CS3202: Logic, Specification and Verification

CS3202-LSV 2006–07

cs3202.lec@cs.st-andrews.ac.uk

Dr. James McKinna, RM 1.03

Dr. Stéphane Lengrand, Rm. 1.02

Lecture 5 (26-27/02/2007):

Predicate Logic

Poor old Socrates

- Socrates is a man
- All men are mortal
- Socrates is mortal

Poor old Socrates

- Socrates is a man: $H(S)$
- All men are mortal: $\forall m.H(m) \Rightarrow M(m)$
- Socrates is mortal: $M(S)$

Poor old Socrates

- Socrates is a man: $H(S)$
- All men are mortal: $\forall m. H(m) \Rightarrow M(m)$
- Socrates is mortal: $M(S)$

What do we need? In the language:

- *terms*, to denote objects of an (often implicit) universe of speech:

  Socrates, S

What do we need? In the language:

- *terms*, to denote objects of an (often implicit) universe of speech:

  Socrates, S

- *predicates*, to make statements about these objects:

  $m$is a man: $H(m)$

  Formally, these are *functions*, turning individual things into propositions

What do we need? In the language:

- *terms*, to denote objects of an (often implicit) universe of speech:

  Socrates, S

- *predicates*, to make statements about these objects:

  $m$is a man: $H(m)$

  Formally, these are *functions*, turning individual things into propositions

- *substitution*, to speak about a (more) particular instance:

  "$H(m)$ plus S equals $H(S)$"

  Trickier than you think!

What do we need? In the language:

- *terms*, to denote objects of an (often implicit) universe of speech:

  Socrates, S

- *predicates*, to make statements about these objects:

  $m$is a man: $H(m)$

  Formally, these are *functions*, turning individual things into propositions

- *substitution*, to speak about a (more) particular instance:

  "$H(m)$ plus S equals $H(S)$"

  Trickier than you think!

- *quantifiers*: "for all" $\forall$ and "there exists" $\exists$

What do we need? In the language:

- *terms*, to denote objects of an (often implicit) universe of speech:

  Socrates, S

- *predicates*, to make statements about these objects:

  $m$is a man: $H(m)$

  Formally, these are *functions*, turning individual things into propositions

- *substitution*, to speak about a (more) particular instance:

  "$H(m)$ plus S equals $H(S)$"

  Trickier than you think!

- *quantifiers*: "for all" $\forall$ and "there exists" $\exists$

  This extends the notion of wff.

What do we need? In the language:

- *terms*, to denote objects of an (often implicit) universe of speech:

  Socrates, S

- *predicates*, to make statements about these objects:

  $m$is a man: $H(m)$

  Formally, these are *functions*, turning individual things into propositions

- *substitution*, to speak about a (more) particular instance:

  “$H(m)$ plus S equals $H(S)$”

  Trickier than you think!

- *quantifiers*: “for all” $\forall$ and “there exists” $\exists$

  This extends the notion of wff.

What do we need? In the reasoning:

- *introduction* and *elimination* rules for $\forall$ and $\exists$

What do we need? In the reasoning:

- *introduction* and *elimination* rules for $\forall$ and $\exists$
  to prove or use wff of the form $\forall x, P(x)$ or $\exists x, P(x)$

What do we need? In the reasoning:

- *introduction* and *elimination* rules for $\forall$ and $\exists$
  to prove or use wff of the form $\forall x, P(x)$ or $\exists x, P(x)$

- ... lots of examples...

What do we need? In the reasoning:

- *introduction* and *elimination* rules for $\forall$ and $\exists$
  to prove or use wff of the form $\forall x, P(x)$ or $\exists x, P(x)$

- ...lots of examples...

Terms

- Well-bracketed expressions / trees,

  denoting “things in the current context” that we are allowed to talk about.

Terms

- Well-bracketed expressions / trees,

  denoting “things in the current context” that we are allowed to talk about.

- Leaves: (labelled with) *constants*

Terms

- Well-bracketed expressions / trees,

  denoting “things in the current context” that we are allowed to talk about.

- Leaves: (labelled with) *constants*

  or (free) *variables*, “things we don’t know about yet”

Terms

- Well-bracketed expressions / trees,

  denoting "things in the current context" that we are allowed to talk about.

