Proofs

Inference upon inference, leading to another inference.
(Richard Keen)

Terminology

A proof is a valid and clear argument that demonstrates the truth of a theorem.
A proof is based on premises/axioms/definitions, statements already assumed/known to be true, and inference rules.

- See Appendix I (real numbers), Appendix II (exponentials and logarithms), and instructor’s web page (inequalities).
- Any axiom/property of real numbers not involving division is also true for integers.

A proof method usually has a form that can be justified by an inference rule.

Where Do Theorems Come From?

We want to know the properties of mathematical structures.
We want to ensure that certain consequences happen.
Consider:
- comparing $x$ and $x^2$.
  When is $x < x^2$, $x = x^2$, or $x > x^2$?
  What implies $x < x^2$, $x = x^2$, or $x > x^2$?
  What does $x < x^2$, $x = x^2$, or $x > x^2$ imply?
- comparing $2x$ and $x^2$.
- comparing $x + y$ and $xy$.

Proving $P(x)$ Implies $Q(x)$

We usually try to prove theorems of the form: $P(x)$ implies $Q(x)$.
Recall $P(x)$ implies $Q(x)$ means $\forall x (P(x) \rightarrow Q(x))$.
Recall $P(x)$ implies $Q(x)$ is true if, whenever $P(x)$ is true, $Q(x)$ is also true.
Recall $P(x)$ implies $Q(x)$ is false if there is any counterexample $x = a$ where $P(a)$ is true and $Q(a)$ is false.

First thing to check: Look for a counterexample. A counterexample proves $\neg(P(x)$ implies $Q(x))$, which is equivalent to $\exists x (P(x) \land \neg Q(x))$. 

Types of Proofs for $p$ implies $q$

I use $p$ implies $q$ as shortcut for $P(x)$ implies $Q(x)$.

<table>
<thead>
<tr>
<th>Type Of Proof</th>
<th>How To Show It</th>
</tr>
</thead>
<tbody>
<tr>
<td>Counterexample of $p$ implies $q$</td>
<td>Find a value where $p$ is true and $q$ is false.</td>
</tr>
<tr>
<td>Direct Proof of $p$ implies $q$</td>
<td>Assume $p$ is true. Derive a chain of implications which ends with $q$.</td>
</tr>
<tr>
<td>Indirect Proof of $p$ implies $q$</td>
<td>Prove $\neg q$ implies $\neg p$ with a direct proof.</td>
</tr>
<tr>
<td>Proof by Contradiction of $p$ implies $q$</td>
<td>Do a direct proof of $(p \land \neg q)$ implies false, that is, implies a contradiction.</td>
</tr>
</tbody>
</table>

Examples of Direct Proofs

- Prove $x < 0$ implies $x < 1$
  - Assume $x < 0$. Want to show $x < 1$.
  - Proof: We know $0 < 1$.
    - $x < 0$ and $0 < 1$ implies $x < 1$.
  - $x < 0$ implies $x < x(x-1)$
  - Assume $x < 0$. Want to show $x < x(x-1)$.
    - Proof: $x < 0$ implies $x - 1 < 0$.
      - $x < 0$ and $x - 1 < 0$ imply $x(x-1) > 0$.
      - $x < 0$ and $x(x-1) > 0$ imply $x < x(x-1)$.

Examples of Indirect Proofs

- Prove $x < 0$ implies $x < 1$
  - Assume $x \geq 1$. Want to show $x \geq 0$.
    - Proof: We know $1 \geq 0$.
      - $x \geq 1$ and $1 \geq 0$ imply $x \geq 1$.
  - Prove $x < 0$ implies $x < x(x-1)$
  - Assume $x \geq x(x-1)$. Want to show $x \geq 0$.
    - Proof: $x \geq x(x-1)$ implies $x \geq x^2 - x$.
      - We know $x^2 \geq 0$.
      - $2x \geq x^2$ and $x^2 \geq 0$ imply $2x \geq 0$.
      - $2x \geq 0$ implies $x \geq 0$. 

