Logic and Proof

Computer Science Tripos Part IB

Lent Term

Mateja Jamnik

Department of Computer Science and Technology

University of Cambridge

mateja.jamnik@cl.cam.ac.uk

Introduction to Logic

Logic concerns statements in some language.

The language can be natural (English, Latin, . . .) or formal.

Some statements are true, others false or meaningless.

Logic concerns relationships between statements: satisfiability, entailment, . . .

Logical proofs model human reasoning (supposedly).

Statements

Statements are declarative assertions:

Black is the colour of my true love's hair.

They are not greetings, questions or commands:

What is the colour of my true love's hair?

I wish my true love had hair.

Get a haircut!

Schematic Statements

Now let the variables X, Y, Z, . . . range over ‘real’ objects

Black is the colour of X’s hair.

Black is the colour of Y.

Z is the colour of Y.

Schematic statements can even express questions:

What things are black?

Interpretations and Validity

An interpretation maps variables to real objects:

The interpretation $Y \mapsto$ coal satisfies the statement

Black is the colour of Y.

but the interpretation $Y \mapsto$ strawberries does not!

A statement A is valid if all interpretations satisfy A.

Satisfiability

A set S of statements is satisfiable if some interpretation satisfies all elements of S at the same time. Otherwise S is unsatisfiable.

Examples of unsatisfiable sets:

$$\{X \subseteq Y,\ Y \subseteq Z,\ \neg(X \subseteq Z)\}$$

$$\{n \text{ is a positive integer},\ n \neq 1,\ n \neq 2,\ \ldots\}$$

Entailment, or Logical Consequence

A set S of statements entails A if every interpretation that satisfies all elements of S, also satisfies A. We write $S \models A$.

$$\{X \subseteq Y,\ Y \subseteq Z\} \models X \subseteq Z$$

$$\{n \neq 1,\ n \neq 2,\ \ldots\} \models n \text{ is NOT a positive integer}$$

$S \models A$ if and only if $\{\neg A\} \cup S$ is unsatisfiable.

If S is unsatisfiable, then $S \models A$ for any A.

$\models A$ if and only if A is valid, if and only if $\{\neg A\}$ is unsatisfiable.

Formal Proof

How can we prove that A is valid? We can't test infinitely many cases.

A formal system is a model of mathematical reasoning

- theorems are inferred from axioms using inference rules.
- formal systems are themselves mathematical objects, hence we have meta-mathematics

Inference Rules

An inference rule yields a conclusion from one or more premises.

Let $\{A_1, \ldots, A_n\} \models B$. If $A_1, \ldots, A_n$ are true then B must be true.

This entailment suggests the inference rule

$$\frac{A_1 \qquad \ldots \qquad A_n}{B}$$

A system's axioms and inference rules must be selected carefully.

Theorems are constructed inductively from the axioms using rules.

Schematic Inference Rules

$$\frac{X \subseteq Y \qquad Y \subseteq Z}{X \subseteq Z}$$

- A proof is correct if it has the right syntactic form, regardless of
- Whether the conclusion is desirable
- Whether the premises or conclusion are true
- Who (or what) created the proof

Consistency vs Satisfiability

A formal system defines a set of theorems.

If every statement is a theorem, then the system is inconsistent.

An unsatisfiable set of axioms leads to an inconsistent formal system (in normal circumstances).

Satisfiability is the semantic counterpart of consistency.

Richard's Paradox

Consider the list of all English phrases that define real numbers, e.g. "the base of the natural logarithm" or "the positive solution to $x^2 = 2$."

- Sort this list alphabetically, yielding a series $\{r_n\}$ of real numbers.
- Now define a new real number such that its nth decimal place is 1 if the nth decimal place of r_n is not 1; otherwise 2.
- This is a real number not in our list of all definable real numbers.

Why Should we use a Formal Language?

And again: consider this 'definition': (Berry's paradox)

The smallest positive integer not definable using nine words

Greater than The number of atoms in the Milky Way galaxy

This number is so large, it is greater than itself!

A formal language prevents ambiguity.

Survey of Formal Logics

propositional logic is traditional boolean algebra.

first-order logic can say for all and there exists.

higher-order logic reasons about sets and functions.

modal/temporal logics reason about what must, or may, happen.

type theories support constructive mathematics.

All have been used to prove correctness of computer systems.

Syntax of Propositional Logic

$P, Q, R, \ldots$	propositional letter
$\mathbf{t}$	true
$\mathbf{f}$	false
$\neg A$	not A
$A \land B$	A and B
$A \lor B$	A or B
$A \to B$	if A then B
$A \leftrightarrow B$	A if and only if B

Semantics of Propositional Logic

$\neg$, $\wedge$, $\vee$, $\to$ and $\leftrightarrow$ are truth-functional: functions of their operands.

