Introduction to proofs

proofs

- Proofs are essential in mathematics and computer science.
- Some applications of proof methods
 - Proving mathematical theorems
 - Designing algorithms and proving they meet their specifications
 - Verifying computer programs
 - Establishing operating systems are secure
 - Making inferences in artificial intelligence
 - Showing system specifications are consistent
 - **.**..

Terminology

Theorem:

A statement that can be shown to be true.

Proposition:

A less important theorem.

Lemma:

A less important theorem that is helpful in the proof of other results.

Terminology

Proof:

A convincing explanation of why the theorem is true.

Axiom:

A statement which is assumed to be true.

Corollary:

A theorem that can be established easily from a theorem that has been proven.

Theorem (example)

Many theorems assert that a property holds for all elements in a domain.

Example:

If x>y, where x and y are positive real numbers, then $x^2 > y^2$.

For all positive real numbers x and y, if x>y, then $x^2>y^2$.

 $\forall x \forall y (R(x,y) \rightarrow S(x,y))$ domain: all positive real numbers

R(x,y): x>y

 $S(x,y): x^2 > y^2$

Theorem

How to prove $\forall x (R(x) \rightarrow S(x))$?

Universal generalization (review):

Show $R(c) \rightarrow S(c)$ where c is an arbitrary element of the domain.

Using universal generalization, $\forall x (R(x) \rightarrow S(x))$ is true.

Theorem

How to prove $\forall x (R(x) \rightarrow S(x))$?

Show $R(c) \rightarrow S(c)$ where c is an arbitrary element of the domain.

Conditional statement (review):

p→q is true unless p is true and q is false.

To show p→q is true, we need to show that if p is true, then q is true.

р	q	p→q
 - -	 	
T	Щ	Ш
F	T	Т
F	F	T

Direct proof

How to prove $\forall x (R(x) \rightarrow S(x))$?

Let c be any element of the domain.

Assume R(c) is true.



S(c) must be true.

These steps are constructed using

- Rules of inference
- Axioms
- Lemmas
- Definitions
- Proven theorems

• , , ,

Direct proof

Direct proof (example)

Theorem:

If n is an odd integer, then n² is odd.

Proof:

Assume n is an odd integer.

By definition, 3 integer k,

such that n = 2k + 1

$$n^2 = (2k + 1)^2$$

$$n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Let $m = 2k^2 + 2k$.

$$n^2 = 2m + 1$$

So, by definition, n² is odd.

Definition:

n is odd integer, if \exists integer k such that n=2k+1.

Direct proof (example)

Theorem:

If n and m are both perfect squares then nm is also a perfect square.

Proof:

Assume n and m are perfect squares. By definition, \exists integers s and t such that $n=s^2$ and $m=t^2$.

$$nm = s^2 t^2 = (st)^2$$

Let k = st.

$$nm = k^2$$

So, by definition, nm is a perfect square.

Definition:

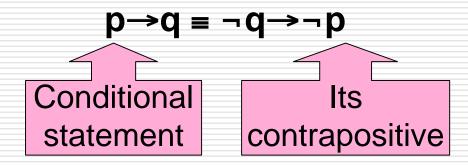
An integer a is perfect square if Integer b such that a=b².

Proof techniques

Direct proof leads from the hypothesis of a theorem to the conclusion.

Proofs of theorems that do not start with the hypothesis and end with the conclusion, are called **indirect proofs**.

Proof by contraposition



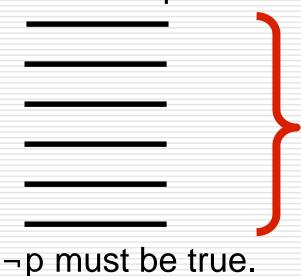
In a proof by contraposition of $p\rightarrow q$, we take $\neg q$ as a hypothesis and we show that $\neg p$ must follow.

Proof by contraposition is an indirect proof.

Proof by contraposition

Proof by contraposition of p→q:

Assume ¬q is true.



These steps are constructed using

- Rules of inference
- Axioms
- Lemmas
- Definitions
- Proven theorems

• . . .

Proof by contraposition

Proof by contraposition (example)

Theorem:

If n is an integer and 3n+2 is odd, then n is odd.

Proof (by contraposition):

Assume n is even.