- Leaves: (labelled with) *constants*

  or (free) *variables*, "things we don't know about yet"

  Example: Natural numbers, constants: $0, 1$, variables n, m as in

$$\forall n, n = 0 \vee (\exists m, n = m + 1)$$

Terms

- Well-bracketed expressions / trees,

  denoting “things in the current context” that we are allowed to talk about.

- Leaves: (labelled with) *constants*

  or (free) *variables*, “things we don’t know about yet”

  Example: Natural numbers, constants: $0, 1$, variables n, m as in

$$\forall n, n = 0 \vee (\exists m, n = m + 1)$$

- Internal nodes: (labelled with) *function symbols*

  which define the syntax of a grammar of terms. Example: $+$ above

Terms

- Well-bracketed expressions / trees,

  denoting "things in the current context" that we are allowed to talk about.

- Leaves: (labelled with) *constants*

  or (free) *variables*, "things we don't know about yet"

  Example: Natural numbers, constants: $0, 1$, variables n, m as in

$$\forall n, n = 0 \vee (\exists m, n = m + 1)$$

- Internal nodes: (labelled with) *function symbols*

  which define the syntax of a grammar of terms. Example: $+$ above

  As functions, they expect a certain number of arguments

  (=number of sub-trees), a.k.a. *arity*. Example: $+$ has arity 2

Terms

- Well-bracketed expressions / trees,

  denoting "things in the current context" that we are allowed to talk about.

- Leaves: (labelled with) *constants*

  or (free) *variables*, "things we don't know about yet"

  Example: Natural numbers, constants: $0, 1$, variables n, m as in

$$\forall n, n = 0 \vee (\exists m, n = m + 1)$$

- Internal nodes: (labelled with) *function symbols*

  which define the syntax of a grammar of terms. Example: $+$ above

  As functions, they expect a certain number of arguments

  (=number of sub-trees), a.k.a. *arity*. Example: $+$ has arity 2

Terms

- Which variables are allowed to appear in terms is *relative* to the current context.

Terms

- Which variables are allowed to appear in terms is *relative* to the current context.

  Example: in $m + 1$ above, m was introduced in the current context by the quantifier $\exists m$

Terms

- Which variables are allowed to appear in terms is *relative* to the current context.

  Example: in $m + 1$ above, m was introduced in the current context by the quantifier $\exists m$

- As usual, we represent term-trees as well-bracketed strings (a.k.a. expressions). Example: $(n + m) + n'$

Terms

- Which variables are allowed to appear in terms is *relative* to the current context.

  Example: in $m + 1$ above, m was introduced in the current context by the quantifier $\exists m$

- As usual, we represent term-trees as well-bracketed strings (a.k.a. expressions). Example: $(n + m) + n'$

- In general, we use x, y, z for variables, t, u, v for terms, f, g for function symbols

Terms

- Which variables are allowed to appear in terms is *relative* to the current context.

  Example: in $m + 1$ above, m was introduced in the current context by the quantifier $\exists m$

- As usual, we represent term-trees as well-bracketed strings (a.k.a. expressions). Example: $(n + m) + n'$

- In general, we use x, y, z for variables, t, u, v for terms, f, g for function symbols

Predicates

- . . . are just what you think (in COQ):
- functions from one type (the universe of speech) to `Prop` (the type of propositions)

  `MyUniverse ->` $\cdots$ `-> MyUniverse -> Prop`

Predicates

- ... are just what you think (in Coq):
- functions from one type (the universe of speech) to `Prop` (the type of propositions)

  `MyUniverse ->` $\cdots$ `-> MyUniverse -> Prop`

- Given a priori as a set of predicate symbols $p, q, r, \ldots$

  (similar to constants and function symbols for terms)

Predicates

- ... are just what you think (in Coq):
- functions from one type (the universe of speech) to `Prop` (the type of propositions)

  `MyUniverse ->` $\cdots$ `-> MyUniverse -> Prop`

- Given a priori as a set of predicate symbols $p, q, r, \ldots$

  (similar to constants and function symbols for terms)

- Again, *arity* = number of arguments (potentially 0!)

