Negation

Negations are statements of the form

$$\boxed{\text{not } P}$$

or, in other words,

$$\boxed{P \text{ is not the case}}$$

or

$$\boxed{P \text{ is absurd}}$$

or

$$\boxed{P \text{ leads to contradiction}}$$

in symbols:

$P \Rightarrow \text{false}$

or, in symbols,

$$\boxed{\neg P}$$

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

$$
\begin{array}{rcl}
\neg(P \Longrightarrow Q) & \Longleftrightarrow & P \wedge \neg Q \\
\neg(P \Longleftrightarrow Q) & \Longleftrightarrow & P \Longleftrightarrow \neg Q \\
\neg(\forall x.\, P(x)) & \Longleftrightarrow & \exists x.\, \neg P(x) \\
\neg(P \wedge Q) & \Longleftrightarrow & (\neg P) \vee (\neg Q) \\
\neg(\exists x.\, P(x)) & \Longleftrightarrow & \forall x.\, \neg P(x) \\
\neg(P \vee Q) & \Longleftrightarrow & (\neg P) \wedge (\neg Q) \\
\neg(\neg P) & \Longleftrightarrow & P \\
\neg P & \Longleftrightarrow & (P \Rightarrow \mathbf{false})
\end{array}
$$

Recall

$(P \Rightarrow Q)$

$\Leftrightarrow$

$(\neg P \vee Q)$

all provable from earlier techniques plus proof by contradiction

Theorem 37 *For all statements* P *and* Q,

$$(\mathrm{P} \implies \mathrm{Q}) \implies (\neg\mathrm{Q} \implies \neg\mathrm{P}) \quad .$$

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

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

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

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

$\boxtimes$

$(P_1 \Rightarrow P_2 \ \& \ P_2 \Rightarrow P_3 \ \& \ \cdots \ \& \ P_{n-1} \Rightarrow P_n)$

$\Rightarrow \quad P_1 \Rightarrow P_n$

Often write

$P_1 \Rightarrow P_2$
$\Rightarrow P_3$
$\vdots$
$\Rightarrow P_n$

Proof by contradiction

The strategy for proof by contradiction:

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

Proof by contradiction

The strategy for proof by contradiction:

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

Proof pattern:

In order to prove

$$\mathrm{P}$$

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.

$\times\!\!\times$ sometimes used to indicate a contradiction.

Scratch work:

Before using the strategy

Assumptions	Goal
	P
$\vdots$	

After using the strategy

Assumptions	Goal
	contradiction
$\vdots$	
$\neg P$	

Theorem 39 *For all statements* P *and* Q,

$$(\neg \mathrm{Q} \implies \neg \mathrm{P}) \implies (\mathrm{P} \implies \mathrm{Q}) \quad .$$

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

Assume P. RTP: Q. We use pf by contradict.

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

But P and $\neg P$ is absurd.

Therefore (by pf by contradiction), Q.

$\therefore \quad P \Rightarrow Q$ $\quad \boxtimes$

PREMISE Well-founded induction & Recursion

($\Longleftarrow$) Easy.

Lemma 41 *A positive real number* x *is rational iff*

$$\exists \textit{ positive integers } m, n : \qquad (\dagger)$$
$$x = m/n \land \neg(\exists \textit{ prime } p : p \mid m \land p \mid n)$$

PROOF: ($\Longrightarrow$) 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 $\neg(\exists \text{prime } p.\ p \mid m_0 \ \&\ p \mid n_0)$.

Use proof by contradiction. Assume $\exists$ prime p. $p \mid m_0$ & $p \mid n_0$.

So $m_0 = p \cdot m_1$ and $n_0 = p \cdot n_1$ for pos. int. m_1, n_1.

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

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.