Discrete Mathematical Models

Lecture 3

Kane Townsend

Semester 2, 2024

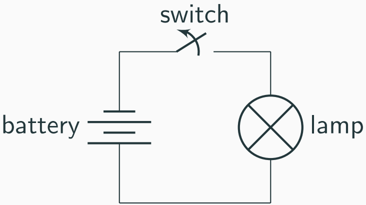
Section A1: Logic (continued)

Logic circuits

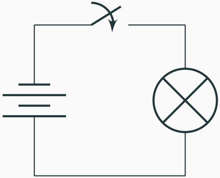
Let's engage in some discrete mathematical modelling...

Circuits

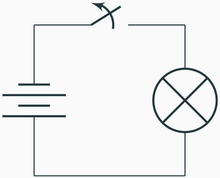
Here is a simple circuit:



It has two possible states:



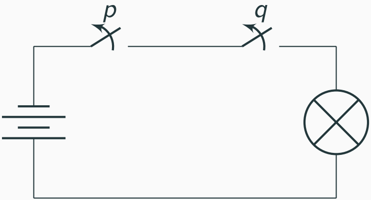
Light ON



Light OFF

The states correspond to the values **True** and **False** of the statement "the light is ON".

Circuits: AND

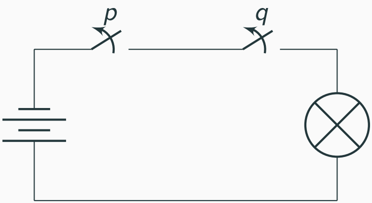


The behaviour of this circuit can be represented by a truth table (which coincides with the truth table for AND):

Switch p is ON	Switch q is ON	Light is ON
T	T	T
T	F	F
F	T	F
F	F	F

The AND gate

The circuit



is called an AND gate.

It takes two inputs:

- the state of switch p
  (denoted by 1 for ON and 0 for OFF)
- the state of switch q

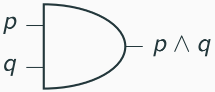
and produces an output:

- the state of the light bulb.

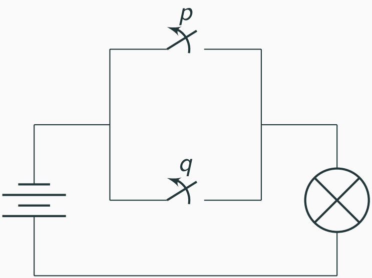
The AND gate

The AND gate is represented by the following input-output table and symbol:

p	q	$p \wedge q$
1	1	1
1	0	0
0	1	0
0	0	0

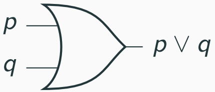


The OR gate

The circuit  gives an OR gate.

It is represented by the following table and symbol:

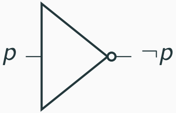
p	q	$p \vee q$
1	1	1
1	0	1
0	1	1
0	0	0



The NOT gate.

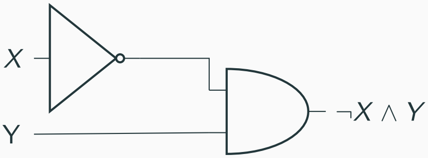
The NOT gate has the following table and symbol:

p	$\neg p$
1	0
0	1



Combining gates

Gates can be combined to create a circuit corresponding to a given compound statement.
Example:

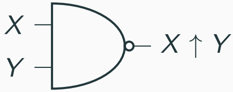


NAND and the NAND gate

The logical connective **NAND** is a shorthand for "NOT AND".
p NAND q is denoted by $p \uparrow q$ (sometimes $p|q$ is used instead of $p \uparrow q$).
So $p \uparrow q \equiv \neg(p \wedge q)$.

A corresponding **NAND gate** is defined as follows:

X	Y	$X \uparrow Y$
1	1	0
1	0	1
0	1	1
0	0	1



The functional completeness of NAND

Claim: The set $\{\uparrow\}$ is a functionally complete set of connectives.

