MATH1005/6005 Revision Lecture 1

For ~~today~~: $\boxed{\text{"Proofs"}}$

Preliminary: $\boxed{\text{arguments}}$

$$\Big[\underbrace{p_1, \ldots, p_n}_{\text{premises}} \;\therefore\; q\Big]$$

conclusion

$$\left.\begin{array}{c} p_1 \\ \vdots \\ p_n \end{array}\right\} \over q$$

What are $p_1, \dots, p_n, q$?

statements or statement forms

i.e. placeholders for statements

An argument is valid if

$p_1 \wedge \dots \wedge p_n \to q$ is a tautology (i.e. "$\to$" is true for any inputs into the statement forms.

What does an argument not do?

Does not tell us that the premises are true.

All it says is something about truth tables of statement forms.

Arguments are just the structure of a proof.

Some valid arguments:

Direct argument

$$\begin{array}{c} p \\ p \to q \\ \hline q \end{array}$$

$$\begin{array}{c} p \to q \\ \neg q \\ \hline \neg p \end{array}$$

Division into cases

$$\begin{array}{c} p \vee q \\ p \to r \\ q \to r \\ \hline r \end{array}$$

$\boxed{\text{Proofs:}}$

function evaluated at $x = 2$ vs. function of x

Proof vs. Argument

Structure as an argument, but the statement forms are replaced by actual statements. Might need to check each statement is actually true.

Structure built out of statement forms. Valid if premises can be combined to produce the conclusion.

Example

Direct argument

$$\begin{array}{c} p \\ (p \to q) \\ \hline q \end{array}$$

Isn't true

upon substitution

But what if

$p =$ Is human

$q =$ has seven legs

Note: $p \to q$ is false for this particular p, q.

To prove something, you need to both:

- have a valid argument structure
- Check that all the premises are actually true

How to actually prove things*

*Involving $\rightarrow$

1. Figure out if you actually believe the statement

2. Identify the assumptions and conclusion

$$[\underbrace{p_1, \dots, p_n} \quad \therefore r]$$

3.* Try to decide on a valid argument structure

Might require new premises

$$[p_1, \dots, p_n, \underbrace{q_1, \dots, q_m}_{\text{new premises}}, r]$$

4. Verify any added premises

*: Creative process, might require trial and error, easier with experience

Example: $\forall n \; p(n)$ where $p(n)$ = "$f(n)$ is divisible by 6"

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

$$f(n) := n^3 + 3n^2 + 2n$$

is divisible by 6.

For this course

$\mathbb{N} = \{1, 2, 3, \dots\}$

$\mathbb{Z}_{\geq} = \{0, 1, 2, 3, \dots\}$

$\mathbb{Z} = \{\dots, -1, 0, 1, \dots\}$

Do we believe the statement? $f(0) = 0$, $f(1) = 6$, $f(-1) = 0$, $f(2) = 24$

all divisible by 6.

Assumption(s): $n \in \mathbb{Z}$

Conclusion: $f(n)$ is divisible by 6

Structure: Direct / contrapositive / ~~counter example~~ / contradiction

contrapositive: assume $f(n)$ not divisible by 6 ⋮ Find $n \notin \mathbb{Z}$

~~counter example~~: since we believe the statement. $\exists n \; \neg p(x)$

contradiction: tricky. $\neg (p \to r) \to c$, c = column of "false" in a truth table

What do the different structures look like?

Direct:

Suppose ($n \in \mathbb{Z}$) p

⋮

So ($f(n)$ is divisible by 6) r

Contrapositive:

Suppose ($f(n)$ is not divisible by 6) $\neg r$

⋮

So ($n \notin \mathbb{Z}$.) $\neg p$

$$\frac{\begin{array}{c} p \\ ??? \\ \vdots \end{array}}{r}$$

How do we fill in the gap?

Some (direct) options

"$p \to r$"

"$p \to p_1 \vee \dots \vee p_n$"

$p_1 \to r$

⋮

$p_n \to r$

e.g. $n \in \mathbb{Z} \to (n \text{ even}) \vee (n \text{ odd})$

n odd $\to r$

n even $\to r$

(since I already know it works).

