Logic LVA 703600 VU3

http://cl-informatik.uibk.ac.at/teaching/ws05/logic/

Georg Moser (VU)[1] Christian Vogt (VU)[2]

[1]georg.moser@uibk.ac.at
office hours: Thursday 1pm–3pm

[2]christian.vogt@uibk.ac.at
office hours: Tuesday 9am–11am

Autumn 2005

Deductive Proofs

A deductive proof is a sequence of statements, such that the truth of some hypothesis leads to a truth of a conclusion.

If H, then C. or H implies C.

Theorem If $n \geq 4$, then $2^n \geq n^2$.

Proof informal

For $n = 4$ correct: $2^4 \geq 4^2$.

For $n \geq 4$: Left hand side (lhs) doubles, if n increases by 1. The rhs multiplies by $\frac{(n+1)^2}{n^2}$

If $n \geq 4$, then $\frac{n+1}{n} \leq 1,25$. Hence $\frac{(n+1)^2}{n^2} \leq 1,5625 < 2$. $\square$

Theorem If n is the sum of the squares of four positive integers, then $2^n \geq n^2$.

(1)	$n = a^2 + b^2 + c^2 + d^2$	hypothesis
(2)	$a \geq 1, b \geq 1, c \geq 1, d \geq 1$	hypothesis
(3)	$a^2 \geq 1, b^2 \geq 1, c^2 \geq 1, d^2 \geq 1$	(2) and arithmetic
(4)	$n \geq 4$	(1) and (3)
(5)	$2^n \geq n^2$	(4) and the previous theorem

□

Reduction to Definitions

Theorem Let S be a finite subset of some infinite set U. Let T be the complement of S with respect to U. Then T is infinite.

Proof

- by definition $S \cup T = U$ and S, T disjoint, hence $|S| + |T| = |U|$.
- by assumption S is finite, hence by definition exists n, such that $|S| = n$.
- by assumption U is infinite, hence no number l exists, such that $|U| = l$.
- suppose T is finite.
- exists m, such that $|T| = m$.
- hence $|U| = |S| + |T| = n + m$.
- contradiction.

□

Proof by Contradiction

Proof

- ...
- suppose T is finite.
- exists m, such that $|T| = m$.
- hence $|U| = |S| + |T| = n + m$.
- contradiction. $\square$

in general

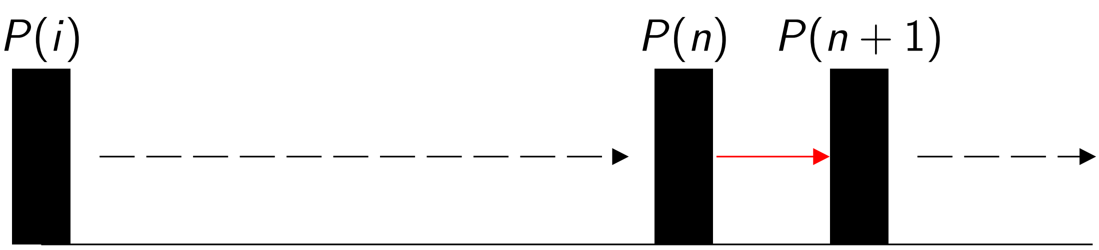
$$\frac{\dfrac{\text{Hypothesis} \quad \text{Negation of Conclusion}}{\perp}}{\text{Conclusion}}$$

Inductions on Natural Numbers

to prove assertion $P(n)$ for all n

- Base: show P for particular number i, usually $i = 0$ or $i = 1$.
- Step: show that if $P(n)$, then $P(n + 1)$.

Principle of Induction Suppose we can show $P(i)$ and can show that for all $n \geq i$, $P(n)$ implies $P(n + 1)$. Then we can conclude that $P(n)$ is true for all $n \geq i$.



Theorem If $n \geq 4$, then $2^n \geq n^2$.

- Base: $n = 4$ implies $2^n = n^2$.
- Step: we have to show: If $2^n \geq n^2$, then $2^{n+1} \geq (n+1)^2$. ($2^n \geq n^2$ induction hypothesis (IH)).

  first, we show $\quad 2n^2 \geq (n+1)^2 \quad (\dagger)$

  we simplify (subtract n^2)

  $$n^2 \geq 2n + 1 \ ,$$

  and simplify (divide by n)

  $$n \geq 2 + \frac{1}{n} \ .$$

  now by IH and ($\dagger$):

  $$2^{n+1} = 2 \cdot 2^n \geq 2 \cdot n^2 \geq (n+1)^2 \ .$$

$\square$

More General Forms of Induction on Numbers

course-value induction: to show $P(n+1)$, we may use the truth of

$$P(i), P(i+1), \ldots, P(n) \ .$$

another extension: use several base cases:

$$P(i), P(i+1), \ldots, P(j) \ .$$

several base cases and course-value induction: we may assume

$$P(i), P(i+1), \ldots, P(n) \ ,$$

to show the step-case $P(n+1)$. Moreover, we may

$$n \geq j \ ,$$

instead of $n \geq i$.