Predicates

- ...are just what you think (in COQ):
- functions from one type (the universe of speech) to `Prop` (the type of propositions)

  `MyUniverse -> ⋯ -> MyUniverse -> Prop`
- Given a priori as a set of predicate symbols $p, q, r, \ldots$

  (similar to constants and function symbols for terms)
- Again, *arity* = number of arguments (potentially 0!)
- Examples: from the one above, $=$ (arity 2), or in maths $\in$ (arity 2), with *infix* notation.

  When applied: $t = u$ and $t \in u$

Predicates

- ...are just what you think (in Coq):
- functions from one type (the universe of speech) to `Prop` (the type of propositions)

  `MyUniverse -> ··· -> MyUniverse -> Prop`

- Given a priori as a set of predicate symbols $p, q, r, \ldots$

  (similar to constants and function symbols for terms)

- Again, *arity* = number of arguments (potentially 0!)
- Examples: from the one above, $=$ (arity 2), or in maths $\in$ (arity 2), with *infix* notation.

  When applied: $t = u$ and $t \in u$

Extended WFF

- Well-bracketed expressions / trees,

Extended WFF

- Well-bracketed expressions / trees,

- Leaves: predicates applied to their arguments. Example: $n = 0$

Extended WFF

- Well-bracketed expressions / trees,
- Leaves: predicates applied to their arguments. Example: $n = 0$
- Internal nodes: logical connectives (as in propositional logic) $\wedge, \vee, \neg, \perp$

Extended WFF

- Well-bracketed expressions / trees,
- Leaves: predicates applied to their arguments. Example: $n = 0$
- Internal nodes: logical connectives (as in propositional logic) $\wedge, \vee, \neg, \bot$

  or *quantifiers+variable*, $\forall x$ (arity 1), $\exists x$ (arity 1)

Extended WFF

- Well-bracketed expressions / trees,
- Leaves: predicates applied to their arguments. Example: $n = 0$
- Internal nodes: logical connectives (as in propositional logic) $\wedge, \vee, \neg, \perp$

  or *quantifiers+variable*, $\forall x$ (arity 1), $\exists x$ (arity 1)

  x is *bound* by the quantifier.

  Its name is irrelevant: $\exists n, \neg(n = 0)$ *means the same* as $\exists m, \neg(m = 0)$

Extended WFF

- Well-bracketed expressions / trees,

- Leaves: predicates applied to their arguments. Example: $n = 0$

- Internal nodes: logical connectives (as in propositional logic) $\wedge, \vee, \neg, \perp$

  or *quantifiers+variable*, $\forall x$ (arity 1), $\exists x$ (arity 1)

  x is *bound* by the quantifier.

  Its name is irrelevant: $\exists n, \neg(n = 0)$ *means the same* as $\exists m, \neg(m = 0)$

- We consider wff up to / modulo *sound renaming of bound variables* (a.k.a. α*-equivalence*)

Extended WFF

- Well-bracketed expressions / trees,
- Leaves: predicates applied to their arguments. Example: $n = 0$
- Internal nodes: logical connectives (as in propositional logic) $\wedge, \vee, \neg, \perp$

  or *quantifiers+variable*, $\forall x$ (arity 1), $\exists x$ (arity 1)

  x is *bound* by the quantifier.

  Its name is irrelevant: $\exists n, \neg(n = 0)$ *means the same* as $\exists m, \neg(m = 0)$
- We consider wff up to / modulo *sound renaming of bound variables* (a.k.a. *α-equivalence*)

  Tricky. We want to avoid name clashes.

  Example: $\forall m, \exists n, \neg(n = m)$ is not the same as $\forall m, \exists m, \neg(m = m)$

Extended WFF

- Well-bracketed expressions / trees,
- Leaves: predicates applied to their arguments. Example: $n = 0$
- Internal nodes: logical connectives (as in propositional logic) $\wedge, \vee, \neg, \perp$

  or *quantifiers+variable*, $\forall x$ (arity 1), $\exists x$ (arity 1)

  x is *bound* by the quantifier.

  Its name is irrelevant: $\exists n, \neg(n = 0)$ *means the same* as $\exists m, \neg(m = 0)$
- We consider wff up to / modulo *sound renaming of bound variables* (a.k.a. *α-equivalence*)

  Tricky. We want to avoid name clashes.

