MATH1510 - Discrete Mathematics
Logic 2 and Proof (v2)
(updated slides 15,20,21,27,30,35,37)

University of Newcastle

UoN

Arguments

Definition

An argument is a sequence of propositions, $p_1, p_2, \ldots, p_k$ called premises, followed by another proposition q, called the conclusion.

We write the argument in the form

$$\begin{array}{l} p_1 \\ p_2 \\ \vdots \\ p_k \\ \therefore q \end{array}$$

where the symbol '$\therefore$' means "therefore".

Validity of Arguments

Definitions

An argument is valid if the proposition

$$(p_1 \wedge p_2 \wedge \ldots \wedge p_k) \to q$$

is a tautology.

Otherwise the argument is invalid. When this happens the argument is called a fallacy.

Note that if any one of the p_i is false then $p_1 \wedge \ldots \wedge p_k$ is false, so $(p_1 \wedge \ldots \wedge p_k) \to q$ is true. Thus we only need to check when all p_i are true.
The key of a proof is in demonstrating that a proposition is *always* true.

Four Common Arguments

$$\begin{array}{l} p \to q \\ p \\ \therefore q \end{array} \qquad \begin{array}{l} p \to q \\ \neg q \\ \therefore \neg p \end{array}$$

$$\begin{array}{l} p \to q \\ q \to r \\ \therefore p \to r \end{array} \qquad \begin{array}{l} p \vee q \\ \neg p \\ \therefore q \end{array}$$

More Arguments

Use a truth table to show that the following argument is valid:

$$\begin{aligned} & p \to q \\ & p \\ \therefore\ & q \end{aligned}$$

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

Prove that the following argument is valid without a truth table:

$$\begin{aligned} & p \to q \\ & p \\ \therefore\ & q \end{aligned}$$

Proof.

Suppose $p \to q$ and p are true. For the argument to be invalid q would have to be false, but then $p \to q$ would be false. Therefore q must be true and the argument is valid. □

Are the following arguments valid?

$$\begin{aligned} & p \to q \\ & q \\ \therefore\ & p \end{aligned} \qquad\qquad \begin{aligned} & p \to q \\ & p \\ \therefore\ & \neg q \end{aligned}$$

Match each of the following arguments to one of the four argument forms on the previous slide.

- All rabbits are white. This animal is not white. Therefore this animal is not a rabbit.
- John is enrolled in one or both of MATH1510 and MATH1110. John is not enrolled in Math1510. Therefore John must be enrolled in Math1110.
- If I drive my car I will have to buy a parking ticket. If it rains I will drive my car. It is raining, therefore I will buy a parking ticket.
- If I have 5 dollars then I will buy a lottery ticket. I have 5 dollars, so I will buy a lottery ticket.

Propositional Functions and Quantifiers

Recall,

Definitions

Let $P(x)$ be a statement involving a variable x, and let D be some set. If $P(x)$ is a proposition for every $x \in D$, then we call $P(x)$ a predicate, or propositional function.

D is called the domain of discourse or just the domain.

Universal Quantifier

Many statements in mathematics (and elsewhere) use phrases like "for every ..." and "for some ...". These phrases are called quantifiers.

Definition

"For every x, $P(x)$", written as $\forall x\ P(x)$, is the universal quantifier.
It is true when $P(x)$ is true for every x in the domain, and it is false when $P(x)$ is false for at least one x.

We sometimes say "for all x, $P(x)$".

Show that the following statement is true:
$\forall\ x \in \mathbb{Z}$, if x is odd then so is x^2.

Existential Quantifier

Definition

"For some x, $P(x)$", written as $\exists x\ P(x)$, is the existential quantifier.
It is true when $P(x)$ is true for some (at least one) x in the domain, and it is false when $P(x)$ is false for every x.

We also say "there exists an x, $P(x)$".

Show that the following statement is false (the domain is the set of real numbers).

$$\exists x \left(\frac{1}{x^2+1} > 1\right).$$

Proof.

We must show that there is no x such that $\frac{1}{x^2+1} > 1$. Equivalently we can show that $\frac{1}{x^2+1} \leq 1$ for all x.

Regardless of what x is we have $0 \leq x^2$. Adding 1 to both sides gives $1 \leq x^2+1$. We can then divide both sides by x^2+1 to get

$$\frac{1}{x^2+1} \leq 1.$$

□

- When is $\forall x\, P(x)$ true?
- When is $\exists x\, P(x)$ true?

- Come up with a $P(x)$ that is always true.
- Come up with a $P(x)$ that is always false.

