# Chapter 2

# Logic and proof

## 2.1 Knights and knaves

You are on a strange island, where some of the inhabitants are knights, and always tell the truth, and some are knaves, and always lie.

You come to a fork in the road, and there are two people there. You know one is a knight, and one is a knave. You need directions, but you are only allowed to ask one yes/no question. What do you ask?

Here's one possible solution (there are others): "If I asked your friend which is the right way, which way would he tell me?" Then take the other path.

Here's another one: again there are two people, Jack and Tim (they could be both knights or both knaves this time).
Jack says: "If Tim is a knave then I'm a knight." Tim says: "We are different." Who is who?

In order to answer this question though, we need to know more about what 'if' means in the logical sense (so it was a bit unfair to spring this on you at this point). However, you should be able to convince yourself that Jack and Time both knaves is definitely a possibility; later we will see that this is the only answer.

Google Raymond Smullyan (`http://en.wikipedia.org/wiki/Raymond_Smullyan`) for more of these.

## 2.2 Basic prepositional logic

Why do we need logic? It allows us to handle things too complicated for our intuition.

**Example 1.** If there is a hockey game every Tuesday and Saturday, **and** today is Tuesday, **then** there is a hockey game today.

This is 'obviously' true. But what about

**Example 2.** A function f is uniformly continuous if for all $\epsilon > 0$, there exists a $\delta > 0$, such that for all $x$ and $y$ in the domain of $f$ with $|x - y| < \delta$, $|f(x) - f(y)| < \epsilon$. The function $xe^{-x}$ is uniformly continuous.

This isn't quite so obvious, and pretty confusing. We need logic to make sure our reasoning is correct.

**Definition 1.** A **preposition** is a statement that is either true or false (but not both).

**Example 3.** "5 is prime" - this is a preposition, and in fact a true preposition.
"4 is prime" - also a preposition, but it's false.
$x^2 - 5x + 4$ - not a preposition, it's not true or false.
$x^2 - 5x + 4 = 12$ - no, since we don't know what $x$ is; we'll come back to these later.

We'll often represent prepositions with letters,

**Example 4.** Let $p$ be the preposition "7 divides 56". Then $p$ is a true preposition.

**Definition 2.** Given any preposition $p$, $\neg p$ (pronounced "not p") is another preposition, with truth value the *negation* of $p$.

**Example 5.** Let $p =$ "8 is prime". Then $\neg p$ is the preposition "8 is not prime". Clearly $p$ is false, but $\neg p$ is true.

**Definition 3.** $p \wedge q$ means "$p$ and $q$"
$p \vee q$ means "$p$ or $q$ (or both)".
$p \rightarrow q$ means 'If $p$ holds, then $q$ must hold', i.e. "$p$ is sufficient for $q$".

$\vee$ and $\wedge$ should be quite familiar to you from logic circuits, where they are are called $+$ and $\cdot$. $p \to q$ is more troublesome. The important thing to note is that if $p$ is false, $p \to q$ is **true**!

**Example 6.** $p :=$ "$10^8$ is the largest number in the world", $q :=$ "7 is prime". Then:
$p \wedge q$ is false, and $p \vee q$ is true. What about $p \to q$? It's true!

You could think of it as being "if $p$ is true, then $q$ must be true; if $p$ is false, it doesn't matter", or "$p$ being true is a sufficient condition for $q$ to be true". To maybe get an idea of why we do it this way, suppose we want to prove "If $n$ is an even integer greater than 2, then $n$ is not prime". We could write that as "if $p(n)$ then $\neg q(n)$", where
$p(n)$ means "n is an even integer greater than 2"
$q(n)$ means "n is prime".

Note that for a *fixed* $n$, $p(n)$ and $q(n)$ are prepositions. Now if we put $n = 8$ say, then $p(8)$ is true, and $\neg q(8)$ is true, so that's fine. But if we put $n = 2$, $p(2)$ is *false*, as is $\neg q(2)$. But the statement we want to prove is clearly true, so it would be bad if "if $p(2)$ then $\neg q(2)$" were false.

NB: The expressions $p \vee q$, $\neg p$ etc are again prepositions, and may be true or false. Thus we can combine these operators to get complicated expressions, for example $\neg(p \vee \neg q) \to (\neg p \wedge q)$. This so called *compound preposition* is either true or false, depending on truth values of the contained prepositions ($p$ and $q$).