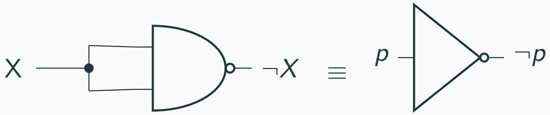
Claim: Every gate is equivalent to one that can be constructed by combining NAND gates alone.

How can we establish that this is true?

NOT from NAND

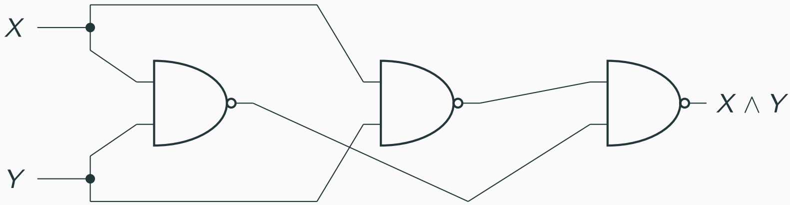
Example:

$$\neg X \equiv X \uparrow X$$

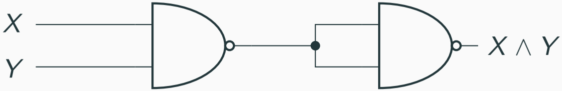


AND from NAND

$X \wedge Y \equiv \neg(X \uparrow Y) \equiv (X \uparrow Y) \uparrow (X \uparrow Y).$

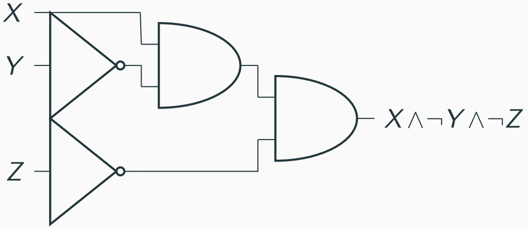


is equivalent to an AND gate.
The circuit can be simplified to use one less NAND gate:



Recogniser Circuits

Consider the circuit and corresponding table below:



X	Y	Z	$X \wedge \neg Y \wedge \neg Z$
1	1	1	0
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

We say that the circuit recognises the input combination $(X, Y, Z) = (1, 0, 0)$ because that's the only input combination that generates an output of 1.

Similarly a circuit for $\neg X \wedge Y \wedge Z$ would recognise the input combination $(X, Y, Z) = (0, 1, 1)$.

Recogniser circuits

Definition: A circuit that outputs 1 for only one input combination is called a recogniser for that input combination.

Q: Design a circuit to output 1 only for

$$(X, Y, Z) = (1, 1, 1) \ \& \ (1, 0, 0)$$

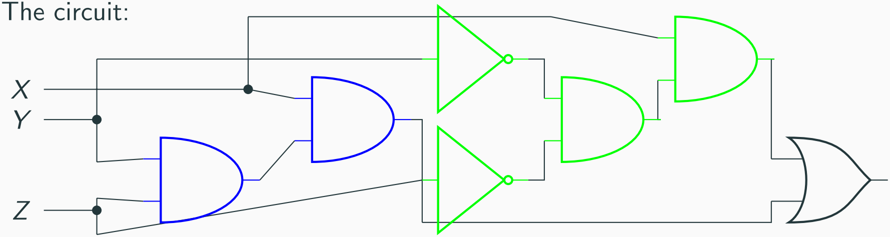
Method: Apply a method like the construction of a compound statement in disjunctive normal form. For outputs equal to 1 express inputs with AND.
Join the resulting expressions with OR.

Example: Input-output tables to circuits

The table:

X	Y	Z	output	$X \wedge Y \wedge Z$	$X \wedge \neg Y \wedge \neg Z$	$W = (X \wedge Y \wedge Z) \vee (X \wedge \neg Y \wedge \neg Z)$
1	1	1	1	1	0	1
1	1	0	0	0	0	0
1	0	1	0	0	0	0
1	0	0	1	0	1	1
0	1	1	0	0	0	0
0	1	0	0	0	0	0
0	0	1	0	0	0	0
0	0	0	0	0	0	0

The circuit:



Predicate logic

Predicates

A **predicate** is a sentence containing one or more variables, with the property that, when a value from a specified **domain** is given to each variable, the sentence becomes a statement. The specified domain is the **domain** of the predicate.