- What is the negation of $\forall x\, P(x)$?
- What is the negation of $\exists x\, P(x)$?

Solutions

- If $P(x)$ is true regardless of the value of x.
- If $P(x)$ is true for some x.
- $\neg(\forall x\, P(x)) \equiv \exists x\, \neg P(x)$.
- $\neg(\exists x\, P(x)) \equiv \forall x\, \neg P(x)$.

Nature of a proof

- Proofs are different from calculations. Firstly a statement must exist to be proven (so you already know the 'answer'). Secondly, proofs are usually not as routine, and require a fair amount of investigation and *creativity*.

- When writing up a proof, make sure it is logically consistent, and provide enough details so that a reader can reconstruct your reasoning.

- Proofs proceed by deductive reasoning, so every step is either 'obviously' true, or uses a result proven earlier. Thus, a proven result *always* remains true. This differs from other kinds of reasoning, which rely on experience, observation, or educated guesses, all are prone to error.

1. Simple proofs

- By inspection, or use the definitions (e.g. $n! < n^n$ for $n > 1$).
- By picture (e.g. Venn diagrams).[1]
- By construction (e.g. area of a triangle).
- By cases (e.g. truth tables).
- To *disprove* something, just produce 1 counter-example. Similarly, to show existence, just produce 1 example.

Are all odd numbers primes?

No, because $9 = 3 \times 3$.

[1] Since we aim to develop your reasoning skills, pictures alone will not be considered complete proofs in assessments.

2. Induction

- If $P(1)$ is true, and if $P(k) \to P(k+1)$, then $P(n)$ is true for all $n \in \mathbb{N}$.
- Very useful for statements depending on a parameter n, especially for graphs (e.g. number of edges in a tree).
- Induction works in a way akin to falling dominoes, or climbing a ladder.
- Used when there is some structure relating one case to the next, just like recursion.
- Strong induction: can assume $P(1), P(2), \ldots, P(k)$ are true.

We introduce the summation notation:

$$\sum_{i=a}^{b} f(i) = f(a) + f(a+1) + \cdots + f(b-1) + f(b).$$

Structure of an Induction Proof

A proof using the Principle of Mathematical Induction proceeds as follows

- Set-up: We set up $P(n)$ to be a statement we want to prove for all n.
- Basis step: Prove the statement for the first value of n, e.g. $P(1)$.
- Inductive step: Assume the statement is true for some integer $k \geq 1$, (i.e. assume $P(k)$ is true). This is called the inductive hypothesis. Use this assumption to prove that $P(k+1)$ is true.
- Conclusion: $P(n)$ is true for all n (greater than the number used in your basis step).

Examples of induction

Show $\sum_{i=1}^{n} i = n(n+1)/2$.

Let $S(n)$ be the sum of the first n natural numbers. Then a recursive program would look like

```
S(1) = 1;  S(k) = S(k-1) + k;
```

so the key recursive step is the inductive step.

Divisibility

Show $9^n - 1$ is always divisible by 4.

Fibonacci numbers

Let $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$. Show

$$\sum_{i=0}^{n} F_i = F_{n+2} - 1.$$

Proof that $\sum_{i=1}^{n} i = n(n+1)/2$.

For $n \geq 1$, let $P(n)$ be the statement $\sum_{i=1}^{n} i = n(n+1)/2$.
Basis case: The LHS of $P(1)$ is 1, as is the RHS, so $P(1)$ is the equation $1 = 1$ which is true.
Inductive step: Suppose for $k \geq 1$ that $P(k)$ is true, so that $1 + 2 + \ldots + k = k(k+1)/2$.
Then we use $P(k)$ to manipulate the LHS of $P(k+1)$:

$$\sum_{i=1}^{k+1} i = (1 + 2 + \ldots + k) + (k+1) = k(k+1)/2 + (k+1)$$
$$= k(k+1)/2 + 2(k+1)/2 = \frac{(k+1)(k+2)}{2}$$

This is says $P(k+1)$ is true. We have shown $P(k) \Rightarrow P(k+1)$. So by Induction, $P(n)$ is true for all $n \geq 1$.

$\square$

3. Contradiction and the pigeon hole principle

- Contradiction: we assume a result to be false; after some logical manipulations, we get a contradiction. By the law of the excluded middle, the result must have been true to start with.
- PHP (simple version): if m objects are put into n boxes and $m > n$, then at least one box contains more than 1 object.
- PHP (less simple version): if m objects are put into n boxes and $m > a \times n$, then at least one box contains more than a objects.
- Works well when *constructions* are not available (e.g. infinitude of primes, facts about people or numbers in general).