One important thing to note (that I didn't really emphasise in class) is that there is an order of precedence; in general, $\neg$ has the highest precedence, followed by $\vee$ and $\wedge$, and finally $\to$. So $p \wedge q \to \neg q \vee \neg p$ means $[(p) \wedge q] \to [(\neg q) \vee (\neg p)]$.

## 2.3 Prepositional equivalence

**Definition 4.** A compound preposition that is always true, no matter what the truth values of the prepositions that occur in it, is called a tautology. One that is always false is called a contradiction.

For example, $p \vee \neg p$ is a tautology, and $p \wedge \neg p$ is a contradiction.

**Definition 5.** Two prepositions p and q are called *logically equivalent* if $p \leftrightarrow q$ is a tautology. This is denoted $p \equiv q$.

**Example 7.** $p \to q \equiv \neg q \to \neg p$. We'll see this later - it's called the contrapositive. You can prove this using a truth table - listing all possible truth values of $p$ and $q$, and checking that the statement is true for all of them.

Here's a list of identities you should know:

| | |
|---|---|
| $p \wedge T \equiv p$<br>$p \vee F \equiv p$ | Identity |
| $p \vee T \equiv T$<br>$p \wedge F \equiv F$ | Domination |
| $p \vee p \equiv p$<br>$p \wedge p \equiv p$ | Idempotent laws |
| $\neg(\neg p) \equiv p$ | Double negative |
| $p \vee q \equiv q \vee p$<br>$p \wedge q \equiv q \wedge p$ | Commutativity |
| $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$<br>$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$ | Associativity |
| $p \vee (q \wedge r) \equiv (p \wedge q) \vee (p \wedge r)$<br>$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ | Distributivity |
| $\neg(p \vee q) \equiv \neg p \wedge \neg q$<br>$\neg(p \wedge q) \equiv \neg p \vee \neg q$ | De Morgan's |
| $p \vee (p \wedge q) \equiv p$<br>$p \wedge (p \vee q) \equiv p$ | Absorption |
| $p \vee \neg p \equiv T$<br>$p \wedge \neg p \equiv F$ | Negation laws |
| $p \to q \equiv \neg p \vee q$ | |

Let's use these ideas to solve the knights and knaves problem.

(Not done yet, I'll put it in soon / eventually).

### 2.3.1 Rules of inference

The equivalences we've seen can be used to prove equivalence of more complicated expressions, because we can replace part of a compound preposition with something that is logically equivalent.

Here's an example where we use rules of inference. Understanding this sort of logic becomes important when we start proving things - you need to be comfortable with using the basic identities (like De Morgan's laws).

$$\begin{aligned}\neg(p \vee (\neg p \wedge q)) &\equiv \neg p \wedge \neg(\neg p \wedge q) \\ &\equiv \neg p \wedge (\neg(\neg p) \vee \neg q) \\ &\equiv \neg p \wedge (p \vee \neg q) \\ &\equiv (\neg p \wedge p) \vee (\neg p \wedge \neg q) \\ &\equiv F \vee (\neg p \wedge \neg q) \\ &\equiv \neg p \wedge \neg q\end{aligned}$$

You should be able to see which law I'm using at each step.

## 2.4 Quantifiers

Take the expression "$n^2 + n + 1$ is prime". Recall this is not a preposition. But let's define $p(n) = ....$ Then for a fixed $n$, this is a preposition, e.g. $p(2)$ is $2^2 + 2 + 1$ is prime - which is true. $p(3)$ is 13 is prime, true. This isn't true for all $n$ though - $p(4) = 21$ which isn't prime.

**Definition 6.** In the above, $n$ in the above is called the *variable*, and the $p$ of $p(n)$ is called a prepositional function or a predicate. Note that a prepositional function can have more than one variable - e.g. $p(m, n, r)$.

How would we write "$n^2 + n + 1$ is prime for all positive integers $n$" as a statement using logical symbols? We could try $p(1) \wedge p(2) \wedge p(3) \cdots$. But this uses an infinite number of conjunctions - which isn't allowed.

So: we define the *quantifier* "for all", written $\forall$:

**Definition 7.** Given a prepositional function $p$, the expression $\forall n p(n)$ is the preposition "for all values of $n$ in the universe of discourse, $p(n)$ is true"

**Definition 8.** We also need to state what the set of possible values for $n$ is ("for all natural numbers $n$..."). This is called the *universe of discourse*.

**Example 8.** Taking the universe to be positive integers, our original statement can be written

$$\forall n \ (n^2 + n + 1 \text{ is prime}). \tag{2.1}$$

This yields a preposition now - it's either true or false. Either $p(n)$ is true for all positive integers $n$, or there is an $n$ such that $p(n)$ is false. So for our example, is (2.1) true or false? FALSE.

