Proofs

A proof clearly shows some proposition is true.

A proof starts from assumptions and ends with a conclusion.

Proofs mainly depend on a rule of inference called modus ponens:

p	we know or assume p
$p \to q$	we know or assume p implies q
q	we conclude q

Note that $(p \wedge (p \to q)) \to q$ is a tautology.

Inference with Predicates

A predicate $P(x)$ implies another predicate $Q(x)$ $\equiv \forall x\,(P(x) \to Q(x))$ is true.

Examples:

$x < y$ and $y < z$ imply $x < z$

$y < z$ implies $x + y < x + z$

$0 < x$ and $y < z$ imply $xy < xz$

$x < 0$ and $y < z$ imply $xy > xz$

$1 < x$ and $y < z$ imply $x^y < x^z$

$0 < x$ and $x < y$ imply $\log x < \log y$

Types of Proofs

We can prove $p \rightarrow q$ in several ways.

Vacuous Proof. Conclude with $\neg p$.

Prove $(x < y \wedge y < x) \rightarrow x < x$

Proof: $\neg(x < y \wedge y < x)$ is equivalent to $x \geq y \vee y \geq x$, which is obviously true.

Trivial Proof. Conclude with q.

Prove $x > 1 \rightarrow x - 1 < x$.

Proof: $x - 1 < x$ is obviously true.

Direct Proof. Assume p. Conclude with q.

Prove $(x<y \wedge y<z) \rightarrow (y-x)^2<(z-x)^2$

Proof:

Assume $x < y \wedge y < z$
Conclude with $(y - x)^2 < (z - x)^2$

$x < y$ implies $0 < y - x$
$y < z$ implies $y - x < z - x$
$0 < y-x < z-x$ implies $(y-x)^2 < (z-x)^2$

Indirect Proof. Assume $\neg q$. Conclude with $\neg p$.

Prove $x < z \rightarrow (x < y \vee y < z)$

Proof:

Assume $x \geq y$ and $y \geq z$.
Conclude with $x \geq z$.

$x \geq y$ and $y \geq z$ implies $x \geq z$

Proof by Contradiction. Show $p \wedge \neg q$ is false.

Assume $p \wedge \neg q$ and conclude with a statement that is obviously false.

Prove $(xy < x + y \wedge x \geq 2) \rightarrow y < 2$

Proof:

Assume $xy < x + y$ and $x \geq 2$ and $y \geq 2$.
Conclude with a contradiction.

$x \geq 2 \rightarrow x - 1 \geq 1$, and $y \geq 2 \rightarrow y - 1 \geq 1$
$x - 1 \geq 1$ and $y - 1 \geq 1$ imply $(x - 1)(y - 1) \geq 1$
$(x - 1)(y - 1) = xy - x - y + 1$
$xy - x - y + 1 \geq 1$ implies $xy \geq x + y$
$xy \geq x + y$ contradicts $xy < x + y$

On Backward Reasoning

To prove $p \to q$ by backward reasoning,
first prove $r \to q$ for some proposition r,
and then prove $p \to r$.

Don't do this unless you say what implies what.

Prove $x^2 > 1 \ \to \ x > 1$ assuming x is positive.

Bad Proof: $x > 1$
$1 > 1/x$ (divide both sides by x)
$x > 1/x$ (implied from both inequalities above)
$x^2 > 1$ (multiply both sides by x)

Halting Problem

Let $H(P, I) \equiv$ program P halts on input I.
No algorithm can solve H.

Proof by Contradiction:

Assume an algorithm $Halt(P, I)$ solves $H(P, I)$.

Let $K(P)$ be the following algorithm:

procedure $K(P$: program$)$
    if $Halt(P,P)$
        then perform an infinite loop
        else return true

What happens for $K(K)$?

$H(K, K)$ is defined to be true if $K(K)$ halts, but if $K(K)$ does not halt if $Halt(K, K)$ is true.

This is a contradiction.
This implies that the assumption is false, proving no algorithm solves the halting problem.