COMS10003

# Proof Strategies

Kerstin Eder

University of Bristol

Department of Computer Science

# Introduction

- A proof is an argument that demonstrates a result beyond reasonable doubt, ideally, beyond all doubt.
- In practice, due to lack of space/time, proofs are rarely given as a complete sequence of logical steps.
  – It is “obvious” that...
  – ... is “trivial”.
- Proofs can be hard to follow and can contain mistakes.

# Proof Strategies

- Several proof strategies, e.g.
  - Direct proof
  - Proof by contradiction
  - Existence proofs
  - Contrapositives and Counterexamples
  - Proof by exhaustion
  - (Mathematical induction)
- Find the easiest or most elegant proof

# Direct Proof

- A proof that follows a sequence of logical statements from a set of assumptions leading to the desired conclusion.
- Standard argument uses basic rules of inference like *Modus Ponens*.
  – Aim to show Q is true.
  – We know that if P is true then Q is true.
  – We can prove P to be true.
  – Therefore, by MP, Q must be true.

# Direct Proof

More formally:

- We are using $P \rightarrow Q$ in our proof.
- If P is false, then the implication is always true.
- In a direct proof, we assume that P is true, and show that Q must therefore be true.

# Direct Proof: Example

"The square of every positive even number is divisible by four."

Formalization:

- transform into an "if…then…" statement

  "If n is a positive even number then its square, $n^2$, is divisible by four."

  P:

  Q:

# Direct Proof: Example

"The square of every positive even number is divisible by four."

"If n is a positive even number then its square, $n^2$, is divisible by four."

- A number, n, that is even and positive can be written as $n=2k$, with $k \in \mathbb{N}$.
- $(2k)^2 = 4k^2$ is divisible by four. ☺

# Direct Proof: Example

"If n is odd, then $n^2$ is odd."

# Observation

- The implication $P \rightarrow Q$ is logically equivalent to:

| P | Q | $P \rightarrow Q$ | $Q \rightarrow P$ | $\neg P \rightarrow \neg Q$ | $\neg Q \rightarrow \neg P$ |
|---|---|---|---|---|---|
| F | F | | | | |
| F | T | | | | |
| T | F | | | | |
| T | T | | | | |

- $\neg Q \rightarrow \neg P$

# Contrapositives

- Note that the implication $P \to Q$ is logically equivalent to **$\neg Q \to \neg P$**.
- Therefore, $P \to Q$ can be proved by demonstrating that its **contrapositive** is true.
- An **indirect proof** is a proof of the contrapositive.

# Contrapositives: Example

"If 3n+2 is odd, then n is odd."

- Assume that conclusion is false, i.e. assume that n is even.
- Then n=2k for some integer k.
- Now, 3n+2 = 3(2k)+2 = 6k+2 = 2 (3k+1), which is a multiple of two, so is even.

The negation of the conclusion of the implication leads to a false hypothesis.

Therefore, the original implication is true.

# Contrapositives: Example

"If $n^2$ is odd, then n is odd."

- Formalize:
  - P:
  - Q:
  - $P \rightarrow Q$:
- Contrapositive:
  - "If n is even, then $n^2$ is even."
  - $n = 2k$ for some integer k
  - $n^2 = (2k)^2 = 4k^2 = 2(2k^2)$ is a multiple of two, so is even.
- Therefore, the original statement is true.

# Vacuous Proof

- We are trying to prove $P \rightarrow Q$.
- But P is false.
  - Then in both cases, $F \rightarrow F$ and $F \rightarrow T$, the implication is true.
- If P can be shown to be false, then a **vacuous proof** of $P \rightarrow Q$ can be given.

"For n=0, show that if $n>1$, then $n^2 > n$."

– "If $0>1$, then $0^2>0$." This is vacuously true.

# Trivial Proof

- We are trying to prove $P \rightarrow Q$.
- We know that Q is true.
  - Then in both cases, $F \rightarrow T$ and $T \rightarrow T$, the implication is true.
- If Q can be shown to be true, then a **trivial proof** of $P \rightarrow Q$ can be given.

"For $n=0$, show that if $a \geq b$, then $a^n \geq b^n$."

- "If $a \geq b$, then $a^0 \geq b^0$" is trivially true.

# Proof by Contradiction

- Given a statement S, assume it is false.
- Prove that $\neg S$ leads to false.
- **Intuition:**
  - To show that S must be true, suppose it is not true, instead, assume the negation of S was true.
  - Demonstrate that a consequence of this assumption is a statement that is known to be false.
  - This shows that your assumption must have been false, so S is therefore true.

# Proof by Contradiction: Example

- Theorem (by Euclid):

  "There are infinitely many prime numbers."