PHP

In a group of 13 people, at least 2 were born in the same month.

PHP

In a hand of 13 cards, there are at least 4 cards of the same suit.

Theorem

At least 2 people on earth have the same number of friends.

Proof.

Let n be the population of earth. We assume friendship requires two different people (you can't be friends with yourself). Then each person can be friends with 0, 1, ..., or n-1 people. But if there is a person with 0 friends then there can not be a person with $n-1$ friends, and conversely if there is a person with $n-1$ friends there can not be a person with 0 friends. So there are n people but only $n-1$ possibilities for the number of friends each person has. **By the pigeonhole principle** there are at least two people with the same number of friends. □

Proof by Contradiction

Theorem

If n is a composite number, then it has a non-trivial factor $\leq \sqrt{n}$. (And the smallest one is a prime.)

Proof.

Suppose n is a composite number that does not have a factor $\leq \sqrt{n}$.

Then we may write $n = pq$ where $p, q > \sqrt{n}$. But then $n > \sqrt{n} \times \sqrt{n}$, i.e. $n > n$.

This is a contradiction. Therefore n must have a factor $\leq \sqrt{n}$.

So to find a factor of a n, we need roughly $\sqrt{n}$ operations, not n. □

Proof by Contradiction

Why does proof by contradiction work?

In order to prove $p \to q$, we assume $\neg q$ along with p. Then (after some work) we get a contradiction.

$$\begin{array}{r} p \\ \neg q \\ \therefore c \end{array}$$

We then use the fact that $(p \wedge \neg q) \to c \equiv p \to q$ to draw our conclusion.

Proof by Contradiction

We can see the equivalence of $p \to q$ and $(p \wedge \neg q) \to c$ from the following truth table.

p	q	$p \to q$	$p \wedge \neg q$	c	$(p \wedge \neg q) \to c$
T	T	T	F	F	T
T	F	F	T	F	F
F	T	T	F	F	T
F	F	T	F	F	T

Proof by contradiction is a key proof method. Knowing how to argue by contradiction is an important way of thinking.

Proof by Contradiction

Theorem

There exists at least one true proposition

Proof.

Suppose, for a contradiction, that there are no true propositions. Then the proposition "there are no true propositions" is true. Now we have a contradiction, so there exists at least one true proposition. □

(This argument contains some subtleties. Not only do we assume that propositions exist, but we also assume that we are allowed to form propositions about the set of all propositions.)

Applications of Proof by Contradiction

Theorem

There are infinitely many prime numbers.

Proof.

Suppose that $p_1 = 2 < p_2 = 3 < ... < p_r$ are all of the primes. Let $P = p_1 p_2 ... p_r + 1$ and let d be a prime dividing P; then d can not be any of $p_1, p_2, ..., p_r$, otherwise d would divide the difference $P - p1p2...pr = 1$, which is impossible. So this prime d is still another prime, and $p_1, p_2, ..., p_r$ would not be all of the primes. □

Theorem

$\sqrt{2}$ is an irrational number, that is, it is not the ratio of two integers.

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

Suppose that $\sqrt{2}$ is rational. Then there exist integers p and q, $q \neq 0$, such that $\sqrt{2} = \frac{p}{q}$ and such that p and q are coprime, $(\mathrm{g.c.d.}(p, q) = 1)$. Rearranging and taking squares gives

$$2q^2 = p^2.$$

Both p and q can be written as a product of (not necessarily distinct) primes $p_1, \ldots, p_m$ and $q_1 \ldots q_n$ respectively. Now write p and q in terms of their prime factorisations:

$$2q_1^2 q_2^2 q_3^2 \ldots q_m^2 = p_1^2 p_2^2 p_3^2 \ldots p_n^2.$$

Since 2 is a factor on the left hand side it must also be a factor on the right hand side, and since p and q are coprime we cannot have 2 as a factor of q. There is only one factor of 2 on the left hand side but there are an even number of 2's on the right hand side. This is not possible, so we cannot have $\sqrt{2} = \frac{p}{q}$, contradicting that $\sqrt{2}$ is rational. Hence $\sqrt{2}$ is irrational. □

4. Minimality

- Well ordering principle: every non-empty subset of $\mathbb{N}$ has a minimal element. Used extensively in graphs: 'choose a cycle of minimal length' etc.
- Proof by descent: use the above to pull out a minimal element, then construct a smaller one, contradicting minimality.