Let's go with the first option

So our proof is:

p

Suppose $n \in \mathbb{Z}$.

$p \to r$

Then $f(n) = n^3 + 3n^2 + 2n$

$= n(n^2 + 3n + 2)$

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

So $f(n)$ is the product of three consecutive integers.
Atleast one will be even, and at least one will be divisible by 3.

Creative, and difficult to teach

So $f(n)$ is divisible by 6.

r

Other sorts of statements and proof strategies

For any statement, the first thing to do is

Statement form	Prove	Disprove
$\forall x \; p(x)$	Assume x is fixed but arbitrary, argue $p(x)$ is true or show $\nexists x \; \neg p(x)$ by contradiction	• $\neg(\exists x \; p(x))$ • $\equiv \forall x \; \neg p(x)$
$\exists x \; p(x)$	• Find an example • Show $\forall x \; \neg p(x)$ must be false by contradiction	$\neg(\forall x \; p(x))$ $\equiv \exists x \; \neg p(x)$
$p \to q$	already covered	$\neg(p \to q) \equiv p \wedge \neg q$ So come up with an example with p and $\neg q$
$p \leftrightarrow q$	$p \to q$ and $q \to p$	Counter example of $p \to q$ **or** $q \to p$.

$\forall x \; p(x)$ example

Statement:

$\overbrace{(\forall z \in \mathbb{Z})}^{p}, \; \underbrace{(z^2 + 3z + 1 \text{ is odd})}_{r}$

This statement <u>is</u> true

Try $\cancel{p \to r}$

Try $\begin{cases} p \to e \vee o \\ e \to r \\ o \to r \end{cases}$

$\left(\begin{array}{l} e: \; z \text{ is even} \\ o: \; z \text{ is odd} \end{array}\right)$

Proof:

Suppose $z \in \mathbb{Z}$

Then z is even or odd (by even/odd theorem).

If z is even, $\exists k \in \mathbb{Z}$ with $z = 2k$

So $z^2 + 3z + 1 = 4k^2 + 6k + 1$

$= 2(2k^2 + 3k) + 1$ odd

If z is odd, $\exists k \in \mathbb{Z}$ with $z = 2k+1$

So $z^2 + 3z + 1 = (2k+1)^2 + 3(2k+1) + 1$

$= 4k^2 + 4k + 1 + 6k + 3 + 1$

$= 4k^2 + 10k + 5$

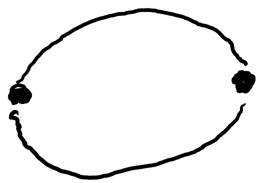
$= 2(2k^2 + 5k + 2) + 1$ odd

So $z^2 + 3z + 1$ is odd.

$\exists x \quad p(x)$ example

Statement:
There exists a graph with at least two vertices, which has a circuit which is both a Hamiltonian circuit and an Euler circuit.

Can prove by giving an example.



Has a circuit which is Euler and Hamiltonian, and it has at least two vertices.

Disproving $\exists$, $\forall$?

Disprove $\exists x \; p(x)$ $\iff$ Prove $\forall x \; \neg p(x)$

" $\forall x \; p(x)$ $\iff$ " $\exists x \; \underline{\neg p(x)}$

Disprove $\rightarrow$ example:

$\neg(p \to q) \equiv \underbrace{p}\wedge \neg \underbrace{q}$

Statement:

Let $a,b,c \in \mathbb{N}$. (If $\overset{p}{\text{c divides ab}}$), then $\overset{q_1}{(\text{c divides a})}$ $\overset{\vee}{\text{or}}$ $\overset{q_2}{(\text{c divides b.})}$

$q = q_1 \vee q_2$

$\neg(p \to (q_1 \vee q_2)) \equiv p \wedge \neg(q_1 \vee q_2)$

$\equiv p \wedge \neg q_1 \wedge \neg q_2$

Counter example:

$a = 4,\ b = 3,\ c = 6$

$2 \quad 2 \quad 4$

$p \wedge (c \text{ is prime}) \to q_1 \vee q_2$

is actually <u>true</u>.

