LOGIC

OUTLINE:

(1) Introduction to logic
(2) Formalization of logic
(3) Propositional logic
(4) Predicate logic
(5) Proof techniques

5. PROOF TECHNIQUES

Introduction

- In mathematics, considerable attention is put not only on the truth of a theorem, but also on its proof.
- The proof of a theorem is the sequence of statements that, starting from axioms and possibly using previously proved theorems, leads to the statement of the theorem in a logically valid way (that is, each subsequent formula is a logical consequence of the preceding ones).
- Proofs are important because

  1) They are objective, based only on the rules of logic, and verifiable at any time (in the past, proofs were not always provided, which led to crazy developments; also, sometimes errors in proofs have been discovered years after publication; check out the history of Fermat's Last Theorem) [related areas of interest for CS: automated theorem proving, software verification, information security, AI];

  2) They give precious insights which can be used to prove other statements, thus advancing mathematics as a whole;

Formal proofs in logic

- A formal proof is a sequence of formulas in a formal language, starting with a (possibly empty) assumption, and in which each subsequent formula is either an assumption (which opens a sub-proof) or a logical consequence of the preceding formulas.
- For each logic, there are many proof systems: natural deduction, tableaux, Hilbert calculi, sequents, ...), which use various combinations of
  - Axioms (formulas declared as true)
  - Rules of inference (manipulation rules which specify how to get new formulas from the previous ones in a proof)

Rules of inference

- Rules of inference can be thought of as “atomic valid arguments” or “atomic proofs”:
  - Each rule of inference consists of only 1 step (that is, the output is only 1 new formula to add to the proof);
  - Any proof is a sequence of rules of inference (CAUTION: in normal scientific practice, to avoid cumbersome, long and tedious proofs, several rules may be combined in a single step, and usually rules are just implied)

(Non exhaustive) list of rules of inference

- Some of the most common rules of inference are listed in the following slides.
- The notation used for rules of inference is the following:

$$\frac{A_1, A_2, \ldots, A_n}{B}\ \textit{rule name}$$

or

$$\begin{array}{c} A_1 \\ A_2 \\ \ldots \\ A_n \\ \hline B \end{array}\ \textit{rule name}$$

where A_1,A_2,...,A_n are formulas already present in the proof (usually called the premises), and B is the new formula obtained (usually called the conclusion)

The assumption rule

- In a derivation, we are always allowed to introduce new assumptions.
- Each new assumption interrupts the current derivation and starts a subderivation in which the assumption itself plays the local role of axiom. Subderivations can be nested (a new assumption in a subderivation starts a sub-subderivation, etc.)

- Like in natural language reasoning, the introduction of an assumption is like the opening of a parenthesis that pauses the principal derivation to momentarily deal with a subproblem (“now, suppose for a moment that....”).
- Once the subproblem has been completely addressed, we can return to the principal derivation, hopefully with the additional information gained by solving the subproblem.
- This is for instance what we do in proving properties case by case: first we assume that case 1 holds, and we try to prove the wanted property in that case (i.e., using the condition expressed by the case as an axiom), then we move to case 2 and so on.

- We can introduce as many assumptions as we want, but they come with a price. In fact, each new assumption opens a new subproblem, which needs to be closed (solved) at some point! The legal ways of closing a subproblem are specified by the other inference rules.
- When we close a subproblem, we say that we *discharge* the opening assumption. To complete the proof of a theorem, we have to discharge all the assumptions we made (otherwise, the proof would not be completely general, but would depend on the truth value of the assumption itself).

- EX: prove that, for any natural number n, the number n^2+n is even.
- Note that n is either even or odd.
- CASE 1: assume n is even. Then $n=2k$ for a suitable natural k. Therefore $n^2+n=n(n+1)=2k(n+1)$, which is even.
- CASE 2: assume n is odd. Then $n+1$ is even, so $n+1=2h$ for a suitable natural h. Therefore $n^2+n=n(n+1)=2nh$, which is even.
- In conclusion, in either case n^2+n is even.