A	B	$\neg A$	$A \wedge B$	$A \vee B$	$A \to B$	$A \leftrightarrow B$
1	1	0	1	1	1	1
1	0	0	0	1	0	0
0	1	1	0	1	1	0
0	0	1	0	0	1	1

Later we shall see things like $\Box A$ that are not.

Interpretations of Propositional Logic

An interpretation is a function from the propositional letters to $\{1, 0\}$.

Interpretation I satisfies a formula A if it evaluates to 1 (true).

Write $\models_I A$

A is valid (a tautology) if every interpretation satisfies A.

Write $\models A$

S is satisfiable if some interpretation satisfies every formula in S.

Implication, Entailment, Equivalence

$A \to B$ means simply $\neg A \lor B$.

$A \models B$ means if $\models_I A$ then $\models_I B$ for every interpretation I.

$A \models B$ if and only if $\models A \to B$.

Equivalence

$A \simeq B$ means $A \models B$ and $B \models A$.

$A \simeq B$ if and only if $\models A \leftrightarrow B$.

An Issue: $A \to B$ Versus $\neg A \vee B$

It's called material implication, and it admits "paradoxes"* such as

$$P \to (Q \to P) \quad \text{and} \quad (P \to Q) \vee (Q \to R)$$

Some say that if $A \to B$ is true then A should somehow cause B

Some "solutions":

- Relevance logic: still investigated by philosophers
- An interpretation in modal logic: see lecture 11

*these are not paradoxes

Aside: Propositions as Types

Idea: instead of “A is true”, say “a is evidence for A”, written $a : A$

- If $a : A$ and $b : B$ then $(a, b) : A \times B$ Looks like conjunction!
- If $a : A$ then $\mathrm{Inl}(a) : A + B$
  If $b : B$ then $\mathrm{Inr}(b) : A + B$ Looks like disjunction!
- if $f(x) : B$ for all $x : A$
  then $\lambda x : A.\, b(x) : A \to B$ Looks like implication!

Also works for quantifiers, etc.: the basis of constructive type theory

Constructive Logic is Weird

If $A \vee B$ then we know which one of A, B is true

$A \vee \neg A$ is not a tautology

If $\exists x\, A$ then we know what x is

$\exists$, $\forall$ are not duals

$A \to B$ isn't the same as $\neg A \vee B$

no material implication

$(P \to Q) \vee (Q \to R)$ is not a tautology, but $P \to (Q \to P)$ still is

Constructive (aka intuitionistic) logic is popular in theoretical CS

this material on constructive logic is NOT examinable

Equivalences

$$A \land A \simeq A$$

$$A \land B \simeq B \land A$$

$$(A \land B) \land C \simeq A \land (B \land C)$$

$$A \lor (B \land C) \simeq (A \lor B) \land (A \lor C)$$

$$A \land \mathbf{f} \simeq \mathbf{f}$$

$$A \land \mathbf{t} \simeq A$$

$$A \land \neg A \simeq \mathbf{f}$$

Dual versions: exchange $\land$ with $\lor$ and $\mathbf{t}$ with $\mathbf{f}$ in any equivalence

Equivalences Linking $\wedge$, $\vee$ and $\to$

$$(A \vee B) \to C \simeq (A \to C) \wedge (B \to C)$$

$$C \to (A \wedge B) \simeq (C \to A) \wedge (C \to B)$$

The same ideas will be realised later in the sequent calculus

Normal Forms in Computational Logic

Formal logics aim for readability, hence have a lot of redundancy

The connective NAND expresses all propositional formulas!

Negation normal form (NNF)

Conjunctive normal form (CNF)

Clause form and Prolog

Normal forms make proof procedures more efficient.

Negation Normal Form

1. Get rid of $\leftrightarrow$ and $\rightarrow$, leaving just $\land$, $\lor$, $\neg$:

$$A \leftrightarrow B \simeq (A \rightarrow B) \land (B \rightarrow A)$$

$$A \rightarrow B \simeq \neg A \lor B$$

2. Push negations in, using de Morgan's laws:

$$\neg\neg A \simeq A$$

$$\neg(A \land B) \simeq \neg A \lor \neg B$$

$$\neg(A \lor B) \simeq \neg A \land \neg B$$

From NNF to Conjunctive Normal Form

3. Push disjunctions in, using distributive laws:

$$A \lor (B \land C) \simeq (A \lor B) \land (A \lor C)$$

$$(B \land C) \lor A \simeq (B \lor A) \land (C \lor A)$$

4. Simplify:

- Delete any disjunction containing P and $\neg P$
- Delete any disjunction that includes another: for example, in $(P \lor Q) \land P$, delete $P \lor Q$.
- Replace $(P \lor A) \land (\neg P \lor A)$ by A