Next, we define the quantifier "exists" written $\exists$:

**Definition 9.** Given a prepositional function $p$, the expression $\exists n\ p(n)$ is the preposition "there exists some value of $n$ such that $p(n)$ is true".

**Example 9.** $\exists n$ ($n^2 + n + 1$ is prime). - this is true.

Sometimes we put extra information about the variable

**Example 10.** $\forall n > 2$ ($n$ even $\rightarrow n$ is not prime)

### 2.4.1 Multiple quantifiers

We can have more than one quantifier in an expression.

**Example 11.** Taking the universe to be the real numbers,

- $\forall x \forall y\ (x + y = y + x)$. (TRUE)
- $\forall x \exists y\ (x + y = 0)$. (TRUE)
- $\forall x \exists y\ (x \cdot y = 1)$. (FALSE, take $x = 0$).

**Example 12.** Write this as a logical expression: "There is a woman who has taken a flight on every airline in the world"

$$\exists w \forall a \exists f\ (P(w, f) \wedge Q(f, a)),$$

where $P(w, f) :=$ "$w$ has taken $f$", $Q(f, a)$ is "$f$ is a flight on $a$".

**Order is important**: compare

- $\forall x \exists y\ (x + y = 0)$. (TRUE)
- $\exists y \forall x\ (x + y = 0)$. (FALSE)

In the first case, we got to choose y depending on $x$. So e.g. if $x$ was 5, we could pick $y = -5$. In the second case, we're supposed to find a fixed $y$ so that for any $x$, $x + y = 0$, which is clearly impossible.

**Exercise 1.** Write "71 is prime" in terms of quantifiers, letting $p(m, n)$ be "m divides n".

### 2.4.2 Negating quantifiers

There are basically two rules you need to know: If it's **not** true that $p(x)$ is true for all $x$, then we must be able to find a particular $x$ where $p(x)$ is false.

$$\neg\exists x\ p(x) \equiv \forall x\ \neg p(x)$$

If it's **not** true that there exists an $x$ s.t. $p(x)$ is true, then for every $x$, $p(x)$ is false, i.e. $\neg p(x)$ is true.

$$\neg\forall x\ p(x) \equiv \exists x\ \neg p(x)$$

To negate an expression with multiple quantifiers, just go in steps:

**Example 13.**

$$\neg\forall x\exists y\ p(x,y) \equiv \exists x\neg(\exists y\ p(x,y)) \equiv \exists x\forall y\ \neg p(x,y).$$

### 2.4.3 Dealing with multiple quantifiers

*I didn't do this in class, and it's not really necessary, but you should definitely read this if you're finding multiple quantifiers confusing.*

When there are lots of quantifiers, things can get *very* confusing! Rather than stringing together long sentences of the form 'there exists an $x$ such that for all $y$, there exists a $z$....' it's sometimes easier to use the following game formulation.

Suppose you're given a complicated preposition with lots of quantifiers:

$$\forall x\exists y\forall z\exists w\exists s p(x,y,z,w,s).$$

You will play the $\exists$ variables $(y,w,s)$, i.e. you get to choose their values. The adversary will play the $\forall$ variables $(x,z)$.

You play in order from left to right (so you need not be playing alternately).
Your goal: make the statement $p(x,y,z,w,s)$ true.
The adversary's goal: make the statement false.

If you can find a winning strategy - i.e. you can make your choices so that you always win, then the preposition is true. Otherwise, it's false. Notice

that your choices can depend on the variables already chosen in the game. Here's an example:

$$\forall\epsilon\exists N\forall n(n \geq N \rightarrow |(n+2)/n - 1| < \epsilon).$$

(This is the statement, "$(n+2)/n \to 1$ as $n \to \infty$", but we don't need to know this).

The adversary goes first, picks $\epsilon$. Now we get to pick $N$, and *our choice can depend on* $\epsilon$. Our challenge is to find a way of picking these values such that the inequality is true for all $n \geq N$, i.e. no matter what $n$ our adversary picks, we win. Suppose our opponent picks $\epsilon = 1/2$. Then if we pick $N = 5$, we win (check this yourself).

What if $\epsilon = 1/100$? Then you can check that $N = 201$ works.

In general, if we pick $N > 2/\epsilon$, we will win (again, this needs some algebra). So we have a winning strategy.