Example: Consider the predicate

$$p(x): \quad x \text{ is a bird},$$

defined over the domain of animals. If $x = \text{cockatoo}$, then $p(x)$ is true. We write $p(\text{cockatoo}) = T$. Further, $p(\text{shark}) = F$ and $p(17@\#)$ is undefined.

More examples

Perhaps the predicate

$$q(x) : x \text{ is allowed to view this file,}$$

defined over a list of users, sounds more relevant to computer scientists.

For

$$r(x, y) : x \text{ shares a land border with } y,$$

with x and y taking values from the set of countries, we have

$$r(\text{Egypt}, \text{Libya}) = T$$

and

$$r(\text{Australia}, \text{Indonesia}) = F.$$

Quantifiers

There are two ways to turn a predicate $p(x)$ into a statement:

- specify a value for x; or
- *quantify* x.

What do we mean by "quantify" x? We mean to specify some notion of how many different x's from the domain make the predicate true.

The universal quantifier

The **universal quantifier**, $\forall$, is read “for all” (or “for every”, “for each”, “for any” etc.).

The **universal statement** $\forall x\, p(x)$ is read aloud “for all x (in the domain), $p(x)$ is true” or “$p(x)$ is true for all x (in the domain)”.

The existential quantifiers

The **existential quantifier**, $\exists$, is read "there exists" (or "for at least one", etc.)

The **existential statement** $\exists x\, p(x)$ is read aloud "There exists an x (in the domain) such that $p(x)$ is true" or "$p(x)$ is true for at least one x (in the domain)" or "$p(x)$ is true for some x (in the domain)".

The **existential quantifier with uniqueness**, $\exists!$, is read "there exists a unique" (or "for exactly one", etc.)

The **existential statement** $\exists! x\, p(x)$ is read aloud "There exists a unique x (in the domain) such that $p(x)$ is true" or "$p(x)$ is true for exactly one x (in the domain)".

Examples

Q: Let

$$p(x) : x \text{ is a bird},$$

with x taking values from the domain $\{\text{cockatoo}, \text{parrot}, \text{shark}\}$. For each of the following statements, write out in words a translation of the statements and evaluate it.

1. $\forall x\ p(x)$
2. $\exists x\ p(x)$
3. $\exists! x\ p(x)$
4. $\exists! x\ \neg p(x)$

Examples

Recall that

$$p(x) : x \text{ is a bird},$$

with x taking values from the domain $\{\text{cockatoo}, \text{parrot}, \text{shark}\}$.

1. $\forall x\, p(x)$
   The statement reads: "For all x in the set $\{\text{cockatoo}, \text{parrot}, \text{shark}\}$, x is a bird". This is false because a shark is not a bird.

2. $\exists x\, p(x)$
   The statement reads: "There is at least one x in the set $\{\text{cockatoo}, \text{parrot}, \text{shark}\}$ such that x is a bird". This is true because a cockatoo is a bird.

Examples

Recall that

$$p(x) : x \text{ is a bird},$$

with x taking values from the domain $\{\text{cockatoo}, \text{parrot}, \text{shark}\}$.

3. $\exists! x\ p(x)$
   The statement reads: "There is exactly one x in the set $\{\text{cockatoo}, \text{parrot}, \text{shark}\}$ such that x is a bird". This is false because there are two animals (cockatoos and parrots) in the domain that are birds.

4. $\exists! x\ \neg p(x)$
   The statement reads: "There is exactly one x in the set $\{\text{cockatoo}, \text{parrot}, \text{shark}\}$ such that x is not a bird". This is true because only one of the animals in the domain (shark) is not a bird.

Another example

Q: Let

$$q(x) : x \text{ is in Australia},$$

with x taking values from the domain
$D = \{\text{Brisbane}, \text{Sydney}, \text{Melbourne}, \text{Adelaide}, \text{Perth}\}$.

Evaluate each of the following statements

1. $\forall x \; q(x)$
2. $\exists x \; q(x)$
3. $\exists! x \; q(x)$
4. $\exists! x \; \neg q(x)$

Examples

Recall that

$$q(x) : x \text{ is in Australia},$$

with x taking values from the domain
$D = \{\text{Brisbane}, \text{Sydney}, \text{Melbourne}, \text{Adelaide}, \text{Perth}\}$.

1. $\forall x\, q(x)$ is true because every city in D is in Australia
2. $\exists x\, q(x)$ is true because Adelaide is in Australia.
3. $\exists! x\, q(x)$ is false because more than one city in D is in Australia
4. $\exists! x\, \neg q(x)$ is false because there are no cities in D that are not in Australia.

Example

With domain the set of users (of some online system), express the statements below symbolically, using the following notation:

$o(x)$: x is online.
$c(x)$: x has changed status.
$u(x)$: x has uploaded pictures.

1. All users are online.
2. No user has changed status.
3. All users who have changed status have uploaded pictures.
4. Some users have changed status.
5. Only one user has not uploaded pictures.

Example

With domain the set of users (of some online system), express the statements below symbolically, using the following notation:

$o(x)$: x is online.
$c(x)$: x has changed status.
$u(x)$: x has uploaded pictures.

1. All users are online. $\forall x\, o(x)$
2. No user has changed status. $\forall x\, \neg c(x)$
3. All users who have changed status have uploaded pictures.
   $\forall x\, (c(x) \rightarrow u(x))$
4. Some users have changed status. $\exists x\, c(x)$
5. Only one user has not uploaded pictures.$\exists! x\, \neg u(x)$.

Notation: $\Rightarrow$ and $\Leftrightarrow$

Let $p(x)$ and $q(x)$ be predicates and suppose the common domain of x is D.

- The notation $p(x) \Rightarrow q(x)$ is short for

$$\forall x \; p(x) \rightarrow q(x)$$

- The notation $p(x) \Leftrightarrow q(x)$ is short for

$$\forall x \; p(x) \leftrightarrow q(x)$$

WARNING: It is not uncommon for mathematicians to use $\rightarrow$ and $\Rightarrow$ interchangeably, as if they mean the same thing.

Order of precedence

This is perhaps best explained by example: the expression

$$\forall x \; p(x) \rightarrow q(x)$$

means

$$\forall x \; \big(p(x) \rightarrow q(x)\big).$$

Negation

What is the negation of “all users are online”?

Negation

What is the negation of "all users are online"?
Answer: Not all users are online, *i.e.* at least one user is offline.

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

Negation

What is the negation of “all users are online”?
Answer: Not all users are online, *i.e.* at least one user is offline.

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

What is the negation of “some users have changed status”?

Negation

What is the negation of "all users are online"?
Answer: Not all users are online, *i.e.* at least one user is offline.

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

What is the negation of "some users have changed status"?
Answer: No user has changed status, *i.e.* all users have not changed status.

Symbolically: $\neg(\exists x\, q(x)) \equiv \forall x\, \neg q(x)$.

Example

Here is a more complicated example from mathematical analysis. The variables x and y take values from the set of real numbers; the variable ϵ and δ take values from the set of positive real numbers.

$$\begin{aligned}
&\neg\Big(\forall\varepsilon\,\exists\delta\,\forall x\,\forall y \quad |x-y|<\delta \to |x^2-y^2|<\varepsilon\Big)\\
&\equiv \exists\varepsilon\,\forall\delta\,\exists x\,\exists y\neg\Big(|x-y|<\delta \to |x^2-y^2|<\varepsilon\Big)\\
&\equiv \exists\varepsilon\,\forall\delta\,\exists x\,\exists y \quad |x-y|<\delta \;\wedge\; \neg(|x^2-y^2|<\varepsilon)\\
&\equiv \exists\varepsilon\,\forall\delta\,\exists x\,\exists y \quad |x-y|<\delta \;\wedge\; |x^2-y^2|\geq\varepsilon
\end{aligned}$$

The order of quantification matters

$$(\forall x\, \exists y\; p(x,y)) \not\equiv (\exists y\, \forall x\; p(x,y))$$
$$(\exists x\, \forall y\; p(x,y)) \not\equiv (\forall y\, \exists x\; p(x,y))$$

Example:

Domains: a set of people and a set of countries.
$p(x, y) =$ "x is a tall inhabitant of y"

$\forall y\, \exists x\; p(x,y)$ says that each country has at least one tall inhabitant.

$\exists x\, \forall y\; p(x,y)$ says that there is a tall individual, a particular one, who inhabits every country.

These two statements are not equivalent!

How to prove things
Putting our logic to work.

How to start

Before trying to prove a statement, you should clearly identify the logical structure of the statement. Doing so allows you to understand the choices you have in choosing a logical structure for your proof.

Let's understand the logical structures that can be used to prove statements with various logical structures.

Proving $\forall$

To prove a statement of the form $\forall x\ p(x)$, one may follow this plan:

Let x be a (fixed but arbitrary) element of the predicate domain. Argue that $p(x)$ is true.

Proving $\forall$

To prove a statement of the form $\forall x \; p(x)$, one may follow this plan:

Let x be a (fixed but arbitrary) element of the predicate domain. Argue that $p(x)$ is true.

Example
Prove the following statement: Whenever x is an integer, $6x^2 + 4$ is even.

Working the example

We need some definitions:

Defn: An integer x is **even** if there exists an integer k such that $x = 2k$.

Defn: An integer x is **odd** if there exists an integer k such that $x = 2k + 1$.

Theorem: (The even/odd theorem)
Every integer is either even or odd; no integer is both even and odd.

We note that the theorem could be stated succinctly using our logic notation:

$$\forall x \ \ (x \text{ is even}) \oplus (x \text{ is odd})$$

where the domain of quantification is understood to be the integers.

Back to our example

Prove the following statement: Whenever x is an integer, $6x^2 + 4$ is even.

Proof: Let x be an integer.

$\vdots$

Hence $6x^2 + 4$ is even. $\square$

What we have written above is the **logical structure of a proof**.

Back to our example

Prove the following statement: Whenever x is an integer, $6x^2 + 4$ is even.

Proof: Let x be an integer. We note that the integers are closed under multiplication and addition.

Since x is an integer and the integers are closed under multiplication, x^2 is an integer.
Since x^2 is an integer and the integers are closed under multiplication, $3x^2$ is an integer.
Since $3x^2$ is an integer and the integers are closed under addition, $3x^2 + 2$ is an integer.
Since $3x^2 + 2$ is an integer, $2(3x^2 + 2)$ is even.
But $2(3x^2 + 2) = 6x^2 + 4$.

Hence $6x^2 + 4$ is even. $\square$

Disproving $\forall$

To disprove a statement of the form $\forall x \; p(x)$, one should prove the statement $\exists x \; \neg p(x)$. (This is called providing a **counterexample**)

An example

Prove or disprove the following statement: For every integer x, $(x-1)^2 + (x-1)$ is positive.

An example

Prove or disprove the following statement: For every integer x, $(x-1)^2 + (x-1)$ is positive.

The statement is false because $x = 0$ is a counterexample. When $x = 0$,

$$(x-1)^2 + (x-1) = (0-1)^2 + (0-1) = (-1)^2 + (-1) = 1 - 1 = 0$$

and 0 is not positive.

Suggested activities

- Look at the materials, including the practice problems, in the Week 1 section on Wattle.
- The workshop quiz in Week 2 will be three questions based on the material for Week 1 lectures.
- Look out for lecture 3.5 coming out tomorrow (the Workshop quiz for week 2 will be on Lectures 1,2,3 only).