  Example: $\forall m, \exists n, \neg(n = m)$ is not the same as $\forall m, \exists m, \neg(m = m)$

Substitution

- looks (usually) just what you think
- but beware!
- need to define what it is to be *free* and *bound* in an expression, formula, etc.
- FV$(\forall x : A.M) =$ FV$(M) \setminus \{x\}$
- lots of room to make mistakes. . . so go to the machine for assistance. . .
- Note: a variable can be substituted for a term which may refer to other variables (possibly *be* a variable). Example:

  $\forall m, \neg(n = 0)\{n \mapsto m + 1\}$ becomes $\forall m, \neg(m + 1 = 0)$

  In other words n is not (yet) substituted for a "value", i.e. a term without (free) variables (all leaves are constants).

Substitution

- *on terms*

$$
\begin{aligned}
x\{x \mapsto t\} &= t \\
y\{x \mapsto t\} &= y \\
f(u_1, \ldots, u_n)\{x \mapsto t\} &= f(u_1\{x \mapsto t\}, \ldots, u_n\{x \mapsto t\})
\end{aligned}
$$

on wff

$$
\begin{aligned}
(p(u_1, \ldots, u_n))\{x \mapsto t\} &= p(u_1\{x \mapsto t\}, \ldots, u_n\{x \mapsto t\}) \\
(A \wedge B)\{x \mapsto t\} &= (A\{x \mapsto t\}) \wedge (B\{x \mapsto t\}) \\
\ldots & \\
(\forall y, A)\{x \mapsto t\} &= \forall y, (A\{x \mapsto t\}) \qquad x \neq y,\ y \notin \mathit{FV}(t) \\
(\exists y, A)\{x \mapsto t\} &= \exists y, (A\{x \mapsto t\}) \qquad x \neq y,\ y \notin \mathit{FV}(t)
\end{aligned}
$$

Inference rules for $\forall$

- We extend Natural Deduction with the following rules:

Inference rules for $\forall$

- We extend Natural Deduction with the following rules:

  $\forall$-introduction:

$$\frac{A}{\forall x, A}\; x \notin \mathsf{FV}(\text{open leaves})$$

Inference rules for $\forall$

- We extend Natural Deduction with the following rules:

  $\forall$-introduction:

$$\frac{A}{\forall x, A}\, x \notin \text{FV}(\text{open leaves})$$

  $\forall$-elimination:

$$\frac{\forall x, A}{A\{x = t\}}$$

Inference rules for $\forall$

- We extend Natural Deduction with the following rules:

  $\forall$-introduction:

$$\frac{A}{\forall x, A}\; x \notin \text{FV}(\text{open leaves})$$

  $\forall$-elimination:

$$\frac{\forall x, A}{A\{x = t\}}$$

Inference rules for $\exists$

- $\exists$-introduction:

$$\frac{A\{x = t\}}{\exists x, A}$$

Inference rules for $\exists$

- $\exists$-introduction:

$$\frac{A\{x = t\}}{\exists x, A}$$

$\exists$-elimination:

$$\frac{\exists x, A \qquad \begin{array}{c}[A] \\ \vdots \\ C\end{array}}{C}\ x \notin \text{FV}(C) \cup \text{FV}(\text{open leaves})$$

Inference rules for $\exists$

- $\exists$-introduction:

$$\frac{A\{x = t\}}{\exists x, A}$$

$\exists$-elimination:

$$\frac{\exists x, A \qquad \begin{array}{c} [A] \\ \vdots \\ C \end{array}}{C} \; x \notin \text{FV}(C) \cup \text{FV}(\text{open leaves})$$

Intuition about $\exists$-elim: an alternative?

- Standard $\exists$-elimination:

$$\frac{\exists x, A \qquad \begin{array}{c}[A] \\ \vdots \\ C\end{array}}{C}\; x \notin \mathsf{FV}(C) \cup \mathsf{FV}(\text{open leaves})$$

Intuition about $\exists$-elim: an alternative?