Recall the party problem, and consider this general form of it: For any positive integers $m$ and $n$, there exists an $N$ such that at any party with at least $N$ people, there will either be $m$ people who all know each other, or $n$ people who all don't know each other.

What does the adversary pick? $m$ and $n$, and then we get to pick $N$ (depending on $m$ and $n$). Now what? The adversary gets to pick which people know each other (i.e. which edges are solid and which are dashed), and tries to do it so that no $m$ people all know each other, and no $n$ people all don't know each other.

## 2.5 Methods of proof

Most of the time, theorems can be written as an implication: if $p$, then $q$, or perhaps $p \leftrightarrow q$.

### 2.5.1 Direct proof

In a direct proof, you use the implication in a straightforward way. If you're trying to show $p \to q$, you assume $p$ is true, and show that $q$ must be too.

**Example 14.** Prove "If $n$ is odd, then $n^2$ is odd".

*Proof.* We assume $n$ is odd (this is the "$p$" part). How can we write an arbitrary odd number? Let $n = 2k + 1$, for some integer $k$. Then $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1$, which is odd. So we're done. □

### 2.5.2 Indirect proof

Recall that we showed $p \to q \equiv \neg q \to \neg p$. This is the basis for an "indirect proof", or "proof by contrapositive".

**Example 15.** Prove that if $x$ and $y$ are two integers for which $x+y$ is even, then $x$ and $y$ have the same parity.

*Proof.* The contrapositive version of this theorem is "If $x$ and $y$ are two integers with opposite parity, then their sum must be odd." So we assume $x$ and $y$ have opposite parity. Since one of these integers is even and the other odd, there is no loss of generality to suppose $x$ is even and $y$ is odd. Thus, there are integers $k$ and $m$ for which $x = 2k$ and $y = 2m + 1$. Now then, we compute the sum $x + y = 2k + 2m + 1 = 2(k + m) + 1$, which is an odd integer by definition. □

### 2.5.3 Proof by contradiction

Sometimes the easiest way to prove something is to suppose (for the purposes of argument) that it is false, and then derive a contradiction. We're using the logical statement $(\neg p \to F) \equiv p$.

**Theorem 1.** *There are infinitely many primes*

*Proof.* Let $q$ be the statement "there are infinitely many primes". Suppose for a contradiction that $\neg q$ holds, i.e. there are finitely many primes. Then we can list these primes, so suppose they are $p_1, p_2, p_r$. Now let $n = p_1 p_2 \cdots p_r + 1$. $n$ is clearly bigger than all the $p_r$, and so cannot be prime because of our assumption. So there exists some prime number $m$ that divides $n$. But $m$ must be one of the $p_i$, since those are the only primes. But $n$ is clearly not divisible by any of the $p_i$, since $n = p_r(\text{some integer}) + 1$. This is clearly a contradiction, and so $q$ must have been true. □

Another one: first some definitions

**Definition 10.** A rational number is a real number that can be written in the form $a/b$, where $a$ and $b \neq 0$ are integers. An irrational number is a real number that is not rational.

E.g. $\pi$, $e$, $\log 2$, $\sqrt{2}$ are all irrational.

Let's prove the last of those.

**Theorem 2.** *$\sqrt{2}$ is irrational.*

*Proof.* Suppose for a contradiction that $\sqrt{2}$ is rational. Then we can write it in the form $a/b$. We can assume that $a$ and $b$ don't have any common factors, otherwise we could just divide through (e.g. $6/8 = 3/4$). So:

$$2 = a^2/b^2.$$

Hence

$$2b^2 = a^2.$$

So $a^2$ is even, and hence so is $a$. Write $a = 2c$. Then $2b^2 = 4c^2$ so $b^2 = 2c^2$. But then $b^2$ is even, and hence $b$. This is a contradiction, since $a$ and $b$ now share a common factor. □

**Exercise 2.** Prove that $\sqrt{n}$, for $n$ not a perfect square, is irrational.

### 2.5.4 Proving both directions

Sometimes, we are asked to show "if and only if". For example, "The integer $n$ is odd if and only if $n^2$ is odd".

To prove $p \leftrightarrow q$, we normally prove $p \to q$ and $q \to p$ *separately.* $q \to p$ is called the *converse* of $p \to q$.

*Proof.* We already showed that $n$ odd implies $n^2$ odd. So we only need to show that if $n^2$ is odd, then $n$ is odd. Let's prove this using the contrapositive - i.e. let's show that if $n$ is even, then $n^2$ is even. Well that's easy - if $n = 2k$, $n^2 = 4k^2$ which is even. □