 \exists integer k, such that n = 2k

3n+2 = 3(2k)+2 = 2(3k+1)

Let m = 3k+1.

3n+2 = 2m

So, 3n+2 is even.

By contraposition, if 3n+2 is odd, then n is odd.

Proof by contraposition (example)

Theorem:

If n =ab, where a and b are positive integers, then $b \le \sqrt{n}$ or $a \le \sqrt{n}$.

Proof (by contraposition):

Assume b > \sqrt{n} and a > \sqrt{n} .

$$ab > (\sqrt{n}) \cdot (\sqrt{n}) = n$$

So, n≠ab.

By contraposition, if n=ab, then $b \le \sqrt{n}$ or $a \le \sqrt{n}$.

Assume P(n) is "if n > 0, then $n^2 > 0$ ".

Show that P(0) is true.

Proof:

P(0) is "if 0>0, then $0^2 > 0$ ".

Since the hypothesis of P(0) is false, then P(0) is true.

Vacuous proof:

p→q is true when p is false.

Assume P(n) is "if ab > 0, then $(ab)^n > 0$ ". Show that P(0) is true.

Proof:

P(0) is "if ab>0, then $(ab)^0 > 0$ ".

$$(ab)^0 = 1 > 0$$

Since the conclusion of P(0) is true, P(0) is true.

Trivial proof:

p→q is true when q is true.

Theorem:

The sum of two rational numbers is rational.

Proof:

Assume r and s are rational.

 $\exists p,q \qquad r = p/q \quad q \neq 0$

 $\exists t, u$ s = t/u $u \neq 0$

r+s = p/q + t/u = (pu+tq) / (qu)

Since $q \neq 0$ and $u \neq 0$ then $qu \neq 0$.

Let m=(pu+tq) and n=qu where $n\neq 0$.

So, r+s = m/n, where $n \neq 0$.

So, r+s is rational.

Definition:

The real number r is rational if r=p/q, \exists integers p and q that $q \neq 0$.

Theorem:

If n is an integer and n² is even, then n is even.

Direct proof or proof by contraposition?

Proof (direct proof):

Assume n² is an even integer.

$$n^2 = 2k$$

(k is integer)

$$n = \pm \sqrt{2k}$$

???

dead end!

Theorem:

If n is an integer and n² is even, then n is even.

Direct proof or proof by contraposition?

Proof (proof by contraposition):

Assume n is an odd integer.

$$n = 2k+1$$
 (k is integer)

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$$

Assume integer $m = 2k^2 + 2k$.

$$n^2 = 2m + 1$$

So, n² is odd.

By contraposition, If n² is even, then n is even.

Proof by contradiction

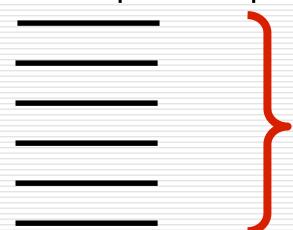
How to prove a proposition by contradiction?

- Assume the proposition is false.
- Using the assumption and other facts to reach a contradiction.
- This is another kind of indirect proof.

Proof by contradiction

Proof by contradiction of $p\rightarrow q$:

Assume p and ¬q is true.



Contradiction.

These steps are constructed using

- Rules of inference
- Axioms
- Lemmas
- Definitions
- Proven theorems

• . . .

Proof by contradiction

Proof by contradiction (example)

Prove that $\sqrt{2}$ is not rational by contradiction.

Proof (proof by contradiction):

Assume $\sqrt{2}$ is rational.

$$\exists a,b$$
 $\sqrt{2} = a/b$ $b \neq 0$

If a and b have common factor, remove it

by dividing a and b by it

$$2 = a^2 / b^2$$

$$2b^2 = a^2$$

So, a² is even and by previous theorem, a is even.

$$\exists k \quad a = 2k.$$

$$2b^2 = 4k^2$$

$$b^2 = 2k^2$$

So, b² is even and by previous theorem, b is even.

$$\exists m \ b = 2m.$$

So, a and b have common factor 2 which contradicts the Assumption.

Definition:

The real number r is rational if r=p/q, ∃ integers p and q ≠0.

Proof by contradiction (example)

Prove if 3n+5 is even then n is odd.