- Standard $\exists$-elimination:

$$\dfrac{\exists x, A \qquad \begin{matrix}[A] \\ \vdots \\ C\end{matrix}}{C}\; x \notin \text{FV}(C) \cup \text{FV}(\text{open leaves})$$

Intuition: $\exists$-elimination:

$$\begin{matrix}A \\ \vdots \\ C\end{matrix} \qquad \text{becomes} \qquad \begin{matrix}\dfrac{\exists x, A}{A} \\ \vdots \\ \dfrac{C}{C}\; x \notin \text{FV}(C) \cup \text{FV}(\text{open leaves})\end{matrix}$$

Intuition about $\exists$-elim: an alternative?

- Standard $\exists$-elimination:

$$\frac{\exists x, A \qquad \begin{array}{c}[A] \\ \vdots \\ C\end{array}}{C}\, x \notin \text{FV}(C) \cup \text{FV}(\text{open leaves})$$

Intuition: $\exists$-elimination:

$$\begin{array}{c} A \\ \vdots \\ C \end{array} \qquad \text{becomes} \qquad \begin{array}{c} \dfrac{\exists x, A}{A} \\ \vdots \\ \dfrac{C}{C}\, x \notin \text{FV}(C) \cup \text{FV}(\text{open leaves}) \end{array}$$

Use of the side-condition

- Writing $P(x)$ for a wff A depending on x,

$$\frac{P(x)}{\forall x, P(x)}$$

is a proof for $P(x) \vdash \forall x, P(x)$

Use of the side-condition

- Writing $P(x)$ for a wff A depending on x,

$$\frac{P(x)}{\forall x, P(x)}$$

is a proof for $P(x) \vdash \forall x, P(x)$ *WRONG!*

Use of the side-condition

- Writing $P(x)$ for a wff A depending on x,

$$\frac{P(x)}{\forall x, P(x)}$$

is a proof for $P(x) \vdash \forall x, P(x)$ *WRONG!*

- Worse:

$$\frac{\exists x, P(x) \qquad \dfrac{[P(x)]}{P(x)}}{\dfrac{P(x)}{\forall x, P(x)}}$$

is a proof for $\exists x, P(x) \vdash \forall x, P(x)$

Use of the side-condition

- Writing $P(x)$ for a wff A depending on x,

$$\frac{P(x)}{\forall x, P(x)}$$

is a proof for $P(x) \vdash \forall x, P(x)$ *WRONG!*

- Worse:

$$\frac{\dfrac{\exists x, P(x) \qquad \dfrac{[P(x)]}{P(x)}}{P(x)}}{\forall x, P(x)}$$

is a proof for $\exists x, P(x) \vdash \forall x, P(x)$ *WRONG!*

Use of the side-condition

- Writing $P(x)$ for a wff A depending on x,

$$\frac{P(x)}{\forall x, P(x)}$$

is a proof for $P(x) \vdash \forall x, P(x)$ *WRONG!*

- Worse:

$$\frac{\exists x, P(x) \qquad \dfrac{[P(x)]}{P(x)}}{\dfrac{P(x)}{\forall x, P(x)}}$$

is a proof for $\exists x, P(x) \vdash \forall x, P(x)$ *WRONG!*

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

  Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\rule{12em}{0pt} \qquad \rule{6em}{0pt}}{\rule{18em}{0pt}}}{\rule{5em}{0pt}}}{}}{(\forall y, p(y)) \Rightarrow \forall z, q(z)}$$

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

  Proof:

$$\frac{\overline{\forall z, q(z)}}{(\forall y, p(y)) \Rightarrow \forall z, q(z)}$$

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

  Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\qquad\qquad\qquad} \qquad \dfrac{}{\qquad\quad}}{q(z)}}{\forall z, q(z)}}{\color{red}{(\forall y, p(y)) \Rightarrow}\forall z, q(z)}$$

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

  Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{p(z) \Rightarrow q(z)} \qquad \dfrac{}{p(z)}}{q(z)}}{\forall z, q(z)}}{\color{red}{(\forall y, p(y)) \Rightarrow}\forall z, q(z)}$$