CS 2233 Discrete Mathematical Structures

Proofs – 5

Setting Up Proofs of $p$ implies $q$

<table>
<thead>
<tr>
<th>Type Of Proof</th>
<th>How To Set It Up</th>
</tr>
</thead>
</table>
| Direct Proof of $p$ implies $q$ | Assume: $p$
  - Want to show: $q$
  - Proof: $\ldots$ |
| Indirect Proof of $p$ implies $q$ | Assume: $\neg q$
  - Want to show: $\neg p$
  - Proof: $\ldots$ |
| Proof by Contradiction | Assume $p \land \neg q$
  - Want to show: contradiction
  - Proof: $\ldots$ |
Examples of Proofs by Contradiction

- Prove $xy = 0$ implies $x = 0 \lor y = 0$
- Assume $xy = 0$ and $x \neq 0 \land y \neq 0$.
  Want to show a contradiction.
  Proof: $x \neq 0$ and $y \neq 0$ imply $xy \neq 0$.
  $xy \neq 0$ contradicts $xy = 0$.
- Prove $x + y < xy \land y < 0$ implies $x < 1$
- Assume $x + y < xy \land y < 0$ and $x \geq 1$.
  Want to show a contradiction.
  Proof: $x \geq 1$ implies $y < x + y$.
  $y < x + y$ and $x + y < xy$ imply $y < xy$.
  $y < 0$ and $y < xy$ imply $1 > x$.
  $1 > x$ contradicts $x \geq 1$.

Proofs of $\exists x P(x)$ and $\forall x P(x)$

To prove $\exists x P(x)$, find a value for $x$ that makes $P(x)$ true. Alternative: find a calculation for $x$.

- Prove $\exists y (x < y^2)$.
  Proof: choose $x = -1$.
- Prove $\forall y \exists x (y^2 < x)$.
  Choose $x = y^2 + 1$.

To prove $\forall x P(x)$, show that $P(x)$ follows from the properties of the domain.

- Prove $\forall x (x^2 \geq 0)$.
- Proof: $x$ can be positive, zero, or negative.
  - Case 1: $x > 0$ implies $x^2 > 0$.
  - Case 2: $x = 0$ implies $x^2 = 0$.
  - Case 3: $x < 0$ implies $x^2 > 0$.
  All cases imply $x^2 \geq 0$.

Proof by Contradiction of $\forall x P(x)$

To prove $\forall x P(x)$ by contradiction, assume $\exists x \neg P(x)$ and show the properties of the domain results in a contradiction.

- Prove $x < x^2 + 1$.
- Assume $x \geq x^2 + 1$.
  Want to show a contradiction, that is, want to show $x \geq x^2 + 1$ is always F.
  Proof:
  - $x \geq x^2 + 1$ and $x^2 + 1 \geq x + 1$ imply $x \geq 1$.
  - $x \geq x^2 + 1$ and $x^2 + 1 > x^2$ imply $x > x^2$.
  - $x \geq 1$ and $x > x^2$ imply $1 > x$.
  - $x \geq 1$ and $1 > x$ is a contradiction.
Proving $\sqrt{2}$ is Irrational

Definition: A number $x$ is rational if can be expressed as $x = a/b$ where $a$ and $b$ are integers.

Property: We can eliminate common factors to get the same $x$.

Proof by contradiction:

- Assume $\sqrt{2} = a/b$, where $a$ and $b$ are integers with no common divisors.
- $\sqrt{2} = a/b$ implies $2 = a^2/b^2$, and $2b^2 = a^2$.
- This implies $a^2$ is even, which implies $a$ is even, and that $c = a/2$ is an integer.
- Then $2b^2 = 4c^2$, which is equiv. to $b^2 = 2c^2$.
- This implies $b$ is even, which is a contradiction.

Halting Problem Can’t Be Totally Solved

Proof by Contradiction:

- Assume program $\text{Halt}(P, I)$ always returns T if program $P$ halts on input $I$, and F otherwise.
- Let $K$ be the following program:

  procedure $K(P$: program)
  if $\text{Halt}(P, P)$
    then perform an infinite loop
  else return T

- Consider what $\text{Halt}(K, K)$ might return.
  Case 1: $\text{Halt}(K, K) = T$ implies $K(K)$ does not halt.
  Case 2: $\text{Halt}(K, K) = F$ implies $K(K)$ halts.
  Both cases are contradictions.