Proof (proof by contradiction):

Assume 3n+5 is even and n is even.

n = 2k (k is some integer)

3n+5 = 3(2k) + 5 = 6k + 5 = 2(3k + 2) + 1

Assume m = 3k+2.

3n+5 = 2m + 1

So, 3n+5 is odd.

Assume p is "3n+5 is even ".

 $p \land \neg p$ is a contradiction.

By contradiction, if 3n+5 is even then n is odd.

Proof by contradiction (example)

Prove if n² is odd then n is odd.

Proof (proof by contradiction):

Assume n² is odd and n is even.

 \exists integer k n = 2k

 $n^2 = 4k^2 = 2(2k^2)$

Let $m = 2k^2$.

 $n^2 = 2m$

So, n² is even.

Let p is "n² is odd ".

 $p \land \neg p$ is a contradiction.

By contradiction, if n² is odd then n is odd.

Proofs of equivalences

How to prove $p \leftrightarrow q$?

р	q	p⇔q
T	+	T
T	F	F
F	T	F
F	F	T

$$p \Leftrightarrow q = (p \rightarrow q) \land (q \rightarrow p)$$

Proofs of equivalences

How to prove $p \leftrightarrow q$?

We need to prove

- p→q
- q→p

Proofs of equivalences

How to prove $p \leftrightarrow p_1 \leftrightarrow p_2 \leftrightarrow ... \leftrightarrow p_n$?

$$p \leftrightarrow p_1 \leftrightarrow p_2 \leftrightarrow ... \leftrightarrow p_n \equiv$$

 $(p_1 \rightarrow p_2) \land (p_2 \rightarrow p_3) \land ... \land (p_{n-1} \rightarrow p_n) \land (p_n \rightarrow p_1)$

We need to prove

- $p_1 \rightarrow p_2$
- $p_2 \rightarrow p_3$
- **.**..
- $p_{n-1} \rightarrow p_n$
- $p_n \rightarrow p_1$

 $\neg p \land \neg q$ is true if and only if $\neg (p \lor q)$ is true.

Proof:

Part1: if $\neg p \land \neg q$ is true then $\neg (p \lor q)$ is true.

- \square ¬p \wedge ¬q is true.
- □ ¬p is true and ¬q is true.
- p is false and q is false.
- pvq is false.
- \square ¬(pvq) is true.

 $\neg p \land \neg q$ is true if and only if $\neg (p \lor q)$ is true.

Proof:

Part2: if $\neg(p \lor q)$ is true then $\neg p \land \neg q$ is true.

- \square ¬(pvq) is true.
- pvq is false.
- p is false and q is false.
- □ ¬p is true and ¬q is true.
- \square ¬p \wedge ¬q is true.

Show these statements about integer n are equivalent

p: n is odd.

q: n+1 is even.

r: n² is odd.

How to prove it?

$$p \leftrightarrow q \leftrightarrow r \equiv (p \rightarrow q) \land (q \rightarrow r) \land (r \rightarrow p)$$

Show these statements about integer n are equivalent

p: n is odd.

q: n+1 is even.

r: n² is odd.

Proof:

1. $p\rightarrow q$: if n is odd then n+1 is even. (direct proof) n is odd. n=2k+1n+1=2k+2=2(k+1) m=k+1

n+1=2m n+1 is even.

Show these statements about integer n are equivalent

p: n is odd.

q: n+1 is even.

r: n² is odd.

Proof:

2. $q \rightarrow r$: if n+1 is even then n^2 is odd. (direct proof)

n+1 is even.

n+1=2k

$$n = 2k-1$$

$$n^2 = 4k^2-4k+1 = 2(2k^2-2k)+1$$

 $m = 2k^2 - 2k$

$$n^2 = 2m + 1$$

n² is odd.

Show these statements about integer n are equivalent

p: n is odd.

q: n+1 is even.

r: n² is odd.

Proof:

r→p: if n² is odd then n is odd.
 by previous example

Counterexample (review)

☐ How to show ∀x P(x) is false?
find a counterexample

Counterexample (example)

Show "every positive integer is a sum of the squares of two integers." is false.

Proof:

3 cannot be written as the sum of the squares of two integers.

Because only squares not exceeding 3 are $0^2 = 0$ and $1^2 = 1$.

There is no way to get 3 as the sum of these squares.

Recommended exercises

1,3,7,9,10,11,15,17,25,27,33,39