$\perp$-introduction ($\perp$I)

- When in a derivation we have obtained both a formula *A* and its negation ¬*A*, then we can infer the formula $\perp$. In symbols: $$\frac{A, \qquad \neg A}{\perp}\ \perp I$$

Ex falso quodlibet ($\perp$-elimination, $\perp$E)

- When in a derivation we have obtained the formula $\perp$, then we can infer any formula *A*. In symbols: $$\frac{\perp}{A}\ \perp E$$

¬-introduction (¬I)

- When in a subderivation from the assumption *A* we have obtained ⊥, then we can infer the formula ¬*A* and close the subderivation (i.e., discharge the assumption *A* (which we denote putting A in square brackets). In symbols:

$$\dfrac{\begin{array}{c}[A]\\ \vdots \\ \bot\end{array}}{\neg A}\ \neg I$$

¬-elimination (¬E)

- When in a subderivation from the assumption $\neg A$ we have obtained $\perp$, then we can infer the formula A <u>and close the subderivation (i.e., discharge the assumption</u> A (which we denote putting ¬A in square brackets). In symbols:

$$\dfrac{\begin{array}{c}[\neg A]\\ \vdots \\ \perp\end{array}}{A}\ \neg E$$

Reductio ad absurdum

- ¬-introduction and ¬-elimination are two of many ways to encode the principle of reductio ad absurdum, which can be stated as follows:
- "If assuming a certain statement we reach a contradiction [expressed in the rules by the false atom $\perp$], then the opposite of the assumed statement holds".
- Reductio ad absurdum provides one type of indirect proof, the proof by contradiction: in order to show that a statement holds, we do not obtain it directly as the result of an argument, but instead we show that its opposite statement leads to a contradiction.

Example of proof by contradiction

- Prove that there are infinitely many prime numbers.

(1) Assume by contradiction that the prime numbers are finitely many.
(2) Then there is a maximum prime number p.
(3) By construction, $p! + 1$ is not divisible by any integer from 2 to p (it gives a remainder of 1 when divided by each).
(4) Hence $p! + 1$ is either prime or divisible by a prime larger than p.
(5) In either case, there is at least one prime bigger than p, in contradiction with step (2).
(6) In conclusion, there must be infinitely many primes.

Conjunction (∧-introduction, ∧I)

- When in a derivation we have already obtained a formula *A* and a formula *B*, then we can infer the formula *A*∧*B*. In symbols:

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

- EX: With one divisibility check I prove that “12 is divisible by 2” [*A*]. Then I apply another divisibility check and I discover that “12 is divisible by 3” [*B*]. Therefore 12 is divisible by 2 and 3.

Simplification ($\wedge$-elimination, $\wedge E$)

- When in a derivation we have already obtained the formula $A \wedge B$, then we can infer either of A or B. In symbols:

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

- EX: 2 and 3 are prime factors of 12 [$A \wedge B$]. Hence in particular 12 is divisible by 2 [A].

Addition (∨-introduction, ∨I)

- When in a derivation we have already obtained a formula *A*, then for all formulas *B* we can infer either $A \vee B$ or $B \vee A$. In symbols:

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

- EX: If I have cloves [*A*] I can make a recipe which calls for cinnamon or cloves [$A \vee B$].

Disjunctive syllogism ($\vee$-elimination, $\vee$E)

- When in a derivation we have already obtained the formulas $A \vee B$ and $\neg A$, then we can infer B. In symbols:

$$\frac{A \vee B, \neg A}{B} \vee E$$

- EX: My age may be even or odd [$A \vee B$], but it is not even [$\neg A$], therefore my age is odd [B].

$\rightarrow$-introduction ($\rightarrow$I)

- When in a subderivation from the assumption A we have obtained a formula B, then we can infer the formula $A \rightarrow B$ <u>and discharge the assumption</u> A (i.e., close the subderivation).

$$\dfrac{\begin{matrix}[A] \\ \vdots \\ B\end{matrix}}{A \rightarrow B} \rightarrow I \; [1]$$

- VARIATION: if we have obtained a formula C, we can infer $D \rightarrow C$ for any D without discharging anything. This actually corresponds to discharging an assumption which has not even been made!

$$\dfrac{C}{D \rightarrow C} \rightarrow I$$

$\rightarrow$-introduction ($\rightarrow$I)

- EX: Assume a certain integer *n* is divisible by 4 [*A*].
- Then *n* can be written as *4•k* for some integer *k*. Then *n* can be written as (*2•2)•k = 2•(2k)*. [intermediate steps]
- Then *n* is divisible by *2* [*B*].
- Therefore we can conclude that if a certain integer is divisible by 4, then it is divisible by 2 [*A*$\rightarrow$*B*].

$$\dfrac{\begin{matrix}[A]\\ \vdots \\ B\end{matrix}}{A \rightarrow B}\ \rightarrow I\ \ [1]$$

‘Duh’ (but useful) conditional statements

- Meaning of the variation of $\rightarrow$I: a conditional statement $D \rightarrow C$, in which the conclusion C is already known to hold, is automatically proven, whatever the premise is. This is said to be a trivial proof.
- Dually, a conditional statement $F \rightarrow A$, in which the premise F is known to be false, is also automatically proven (via $\perp$E followed by $\rightarrow$I). This is said to be a vacuous proof.
- These conditional statements, despite their dullness, appear quite often in mathematical reasoning, especially as a part of proofs by induction (treated in the next episodes).

