Lesson - Logic, sets and proof techniques

Year: University Year 1

At university, mathematics changes character. You are asked to **prove** that a statement is true in every case, not just the ones you tried. This chapter gives the language (logic and sets) and the four standard proof techniques that every later module relies on.

Starter activity

Here is a puzzle. On an island, knights always tell the truth and knaves always lie. You meet two islanders, Ann and Ben. Ann says "At least one of us is a knave". Can you decide what each of them is? Write out each possible case, check whether it is consistent with what Ann said, and see whether you can reach a firm conclusion. You have just done a small proof by cases!

Statements and logical connectives

Definition: statement and connectives

A **statement** (or proposition) is a sentence that is either true or false. For statements P and Q we form: *not* $\neg P$; *and* $P \wedge Q$; *or* $P \vee Q$ (inclusive); *implication* $P \Rightarrow Q$, meaning "if P then Q"; and *equivalence* $P \Leftrightarrow Q$, meaning each implies the other.

Property: implication

$P \Rightarrow Q$ is false only when P is true and Q is false, and it is equivalent to $\neg P \vee Q$. Its **contrapositive** $\neg Q \Rightarrow \neg P$ is always equivalent. Its **converse** $Q \Rightarrow P$ is not equivalent in general.

Rule: De Morgan's laws

$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$ and $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$.

Quantifiers

Definition: quantifiers

$\forall$ means "for all" and $\exists$ means "there exists". To negate, swap the quantifier and negate the body: $\neg(\forall x\, P(x)) \equiv \exists x\, \neg P(x)$ and $\neg(\exists x\, P(x)) \equiv \forall x\, \neg P(x)$.

Example 1

Compare $\forall x\, \exists y\, (x + y = 0)$ and $\exists y \forall x\, (x + y = 0)$ over $\mathbb{R}$.

The first is true: take $y = -x$. The second is false: no single y works for every x. The order of quantifiers matters. To disprove a "for all" claim, one **counterexample** is enough.

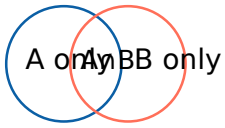
Sets

Definition: sets and operations

A set is a collection of elements; $x \in A$ means x belongs to A, and $A \subseteq B$ means every element of A is in B. The operations are union $A \cup B$, intersection $A \cap B$, difference $A \setminus B$ and complement A^c.

Rule: set identities

De Morgan's laws: $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$. To prove $A = B$, show $A \subseteq B$ and $B \subseteq A$. For finite sets $|A \cup B| = |A| + |B| - |A \cap B|$, and the **power set** $\mathcal{P}(S)$ has $2^{|S|}$ elements.



Functions and relations

Definition: injective, surjective, bijective

A function $f : X \to Y$ assigns to each $x \in X$ exactly one $f(x) \in Y$. It is **injective** if $f(a) = f(b) \Rightarrow a = b$, **surjective** if every $y \in Y$ equals some $f(x)$, and **bijective** if both. Only bijections have inverses.

Definition: equivalence relation

An **equivalence relation** is reflexive, symmetric and transitive. It splits the set into disjoint equivalence classes.

Four proof techniques

Method: direct proof

1. Assume P.
2. Deduce Q step by step, justifying each line.
3. Finish with a conclusion sentence.

Example 2: direct proof

Prove that if n is odd then n^2 is odd.

Write $n = 2k + 1$. Then $n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which is odd.

Method: contrapositive

1. To prove $P \Rightarrow Q$, state $\neg Q \Rightarrow \neg P$.
2. Prove that instead, then say it is equivalent.

Example 3: contrapositive

Prove that if n^2 is even then n is even.

The contrapositive is: if n is odd then n^2 is odd, which was just shown.

Method: contradiction

1. Assume the statement is false.
2. Derive an impossibility.
3. Conclude that the statement is true.

Example 4: contradiction

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

Suppose $\sqrt{2} = p/q$ in lowest terms. Then $p^2 = 2q^2$, so p^2 is even, hence p is even, $p = 2r$, so $q^2 = 2r^2$ and q is even too, contradicting lowest terms.

Method: induction

1. To prove $P(n)$ for all integers $n \geq n_0$, prove the *base case* $P(n_0)$.
2. Assume $P(k)$ (the inductive hypothesis).
3. Prove $P(k+1)$ using it.
4. Write the conclusion.

Example 5: induction

Prove that $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

Base: $n = 1$ gives $1 = 1$. Step: assume it for k; then $1 + \cdots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$, the formula for $k+1$.

Watch out

- Do not confuse a statement with its converse.
- Do not "prove" a general claim by checking examples.
- Do not assume what you want to prove.
- In induction never forget the base case.

Reading and writing proofs

Key fact: how a proof is built

A proof is a chain of statements, each of which is either an assumption, a definition, a known result, or follows from earlier statements by a valid rule of logic. At university you are expected to write in complete sentences: begin by saying what you assume, name your variables ("let n be an odd integer"), state the method ("we argue by contradiction"), and finish with a clear conclusion that matches the statement you set out to prove. A good proof is not a calculation hidden in symbols; it is an explanation that a classmate can follow without asking you questions. When a proof seems too hard, try small cases, look for a pattern, and ask which of the four standard methods suits the shape of the statement.

