COMS10003
Proof

Kerstin Eder

University of BRISTOL

Department of COMPUTER SCIENCE

Initial investigation

- Conjecture 1:

  Let n be an integer larger than 1 and n is prime, then 2^n-1 is prime.

  Is this conjecture correct?

- Conjecture 2:

  Let n be an integer larger than 1 and n is ***not*** *prime, then 2^n-1 is* ***not*** *prime.*

  Is this conjecture correct?

Testing is not enough

“Testing shows the presence,
not the absence of bugs.”

Edsger Wybe Dijkstra

(May 11 1930 – August 6 2002)

Mathematics according to Russell

- **According to Bertrand Russell: (1872-1970)**

  "Pure mathematics consists entirely of such asseverations as that, if such and such a proposition is true of anything, then such and such another proposition is true of that thing...It's essential not to discuss what the anything is of which it is supposed to be true...If our hypothesis is about anything and not about some one or more particular things, then our deductions constitute mathematics.

  Thus mathematics may be defined as the subject in which we never know what we are talking about, nor whether what we are saying is true."

Pure maths and logic are concerned with the structure of argument rather than content.

Mathematical Reasoning

- In mathematics we construct formal arguments called proofs.

The aim of a PROOF is to show beyond reasonable doubt, on the basis of accepted RULES OF INFERENCE, that a hypothesis is true GIVEN certain assumptions and AXIOMS.

- But what are
  - RULES OF INFERENCE and
  - AXIOMS?

What are Axioms?

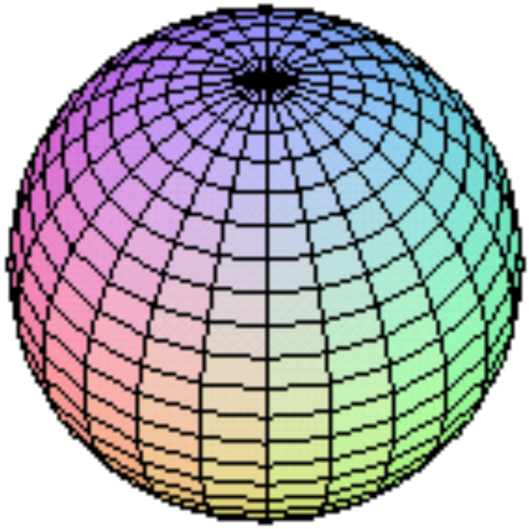
- Axioms are statements (facts) that are (assumed to be) undeniably true.

Euclid's Axioms

1. A straight line segment can be drawn joining any two points.
2. Any straight line segment can be extended indefinitely in a straight line.
3. Given any straight line segment, a circle can be drawn having the segment as radius and one end point as centre.
4. All right angles are equal to one another.
5. Given any straight line, and a point not on it, there exists one, and only one, straight line which passes through that point and never intersects the first line, no matter how far they are extended.

Non-Euclidean Geometry

- Axioms can sometimes turn out to not be as certain as first thought!



- On the surface of a sphere lines=great circles

What are Inference Rules?

- Inference rules are accepted ways to show one statement follows from another.

Example: Modus Ponens

IF A THEN B is true.
A is true.

B is true.

IF it is sunny THEN we will play.

It is sunny.

We will play.

Inference Rules

Example: Syllogism

All X are Y.
Z is an X.

Z is Y.

Sometimes inference rules seem obvious but that’s how it should be!

All men are mortal.
Socrates is a man.