Proof strategy based on $\rightarrow$I

- To prove a statement in the shape of a conditional $A \rightarrow B$, start assuming the premise A and seek a logical path to the conclusion B. If you find one, then by $\rightarrow$I the statement $A \rightarrow B$ follows.

$$\dfrac{\begin{array}{c}[A] \\ \vdots \\ B\end{array}}{A \rightarrow B} \rightarrow I \quad [1]$$

Modus ponens ($\rightarrow$-elimination, $\rightarrow$E)

- When in a derivation we have already obtained the formulas $A \rightarrow B$ and A, then we can infer B. In symbols:

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

- EX: If 12 is divisible by 4, then 12 is divisible by 2 [$A \rightarrow B$]. But 12 is divisible by 4 [A]. Therefore, 12 is divisible by 2 [B].

Modus tollens

- When in a derivation we have already obtained the formulas $\neg A$ and $A \rightarrow B$, then we can infer B. In symbols:

$$\frac{A \rightarrow B, \qquad \neg B}{\neg A} \rightarrow E$$

- EX: If 13 is divisible by 4, then 13 is divisible by 2 [$A \rightarrow B$]. But 13 is not divisible by 2 [$\neg B$]. Therefore, 13 is not divisible by 4 [$\neg A$].

Proof of the contrapositive

- The contrapositive of a conditional $A \to B$ is the conditional $\neg B \to \neg A$.
- We have already seen that $A \to B \equiv \neg B \to \neg A$.
- The combo (modus tollens + $\to$-introduction) tells us that in fact the 2 conditionals are not just logically equivalent, but a **proof** of one conditional gives rise to a proof of the other conditional.
- This observation provides the other type of indirect proof, the proof of the contrapositive: if we want to prove a conditional statement $A \to B$, we can prove $\neg B \to \neg A$ instead (which is often easier and more natural).

Example of proof of the contrapositive

- EX: prove that if the sum of two given natural numbers is greater than 10, then at least one of the numbers is greater than 5.
- Let n and k be the given natural numbers. Let A be the proposition "$n+k > 10$", B be the proposition "$n > 5$" and C be the proposition "$k > 5$". We are required to prove that $A \rightarrow (B \vee C)$. Instead of proceeding directly, we prove the contrapositive: $\neg(B \vee C) \rightarrow \neg A$., that is, if it is not the case that at least one of the numbers is greater than 5, then their sum is not greater than 10.
- Suppose it is not the case that at least one of the natural numbers n, k is greater than 5. Then n and k are both at most 4. Therefore their sum is at most 8, which is not greater than 10.

Resolution rule (Res)

- When in a derivation we have already obtained the formulas $A \vee B$ and $\neg A \vee C$, then we can infer $B \vee C$. In symbols:

$$\frac{A \vee B, \quad \neg A \vee C}{B \vee C}\ Res$$

- EX: If you know that I am in Italy or I am in Germany [$A \vee B$], and you also know that I am not in Italy or I am in Canada [$\neg A \vee C$], then you can conclude I am in Germany or in Canada [$B \vee C$].
- Resolution is fundamental in logic programming languages and is particularly suited for automatic theorem provers. It copes perfectly with formulas in conjunctive normal form (CNS, see Assignment 1).

Universal instantiation (∀-elimination, ∀E)

- When in a derivation we have already obtained the formula $\forall x\, P(x, \ldots)$ then we can infer $P(c, \ldots)$ for any c in the domain. In symbols:

$$\frac{\forall x\, P(x, \ldots)}{P(c, \ldots)} \;\forall E$$

- EX: Every natural number has a decomposition into primes [$\forall x\, P(x)$]. Therefore 14 has a decomposition into prime [$P(14)$].
- Note that the predicate P may depend on several input variables other than x.

Universal generalization (∀-introduction, ∀I)

- When in a derivation we have already obtained the formula *P(c, ...)* **for an ARBITRARY** *c* in the domain, then we can infer ∀*x P(x, ...)*. In symbols:

$$\frac{P(c,\ldots) \quad (c \text{ } arbitrary)}{\forall x P(x,\ldots)} \forall I$$

=> has no property in the domain.