Converting a Non-Tautology to CNF

$$P \lor Q \to Q \lor R$$

1. Elim $\to$: $\neg(P \lor Q) \lor (Q \lor R)$
2. Push $\neg$ in: $(\neg P \land \neg Q) \lor (Q \lor R)$
3. Push $\lor$ in: $(\neg P \lor Q \lor R) \land (\neg Q \lor Q \lor R)$
4. Simplify: $\neg P \lor Q \lor R$

Not a tautology: try $P \mapsto \mathbf{t}$, $Q \mapsto \mathbf{f}$, $R \mapsto \mathbf{f}$

Tautology checking using CNF

$$((P \to Q) \to P) \to P$$

1. Elim $\to$: $\neg[\neg(\neg P \lor Q) \lor P] \lor P$
2. Push $\neg$ in: $[\neg\neg(\neg P \lor Q) \land \neg P] \lor P$

   $[(\neg P \lor Q) \land \neg P] \lor P$
3. Push $\lor$ in: $(\neg P \lor Q \lor P) \land (\neg P \lor P)$
4. Simplify: $\mathbf{t} \land \mathbf{t}$

   $\mathbf{t}$ *It's a tautology!*

In $A_1 \wedge \ldots \wedge A_n$ each A_i can falsify the conjunction, if $n > 0$

Dually, DNF can detect unsatisfiability.

DNF was investigated in the 1960s for theorem proving by contradiction.

We shall look at superior alternatives:

- Davis-Putnam methods, aka SAT solving
- binary decision diagrams (BDDs)

All can take exponential time—propositional satisfiability is NP-complete—but can solve big problems

A Simple Proof System

Axiom Schemes

K $\quad A \rightarrow (B \rightarrow A)$

S $\quad (A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

DN $\quad \neg\neg A \rightarrow A$

Inference Rule: Modus Ponens

$$\frac{A \rightarrow B \qquad A}{B}$$

This system regards $\neg$, $\vee$, $\wedge$ as abbreviations

A Simple (?) Proof of $A \to A$

$$(A \to ((D \to A) \to A)) \to \qquad (1)$$
$$((A \to (D \to A)) \to (A \to A)) \quad \text{by S}$$

$$A \to ((D \to A) \to A) \quad \text{by K} \qquad (2)$$

$$(A \to (D \to A)) \to (A \to A) \quad \text{by MP, (1), (2)} \qquad (3)$$

$$A \to (D \to A) \quad \text{by K} \qquad (4)$$

$$A \to A \quad \text{by MP, (3), (4)} \qquad (5)$$

Lengths of proofs here grow exponentially

Aside: Propositions as Types Again*

Those axioms are not arbitrary (though many other such systems are)

Ever see a type-checking rule for function application?

$$\frac{f : A \to B \qquad a : A}{f(a) : B}$$

looks like Modus Ponens!

Axioms S and K give the types of combinators for expressing functions

A correspondence between terms and proofs, with links to λ-calculus

*not examinable

Some Facts about Deducibility

A is deducible from the set S if there is a finite proof of A starting from elements of S. Write $S \vdash A$. We have some fundamental resuilts:

Soundness Theorem. If $S \vdash A$ then $S \models A$.

Completeness Theorem. If $S \models A$ then $S \vdash A$.

Deduction Theorem. If $S \cup \{A\} \vdash B$ then $S \vdash A \to B$.

But meta-theory does not help us **use** the proof system.

Gentzen's Natural Deduction Systems

The context of assumptions may vary.

To deduce $A \rightarrow B$, we get to assume A temporarily:

$$\frac{\begin{matrix} A \\ \vdots \\ B \end{matrix}}{A \rightarrow B}$$

Each logical connective is defined independently.

