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

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

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

$\neg(\neg P)$

$\Longleftrightarrow [(\neg P) \Rightarrow false]$

$\Longleftrightarrow [(P \Rightarrow false) \Rightarrow false]$

$$\neg(P \Longrightarrow Q) \iff P \land \neg Q$$

$$\neg(P \iff Q) \iff P \iff \neg Q$$

$$\neg(\forall x.\, P(x)) \iff \exists x.\, \neg P(x)$$

$$\neg(P \land Q) \iff (\neg P) \lor (\neg Q)$$

$$\neg(\exists x.\, P(x)) \iff \forall x.\, \neg P(x)$$

$$\neg(P \lor Q) \iff (\neg P) \land (\neg Q)$$

$$\neg(\neg P) \iff P$$

In classical logic.

Standard Definition.

$$\boxed{\neg P \iff (P \Rightarrow \mathbf{false})}$$

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

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

PROOF: For statements P and Q

Assume : $P \Rightarrow Q$ (2)

Assume : $\neg Q \Leftrightarrow (Q \Rightarrow \text{false})$ (4)

<u>RTP</u>: $\neg P \Leftrightarrow (P \Rightarrow \text{false})$

<u>Assume</u>: P (1)

By (1) & (2), we have Q (3)

By (3) & (4), we have false and we are done.

$\boxtimes$

eg. yields that $(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)$

Proof by contradiction

The strategy for proof by contradiction:

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

to prove this is to assume $\neg P$ and reach a contradiction or absurdity.

relies on accepting that $P \Leftrightarrow \neg(\neg P)$

Proof by contradiction

The strategy for proof by contradiction:

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

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.

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,

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

PROOF: For statements P and Q.

Assume: $\neg Q \Rightarrow \neg P$ (2)

Assume: P (4)

RTP: Q

We use proof by contradiction.

So we assume that Q is not the case; that is $\neg Q$ (1)

By (1) and (2), we get $\neg P$ (3)

From (3) and (4) we get a contradiction.

namely that both P and $\neg P$ hold.

Hence, our assumption that $\neg Q$ is absurd and so we have Q as required.

$\boxtimes$

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

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

PROOF: Let x be a positive real number.

($\Leftarrow$) Assume ($\dagger$)

RTP: x is rational $\Leftrightarrow$ $x = i/j$ for integers i and j.

($\dagger$) $\Rightarrow$ $\exists$ int. m and n. $x = m/n$

Hence, x is rational.

($\Rightarrow$) Assume x is rational, That is
(*) of the form m/n for integers m and n

Since x is positive we may take m and n also positive.

RTP: (+)

We show it by contradiction

So, Assume: (+) is not the case; That is, Assume

$\neg(\exists \text{ pos int } m,n.\ x = m/n \wedge \neg(\exists \text{ prime } p.\ p \mid m \wedge p \mid n))$

$\iff \forall \text{ pos. int. } m,n.\ \neg(x = m/n \wedge \neg(\exists \text{ prime } p.\ p \mid m \wedge p \mid n))$

$\iff \forall \text{ pos. int } m,n.\ \neg(x = m/n) \vee (\exists \text{ prime } p.\ p \mid m \wedge p \mid n)$

$\iff$

(††) $\forall \text{ pos. int } m,n.\ x = m/n \Rightarrow (\exists \text{ prime } p.\ p \mid m \wedge p \mid n)$

By assumption$^{(*)}$, $x = m/n$ for pos. int. m and n.

By (††) it follows that there is a prime, say p_0, such that $p_0 | m$ and $p_0 | n$; that is,

$m = p_0 \cdot m_0$ and $n = p_0 \cdot n_0$ for pos. int m_0 and n_0

Then $x = m/n = p_0 \cdot m_0 / p_0 \cdot n_0 = m_0/n_0$

So, by (‡), there is a prime, say p_1, such that

$p_1 | m_0$ and $p_1 | n_0$; that is, $m_0 = p_1 \cdot m_1$ and

$n_0 = p_1 \cdot n_1$ for pos. int. m_1 and n_1.

Analogously, $x = m_0/n_0 = p_1 \cdot m_1 / p_1 \cdot n_1 = m_1/n_1$

and we may repeat the same argument to find a prime p_2 such that

$$m_1 = p_2 \cdot m_2 \quad \text{and} \quad n_1 = p_2 \cdot n_2$$

for pos. int. m_2 and n_2.

Iterating this ℓ times we have

$$m = p_0 \cdot m_0 = p_0 \cdot p_1 \cdot m_1 = p_0 \cdot p_1 \cdot p_2 \cdot m_2$$

$$= \cdots = p_0 \cdot p_1 \cdot \cdots \cdot p_{\ell-1} \cdot m_\ell$$

and for $\ell \geqslant m$ we get

$$m = p_0 \cdots p_{\ell-1} \geqslant 2^\ell$$ a contradiction

$\boxtimes$

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.

Natural numbers

In the beginning there were the *natural numbers*

$$\mathbb{N} : \quad 0\ ,\quad 1\ ,\quad \ldots\ ,\quad n\ ,\quad n+1\ ,\quad \ldots$$

generated from *zero* by successive increment; that is, put in ML:

```
datatype
  N = zero | succ of N
```

The basic operations of this number system are:

- Addition

$$\underbrace{\overbrace{*\cdots*}^{m}\overbrace{*\cdots\cdots*}^{n}}_{m+n}$$

- Multiplication

$$m\left\{\begin{array}{ccc} \multicolumn{3}{c}{\overbrace{*\cdots\cdots\cdots\cdots*}^{n}} \\ \vdots & m\cdot n & \vdots \\ \multicolumn{3}{c}{*\cdots\cdots\cdots\cdots*} \end{array}\right.$$

The *additive structure* $(\mathbb{N}, 0, +)$ of natural numbers with zero and addition satisfies the following:

- Monoid laws

$$0 + n = n = n + 0 \quad , \quad (l + m) + n = l + (m + n)$$

- Commutativity law

$$m + n = n + m$$

and as such is what in the mathematical jargon is referred to as a *commutative monoid*.

Also the *multiplicative structure* $(\mathbb{N}, 1, \cdot)$ of natural numbers with one and multiplication is a commutative monoid:

- Monoid laws

$$1 \cdot n = n = n \cdot 1 \quad , \quad (l \cdot m) \cdot n = l \cdot (m \cdot n)$$

- Commutativity law

$$m \cdot n = n \cdot m$$

Monoids

Algebraic structures with

- elements
- a neutral element, say e
- a binary operation, say m

s.t.

$$m(e, x) = x = m(x, e)$$

$$m(m(x, y), z) = m(x, m(y, z))$$

A monoid is commutative whenever it further satisfies. $m(x, y) = m(y, x)$.

Exercise Let (M, e, m) be a monoid

elements

neutral element

multiplication.

Let also (M, e', m) be a monoid.

Show $e = e'$.