- IMPORTANT REMARK: *c* must be completely arbitrary, that is, we cannot make any assumption about *c* besides the fact that it belongs to the domain under consideration. Another common way to express this is by saying that *c* is a *generic* element of the domain.
- It is very common in mathematics to use this rule without mentioning it explicitly.
- It is also very common in bad mathematics to misuse this rule by inadvertently impose extra conditions on the arbitrary element *c*.

Universal generalization

- Universal generalization is the rule we use when we show that a universal statement (i.e., a statement of the shape $\forall x$ *(something)* holds by taking an arbitrary *c* from the domain and showing that the particular statement for *c* is true.
- We have already found an example when dealing with predicative logical equivalences [next slide]

Example 1

- Prove or disprove: $\neg\forall x\, P(x) \equiv \exists x\, \neg P(x)$
- Let us fix an arbitrary interpretation.

(1) The LHS $\neg\forall x\, P(x)$ is true in the given interpretation iff not all objects of the chosen domain have the property assigned to the predicate symbol P.

(2) The RHS $\exists x\, \neg P(x)$ is true in that same interpretation iff there is an object of the chosen domain not having the property assigned to the predicate symbol P.

- Notice that, no matter what we choose as domain or what we choose as property associated with P, (1) and (2) are two ways of saying the same thing.
- Therefore $\neg\forall x\, P(x) \equiv \exists x\, \neg P(x)$

Existential instantiation (∃-elimination, ∃E)

- When in a derivation we have already obtained the formula ∃*x* *P(x, …)* then we can infer *P(c, …)* **for a NEW** *c* in the domain (i.e., *c* must have never appeared before in the proof). In symbols:

$$\frac{\exists x\, P(x, \ldots)}{P(c, \ldots)}\ \exists E$$

- EX: Prime numbers exist [∃*x* *P*(*x*)]. Therefore, let's take a prime number *c* [*P*(*c*)].
- IMPORTANT REMARK: in general, we have no knowledge of what *c* is, but only that a *c* exists for which *P(c, …)* is true. Since it exists, we can name it *c*, but there is no reason guaranteeing that it is one of the elements already introduced in the course of the proof. That's why *c* must be new.

Existential generalization (∃-introduction, ∃I)

- When in a derivation we have already obtained the formula *P(c, ...)* for a certain *c* in the domain, then we can infer ∃*x P(x, ...)*. In symbols:

$$\frac{\exists x\, P(x, \ldots)}{\exists P(c, \ldots)}\ \exists E$$

=> C can be anything that satisfy

- EX: 2 is a prime number [*P(2)*]. Therefore, Prime numbers exist [∃*x P*(*x*)].

A compound argument

- All men are mortal. Socrates is a man. THEREFORE Socrates is mortal.
- Define 2 predicates: $H(x)$ = “x is a man” and $M(x)$ = “x is mortal”.
  Define a constant s = “Socrates”.
- “All men are mortal, Socrates is a man therefore Socrates is mortal” is rendered as

$$(\forall x\, (H(x) \rightarrow M(x))) \wedge H(s) \rightarrow M(s)$$

- How can we show this is a valid argument using the rules of inference?

A compound argument

We want to show $[(\forall x\,(H(x) \to M(x))) \land H(s)] \to M(s)$

1)	$(\forall x\,(H(x) \to M(x))) \land H(s)$	*assumption [discharged in 6] (p.7)*
2)	$\forall x\,(H(x) \to M(x))$	$\land$*E from 1 (p.17)*
3)	$H(s) \to M(s)$	$\forall$*E from 2 (p.29)*
4)	$H(s)$	$\land$*E from 1 (p.17)*
5)	$M(s)$	$\to$*E from 3, 4 (p.24)*
6)	$[(\forall x\,(H(x) \to M(x))) \land H(s)] \to M(s)$	$\to$*I from 1, 6 [discharges 1] (p.20)*

Constructive vs nonconstructive existence proofs

- A proof of a proposition of the form $\exists x\, P(x)$ is called an existence proof. Some existence proofs are obtained by 1 showing an explicit element c such that $P(c)$ is true, and then 2 using existential generalization.
  - EX: In number theory, a perfect number is a positive integer that is equal to the sum of its positive divisors, excluding the number itself.
  - Nice property indeed, but do perfect numbers exist?
  - 6 is divisible by 1,2,3,6, and 1+2+3=6, so 6 is a perfect number.
  - Therefore, perfect numbers exist.
- Proofs like this are called constructive existence proofs because they explicitly construct an element that works.

