

Negation

Negations are statements of the form

not P

or, in other words,

P is not the case

or

P is absurd

or

P leads to contradiction

in symbols:

$P \Rightarrow \text{false}$

or, in symbols,

$\neg P$

A first proof strategy for negated goals and assumptions:

If possible, reexpress the negation in an *equivalent* form and use instead this other statement.

Logical equivalences

$\neg(P \implies Q)$	\iff	$P \wedge \neg Q$
$\neg(P \iff Q)$	\iff	$P \iff \neg Q$
$\neg(\forall x. P(x))$	\iff	$\exists x. \neg P(x)$
$\neg(P \wedge Q)$	\iff	$(\neg P) \vee (\neg Q)$
$\neg(\exists x. P(x))$	\iff	$\forall x. \neg P(x)$
$\neg(P \vee Q)$	\iff	$(\neg P) \wedge (\neg Q)$
$\neg(\neg P)$	\iff	P
$\neg P$	\iff	$(P \implies \text{false})$

Recall
 $(P \implies Q)$
 \iff
 $(\neg P \vee Q)$

all provable
from earlier
techniques plus
proof by contradiction

Theorem 37 For all statements P and Q ,

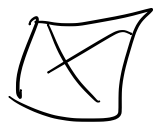
$$(P \implies Q) \implies (\neg Q \implies \neg P) .$$

PROOF: Assume $P \implies Q$. RTP $(\neg Q \implies \neg P)$.

Assume $\neg Q$, i.e. $Q \implies \text{false}$

[Before $(P \implies Q \ \& \ Q \implies R) \implies P \implies R$]

As earlier, deduce $P \implies \text{false}$, $\neg P$.



$(P_1 \implies P_2 \ \& \ P_2 \implies P_3 \ \& \ \dots \ \& \ P_{n-1} \implies P_n)$

$\implies P_1 \implies P_n$

Often write

$P_1 \implies P_2$
 $\implies P_3$
 $\implies P_n$

Proof by contradiction

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg P \implies \text{false}$

Proof by contradiction

The strategy for proof by contradiction:

To prove a goal P by contradiction is to prove the equivalent statement $\neg P \implies \text{false}$

Proof pattern:

In order to prove

P

1. **Write:** We use proof by contradiction. So, suppose P is false.
2. Deduce a logical contradiction.
3. **Write:** This is a contradiction. Therefore, P must be true.

✗ sometimes used to indicate a contradiction.

Scratch work:

Before using the strategy

Assumptions

Goal

P

⋮

After using the strategy

Assumptions

Goal

contradiction

⋮

$\neg P$

Theorem 39 For all statements P and Q ,

$$(\neg Q \implies \neg P) \implies (P \implies Q) .$$

PROOF: Assume $\neg Q \implies \neg P$ (1) RTP $P \implies Q$.

Assume P . RTP Q . We use pf by contradiction.

Assume $\neg Q$. By assumption (1), $\neg P$.

But P and $\neg P$ is absurd.

Therefore (by pf by contradiction), Q .

$\therefore P \implies Q$ 

PROMISE Well-founded induction & recursion (←) Easy.

Lemma 41 A positive real number x is rational iff

\exists positive integers m, n :

$$x = m/n \wedge \neg(\exists \text{ prime } p : p \mid m \wedge p \mid n) \quad (\dagger)$$

PROOF: (\Rightarrow) Assume x is a positive rational. By defn, $x = m/n$ for some pos. ints. m, n . So there is a pair m_0, n_0 s.t. $x = m_0/n_0$ and m_0 is least.

RTP $\rightarrow (\exists \text{ prime } p. p \mid m_0 \wedge p \mid n_0)$

Use proof by contradiction. Assume $\exists \text{ prime } p. p \mid m_0 \wedge p \mid n_0$.

So $m_0 = p \cdot m_1$ and $n_0 = p \cdot n_1$ for

pos. int. m_1, n_1 .

$$\therefore x = m_0/n_0 = \frac{p \cdot m_1}{p \cdot n_1} = m_1/n_1. \text{ But } m_1 < m_0 \quad \times$$

Uses the principle that any non-empty subset of natural numbers has a least element.

Numbers

Objectives

- ▶ Get an appreciation for the abstract notion of number system, considering four examples: natural numbers, integers, rationals, and modular integers.
- ▶ Prove the correctness of three basic algorithms in the theory of numbers: the division algorithm, Euclid's algorithm, and the Extended Euclid's algorithm.
- ▶ Exemplify the use of the mathematical theory surrounding Euclid's Theorem and Fermat's Little Theorem in the context of public-key cryptography.
- ▶ To understand and be able to proficiently use the Principle of Mathematical Induction in its various forms.