Introduction and elimination rules: how to deduce and use $A \wedge B$:

$$\frac{A \qquad B}{A \wedge B} \qquad\qquad \frac{A \wedge B}{A} \qquad \frac{A \wedge B}{B}$$

A Typical Natural Deduction Proof

$$\dfrac{\dfrac{\cancel{A \vee B} \qquad \dfrac{\cancel{A}}{B \vee A} \qquad \dfrac{\cancel{B}}{B \vee A}}{B \vee A}}{A \vee B \to B \vee A}$$

Nice simple rules like

$$\frac{A}{A \vee B} \qquad \frac{B}{A \vee B} \qquad \frac{A \to B \qquad A}{B}$$

But the “crossing-out” process is confusing, and Natural Deduction works better for constructive logic

The Sequent Calculus

Sequent $A_1, \ldots, A_m \Rightarrow B_1, \ldots, B_n$ means,

$$\text{if } A_1 \land \ldots \land A_m \text{ then } B_1 \lor \ldots \lor B_n$$

$A_1, \ldots, A_m$ are assumptions; $B_1, \ldots, B_n$ are goals

Γ and Δ are sets in $\Gamma \Rightarrow \Delta$

$A, \Gamma \Rightarrow A, \Delta$ is trivially true (and is called a basic sequent).

Sequent Calculus Rules

$$\frac{\Gamma \Rightarrow \Delta, A \qquad A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta} \text{(cut)}$$

$$\frac{\Gamma \Rightarrow \Delta, A}{\neg A, \Gamma \Rightarrow \Delta} (\neg l) \qquad \frac{A, \Gamma \Rightarrow \Delta}{\Gamma \Rightarrow \Delta, \neg A} (\neg r)$$

$$\frac{A, B, \Gamma \Rightarrow \Delta}{A \land B, \Gamma \Rightarrow \Delta} (\land l) \qquad \frac{\Gamma \Rightarrow \Delta, A \qquad \Gamma \Rightarrow \Delta, B}{\Gamma \Rightarrow \Delta, A \land B} (\land r)$$

More Sequent Calculus Rules

$$\frac{A, \Gamma \Rightarrow \Delta \qquad B, \Gamma \Rightarrow \Delta}{A \lor B, \Gamma \Rightarrow \Delta}\ (\lor l) \qquad \frac{\Gamma \Rightarrow \Delta, A, B}{\Gamma \Rightarrow \Delta, A \lor B}\ (\lor r)$$

$$\frac{\Gamma \Rightarrow \Delta, A \qquad B, \Gamma \Rightarrow \Delta}{A \to B, \Gamma \Rightarrow \Delta}\ (\to l) \qquad \frac{A, \Gamma \Rightarrow \Delta, B}{\Gamma \Rightarrow \Delta, A \to B}\ (\to r)$$

Proving the Formula $A \land B \to A$

$$\dfrac{\dfrac{\overline{A, B \Rightarrow A}}{A \land B \Rightarrow A}\,(\land l)}{\Rightarrow (A \land B) \to A}\,(\to r)$$

- Begin by writing down the sequent to be proved
- Be careful about skipping or combining steps
- You can't mix-and-match proof calculi. Just use sequent rules.

Another Easy Sequent Calculus Proof

$$\cfrac{\cfrac{\cfrac{\overline{A, B \Rightarrow B, C}}{A \Rightarrow B, B \to C}\;(\to r)}{\Rightarrow A \to B,\; B \to C}\;(\to r)}{\Rightarrow (A \to B) \lor (B \to C)}\;(\lor r)$$

this was a "paradox of material implication"

Part of a Distributive Law

$$
\dfrac{\dfrac{\dfrac{}{A \Rightarrow A, B} \qquad \dfrac{\dfrac{}{B, C \Rightarrow A, B}}{B \land C \Rightarrow A, B}\,(\land l)}{\dfrac{A \lor (B \land C) \Rightarrow A, B}{A \lor (B \land C) \Rightarrow A \lor B}\,(\lor r)}\,(\lor l) \qquad \text{similar}}{A \lor (B \land C) \Rightarrow (A \lor B) \land (A \lor C)}\,(\land r)
$$

Second subtree proves $A \lor (B \land C) \Rightarrow A \lor C$ similarly

A Failed Proof

$$\dfrac{\dfrac{\dfrac{A \Rightarrow B, C \qquad \overline{B \Rightarrow B, C}}{A \vee B \Rightarrow B, C}\;(\vee l)}{A \vee B \Rightarrow B \vee C}\;(\vee r)}{\Rightarrow (A \vee B) \to (B \vee C)}\;(\to r)$$

$A \mapsto \mathbf{t}$, $B \mapsto \mathbf{f}$, $C \mapsto \mathbf{f}$ falsifies the unproved sequent!

Relevance to Automatic Theorem Proving

- Hao Wang's "Toward mechanical mathematics" (1960): spectacular results for both propositional and first-order logic
- Based on backward proof using the sequent calculus rules
- Modern tableaux calculi generalise these ideas

The sequent calculus is not practical for proving theorems on paper, as you will soon discover!