37181 DISCRETE MATHEMATICS

©Murray Elder, UTS

Lecture 3: proofs

PLAN

- proof methods:
  - direct
  - contrapositive
  - contradiction

PROOFS

Proofs in mathematics or computer science are based on the argument forms we started to learn last week.

To start with, the main types of proof styles are:

- direct
- contrapositive
- contradiction
- induction

$p \to q$

$\neg q \to \neg p$

$(\neg p \to F) \to p.$

If you do more math or theoretical computer science you will see more styles.

there exists

Definition

Let $a, b \in \mathbb{Z}$. We say a *divides* b if $\exists s \in \mathbb{Z}$ such that $b = as$.

in

set of
all integers
(whole numbers)

in $\mathbb{Z}$

Eg 20 divides 100

because : $\boxed{s = 5}$ $100 = 20 \cdot \underbrace{5}$

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\underbrace{\exists s \in \mathbb{Z}}$ such that $b = as$.

For example, 3 divides -18 since

$$-18 = 3 \cdot (-6)$$

not $\forall s \in \mathbb{Z}\,(b \neq as)$

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\exists s \in \mathbb{Z}$ such that $b = as$.

For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since

if $\cancel{b = a \cdot s}$ $14 \cdot 3s$

$s = \frac{14}{3} = 12\frac{2}{3}$

not in $\mathbb{Z}$.

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\exists s \in \mathbb{Z}$ such that $b = as$.

For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since for all $s \in \mathbb{Z}$ $14 \neq 3s$.

DIVIDES

Definition

Let $a, b \in \mathbb{Z}$. We say *a divides b* if $\exists s \in \mathbb{Z}$ such that $b = as$.

For example, 3 divides -18 since there exists -6 such that $-18 = 3 \cdot (-6)$

3 does not divide 14 since for all $s \in \mathbb{Z}$ $14 \neq 3s$.

Notation: $a \mid b$ means "a divides b"

divides

Sometimes it is easy to show step-by-step that p implies q (or using *~~syllogism~~* $(p \to r)$ and $(r \to s)$ and $(s \to t)$ and $(t \to q)$). $\longrightarrow (p \to q)$

$\wedge \quad \wedge \quad \wedge$

Recall that an integer n is *even* if

$$2 \mid n.$$

DIRECT

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* ($p \to r$) and ($r \to s$) and ($s \to t$) and ($t \to q$)).

Recall that an integer n is *even* if $2 \mid n$, that is, it can be written as $n = 2d$ for some $d \in \mathbb{Z}$.

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* $(p \rightarrow r)$ and $(r \rightarrow s)$ and $(s \rightarrow t)$ and $(t \rightarrow q)$).

Recall that an integer n is *even* if $2 \mid n$, that is, it can be written as $n = 2d$ for some $d \in \mathbb{Z}$.

Lemma

Let $n \in \mathbb{Z}$. If n is even then n^2 is even.

Proof: Since n is even, $\exists\, d \in \mathbb{Z}$ so that $n = 2d$.

Then $n^2 = 4d^2 = 2\underbrace{(2d^2)}$ and $2d^2 \in \mathbb{Z}$. $\therefore$ therefore $\Rightarrow n^2$ is even.

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* $(p \to r)$ and $(r \to s)$ and $(s \to t)$ and $(t \to q)$).

Recall that an integer n is *even* if $2 \mid n$, that is, it can be written as $n = 2d$ for some $d \in \mathbb{Z}$.

Lemma

Let $n \in \mathbb{Z}$. If n is even then n^2 is even.

Proof.

By hypothesis, $n = 2s$ for some $s \in \mathbb{Z}$. Then

$n^2 = 2s \cdot 2s = 2(2s^2)$ so is even

$\square$

DIRECT

Sometimes it is easy to show step-by-step that p implies q (or using *syllogism* $(p \to r)$ and $(r \to s)$ and $(s \to t)$ and $(t \to q)$).

Recall that an integer n is *even* if $2 \mid n$, that is, it can be written as $n = 2d$ for some $d \in \mathbb{Z}$.

Lemma

Let $n \in \mathbb{Z}$. If n is even then n^2 is even.

Proof.