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

  Proof:

$$
\dfrac{\dfrac{\dfrac{\dfrac{\forall x, (p(x) \Rightarrow q(x))}{p(z) \Rightarrow q(z)} \qquad \dfrac{}{p(z)}}{q(z)}}{\forall z, q(z)}}{\color{red}{(\forall y, p(y)) \Rightarrow}\color{black}{\forall z, q(z)}}
$$

since $p(z) \Rightarrow q(z)$ is $(p(x) \Rightarrow q(x))\{x \mapsto z\}$

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

  Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x, (p(x) \Rightarrow q(x))}{p(z) \Rightarrow q(z)} \qquad \dfrac{[\forall y, p(y)]}{p(z)}}{q(z)}}{\forall z, q(z)}}{(\forall y, p(y)) \Rightarrow \forall z, q(z)}$$

  since $p(z) \Rightarrow q(z)$ is $(p(x) \Rightarrow q(x))\{x \mapsto z\}$

  and $p(z)$ is $(p(y))\{y \mapsto z\}$

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

  Proof:

$$
\dfrac{\dfrac{\dfrac{\forall x, (p(x) \Rightarrow q(x))}{p(z) \Rightarrow q(z)} \qquad \dfrac{[\forall y, p(y)]}{p(z)}}{\dfrac{q(z)}{\forall z, q(z)}\star}}{(\forall y, p(y)) \Rightarrow \forall z, q(z)}
$$

  since $p(z) \Rightarrow q(z)$ is $(p(x) \Rightarrow q(x))\{x \mapsto z\}$

  and $p(z)$ is $(p(y))\{y \mapsto z\}$

  Note that the step $\star$ is correct because

  $z \notin \mathsf{FV}(\forall x, (p(x) \Rightarrow q(x))) \cup \mathsf{FV}(\forall y, p(y))$

Example of theorem

- $\forall x, (p(x) \Rightarrow q(x)) \vdash (\forall y, p(y)) \Rightarrow \forall z, q(z)$

  Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{\forall x, (p(x) \Rightarrow q(x))}{p(z) \Rightarrow q(z)} \qquad \dfrac{[\forall y, p(y)]}{p(z)}}{q(z)}}{\forall z, q(z)}\star}{(\forall y, p(y)) \Rightarrow \forall z, q(z)}$$

  since $p(z) \Rightarrow q(z)$ is $(p(x) \Rightarrow q(x))\{x \mapsto z\}$

  and $p(z)$ is $(p(y))\{y \mapsto z\}$

  Note that the step $\star$ is correct because

  $z \notin \mathsf{FV}(\forall x, (p(x) \Rightarrow q(x))) \cup \mathsf{FV}(\forall y, p(y))$

Example of theorem

- $\exists x, (p(x) \vee q(x)) \vdash (\exists y, p(y)) \vee (\exists z, q(z))$

Example of theorem

- $\exists x, (p(x) \vee q(x)) \vdash (\exists y, p(y)) \vee (\exists z, q(z))$

  Proof:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{} \qquad \dfrac{}{}}{\qquad}}{\qquad}}{(\exists y, p(y)) \vee (\exists z, q(z))}$$

Example of theorem

- $\exists x, (p(x) \vee q(x)) \vdash (\exists y, p(y)) \vee (\exists z, q(z))$

  Proof:

$$\dfrac{\exists x, p(x) \vee q(x) \qquad \dfrac{\dfrac{\dfrac{}{}}{} \qquad \dfrac{\dfrac{}{}}{}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}$$

Example of theorem

- $\exists x, (p(x) \lor q(x)) \vdash (\exists y, p(y)) \lor (\exists z, q(z))$

  Proof:

$$\dfrac{\exists x, p(x) \lor q(x) \qquad \dfrac{[p(x) \lor q(x)] \qquad \dfrac{\dfrac{\quad}{\quad}}{(\exists y, p(y)) \lor (\exists z, q(z))} \qquad \dfrac{\dfrac{\quad}{\quad}}{(\exists y, p(y)) \lor (\exists z, q(z))}}{(\exists y, p(y)) \lor (\exists z, q(z))}}{(\exists y, p(y)) \lor (\exists z, q(z))}$$

Example of theorem

- $\exists x, (p(x) \vee q(x)) \vdash (\exists y, p(y)) \vee (\exists z, q(z))$

  Proof:

$$\dfrac{\exists x, p(x) \vee q(x) \qquad \dfrac{[p(x) \vee q(x)] \qquad \dfrac{\dfrac{\qquad}{\exists y, p(y)}}{(\exists y, p(y)) \vee (\exists z, q(z))} \qquad \dfrac{\dfrac{\qquad}{\qquad}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}$$