General tips :

Rational Numbers and IEEE half-precision floating point

What are rational numbers?

At a more abstract level:

$\mathbb{Q}$

How can we represent rational numbers?

Idea 1:

Idea 2: Pick a base $b \in \{2,3,4,\dots\}$, and try write

$$q = a_N b^N + a_{N-1} b^{N-1} + \dots \quad , \quad a_N \in \{0, \dots, b-1\}$$

$$\parallel$$

$$(a_N a_{N-1} \dots a_0 . a_{-1} \dots)_b$$

Idea 3:

$$q = (-1)^s \, m \, b^n \quad , \qquad s \in \{0,1\}, \quad n \in \mathbb{Z}, \quad 1 \le m < b,$$

combined with

$$m = (a_0 . a_{-1} a_{-2} \dots)_b$$

IEEE half-precision:

If we take $b = 2$ (i.e. what computers naturally handle)

we can optimise a bit further:

m will always be of the form:

So:

We can package everything into a bit-string as follows:

$$\underbrace{*}_{s}\quad \underbrace{*\,*\,*\,*\,*}_{n+15}\quad \underbrace{*\,*\,*\,*\,*\,*\,*\,*\,*\,*}_{m=(1.(\dots))_2}$$

(or with a different number of bits for exponent / mantissa or different offset)

Example

Suppose x is stored in half-precision floating point as

$$1\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0$$

What is x?

Example

Suppose $y = (101100)_2$. Represent y in half-precision floating point.

Pigeon-hole Principle

If N objects are classified into k categories, at least one category has at least $\lceil \frac{N}{k} \rceil$ objects

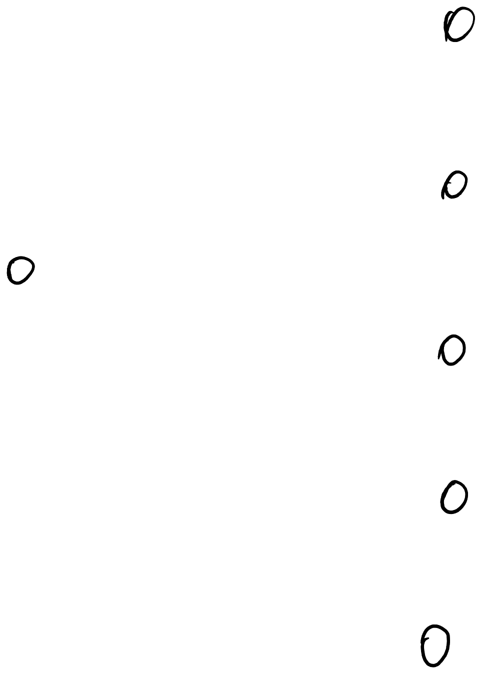
Example:

A group of n people greet each other, with some shaking others' hands. Then at least two people have shaken the same number of hands.

Equiv.: In any simple graph with n vertices, at least two vertices have the same degree

Example:

Show that in any group of 6 people, there are three who have either all met before or all not met before.



Permutations and Combinations

Permutations: r out of n

Combinations: r out of n

DIY Examples of Permutations

DIY Examples of combinations

Stars and Bars

Idea: want to count the number of ways to split n objects into r groups (possibly empty).

Example:

A 4-tuple of number $(x_1, \dots, x_4)$ with each $x_i \in \{0, 1, 2, \dots\}$ is called valid if $x_1 + x_2 + x_3 + x_4 = 10$.

How many valid 4-tuples are there?

Difficult Example:

How many functions $f: \{1, 2, 3, 4\} \to \{0, 1, \dots, 9\}$ are non-decreasing? (Non-decreasing means $(x \le y) \Rightarrow (f(x) \le f(y))$)

Hint: