Formal Logic

At the start of the course we introduced the basic elements of mathematical logic, exploring manipulations of expressions and the equivalence with set theory. It's now time to formalise all that with definitions and language.

Definitions

A logical <u>statement</u> is permitted only one of two values; either true T or false F. (There are useful logics allowing other options, but we will not be studying those in this course.)

We can use tables of truth values to define the basic <u>connectives</u> of <u>propositional logic</u>. In particular, we <u>define</u> $\neg$ (not), $\wedge$ (and), $\vee$ (or), $\Rightarrow$ (implies), $\Leftrightarrow$ (iff) as follows. Let P and Q be logical statements, then

P	$\neg P$
T	F
F	T

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P \vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$P \Leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

We can use these tables to analyse more complicated expressions.

As an example, let's analyse the expression

$$(A \Rightarrow B) \Rightarrow (A_\vee C \Rightarrow B_\vee C)$$

using a truth table ...

A	B	C	$A \Rightarrow B$	$A_\vee C$	$B_\vee C$	$A_\vee C \Rightarrow B_\vee C$	$(A \rightarrow B) \Rightarrow (A_\vee C \Rightarrow B_\vee C)$
T	T	T	T	T	T	T	T
T	T	F	T	T	T	T	T
T	F	T	F	T	T	T	T
T	F	F	F	T	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	F	T	T	T
F	F	T	T	T	T	T	T
F	F	F	T	F	F	T	T

So our expression is permanently true, independent of the truth values of its component 'atomic' statements. Such an expression is called a <u>tautology</u>. There's a special notation for this, namely ...

$$\models (A \Rightarrow B) \Rightarrow (A_\vee C \Rightarrow B_\vee C)$$

so " $\models$ " means the expression following it is <u>valid</u> under all truth values.

Some expressions don't make sense, so

<u>Definition</u>

A well-formed formula (aka wff) is given by ...

(i) an atomic statement (either T or F value) is a wff,

(ii) if A is a wff then $\neg A$ is a wff,

(iii) if A and B are wffs then $A_\vee B$, $A_\wedge B$, $A \Rightarrow B$ and $A \Leftrightarrow B$ are wffs.

Definition

We say that two wffs A and B are equivalent if they have the same truth values, i.e. if $\models A \Leftrightarrow B$.

Examples

- Notice that $(P \Rightarrow Q)$ is equivalent to $(\neg P \vee Q)$.
- Also $P \vee (Q \wedge R)$ is equivalent to $(P \vee Q) \wedge (P \vee R)$.

Definition

The statement Q is a consequence of statements $P_1, \ldots, P_m$, written

$$P_1, \ldots, P_m \models Q$$

if $\forall$ truth assignments to the atomic statements within the P_i, Q has the value T whenever every P_i takes the value T. Notice that we don't care if Q is also T sometimes if not all the P_i are T!!

Notice also that
$$\begin{aligned} &P_1, \ldots, P_m \models Q \quad \text{iff} \\ &P_1 \wedge \cdots \wedge P_m \models Q \quad \text{iff} \\ &P_1 \wedge \cdots \wedge P_{m-1} \models P_m \to Q \quad \text{iff} \\ &\models P_1 \wedge \cdots \wedge P_m \to Q. \end{aligned}$$

Before we continue, we list a collection of tautologies which are easy to check and which are basic to the subject...

1 $\models A \wedge (A \to B) \to B$

2 $\models \neg B \wedge (A \to B) \to \neg A$

3 $\models \neg A \wedge (A \vee B) \to B$

4 $\models A \to (B \to A \wedge B)$

5 $\models A \wedge B \to A$

6 $\models A \to A \vee B$

7 $\models (A \to B) \wedge (B \to C) \to (A \to C)$

8 $\models (A \wedge B \to C) \to (A \to (B \to C))$

9 $\models (A \to (B \to C)) \to (A \wedge B \to C)$

10 $\models ((A \to B) \wedge \neg B) \to \neg A$

11 $\models (A \to B) \to (A \vee C \to B \vee C)$

12 $\models (A \to B) \to (A \wedge C \to B \wedge C)$

13 $\models (A \to B) \to ((B \to C) \to (A \to C$

14 $\models (A \leftrightarrow B) \wedge (B \leftrightarrow C) \to (A \leftrightarrow C$

15 $\models A \leftrightarrow A$

16 $\models A \leftrightarrow \neg\neg A$

17 $\models (A \leftrightarrow B) \leftrightarrow (B \leftrightarrow A)$

18 $\models (A \to B) \wedge (C \to B) \leftrightarrow (A \vee C \to B)$

19 $\models (A \to B) \wedge (A \to C) \leftrightarrow (A \to B \wedge C)$

20 $\models (A \to B) \leftrightarrow (\neg B \to \neg A)$

21 $\models A \vee B \leftrightarrow B \vee A$

22 $\models A \wedge B \leftrightarrow B \wedge A$

23 $\models (A \vee B) \vee C \leftrightarrow A \vee (B \vee C)$

24 $\models (A \wedge B) \wedge C \leftrightarrow A \wedge (B \wedge C)$

25 $\models A \vee (B \wedge C) \leftrightarrow (A \vee B) \wedge (A \vee C)$

26 $\models A \wedge (B \vee C) \leftrightarrow (A \wedge B) \vee (A \wedge C)$

27 $\models A \vee A \leftrightarrow A$

28 $\models A \wedge A \leftrightarrow A$

29 $\models \neg(A \vee B) \leftrightarrow \neg A \wedge \neg B$

30 $\models \neg(A \wedge B) \leftrightarrow \neg A \vee \neg B$

31 $\models A \to B \leftrightarrow \neg A \vee B$

32 $\models A \to B \leftrightarrow \neg(A \wedge \neg B)$

33 $\models A \vee B \leftrightarrow \neg A \to B$

34 $\models A \vee B \leftrightarrow \neg(\neg A \wedge \neg B)$

35 $\models A \wedge B \leftrightarrow \neg(A \to \neg B)$

36 $\models A \wedge B \leftrightarrow \neg(\neg A \vee \neg B)$

37 $\models (A \leftrightarrow B) \leftrightarrow (A \to B) \wedge (B \to A)$

Actual derivations in propositional logic are given as sequences of logical expressions coupled with a rule justifying that expression:

rule p — the expression is a premise,

rule t — $\exists$ expressions $P_1, \ldots, P_m$ preceding this expression Q in the sequence and $\models P_1 \wedge \ldots \wedge P_m \to Q$.

<u>Example</u>

Show that $A \vee B,\ A \to C,\ B \to D \models C \vee D$.

the lines of the derivation on which this line depends

(1)	$P_1: A \to C$	rule p
(1)	$P_2: A \vee B \to C \vee B$	rule t and tautology 11 $\models P_1 \to P_2$
(3)	$P_3: B \to D$	rule p
(3)	$P_4: C \vee B \to C \vee D$	rule t and tautology 11 $\models P_3 \to P_4$
(1,3)	$P_5: A \vee B \to C \vee D$	rule t and tautology 7 $\models P_2 \wedge P_4 \to P_5$
(6)	$P_6: A \vee B$	rule p
(1,3,6)	$P_7: C \vee D$	rule t and tautology 1 $\models P_5 \wedge P_6 \to P_7$

Since we've used our (partial!) list of tautologies as stepping stones in our sequence of derivations, it's worth noting that some have aquired special names; e.g. tautology #1 is called <u>modus ponens</u>, and #2 <u>modus tollens</u>

Noticing that if we show $\models P_1, \ldots, P_m, Q \to R$ then we have effectively shown $P_1, \ldots, P_m \models Q \to R$ allows us to be a little more creative in our derivations. As an example we'll give a different derivation of the previous example, calling this rule cp ...

Example

Show that $A \vee B,\ A \to C,\ B \to D \models C \vee D$.

First notice that by tautology #31 $C \vee D$ is equivalent to $\neg C \to D$, so we'll try to show that

$$A \vee B,\ A \to C,\ B \to D,\ \neg C \models D$$

(1)	P_1:	$A \vee B$	rule p	
(2)	P_2:	$A \to C$	rule p	
(3)	P_3:	$B \to D$	rule p	
(4)	P_4:	$\neg C$	rule p	
(2,4)	P_5:	$\neg A$	rule t and taut 2	$\models P_2, P_4 \to P_5$
(1,2,4)	P_6:	B	rule t and taut 3	$\models P_1, P_5 \to P_6$
(1,2,3,4)	P_7:	D	rule t and taut 1	$\models P_3, P_6 \to P_7$
(1,2,3)	P_8:	$\neg C \to D$	rule cp	
(1,2,3)	P_9:	$C \vee D$	rule t and taut 31	

This approach is sometimes called a "conditional proof". It should be said that many authors prefer to refer to stating a premise (our rule p) as needing no rule, and then list rules of deduction as

rule mp — modus ponens
rule cp — conditional proof (just as we've done)
rule mt — modus tollens

We now move on to the other common first order logic which relates terms, predicates and quantifiers; called <u>predicate calculus</u>.

Definitions

A <u>variable</u> is denoted by a letter. (This cryptic definition is to allow a letter, typically from the latter end of the alphabet, to stand intuitively for anything at least locally unknown or undetermined.)

A <u>constant</u>, typically denoted by a letter from the front end of the alphabet, denotes a specific well-defined object. For example, a constant could be the number 5, or the number π, or a specific person or country.

A <u>term</u> is a variable or a constant.

An <u>n-place predicate</u> $P(x_1, \ldots, x_n)$ is an expression involving the variables $x_1, \ldots, x_n$ such that assigning appropriate values to these x_i makes P into a statement. For convenience we define a 0-place predicate to be a statement.

A <u>prime formula</u> is an expression obtained from a predicate by substituting (not necessarily distinct) variables for the original variables in P. So for example, if $P(x, y, z)$ is a predicate then $P(x, y, z)$, $P(z, y, x)$, $P(u, v, w)$, $P(x, x, y)$ and $P(z, z, z)$ are examples of prime formulae.

The phrase "for all x", denoted $\forall x$, is a <u>universal quantifier</u>, and the phrase "there exists x", denoted $\exists x$, is called an <u>existential quantifier</u>.

A <u>formula</u> is an expression built up from prime formulae by using the operators $\neg$, $\wedge$, $\vee$, $\rightarrow$ and $\leftrightarrow$. We also allow the word "formula" to include expressions built from $(\forall x) P$ and $(\exists x) P$, where P is a formula and x is a variable.

To save unnecessary use of parentheses we'll adopt the convention that operators and quantifiers will have the least possible scope, so for example $\exists x\, A \vee B$ will mean $((\exists x) A) \vee B$.

Remarks

We should observe that $(\forall x) P(x)$ represents the expression

$$P(a_1) \wedge P(a_2) \wedge \dots \wedge P(a_n) \wedge \dots$$

where the a_i range over all the values in the domain of the variable x. Similarly, $(\exists x) P(x)$ represents

$$P(a_1) \vee P(a_2) \vee \dots \vee P(a_n) \vee \dots \quad .$$

As we've remarked frequently during this course, the order matters, so in particular

$$\models (\exists y)(\forall x) P(x,y) \longrightarrow (\forall x)(\exists y) P(x,y)$$

yet the reverse direction is not valid in general; consider for example the predicate $P(x,y) \equiv$ "$x = y$" !!

We've also seen (in the first lecture) that

$$\models \neg \forall x \; P(x) \longleftrightarrow \exists x \; \neg P(x)$$

$$\models \neg \exists x \; P(x) \longleftrightarrow \forall x \; \neg P(x) .$$

Definitions

The *scope* of a quantifier in a formula is that formula to which the quantifier applies.

An occurence of a variable in a formula is *bound* iff that occurence lies within the scope of a quantifier using that variable or is the explicit occurence in a quantifier. An occurence of a variable is *free* if it's not bound. Furthermore, a variable itself is *free* in a formula iff at least one occurence is free, and it's *bound* iff at least one occurence is bound. Notice that a variable can be both free and bound in a formula!

Examples

bound   free

$$(\forall x) P(x,y)$$

bound   bound

$$(\exists y)(\forall x)\big(P(x,y) \longrightarrow (\forall z) Q(z)\big)$$

$$(\forall z)\big(P(z) \wedge (\exists x) Q(x,z) \longrightarrow (\exists y) R(z,y)\big) \vee Q(z,x)$$

bound   bound   bound   free

Remarks

Notice that if a variable is free in a formula, then it really does behave like a 'variable' in the colloquial mathematical sense since the formula is effectively a statement about that variable. Hence we could define a "statement" to be a formula having no free variables.

We can give two further deductive rules relevant to predicate calculus, namely

rule ui $\models (\forall x) P(x) \longrightarrow P(a)$ for "a" any value in the domain of the variable x.

this rule is commonly called universal instantiation or universal specification.

rule ug $\models P(x) \longrightarrow (\forall x) P(x)$ where $P(x)$ is an earlier formula in the sequence of deductions such that x is not a variable having a free occurence in <u>any</u> premise. This rule is universal generalisation, and is typified <u>by</u> proofs starting with "Let x be ..." and then observing some property $P(x)$, so deducing from the initial arbitrariness of x that $P(x)$ holds for all x.

There are, of course, the related rules...

rule ei $\models (\exists x) P(x) \longrightarrow P(a)$ for "a" a 'chosen' value for x lying in the domain of x, even though its actual value is unknown to us.

rule eg $\models P(a) \longrightarrow (\exists x) P(x)$, i.e. knowing that there is a value in the domain of x for which $P(x)$ holds allows us to deduce $(\exists x) P(x)$!!

Examples (from Stoll, "Set Theory and Logic", 1961)

- No human beings are quadrupeds. All women are human beings. Therefore no women are quadrupeds.

  Let $H(x)$ mean "x is a human being"
  $Q(x)$ " "x is a quadruped"
  $W(x)$ " "x is a woman"

  So we must show that

$$\begin{array}{l} (\forall x)(H(x) \to \neg Q(x)) \\ \underline{(\forall x)(W(x) \to H(x))} \\ (\forall x)(W(x) \to \neg Q(x)) \end{array}$$

(1)	$\forall x (H(x) \to \neg Q(x))$	rule p
(2)	$\forall x (W(x) \to H(x))$	rule p
(3)	$W(y) \to H(y)$	rule ui and (2)
(4)	$H(y) \to \neg Q(y)$	rule ui and (1)
(5)	$W(y) \to \neg Q(y)$	rule t and (3), (4)
(6)	$\forall x (W(x) \to \neg Q(x))$	rule ug and (5)

- Everybody who buys a ticket receives a prize. Therefore, if there are no prizes, then nobody buys a ticket.

  Let $B(x,y)$: x buys y $T(x)$: x is a ticket
  $P(x)$: x is a prize $R(x,y)$: x receives y

  So we must show

$$\begin{array}{l} \underline{(\forall x)\big((\exists y)(B(x,y) \wedge T(y)) \to (\exists y)(P(y) \wedge R(x,y))\big)} \\ \neg(\exists x)P(x) \to (\forall x)(\forall y)(B(x,y) \to \neg T(y)) \end{array}$$

(1) $(\forall x)\big((\exists y)(B(x,y) \wedge T(y)) \to (\exists y)(P(y) \wedge R(x,y))\big)$ p

we're going to use CP

(2)	$\neg(\exists x)P(x)$	p
(3)	$(\forall x)\neg P(x)$	t and (2)
(4)	$\neg P(y)$	ui and (3)
(5)	$\neg P(y) \vee \neg R(x,y)$	t and (4)
(6)	$(\forall y)(\neg P(y) \vee \neg R(x,y))$	ug and (5)
(7)	$\neg(\exists y)(P(y) \wedge R(x,y))$	t and (6)
(8)	$(\exists y)(B(x,y) \wedge T(y)) \to (\exists y)(P(y) \wedge R(x,y))$	ui and (1)
(9)	$\neg(\exists y)(B(x,y) \wedge T(y))$	t (7, 8)
(10)	$(\forall y)(\neg B(x,y) \vee \neg T(y))$	t (9)
(11)	$(\forall y)(B(x,y) \to \neg T(y))$	t (10)
(12)	$(\forall x)(\forall y)(B(x,y) \to \neg T(y))$	ug (11)
(13)	$\neg(\exists x)P(x) \to (\forall x)(\forall y)(B(x,y) \to \neg T(y))$	cp (2, 12)

- Every member of the committee is wealthy and a Republican. Some committee members are old. Therefore, there are some old Republicans.

C committee, W wealthy
R Republican, O old

(1)	$(\forall x)(C(x) \to W(x) \wedge R(x))$	p
(2)	$(\exists x)(C(x) \wedge O(x))$	p
(3)	$C(\alpha) \wedge O(\alpha)$	ei (2)
(4)	$C(\alpha) \to W(\alpha) \wedge R(\alpha)$	ui (1)
(5)	$C(\alpha)$	t (3)
(6)	$W(\alpha) \wedge R(\alpha)$	t (4,5)
(7)	$O(\alpha)$	t (3)
(8)	$R(\alpha)$	t (6)
(9)	$O(\alpha) \wedge R(\alpha)$	t (7,8)
(10)	$(\exists x)(O(x) \wedge R(x))$	eg (9)

here we let α be our "choice"

- Some Republicans like all Democrats. No Republican likes any Socialist. Therefore, no Democrat is a Socialist.

(1)	$\exists x\,(R(x) \wedge \forall y\,(D(y) \to L(x,y)))$	p
(2)	$\forall x\,(R(x) \to \forall y\,(S(y) \to \neg L(x,y)))$	p
(3)	$D(x)$	p, x
(4)	$R(\alpha) \wedge \forall y\,(D(y) \to L(\alpha,y))$	ei (1)
(5)	$\forall y\,(D(y) \to L(\alpha,y))$	t (4)
(6)	$D(x) \to L(\alpha,x)$	ui (5)
(7)	$L(\alpha,x)$	t, x (3,6)
(8)	$R(\alpha) \to \forall y\,(S(y) \to \neg L(\alpha,y))$	us (2)
(9)	$R(\alpha)$	t (4)
(10)	$\forall y\,(S(y) \to \neg L(\alpha,y))$	t (8,9)
(11)	$S(x) \to \neg L(\alpha,x)$	ui (10)
(12)	$\neg S(x)$	t, x (7,11)
(13)	$D(x) \to \neg S(x)$	cp (3,12)
(14)	$\forall x\,(D(x) \to \neg S(x))$	ug (13)

we're going to use cp

α is again our "choice"

we're explicit about the intro of this free occurence of x

We can formalize the technique of 'proof by contradiction'. We define a set $\{P_1, \ldots, P_m\}$ of statements to be <u>satisfiable</u> iff there exists at least one assignment of truth values to the prime components of the P_i so that all the P_i are simultaneously T. A <u>contradiction</u> is a formula which always takes the value F.

Hence proof by contradiction amounts to ...

$$P_1, \ldots, P_m \vDash Q \quad \text{if} \quad P_1, \ldots, P_m, \neg Q \vDash \text{any contradiction}$$

provided that the set $\{P_1, \ldots, P_m\}$ is satisfiable. We can actually <u>prove</u> this! ⌈Suppose $\{P_1, \ldots, P_m\}$ satisfiable and suppose $\exists$ some formula C for which $P_1, \ldots, P_m, \neg Q \vDash C \wedge \neg C$.

Assign truth values to the prime components of the P_i so that they are all simultaneously T, then $P_1, \ldots, P_m \vDash \neg Q \to (C \wedge \neg C)$ and so $\neg Q \to (C \wedge \neg C)$ is T.

⌊But $(C \wedge \neg C)$ is F, hence $\neg Q$ must be F, and so Q is T.

<u>Example</u>

Show that $\{A \leftrightarrow B, B \to C, \neg C \vee D, \neg A \to D, \neg D\}$ is not satisfiable.

(1)	$A \leftrightarrow B$	p	
(2)	$B \to C$	p	
(3)	$\neg C \vee D$	p	
(4)	$\neg A \to D$	p	
(5)	$\neg D$	p	
(6)	$\neg\neg A$	t	(4, 5)
(7)	A	t	(6)
(8)	$A \to C$	t	(1, 2)
(9)	C	t	(7, 8)
(10)	$\neg C$	t	(3, 5)
(11)	$C \wedge \neg C$	t	(9, 10)

Before we leave this topic, we should give two formal definitions which help to clarify our manipulations within predicate calculus. To substitute a variable y for a variable x in a formula P means to replace each free occurence of x in P by y. A formula $P(x)$ is free for y if no free occurence of x in $P(x)$ is in the scope of $(\forall y)$ or $(\exists y)$.

Examples

For $A(x) = P(x,y) \wedge (\forall y) Q(y)$, $A(x)$ is free for y.

For $B(x) = (x=1) \wedge (\exists y)(y \neq x)$, $A(x)$ is not free for y

---

Definition

A Boolean algebra is a non-empty set A together with two binary operations (addition and multiplication) and a unary operation (complement, denoted $\bar{a}$) such that

(i) $a+b,\ ab,\ \bar{a} \in A \quad \forall a,b \in A$ (the operations are closed)

(ii) $a+(b+c) = (a+b)+c \quad \forall a,b,c \in A$

(iii) $\exists\ 0 \in A$ with $a+0 = a \quad \forall a \in A$

(iv) $a+b = b+a \quad \forall a,b \in A$

(v) $a(bc) = (ab)c \quad \forall a,b,c \in A$

(vi) $\exists\ 1 \in A$ with $a1 = a \quad \forall a \in A$

(vii) $ab = ba \quad \forall a,b \in A$

(viii) $a+\bar{a} = 1$ and $a\bar{a} = 0 \quad \forall a \in A$

(ix) $a(b+c) = ab+ac \quad \forall a,b,c \in A$

(x) $a+(bc) = (a+b)(a+c) \quad \forall a,b,c \in A$

This relates to set theory by $\cup$ being $+$, $\cap$ being multiplication, set complement being $\bar{a}$, and $\emptyset$ being 0 with the universe being 1. For logic, the suite $\vee, \wedge, \neg, F, T$ correspond to $+, \times, \bar{a}, 0, 1$. Notice that these 'models' allow use to see the reasons behind (viii) and (x).

Examples

- $a0 = 0 \quad \forall a \in A$

  0 is unique, for if we assume $a + p = a \quad \forall a \in A$

  then $p = p + 0$ by axiom (iii)

  $= 0 + p$ by axiom (iv)

  $= 0$ by our assumption.

  $a + a0 = a1 + a0 = a(1+0) = a1 = a$

  so $a0 =$ the unique 0.

- $a + a = a \quad \forall a \in A$

  $a + a = (a+a)1 = (a+a)(a+\bar{a})$

  $= a + a\bar{a}$ by axiom (x)

  $= a + 0 = a$

- $a + 1 = 1 \quad \forall a \in A$

  $a + 1 = a + (a + \bar{a}) = (a+a) + \bar{a} = a + \bar{a} = 1$

- $aa = a \quad \forall a \in A$

  $aa = aa + 0 = aa + a\bar{a} = a(a+\bar{a})$ by axiom (ix)

  $= a1 = a$

Many other similar results can be shown simply. There is also the very useful <u>principle of duality</u> which observes that any theorem of Boolean algebra has an equally valid dual theorem where addition and multiplication have been swapped, as have 0 and 1. This holds because our list of axioms contains its dual statements, so any proof of the original theorem can be converted into a proof of its dual result by exchanging each step in the proof by its dual.

Definition

An expression in Boolean algebra is in <u>disjunctive normal form</u>, commonly written as DNF, if it is the <u>sum</u> of <u>products</u>, each of which contains each variable of the expression precisely once, although in either the form a or $\bar{a}$.

Examples

- The expression $ab + b\bar{c}$ is not in DNF. However, we can remedy that as follows.

$$ab + b\bar{c} = ab(c+\bar{c}) + (a+\bar{a})b\bar{c} \quad \text{using axiom (viii)}$$
$$= abc + ab\bar{c} + ab\bar{c} + \bar{a}b\bar{c} \quad \text{axiom (ix)}$$

which is in DNF. Notice that this approach is redolent of the algorithm in the first h/w for solving a set equation.

Notice that if, for example, our model of Boolean algebra were to be logic, then applying truth values to each of the summands would yield the overall truth value very simply. (There is also the dual conjunctive normal form if you prefer that approach.)