}$$ ... stuck ??

Instead:

$$\text{If } \overbrace{3n+2 \text{ is odd}}^{p}, \text{ then } \underbrace{n \text{ is odd}}_{q}.$$

contrapos: $\neg q \rightarrow \neg p$

If n is even

then $\boxed{3n+2 \text{ is even}}$. $2\cdot(\ )$

try: n even $\Rightarrow \exists k \in \mathbb{Z}$, s.t. $2k = n$

consider $3n+2 = 3(2k)+2$

$= 6k+2$

$= 2\underbrace{(3k+1)}_{\in \mathbb{Z}}$

so $3n+2$ is even. ☒

Two way implications

Example: For any $n \in \mathbb{Z}$,

n is odd $\Longleftrightarrow$ n^2 is odd.

- Here, $\Longleftrightarrow$ reads as "if and only if"

- Sometimes written $p \leftrightarrow q$

so $(p \to q) \wedge (q \to p)$

How to prove:

Let's try:

For any $n \in \mathbb{Z}$,
n is odd $\iff n^2$ is odd.

Proof:

$\Rightarrow$:

$\Leftarrow$:

Proof by contradiction: (or indirect proof)

Recall that a contradiction is a logical statement which is always false

Ex: $2=1$
$x = x+1$ } F

Consider $p \to q$:

p	q	$p \to q$
T	T	
T	F	
F	T	
F	F	

Bad row: want to exclude.

so: $p \wedge \neg q$ is thing to avoid!

Proof by contradiction:
Assume $p \wedge \neg q$, then show some logical contradiction exists.

Example: If n^2 is even, then n is even.

Another:

Prove that $\sqrt{2}$ is irrational.

Recall: x rational means

$\exists p, q \in \mathbb{Z}$ s.t. $x = p/q$

Proof: assume $\sqrt{2}$ is rational, + then make a contradiction