By hypothesis, $n = 2s$ for some $s \in \mathbb{Z}$. Then $n^2 = (2s)^2 = 4s^2 = 2(2s^2)$ is even. $\square$

Lemma

If $n \in \mathbb{Z}$ is even then n^3 is even.

Proof.

By hypothesis, $\exists s \in \mathbb{Z}$ so that $n = 2s$.

Then $n^3 = (2s)^3 = 8s^3$
$= 2(4s^2)$

$\therefore$ n^3 is even. $\square$

YOUR TURN

Lemma

If $n \in \mathbb{Z}$ is even then n^3 is even.

Proof.

By hypothesis, $n = 2s$ for some $s \in \mathbb{Z}$. Then $n^3 = (2s)^3 = 2(4s^3)$ is even. $\square$

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

n^2 is even, so $\exists\, s \in \mathbb{Z}$

so that $n^2 = 2s$

$n = \sqrt{2s}$

$\sqrt{n^2}, \sqrt{2s}$

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

? direct doesn't work $\square$

Recall that $p \to q$ is logically equivalent to (has the same truth values as) $\neg q \to \neg p$.

Check this with a truth table.

p	q	$p \to q$	$\neg q$	$\to$	$\neg p$
1	1	1	0	1	0
1	0	0	1	0	0
0	1	1	0	1	1
0	0	1	1	1	1
			1	2	1

Recall that $p \to q$ is logically equivalent to (has the same truth values as) $\neg q \to \neg p$.

Check this with a truth table.

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

$p \to q$

Instead of trying to prove this directly, we will prove $\neg$ (n is even) implies $\neg$ (n^2 is even).

n is odd

CONTRAPOSITIVE

Recall that $p \to q$ is logically equivalent to (has the same truth values as) $\neg q \to \neg p$.

Check this with a truth table.

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Instead of trying to prove this directly, we will prove $\neg$ (n is even) implies $\neg$ (n^2 is even).

In other words, if n is odd then n^2 is odd.

CONTRAPOSITIVE

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

definition of odd

Proof.

If n is odd, then $n = 2s + 1$ for some $s \in \mathbb{Z}$,

$$n^2 = (2s+1)(2s+1)$$

$$= 4s^2 + 4s + 1$$

$$= 2(\underbrace{2s^2+2s}) + 1 \quad \therefore \; n^2 \text{ is odd}$$

By contrapositive, the statement is proved $\square$

 $(p \to q) \leftrightarrow (\neg q \to \neg p)$

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

If n is odd, then $n = 2s + 1$ for some $s \in \mathbb{Z}$, so
$n^2 = 4s^2 + 4s + 1 = 2(2s^2 + 2s) + 1$ which is an odd number.

CONTRAPOSITIVE

Lemma

Let $n \in \mathbb{Z}$. If n^2 is even then n is even.

Proof.

If n is odd, then $n = 2s + 1$ for some $s \in \mathbb{Z}$, so
$n^2 = 4s^2 + 4s + 1 = 2(2s^2 + 2s) + 1$ which is an odd number.

Since the statement we have proved (the contrapositive) is logically equivalent to the original statement to be shown, we are done. $\square$

$\in \mathbb{Z}$ Eg 7, 5, 3, 2

37181

Definition:
A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

n even → $n \leq 2$ or n not prime

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

[Contrapositive]

Universe of discourse.

Proof If n is even

then $n = 2s$ some $s \in \mathbb{Z}$

Suppose $n > 2$, (if not, $n \leq 2$ and we are done)

then $2 \mid n$ and $2 \neq n$ and $n \mid n$

n has at least two distinct positive divisors, so n is not prime.

So by contrapositive, statement is proved □

Definition:
A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

Contrapositive is:

n even $\longrightarrow$ $n \leq 2$ or n not prime.

PRIMES

Definition:
A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

Contrapositive is:

Proof.

PRIMES

Definition:
A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

Contrapositive is:

also $p \lor \neg p$ is always true.

Proof.

If n is even then $n = 2s$ so 2 divides n. Then $n \leqslant 2$ or $n > 2$, and if $n > 2$ it it cannot be prime since it has 2 as a divisor. $\square$

and n as a divisor

and $n \neq 2$.

Definition:
A *prime number* is an integer $p > 1$ whose only positive divisors are itself and 1.