- Proof:
  - Assume there is a finite number of primes.
  - List them in sequence: $p_1$, $p_2$, $p_3$, ..., $p_n$.
  - Now, consider $x = p_1 p_2 p_3 \ldots p_n + 1$.
  - x is not divisible by any of the primes in our list.
    - Dividing x by any of the primes in our list leaves a remainder of 1!
  - We know that all non-prime numbers can be written as products of primes.
  - The only divisors of x are 1 and x itself.
  - Therefore, x must be a prime not in our list.
  - This contradicts our assumption.
  - Therefore, there are infinitely many prime numbers.

# Proof by Contradiction

- For a statement $P \rightarrow Q$ you only need to consider the case when P is true and Q is false:
  - To prove $P \rightarrow Q$,
    assume its negation is true, i.e. $\neg(P \rightarrow Q)$.
  - Note that $\neg(P \rightarrow Q) = \neg(\neg P \vee Q) = P \wedge \neg Q$.
  - If we can show that $P \wedge \neg Q$ leads to a contradiction (such as $P \wedge \neg P$ or $\neg Q \wedge Q$), then we can conclude that $P \wedge \neg Q$ must be false.
  - Therefore, $P \rightarrow Q$ must be true.

# Proof by Contradiction

More formally, proof by contradiction is based on the following logical equivalences:

For P and Q propositions,

- $(\neg(P \rightarrow Q) \rightarrow \neg P) \Leftrightarrow (P \rightarrow Q)$, i.e.
  $((P \wedge \neg Q) \rightarrow \neg P) \Leftrightarrow (P \rightarrow Q)$ or
- $(\neg(P \rightarrow Q) \rightarrow Q) \Leftrightarrow (P \rightarrow Q)$, i.e.
  $((P \wedge \neg Q) \rightarrow Q) \Leftrightarrow (P \rightarrow Q)$.

(SSE: If this is not intuitive, write the truth tables for the above equivalences.)

# Existence Proofs

- To prove a statement $\exists x P(x)$, we only need to show that P(n) for some n.
- Two types of proof:
  - In **constructive proof** we find a specific value of n for which P(n) holds.
  - In **non-constructive proof** we show that such an n exists, but we don't actually find it.
    - Strategy:
      - Assume that it does not exist and derive a contradiction.

# Constructive Existence Proof: Examples

"A square exists that is the sum of two other squares."

- Proof: $3^2 + 4^2 = 5^2$

"A cube exists that is the sum of three other cubes."

- Proof: $3^3 + 4^3 + 5^3 = 6^3$

# Uniqueness Proofs

- If a theorem states that only one such value exists, then we must demonstrate:
  - Existence: that such a value exists, and
  - Uniqueness: that there is only one such value.

"If the equation $5x + 3 = a$ has a solution, then it is unique."

- Existence: $5x+3 = a$, yields $x = (a-3)/5$
- Uniqueness: $5x_1+3 = 5x_2+3 = a$, yields $x_1=x_2$

# Counter examples

- Given a statement $\forall x P(x)$, find a single example for which it is not true.

"Every positive integer is the square of another positive integer."

  - Need to find a number for which the square root is not an integer.

- Note:
  - One can disprove a statement with a single counter example.
  - But, one can't prove a statement by example.
    - Prove that "all numbers are even."

# Proof by Exhaustion

- The problem is split into subcases.
  - Proof by Exhaustion is sometimes called a **case spit.**
- Each subcase is proven individually.
- More formally:
  - Show that $(P_1 \vee P_2 \vee P_3 \vee \ldots \vee P_n) \rightarrow Q$
  - by demonstrating that
  - $P_1 \rightarrow Q \wedge P_2 \rightarrow Q \wedge P_3 \rightarrow Q \wedge \ldots \wedge P_n \rightarrow Q$
- Need to make sure we include ALL cases.
- There is no limit to the number of cases. ☺

# Mathematical Induction

- Show that the statement holds for n=1, i.e. prove P(1).
  - If P(n) holds from n=0, then prove P(0).
- Assume P(k) is true for some k ≥ 1.
  - To obtain P(k) from P(n) set n=k in P(n).
    - This is simply a syntactic replacement of n with k in P(n).
- Prove that if P(k) is true, then P(k+1) is true.
- Based on P(1) being true and P(k) → P(k+1) being true, we can now conclude P(2).
  - Based on P(2) and P(k) → P(k+1), we can derive P(3).
  - Based on P(3) and P(k) → P(k+1), we can derive P(4).
  - …
- This establishes P(n) for all n by the principle of mathematical induction.

# Summary

- Proof strategies:
  - Direct proof
  - Proof by contradiction
  - Existence proofs
  - Contrapositives and Counter examples
  - Proof by exhaustion (case split)
  - (Mathematical induction)
- Workshop: Practice individual strategies