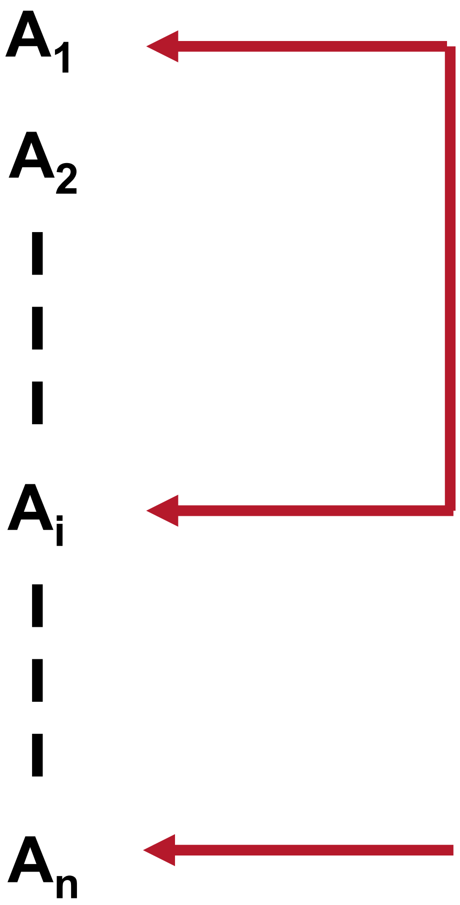
Socrates is mortal.

All rabbits eat carrots.
Max is a rabbit.

Max eats carrots.

What is a Proof?

One way of defining a proof is as a special kind of list:



A_1

A_2

A_i

A_n

A_i is either
an axiom,
an assumption or
follows from $A_1 \ldots A_{i-1}$
by application of an
inference rule.

Hypothesis to be proved.

Proof in Logic

Axiom Schema

Axiom 1: $A \rightarrow (B \rightarrow A)$

Axiom 2: $(A \rightarrow (B \rightarrow C)) \rightarrow ((A \rightarrow B) \rightarrow (A \rightarrow C))$

Axiom 3: $(\neg B \rightarrow \neg A) \rightarrow ((\neg B \rightarrow A) \rightarrow B)$

Inference Rules

Modus Ponens

$$\frac{\begin{array}{l} A \rightarrow B \\ A \end{array}}{B}$$

A Formal Proof

Prove that $A \to A$ using only Axioms 1-3 and Modus Ponens:

A Formal Proof

Prove that $A \rightarrow A$ using only Axioms 1-3 and Modus Ponens:

1. $(A \rightarrow ((A \rightarrow A) \rightarrow A)) \rightarrow ((A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A))$ — **Axiom 2 with**
B = $A \rightarrow A$
C = A

2. $A \rightarrow ((A \rightarrow A) \rightarrow A)$ — **Axiom 1 with**
B = $A \rightarrow A$

3. $(A \rightarrow (A \rightarrow A)) \rightarrow (A \rightarrow A)$ — **Modus Ponens 1,2**

4. $A \rightarrow (A \rightarrow A)$ — **Axiom 1 with**
B = A

5. $A \rightarrow A$ — **Modus Ponens 3,4**

Propositional Logic and Proof

Language of Propositional Logic: Well-Formed Formulae

The **alphabet** consist of the following sets:

- A set of propositional variables $PROP = \{p, q, r, s, ...\}$.
- A set of propositional connectives $\{\mathbf{true}, \mathbf{false}, \neg, \wedge, \vee, \oplus, \Rightarrow, \Leftrightarrow\}$.
- A set of punctuation symbols $\{(,)\}$.

The **grammar** defines what constitutes a well-formed formula (wff):

- Each of the elements in $PROP$ is a wff.
- Each of **true** and **false** is a wff.
- If p is a wff, then $(\neg p)$ is a wff.
- If p and q are wffs, then so are $(p \wedge q)$, $(p \vee q)$, $(p \oplus q)$, $(p \Rightarrow q)$, $(p \Leftrightarrow q)$.