Example of theorem

- $\exists x, (p(x) \vee q(x)) \vdash (\exists y, p(y)) \vee (\exists z, q(z))$

  Proof:

$$
\dfrac{\exists x, p(x) \vee q(x) \qquad \dfrac{[p(x) \vee q(x)] \qquad \dfrac{\dfrac{[p(x)]}{\exists y, p(y)}}{(\exists y, p(y)) \vee (\exists z, q(z))} \qquad \dfrac{\dfrac{}{}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}
$$

since $p(x)$ is $(p(y))\{y \mapsto x\}$

Example of theorem

- $\exists x, (p(x) \vee q(x)) \vdash (\exists y, p(y)) \vee (\exists z, q(z))$

  Proof:

$$\dfrac{\exists x, p(x) \vee q(x) \qquad \dfrac{[p(x) \vee q(x)] \qquad \dfrac{\dfrac{[p(x)]}{\exists y, p(y)}}{(\exists y, p(y)) \vee (\exists z, q(z))} \qquad \dfrac{\dfrac{}{\exists z, q(z)}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}$$

  since $p(x)$ is $(p(y))\{y \mapsto x\}$

Example of theorem

- $\exists x, (p(x) \vee q(x)) \vdash (\exists y, p(y)) \vee (\exists z, q(z))$

  Proof:

$$\dfrac{\exists x, p(x) \vee q(x) \qquad \dfrac{[p(x) \vee q(x)] \qquad \dfrac{\dfrac{[p(x)]}{\exists y, p(y)}}{(\exists y, p(y)) \vee (\exists z, q(z))} \qquad \dfrac{\dfrac{[q(x)]}{\exists z, q(z)}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}$$

  since $p(x)$ is $(p(y))\{y \mapsto x\}$ and $q(x)$ is $(q(z))\{z \mapsto x\}$

Example of theorem

- $\exists x, (p(x) \vee q(x)) \vdash (\exists y, p(y)) \vee (\exists z, q(z))$

  Proof:

$$
\dfrac{\exists x, p(x) \vee q(x) \qquad \dfrac{[p(x) \vee q(x)] \qquad \dfrac{\dfrac{[p(x)]}{\exists y, p(y)}}{(\exists y, p(y)) \vee (\exists z, q(z))} \qquad \dfrac{\dfrac{[q(x)]}{\exists z, q(z)}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))}}{(\exists y, p(y)) \vee (\exists z, q(z))} \star
$$

since $p(x)$ is $(p(y))\{y \mapsto x\}$ and $q(x)$ is $(q(z))\{z \mapsto x\}$

Note that the step $\star$ is correct because

$x \notin$ FV$((\exists y, p(y)) \vee (\exists z, q(z)))$ and at that point there is no open assumption

Example of theorem

- $\exists x, (p(x) \lor q(x)) \vdash (\exists y, p(y)) \lor (\exists z, q(z))$

  Proof:

$$\dfrac{\exists x, p(x) \lor q(x) \qquad \dfrac{[p(x) \lor q(x)] \qquad \dfrac{\dfrac{[p(x)]}{\exists y, p(y)}}{(\exists y, p(y)) \lor (\exists z, q(z))} \qquad \dfrac{\dfrac{[q(x)]}{\exists z, q(z)}}{(\exists y, p(y)) \lor (\exists z, q(z))}}{(\exists y, p(y)) \lor (\exists z, q(z))}}{(\exists y, p(y)) \lor (\exists z, q(z))}\star$$

  since $p(x)$ is $(p(y))\{y \mapsto x\}$ and $q(x)$ is $(q(z))\{z \mapsto x\}$

  Note that the step $\star$ is correct because

  $x \notin \mathsf{FV}((\exists y, p(y)) \lor (\exists z, q(z)))$ and at that point there is no open assumption

