FOCS Notes
Lecture
1/24/2020

Agenda:

- Proofs:
  - Direct proof $\rightarrow$ if $x > 1$ then $x > 0$
  - Proof by contrapositive $\rightarrow$ if x^2 is even, then x is even
  - Proof by contradiction $\rightarrow$ $\sqrt{2}$ is irrational
  - Proof by reductio ad absurdum $\rightarrow$ if $a > c \ and \ b > c$, then $max(a, b) > c$

Implication: $p \rightarrow q$

p	q	$p \rightarrow q$
T	T	T
T	F	F
F	T	T
F	F	T

If x^2 is even, then x is even
p = "Cats dont like Sally"
q = "Sally is a millionaire"
$p \rightarrow q$ if p is T then q must be T

Implications: Reasoning without facts
Reasoning: It rained last night (fact); the ground is wet (deduced)
Reasoning without facts: If it rained last night then the ground is wet.
Ex: if $ax^2 + bx + c = 0$, then $x = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$

Proving an Implication
Direct Proof: $p \rightarrow q$

1. Assume p
2. Show using logic and theorems and axioms, that q is true

Ex: if p and q are rational, then $p + q$ is rational

Proof. We prove this via direct proof. Assume $p, q \in \mathbb{Q}$ or equivalently $p = \frac{a}{b}$ and $q = \frac{c}{d}$ for $a, c \in \mathbb{Z} \ and \ b, d \in \mathbb{N}$. By algebraic manipulations, $p + q = \frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{cb}{bd} = \frac{ad+cb}{bd}$. Clearly $ab + cb \in \mathbb{Z}$ and $bd \in \mathbb{N}$, so $p + q \in \mathbb{Q}$ as claimed. □

Template for a direct proof of $p \rightarrow q$

1. Start off by assuming that p is true
2. Restate that assumption mathematically
3. Use mathematical & logical deductions to relate the assumption to q
4. Argue we've shown q is true
5. Conclude that q is true, so $p \rightarrow q$

A proof is a mathematical essay

1. State your strategy - (State the proof method)
2. Ensure your proof flows logically
3. Keep it simple
4. Justify your steps
5. End your proof
6. Recheck your proof

Ex (Direct Proof)
Claim: $\forall x \in \mathbb{R}$: if $4^x - 1$ is divisible by 3, then $4^{x+1} - 1$ is divisible by 3

Proof. We use direct proof. Assume $4^x - 1$ is divisible by 3, that is, $4^x - 1 = 3n\ for\ n \in \mathbb{Z}$.
As a consequence, $4^x = 3n+1$ and therefore $4^{x+1} = 4(3n+1) = 12n+4$. Clearly this implies $4^{x+1} - 1 = 12n+3 = 3(4n+1)$. That is, $4^{x+1} - 1$ is divisible by 3, as claimed. □

<u>Proof by Contraposition</u>
If we want to prove that $p \to q$ is true, it suffices to show that $\neg q \to \neg p$ (the contrapositive). Proving $p \to q$ via establishing $\neg q \to \neg p$ using the direct method is called proof by contraposition
<u>Ex</u> if x^2 is even then x is even

Proof. We use proof by contraposition. Assume x is not even, that is $x = 2n+1\ for\ n \in \mathbb{Z}$. This means that $x^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 2(2n^2 + 2n) + 1$ so x^2 is odd. Thus we have shown that x is odd implies x^2 is odd. The contrapositive: x^2 is even implies x is even, is therefore true. □

<u>Template for proof by contraposition for $p \to q$</u>

1. Start by assuming that q is false
2. Restate this in mathematical terms
3. Use mathematical and logical deductions to relate this assumption to p
4. Argue that you have shown p is false
5. End by concluding that p is false

<u>Ex</u> If r is irrational, then $\sqrt{r}$ is irrational

Proof. We use contraposition. Assume that $\sqrt{r}$ is rational, that is, $r = \frac{a}{b}$ for some $a \in \mathbb{Z}\ and\ b \in \mathbb{N}$. Squaring $\sqrt{r}$, we get that $r = \frac{a^2}{b^2}$; clearly $a^2 \in \mathbb{Z}$ and $b^2 \in \mathbb{N}$, so $r \in \mathbb{Q}$. □

<u>Equivalence/If and Only If</u>
$p \iff q$ means $p \to q$ is true and $q \to p$ is true

p	q	$p \iff q$
T	T	T
T	F	F $\leftarrow$ because this shows that $p \to q$ is not true
F	T	F $\leftarrow$ because this shows that $q \to p$ is not true
F	F	T

Thus we see that $p \iff q$ is true when there are no example where p and q have different truth values
To prove that $p \iff q$ is true:

1) prove that $p \to q$ (so row 2 cannot occur)
2) prove that $q \to p$ (so row 3 cannot occur)

Ex x is divisible by 3 $\iff$ x^2 is divisible by 3 ($p \iff q$)

Proof. First, we show that $p \to q$ by direct proof. Assume that x is divisible by 3, i.e, $x = 3k$ for some $k \in \mathbb{Z}$. This means $x^2 = 9k^2 = 3(3k^2)$, which establishes that x^2 is divisibly by 3, as claimed.
Next, we show that $q \to p$ by contraposition. Assume that x is not divisible by 3. There are two cases:

i) $x = 3k + 1$

ii) $x = 3k + 2$

for some $k \in \mathbb{Z}$.
Consider case i): $x^2 = (3k+1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$.
Consider case ii): $x^2 = (3k+2)^2 = 9k^2 + 12k + 4 = 9k^2 + 12k + 3 + 1 = 3(3k^2 + 4k + 1) + 1$
In both cases, we see that x^2 is not divisible by 3. □

Proof by Contradiction
Ex: $x = 3$ and x is even is a contradiction

Proof. $x = 3 = 2 + 1$ and $x = 2k$ for some $k \in \mathbb{Z}$. $2 + 1 = 2k \;\to\; 2(k-1) = 1$ □

Principle of Contradiction
If you derive a contradiction, then one of your assumptions is false.
Ex let a, b be integers, then $a^2 - 4b \neq 2$

Proof. We use proof by contradiction. Assume there are integers a and b such that $a^2 - 4b = 2$. This implies $a^2 = 2 + 4b = 2(2b+1)$. This means a is even, that is $a = 2k$ for some $k \in \mathbb{Z}$. But this implies $a^2 - 4b = 4k^2 - 4b = 4(k^2 - b) \neq 2$ because $a^2 - 4b$ is an integer multiple of 4. This contradiction allows us to conclude that there are no integers a and b such that $a^2 - 4b = 2$ by the principle of contradiction. □

Template for proof by contradiction (of p)

1. Assume p is false
2. Restate in mathematical terms
3. Derive a contradiction (using mathematically valid arguments)
4. Conclude that our assumption that p is false is incorrect. Therefore p is true

Picking a proof template

situation	suggested type of proof
Clear how conclusion follows from assumption	Direct proof
Clear that if the conclusion is false then the assumption has to be false	Contraposition
Prove something exists	Show an example
Prove something doesn't exist	Contradiction
Prove uniqueness	Contradiction