Proof.

Another proof that $\sqrt{2}$ is irrational Suppose not, then $\sqrt{2} = m/n$ with n chosen to be minimal. But $m/n = (2n-m)/(m-n)$ and $m-n < n$, contradicting minimality. How does $m/n = (2n-m)/(m-n)$? Note that $m\sqrt{2} = 2n$ and $n\sqrt{2} = m$ and rewrite $\sqrt{2}/1$ by multiplying top and bottom by $m-n$. □

5. Double counting

- Simply count the same set in two ways to obtain an equality.
- Inclusion-exclusion: $|A| + |B| = |A \cup B| + |A \cap B|$.

The sum of degrees in a graph is twice the number of edges.

$\sum_{i=1}^{n} i$ again

Write out like this:

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & (n-2) & (n-1) & n \\ n & (n-1) & (n-2) & \cdots & 3 & 2 & 1 \end{array}$$

6. Standard tricks

- The contrapositive of p can be easier to prove than p.
- To show $p \leftrightarrow q$, just show $p \to q$ and $q \to p$.
- Similarly, to show $A = B$, just show $A \subseteq B$ and $B \subseteq A$.
- Use symmetry.

Contrapositive

'A graph with degree of each vertex > 1 has a cycle' may be more intuitive than 'a graph without a cycle has a vertex with degree 1'.

More examples

A graph G is bipartite if and only if it has no cycles of odd lengths

1. If G is bipartite, easy to see that it can't have an odd cycle.

2. If G has no odd cycles, then pick a vertex v and let U (resp. V) be the set of vertices whose shortest path to v is odd (resp. even). If (say) u_1, u_2 are adjacent, then we get an odd cycle, so this can't happen. So G is bipartite.

Symmetry

Person A throws a coin $n+1$ times and person B throws a coin n times. What is the chance that A got more tails than B?

(Hint: A either got more tails, or more heads, than B.)

Some common fallacies

In a fallacy, the conclusion is not necessarily incorrect; it simply cannot be arrived at using that argument. (The conclusion may also be nonsense, e.g. wiki 'all horses are the same colour'.)

- × Sweeping generalisation based on simple observation or personal experience (e.g. 'the first 100 cases obey this property', 'all the ones I've met behave this way').
- × Appealing to authority or majority.
- × Argument by repetition (politics, ads), or by assertion ('diamonds are forever', De Beers, 1947).
- × Confusing a statement with its converse (e.g. 'if you have the flu then you cough; so, if you cough, then you have the flu', 'if it rains then it's cloudy; it's not raining, so it's not cloudy').
- × Circular reasoning (e.g. 'Whatever is less dense than water will float, because whatever is less dense than water will float'). Also, circular definition (e.g. mountain and hill).

More fallacies

- × Confusing precedence with causation (e.g. 'it rained before the car broke down, so the rain caused the car to break down').
- × Confusing correlation with causation (e.g. 'cars break down more often in the rain, so rain causes cars to break down').
- × Using something without showing its existence.
- × Choosing the same notation for different objects.
- × Loaded question, i.e. a question containing unjustified assumptions (e.g. 'are maths lecturers evil by making the subject hard?').
- × Misrepresenting opponent's position (e.g. A says 'sunny days are good', B replies 'if all days were sunny, we'd never have rain, and without rain, we'd have famine; so you are wrong').
- × Taking unlikely outcomes for granted (e.g. 'if you go out in the sun you will get skin cancer').
- × False dichotomy (e.g. 'you are either with us, or against us').

Where is the fallacy?

I shall prove $1 = 0$

Suppose $1 = 0$, then I double both sides to obtain $2 = 0$. I now subtract 1 from both sides to get $1 = -1$. Squaring both sides, I get $1 = 1$, which is true. Hence $1 = 0$.

From an Australian ad

An ad about speeding presents the viewer with 2 choices: either be 5 minutes late, or never be able to walk again.

Textbook exercises

Exercises Section 1.4:

- 1, 5, 6, 10, 11, 15, 17, 18, 19, 20, 21

Exercises Section 1.5:

- 1, 4, 10, 15, 17, 21, 31, 38, 47, 49, 57, 60, 65

Exercises Section 2.1:

- 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 19, 20, 21, 22, 23, 24, 25, 44, 47, 50, 53, 55, 59

Exercises Section 2.2:

- 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 18, 19, 27, 32, 43, 47

Exercises Section 2.4:

- 1, 2, 3, 4, 5, 12, 18, 21, 22, 27, 29, 71,