Lemma

Let $n \in \mathbb{Z}$. If $n > 2$ and n is prime then n is odd.

Contrapositive is:

Proof.

If n is even then $n = 2s$ so 2 divides n. Then $n \leqslant 2$ or $n > 2$, and if $n > 2$ it it cannot be prime since it has 2 as a divisor. $\square$

Note in my proof, I added a hypothesis $q \vee \neg q$ half way!

If you start to list prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots$$

$, \ldots, 37181$

If you start to list prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots$$

they seem to appear less and less often. So do they run out eventually?

Run out.

Finite list.

p	F	$(\neg p \to F) \to p$
1	0	crazy 1
0	0	

If you start to list prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots$$

they seem to appear less and less often. So do they run out eventually?

$\phi \wedge \neg \phi$

0

0

Theorem (Euclid)

There are infinitely many different primes.

If you start to list prime numbers,

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ \ldots$$

they seem to appear less and less often. So do they run out eventually?

Theorem (Euclid)

There are infinitely many different primes.

This time we have a statement $p =$ "there are infinitely many primes", and we will prove that $\neg p$ implies a contradiction, *i.e.* use $(\neg p \to F) \to p$.

Assume

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the distinct primes:

$$p_1,\ p_2,\ \ldots,\ p_n.$$

PROOF BY CONTRADICTION

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the distinct primes:

$$p_1,\ p_2,\ \ldots,\ p_n.$$

Any other number not on this list is not a prime. Okay, now I will challenge that. Consider

$$N = (p_1 p_2 \cdots p_n) + 1$$

N is bigger than every number p_i on the list above. Therefore N cannot be prime.

~~But if $a \mid N$, either $a = p_i$ some $1 \leq i \leq n$~~

~~Or [illegible] prime has a~~

Suppose N is not prime,

then some $p_i \mid N$

"one of the primes in the list above"

p_i

$1 \le i \le n$

so $\frac{N}{p_i} \in \mathbb{Z}$

but $= \underbrace{p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n}_{\text{integer}} + \underbrace{\frac{1}{p_i}}_{0 < \frac{1}{p_i} < 1}$

Lemma

Let $n \in \mathbb{Z}$. If n is not prime then there exists a prime number p so that $p \mid n$.

$a > 1$

PROOF BY CONTRADICTION

Theorem (Euclid)

There are infinitely many different primes.

Proof.

Suppose (for contradiction) this is not true. So here are all the distinct primes:

$$p_1,\ p_2,\ \ldots,\ p_n.$$

Any other number not on this list is not a prime. Okay, now I will challenge that. Consider

$$N = (p_1 p_2 \cdots p_n) + 1$$

Is N prime or not?

□

Ex If n is divisible by 7 then n^2 is divisible by 7.

Proof (Direct) By hypothesis, $\exists s \in \mathbb{Z}$ so that

$$n = 7s$$

Then $$n^2 = 49s^2 = 7(7s^2).$$

$\therefore$ n^2 is divisible by 7.

Ex2 Prove that if n^2 is divisible by 7 then n is divisible by 7.

Proof (Contrapositive)

Suppose n is not divisible by 7

Then $\exists s \in \mathbb{Z}$ so that

$$n = 7s + i$$

$1, 2, 3, 4, 5, 6$

$1 \leq i \leq 6$
$i \in \mathbb{Z}$

$23 = 21 + 2$
$= 28 - 5$

$n^2 = (7s+i)^2$
$= 49s^2 + 14si + i^2 = 7(7s^2 + 2si) + \_$

between 1 and 6

Next lecture: more proof practice

- rational and irrational numbers
- first element
- well ordering principle

Contrapositive to prove implication statements.

$p \to q \Leftrightarrow \neg q \to \neg p$

Contradiction

$(\neg p \to F) \to p$

crazy

$\boxed{a \to b}$

$\neg(a \to b)$ $\neg(\neg a \vee b)$

$a \wedge \neg b \to \neg a$ $a \wedge \neg a$

Statement p : $\boxed{a \to b}$

Assume $\neg p$: $\neg(a \to b)$

$\equiv a \wedge \neg b$

Then ~~in contr~~ argue that $\neg b \to \neg a$ $a \wedge \neg a$