Proofs and Rules of Inference

CS 330: Discrete Structures

What is a proof?

– mathematical reasoning

– deductive reasoning

– valid argument that establishes the truth of a conjecture

– systematic demonstration that if some set of assumptions (hypotheses) are true, then some conclusion must also be true

– proofs may leverage "known facts" — axioms.

There are many techniques we can use to build proofs, but there is no prescribed recipe for how we go about coming up w/ a proof!

Good analogy: how to solve a jigsaw puzzle?

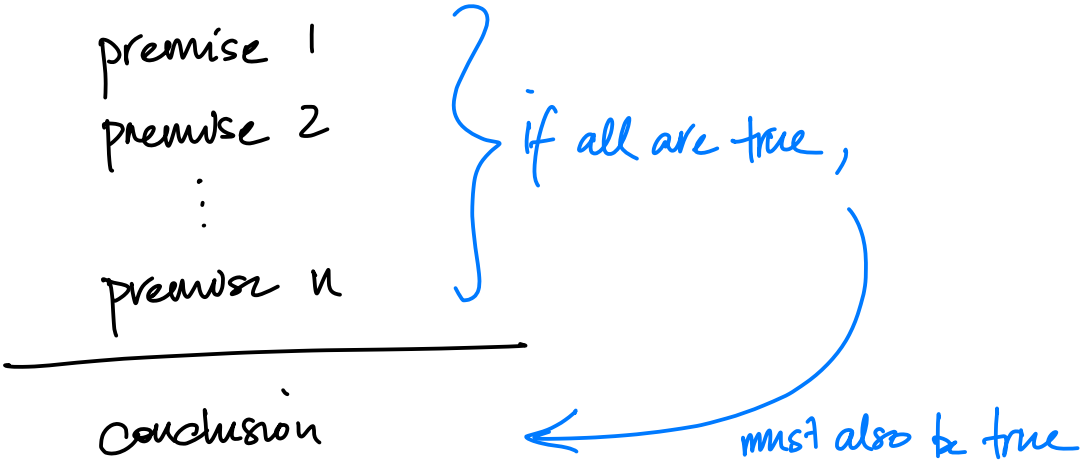
Rules of inference describe valid transformations of logical statements based on tautologies.

- inference: (noun) a conclusion reached on the basis of evidence and reasoning
- what logical assertions can we make based on some set of premises?

  e.g., assuming propositions p, $p \to q$ are true, what can we assert?

  q must be true!

Rule of inference syntax:



Rule: Modus Ponens (Latin: "mode that affirms")

tautology: $((p \to q) \wedge p) \to q$

$p \to q$

p

---

q

e.g., if the AC is on, I will be cold

the AC is on

therefore, I will be cold

Rule: Modus Tollens (Latin: "mode that denies")