Method: choosing a proof technique

1. If the statement is an implication $P \Rightarrow Q$, try a direct proof: assume P and work towards Q.
2. If Q is awkward but not-Q is easy to use, prove the contrapositive: assume not-Q and show not-P.
3. If the claim says that something does not exist or cannot happen, assume the opposite and look for a contradiction.
4. If the claim is about every positive integer and the case $n+1$ can be built from the case n, use induction.
5. To disprove a "for all" statement, find one counterexample.

Worked example 6: Negating nested quantifiers

Write the negation of "for every $\varepsilon > 0$ there exists $\delta > 0$ such that $|x|$ implies $|x^2|$".

To negate a statement, change every "for every" into "there exists" and every "there exists" into "for every", working from left to right, and then negate the final condition. The negation is: there exists $\varepsilon > 0$ such that for every $\delta > 0$ there is an x with $|x|$ and $|x^2| \geq \varepsilon$. Note that the negation of an implication $A \Rightarrow B$ is "A and not B". The order of the quantifiers matters, and swapping them changes the meaning completely.

Worked example 7: De Morgan's laws for sets

Prove that $(A \cup B)^c = A^c \cap B^c$.

We show that the two sets have the same elements. Let $x \in (A \cup B)^c$. Then x is not in $A \cup B$, so x is in neither A nor B. That is, $x \in A^c$ and $x \in B^c$, so $x \in A^c \cap B^c$. Conversely, if $x \in A^c \cap B^c$, then x is in neither A nor B, so $x \notin A \cup B$ and $x \in (A \cup B)^c$. Since each set is contained in the other, they are equal. This "two inclusions" method is the standard way to prove set equalities.

Worked example 8: Injective, surjective and bijective

Let $f : \mathbb{R} \to \mathbb{R}$ be defined by $f(x) = x^3 - x$. Decide whether f is injective or surjective.

We have $f(0) = f(1) = f(-1) = 0$, so three different inputs give the same output and f is not injective. For surjectivity, f is a cubic with positive leading coefficient: it tends to $-\infty$ as $x \to -\infty$ and to $+\infty$ as $x \to \infty$, and it is continuous, so by the intermediate value theorem every real number is a value. So f is surjective but not injective. If we defined $g(x) = x^3$ instead, we would have a bijection.

Worked example 9: A contrapositive proof

Prove that if n^2 is divisible by 3 then n is divisible by 3.

We prove the contrapositive: if n is not divisible by 3 then n^2 is not divisible by 3. If n is not divisible by 3, then $n = 3k + 1$ or $n = 3k + 2$. In the first case $n^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$, which leaves remainder 1. In the second case $n^2 = 9k^2 + 12k + 4 = 3(3k^2 + 4k + 1) + 1$, which also leaves remainder 1. In both cases n^2 is not divisible by 3, which proves the contrapositive and therefore the original statement.

Worked example 10: A proof by contradiction with an infinite set

Prove that there are infinitely many primes.

Suppose that there are only finitely many primes, $p_1, p_2, \ldots, p_k$. Form the number $N = p_1 p_2 \cdots p_k + 1$. Dividing N by any p_i leaves remainder 1, so no prime on the list divides N. But every integer greater than 1 has a prime factor, so N has a prime factor that is not on the list. This contradicts our assumption that the list contained all the primes. This argument is more than 2 000 years old and appears in Euclid's Elements.

Worked example 11: Induction with an inequality

Prove that $n! > 2^n$ for all integers $n \geq 4$.

Base case $n = 4$: $4! = 24 > 16 = 2^4$. For the inductive step assume $k! > 2^k$ for some $k \geq 4$. Then $(k+1)! = (k+1) \cdot k! > (k+1) \cdot 2^k \geq 2 \cdot 2^k = 2^{k+1}$, because $k + 1 \geq 5 > 2$.

Hence the statement holds for $k+1$. Notice that the base case starts at 4, not 1: the statement is false for $n=2$ and $n=3$, and an induction proof always starts where the statement first becomes true.

Note: statements, proofs and examples

An example never proves a general statement, but a single counterexample disproves it. To show that "all swans are white" is false, one black swan is enough. To prove it true you would have to look at every swan, which is impossible, so you need a general argument. This is why mathematicians insist on proofs, and why the conjecture that n^2+n+41 is always prime, which holds for 40 values of n, is still false.

Watch out: logical traps

- The converse $Q \Rightarrow P$ is not equivalent to $P \Rightarrow Q$. "If it rains the grass is wet" does not mean "if the grass is wet it rains".
- In an induction proof you must prove the base case as well as the step, and your step must use the hypothesis.
- Never begin a proof by assuming what you want to prove (circular reasoning). Always begin from the assumptions and work forwards.
- "For all x there exists y" and "there exists y for all x" are different statements.

Did you know?

The method of induction was used by Blaise Pascal in 1654, but the idea goes back to Euclid's proof that there are infinitely many primes. In 1931 Kurt Gödel proved a shocking result: in any consistent formal system strong enough to describe arithmetic there are true statements that cannot be proved within the system. So even mathematics has limits to what proofs can reach.

Otto's tip

Before writing a proof, ask which technique fits. "Even" or "odd" often yields to direct proof; "there is no" suggests contradiction; a formula in n suggests induction.