Constructive vs nonconstructive existence proofs

- Some other existence proofs are nonconstructive instead: they show that an existentially quantified statement is true without providing a particular element satisfying it.
  - EX: Show that there exist irrational numbers x and y such that x^y is rational.
  - $\sqrt{2}$ is irrational.
  - Consider now the number $\sqrt{2}^{\sqrt{2}}$.
    1) If it is rational, then we are done: $x=\sqrt{2}$ and $y=\sqrt{2}$ are 2 irrationals such that x^y is rational.
    2) If $\sqrt{2}^{\sqrt{2}}$ is irrational, then set $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$. Then $x^y=(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}}=(\sqrt{2})^2=2$, which is rational.

  We do not know whether to choose $x=\sqrt{2}$ *and* $y=\sqrt{2}$ or $x=\sqrt{2}^{\sqrt{2}}$ and $y=\sqrt{2}$, but just that one of these pairs works.

Existence and uniqueness proofs

- Some theorems asserts that there exists a unique element with a certain property.
- The proof of such statement is composed of 2 parts:
  1) First we show that an element with the desired property exists (this is a normal existence proof)
  2) Then we show that no more than 1 element with the desired property exists (this is usually achieved by showing that, if there are 2 elements x and y with the desired property, then $x=y$)

Existence and uniqueness proofs

- EX: show that the addition of integer numbers has exactly one neutral element (i.e., an integer r such that, for any integer s, $r+s = s+r = s$).
- EXISTENCE: 0 has the desired property.
- UNIQUENESS: suppose there is another r such that $r+s = s$ for any integer s. Then

  $r = r+0$ (because 0 is neutral)

  $= 0$ (because r is neutral)

(Dis)proofs by counterexample

- Sometimes we want to establish that a universal statement ($\forall x\, P(x)$) is false, or equivalently that its negation $\neg\forall x\, P(x)$ is true.
- Thanks to the logical equivalence $\neg\forall x\, P(x) \equiv \exists x\, \neg P(x)$, it is enough to find an element c of the domain under consideration such that $P(c)$ is false. Such a c is a counterexample disproving the statement $\forall x\, P(x)$.
- We have already seen an example related to logical equivalences: when we want to show that 2 predicative formulas are not logically equivalent, we need to prove that for not all interpretations they have the same truth value. A counterexample in that context is a single interpretation in which the 2 formulas have different truth values [next slide].

Example 2

- Prove or disprove: $\forall x\ \exists y\ P(x,y) \equiv \exists y\ \forall x\ P(x,y)$
- Let us fix the following interpretation:
  - Domain: the natural numbers.
  - Interpretation of $P(x,y)$: "$x < y$".

(1) The LHS $\forall x\ \exists y\ P(x,y)$ says that for any natural number (x) we can find a bigger natural number (y). This is a true fact, asserting that natural numbers are unbounded from above.

(2) The RHS $\exists y\ \forall x\ P(x,y)$ says that there is a natural number greater than any other. This is false for the same reason that makes the previous statement true: natural numbers are unbounded from above.

- We found ONE interpretation in which the formulas have different truth values.

  This is enough to conclude that $\forall x\ \exists y\ P(x,y) \not\equiv \exists y\ \forall x\ P(x,y)$

Suggested homework

- Finding good proofs is an art which cannot be condensed in a few precise rules, and a skill which gets refined with exercise.
- Sections 1.6, 1.7 and 1.8 of the textbook provide many interesting remarks and examples.
- I strongly suggest to read those sections in order to get more familiar with proof techniques and strategies.

Rule	Tautology	Name
$p \to q$ p $\therefore q$	$((p \to q) \wedge p) \Rightarrow q$	Modus Ponens (Law of Detachment)
$p \to q$ $\neg q$ $\therefore \neg p$	$((p \to q) \wedge \neg q) \Rightarrow \neg q$	Modus Tollens
$p \to q$ $q \to r$ $\therefore p \to r$	$((p \to q) \wedge (q \to r)) \Rightarrow (p \to r)$	Hypothetical Syllogism (Transitivity)
$p \vee q$ $\neg p$ $\therefore q$	$((p \vee q) \wedge \neg p) \Rightarrow q$	Disjunctive Syllogism
p $\therefore p \vee q$	$p \Rightarrow p \vee q$	Addition
$p \wedge q$ $\therefore p$	$(p \wedge q) \Rightarrow p$	Simplification
p q $\therefore p \wedge q$	$(p) \wedge (q) \Rightarrow (p \wedge q)$	Conjunction
$p \vee q$ $\neg p \vee r$ $\therefore q \vee r$	$((p \vee q) \wedge (\neg p \vee r)) \Rightarrow (q \vee r)$	Resolution

Calcworkshop.com