tautology: $((p \to q) \wedge \neg q) \to \neg p$

$p \to q$

$\neg q$

$\neg p$

e.g. if the AC is on, I will be cold

I am not cold

therefore, the AC is not on

Rule: Hypothetical Syllogism

tautology: $((p \to q) \wedge (q \to r)) \to (p \to r)$

$p \to q$

$q \to r$

$p \to r$

if I eat candy, I will be wired

if I am wired, I can't sleep

Therefore, if I eat candy, I can't sleep

Rule: Disjunctive Syllogism

tautology: $(\neg p \wedge (p \vee q)) \rightarrow q$

$\neg p$

$p \vee q$

---

q

e.g.,

I will not take ECON

I will either take ECON or SOC

therefore, I will take SOC

Rule: Resolution

tautology: $((p \vee q) \wedge (\neg p \vee r)) \rightarrow (q \vee r)$

$$\frac{\begin{array}{c} p \vee q \\ \neg p \vee r \end{array}}{q \vee r}$$

$x < 10$ or $y > 20$

$x \geq 10$ or $z < 0$

$\therefore y > 20$ or $z < 0$

Rule: Addition

tautology: $p \rightarrow (p \vee q)$

$$\frac{p}{p \vee q}$$

$2+2=4$

$2+2=4$ or I am a rockstar

Rule: Simplification / Decomposition

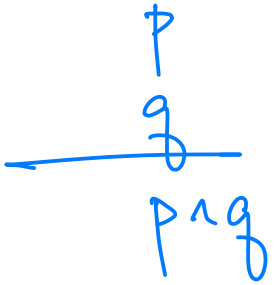
tautology: $(p \wedge q) \rightarrow p$

$$\frac{p \wedge q}{p} \qquad \frac{p \wedge q}{q}$$

- useful for "breaking down" compound hypotheses

Rule: Conjunction / Construction

tautology: $((p) \wedge (q)) \rightarrow p \wedge q$



Remember that we can also replace any logical expression (or part of a compound expression) w/ an equivalent one.

e.g. using De Morgan's Law

$$\frac{(\neg p \vee \neg q) \wedge r}{\neg(p \wedge q) \wedge r}$$

We can also introduce known tautologies based on preceding statements.

E.g., using Disjunctive syllogism tautology $((\neg p \wedge (p \vee q)) \rightarrow q)$

$$\frac{\neg(a \wedge b) \wedge ((a \wedge b) \vee c)}{\dfrac{\neg(a \wedge b) \wedge ((a \wedge b) \vee c) \rightarrow c}{c}}$$

A valid argument is a sequence of statements, where each statement either:

- is a premise (we can state a premise at any time)
- follows from preceding ones based on rules of inference

the last statement is the conclusion — sometimes (but not always!) what we are trying to prove.

Eg., premises $\begin{cases} \neg p \to (q \wedge r) \\ p \to s \\ \neg s \end{cases}$

prove : q

1. $p \to s$ (premise)
2. $\neg s$ (premise)
3. $\neg p$ (modus tollens)
4. $\neg p \to (q \wedge r)$ (premise)
5. $q \wedge r$ (modus ponens)
6. q (simplification)

E.g., premises $\begin{cases} p \wedge q \\ p \to \neg(q \wedge r) \\ s \to r \end{cases}$

prove: $\neg s$

1. $p \wedge q$ (premise)
2. p } (simplification)
3. q }
4. $p \to \neg(q \wedge r)$ (premise)
5. $\neg(q \wedge r)$ (modus ponens)
6. $\neg q \vee \neg r$ (De Morgans)
7. $\neg r$ (Disj. syllogism)
8. $s \to r$ (premise)
9. $\neg s$ (modus tollens)

Rules of inference for quantified statements:

- universal instantiation (UI): $\dfrac{\forall x\, P(x)}{P(c)}$

- universal generalization (UG): $\dfrac{P(c) \text{ for arbitrary } c}{\forall x\, P(x)}$

- existential instantiation (EI): $\dfrac{\exists x\, P(x)}{P(c) \text{ for some } c}$

- existential generalization (EG): $\dfrac{P(c) \text{ for some } c}{\exists x\, P(x)}$

E.g. premises $\begin{cases} \forall x\,(P(x) \to (Q(x) \wedge S(x))) \\ \forall x\,(P(x) \wedge R(x)) \end{cases}$

prove: $\forall x\,(R(x) \wedge S(x))$

1. $\forall x\,(P(x) \wedge R(x))$ (premise)
2. $P(c) \wedge R(c)$ (UI)
3. $P(c)$ (simplification)
4. $\forall x\,(P(x) \to (Q(x) \wedge S(x)))$ (premise)
5. $P(c) \to (Q(c) \wedge S(c))$ (UI)
6. $Q(c) \wedge S(c)$ (MP)
7. $S(c)$ (simpl.)
8. $R(c)$ (simpl.)
9. $R(c) \wedge S(c)$ (conj.)
10. $\forall x\,(R(x) \wedge S(x))$ (UG)

Note: mathematical theorems are often stated using free variables in its hypotheses and conclusion, and universal quantification over these free variables is implied.