Principle of Structural Recursion

Definition recursive definition of trees

- Base: a single node is a tree; this node is called root.
- Step: if $T_1, T_2, \ldots, T_k$ are trees, form a new tree:
  1. start with new node N, the root
  2. take copies of the trees $T_1, T_2, \ldots, T_k$.
  3. add k edges from N to the roots of (the copies of) $T_1, T_2, \ldots, T_k$.

Definition recursive definition of expressions

- Base: each number, each letter is an expression.
- Step: if E, F are expressions, then $E + F$, $E \cdot F$, and (E) are expressions.

Principle of Structural Induction

Goal show $P(X)$ for all structures X, defined via a recursive definition.

Principle

- Base: show $P(X)$ for the the structures, constructed without premisses X.
- Step: for X, that is built recursively from $Y_1, Y_2, \ldots, Y_k$

  assume IH: $P(Y_1), P(Y_2), \ldots, P(Y_k)$

  show $P(X)$ based on IH.

Theorem Each tree contains exactly one more node than it has edges.

$S(T)$ expresses "If T is a tree and contains n nodes and e edges, then $n = e + 1$."

Proof

- Base: Obviously $n = e + 1$, if T consists of one node only.
- Step: Suppose T includes $T_1, \ldots, T_k$ as direct sub-trees.

  IH: $S(T_1), \ldots, S(T_k)$ holds

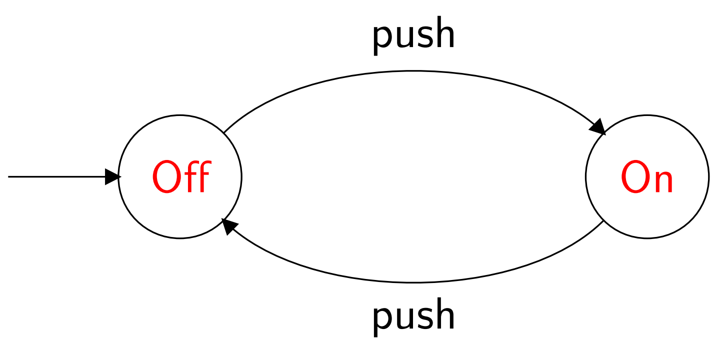
  Let $n_1, \ldots, n_k$ denote the number of nodes in $T_1, \ldots, T_k$; and $e_1, \ldots, e_k$ the number of edges in $T_1, \ldots, T_k$.

  By IH: for all $i \in [1, k]$: $n_i = e_i + 1$.

$$
\begin{aligned}
n &= 1 + n_1 + \cdots + n_k = \\
&= 1 + (e_1 + 1) + \cdots + (e_k + 1) \\
&= 1 + \underbrace{(e_1 + \cdots + e_k + k)}_{\text{number of edges in } T} .
\end{aligned}
$$

Deductive Proofs Reduction to Definitions Proof by Contradiction Inductive Proofs

on-off switch



Goal

show that the automata A is off after n pushes if and only if (iff) n is even, and is on after n pushes iff n is odd.

Mutual Inductions (on Numbers)

Challenge

the statements: A is off after n pushes iff n is even and A is is on after n pushes iff n is odd. are interdependent.

Mutual Induction

to prove a group of statements $P_1(n), \dots, P_k(n)$:

- keep the statements separate
- prove for all statements base and induction step separately.

For on-off switch, we show

- $P_1(n)$: The automata A is off after n pushes iff n is even.
- $P_2(n)$: The automata A is on after n pushes iff n is odd.

by using mutual induction.

- Base: we have to show ($P_1(0)$; if), ($P_1(0)$; only-if), ($P_2(0)$; if), ($P_2(0)$; only-if).

  case ($P_1(0)$; if): we have to show: A is off after 0 pushes, if 0 is even. trivial.

  case ($P_1(0)$; only-if): we have to show: A is off after 0 pushes, only-if 0 is even; that is A is off implies 0 is even, again trivial.

- Step: we have to show ($P_1(n+1)$; if), ($P_1(n+1)$; only-if), ($P_2(n+1)$; if), ($P_2(n+1)$; only-if).

  IH: $P_1(n)$ and $P_2(n)$.

  case ($P_1(n+1)$; only-if): we have to show: A off after $(n+1)$ pushes implies $n+1$ is even.

  assumption: A is off after $n+1$ pushes; hence A is on after n pushes, by IH: (($P_2(n)$; only-if), n is odd, hence $n+1$ is even.

  $\square$

Summary

1. Deductive Proofs
2. "If-then" and "if and only-if" Assertions
3. Reduction to Definitions
4. Proofs by Contradiction
5. Induction on Numbers
6. Structural Induction
7. Mutual Induction