Logical Equivalences

Equivalence	Name
$p \wedge \mathbb{T} \equiv p$ $p \vee \mathbb{F} \equiv p$	Identity Laws
$p \vee \mathbb{T} \equiv \mathbb{T}$ $p \wedge \mathbb{F} \equiv \mathbb{F}$	Domination Laws
$p \vee p \equiv p$ $p \wedge p \equiv p$	Idempotent Laws
$\neg(\neg p) \equiv p$	Double Negation Law
$p \vee q \equiv q \vee p$ $p \wedge q \equiv q \wedge p$	Commutative Laws
$p \vee (q \vee r) \equiv (p \vee q) \vee r$ $p \wedge (q \wedge r) \equiv (p \wedge q) \wedge r$	Associative Laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive Laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's Laws

Symbolic Manipulation

- Instead of using truth tables to determine the equivalence of propositions, we can use the logical equivalences.
- A proposition in a compound proposition can be replaced by an equivalent proposition without changing the truth value of the compount proposition.
- Determine whether $\neg(p \vee (\neg p \wedge q))$ is logically equivalent to $\neg p \wedge \neg q$.

$$
\begin{array}{rcll}
\neg(p \vee (\neg p \wedge q)) & \equiv & \neg p \wedge \neg(\neg p \wedge q) & |Second\ De\ Morgan's \\
 & \equiv & \neg p \wedge (\neg\neg p \vee \neg q) & |First\ De\ Morgan's \\
 & \equiv & \neg p \wedge (p \vee \neg q) & |Double\ Negation \\
 & \equiv & (\neg p \wedge p) \vee (\neg p \wedge \neg q) & |Distributive\ Law \\
 & \equiv & F \vee (\neg p \wedge \neg q) & |Contradiction\ p \wedge \neg p \\
 & \equiv & (\neg p \wedge \neg q) \vee F & |Commutativity \\
 & \equiv & \neg p \wedge \neg q & |Identity\ Law
\end{array}
$$

Follows From

- A follows from B if for every row of the truth table in which B is true A is also true.

Notation: $B \models A$

Show that Q follows from $P \wedge (P \rightarrow Q)$.

P	Q	$(P \rightarrow Q)$	$P \wedge (P \rightarrow Q)$
T	T	T	T
T	F	F	F
F	T	T	F
F	F	T	F

Valid Arguments

If you are caught speeding, then you will be fined.

Paul was caught speeding.

Therefore, Paul will be fined.

An argument is **valid** if the conjunction of the premises imply the conclusion.

Premises:

Conclusion:

Valid Arguments

If you are caught speeding, then you will be fined.

Paul was caught speeding.

Therefore, Paul will be fined.

An argument is **valid** if the conjunction of the premises imply the conclusion.

A tautology!

Speeding	Fine	Speeding → Fine	(Speeding →Fine) ∧ Speeding	((Speeding →Fine) ∧ Speeding) →Fine
T	T	T	T	T
T	F	F	F	T
F	T	T	F	T
F	F	T	F	T

Invalid Arguments

If you are caught speeding, then you will be fined.

Paul will be fined.

Therefore, Paul was caught speeding.

Premises:

Conclusion:

Why is this argument not valid?

Invalid Arguments

If you are caught speeding, then you will be fined.

Paul will be fined.

Therefore, Paul was caught speeding.

An argument is **valid** if the conjunction of the premises imply the conclusion.

Speeding	Fine	Speeding ➔ Fine	(Speeding ➔Fine) /\ Fine	((Speeding ➔Fine) /\ Fine) ➔Speeding
T	T	T	T	T
T	F	F	F	T
F	T	T	T	F
F	F	T	F	T

Another example - I

If Jen does not attend her lectures, she will fail the course.

Jen does not attend her lectures.

Therefore, Jen will fail the course.

Is this argument valid?

Another example - II

If Jen does not attend her lectures, she will fail the course.

Jen failed the course.

Therefore, Jen did not attend her lectures.

How can you check whether this argument is valid?

Summary

- Limits of testing and reasons for proofs
- Learnt about proof
  - Axioms
  - Inference rules
- Proof in propositional logic
- Next:
  - Inductive Proof
  - Proof Methods