E.g., conjecture: "if $\underbrace{n > 4}_{P(n)}$ then $\underbrace{2^n > n^2}_{Q(n)}$"

i.e., $P(n) \to Q(n)$ for arbitrary n

universal generalization:

we want to prove $\forall n\,(P(n) \to Q(n))$

"form" of proof goal: $p \to q$

Methods of Proof of form $p \to q$

1. Trivial proof : q known to be true

   e.g., "if it is raining then $1+2=3$"

2. Vacuous proof : p known to be false

   e.g., "if $2>3$ then Elon Musk is a genius"

Methods of Proof of form $p \to q$

3. Direct proof: assume p; prove q
   - use axioms, rules of inference, equivalences

4. Indirect proof
   a) proof of the contrapositive (recall $p \to q \equiv \neg q \to \neg p$)
      - assume $\neg q$; prove $\neg p$
   b) proof by contradiction
      - assume $p \wedge \neg q$; derive a contradiction (e.g., $r \wedge \neg r$)

Methods of Proof of other forms

5. proof of biconditional $p \leftrightarrow q$
   - prove $p \to q$ and $q \to p$

6. proof of conjunction $p \wedge q$
   - prove p and q separately.

7. if hypothesis is a disjunction, e.g., $(p_1 \vee p_2 \vee \ldots \vee p_k) \to q$
   - use equivalence $(p \vee q) \to r \equiv (p \to r) \wedge (q \to r)$
   - $(p_1 \vee p_2 \vee \ldots \vee p_k) \to q \equiv (p_1 \to q) \wedge (p_2 \to q) \wedge \ldots \wedge (p_k \to q)$
   - prove each case separately.

Methods of Proof involving quantifiers

8. proof of form $\forall x P(x)$

   - show $P(c)$ for arbitrary c

9. proof of form $\neg \forall x P(x) \equiv \exists x \neg P(x)$

   - find a counterexample c where $\neg P(c)$

9. proof of form $\exists x P(x)$ — "existence proof"

   - "constructive" proof: find c where $P(c)$

   - "nonconstructive" proof: assume no c exists where $P(c)$; derive a contradiction.

Many others!

- mathematical induction
- structural induction
- cantor diagonalization
- combinatorial proofs
- etc.

E.g. Direct proof

For all integers x, if x is odd (i.e., we can write it as $2y+1$, where y is an integer), then x^2 is also odd.

proof:

- let x be an arbitrary integer
- x is odd, so $x = 2y+1$
- $x^2 = (2y+1)^2 = 4y^2 + 4y + 1 = 2(2y^2+2y) + 1$
- $2y^2+2y$ is also an integer z; i.e. $x^2 = 2z+1$

$\therefore x^2$ is odd

E.g., proof of biconditional / conjunction / cases, by contrapositive

For all integers x, x^2 is odd if and only if x is odd.

Proof:

must show $(x \text{ is odd} \rightarrow x^2 \text{ is odd}) \wedge (x^2 \text{ is odd} \rightarrow x \text{ is odd})$

already proved! handle second case

- try contrapositive: x is even $\rightarrow$ x^2 is even
  - if x is even, we can write it as $2y$
  - $x^2 = 4y^2 = 2(2y^2) = 2z$
  - $\therefore x^2$ is even

$\therefore x$ is odd $\leftrightarrow$ x^2 is odd

E.g. proof by contradiction

There are infinitely many prime numbers

Proof:

- assume there is a finite list of primes $p_1, p_2, \ldots, p_n$
- let $m = p_1 \times p_2 \times \ldots \times p_n + 1$
- m is not divisible by p_1 (would give quotient of $p_2 \times \ldots \times p_n$, remainder of 1)

  also not divisible by $p_2, \ldots, p_n$
- all integers > 1 are either prime or a product of primes,
- m is either a new prime or a product of a prime not in our list
- but this contradicts our assumption of a finite list of primes!
- $\therefore$ there are infinitely many primes.