Example of theorem

- $(\exists y, p(y)) \vee (\exists z, q(z)) \vdash \exists x, (p(x) \vee q(x))$

Example of theorem

- $(\exists y, p(y)) \vee (\exists z, q(z)) \vdash \exists x, (p(x) \vee q(x))$

  Proof:

$$\frac{}{\exists x, (p(x) \vee q(x))}$$

Example of theorem

- $(\exists y, p(y)) \lor (\exists z, q(z)) \vdash \exists x, (p(x) \lor q(x))$

  Proof:

$$\dfrac{(\exists y, p(y)) \lor (\exists z, q(z)) \qquad \exists x, (p(x) \lor q(x)) \qquad \exists x, (p(x) \lor q(x))}{\exists x, (p(x) \lor q(x))}$$

Example of theorem

- $(\exists y, p(y)) \vee (\exists z, q(z)) \vdash \exists x, (p(x) \vee q(x))$

  Proof:

$$\dfrac{(\exists y, p(y)) \vee (\exists z, q(z)) \qquad \dfrac{[\exists y, p(y)] \quad \dfrac{\dfrac{}{}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))} \qquad \dfrac{\dfrac{\dfrac{}{}}{}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))}$$

Example of theorem

- $(\exists y, p(y)) \vee (\exists z, q(z)) \vdash \exists x, (p(x) \vee q(x))$

  Proof:

$$\dfrac{(\exists y, p(y)) \vee (\exists z, q(z)) \qquad \dfrac{[\exists y, p(y)] \qquad \dfrac{\dfrac{[p(y)]}{p(y) \vee q(y)}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))} \qquad \dfrac{\dfrac{\dfrac{}{}}{}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))}$$

  since $p(y) \vee q(y)$ is $(p(x) \vee q(x))\{x \mapsto y\}$

Example of theorem

- $(\exists y, p(y)) \lor (\exists z, q(z)) \vdash \exists x, (p(x) \lor q(x))$

  Proof:

$$\dfrac{(\exists y, p(y)) \lor (\exists z, q(z)) \qquad \dfrac{[\exists y, p(y)] \quad \dfrac{\dfrac{[p(y)]}{p(y) \lor q(y)}}{\exists x, (p(x) \lor q(x))}}{\exists x, (p(x) \lor q(x))} \qquad \dfrac{[\exists z, q(z)] \quad \dfrac{\dfrac{\qquad}{\qquad}}{\qquad}}{\exists x, (p(x) \lor q(x))}}{\exists x, (p(x) \lor q(x))}$$

  since $p(y) \lor q(y)$ is $(p(x) \lor q(x))\{x \mapsto y\}$

Example of theorem

- $(\exists y, p(y)) \vee (\exists z, q(z)) \vdash \exists x, (p(x) \vee q(x))$

  Proof:

$$\dfrac{(\exists y, p(y)) \vee (\exists z, q(z)) \qquad \dfrac{[\exists y, p(y)] \quad \dfrac{\dfrac{[p(y)]}{p(y) \vee q(y)}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))} \qquad \dfrac{[\exists z, q(z)] \quad \dfrac{\dfrac{}{\qquad}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))}$$

  since $p(y) \vee q(y)$ is $(p(x) \vee q(x))\{x \mapsto y\}$

Example of theorem

- $(\exists y, p(y)) \lor (\exists z, q(z)) \vdash \exists x, (p(x) \lor q(x))$

  Proof:

$$
\dfrac{(\exists y, p(y)) \lor (\exists z, q(z)) \qquad \dfrac{[\exists y, p(y)] \quad \dfrac{\dfrac{[p(y)]}{p(y) \lor q(y)}}{\exists x, (p(x) \lor q(x))}}{\exists x, (p(x) \lor q(x))} \qquad \dfrac{[\exists z, q(z)] \quad \dfrac{\dfrac{[q(z)]}{p(z) \lor q(z)}}{\exists x, (p(x) \lor q(x))}}{\exists x, (p(x) \lor q(x))}}{\exists x, (p(x) \lor q(x))}
$$

  since $p(y) \lor q(y)$ is $(p(x) \lor q(x))\{x \mapsto y\}$

  and $p(z) \lor q(z)$ is $(p(x) \lor q(x))\{x \mapsto z\}$

Example of theorem

- $(\exists y, p(y)) \vee (\exists z, q(z)) \vdash \exists x, (p(x) \vee q(x))$

  Proof:

$$
\dfrac{(\exists y, p(y)) \vee (\exists z, q(z)) \qquad \dfrac{[\exists y, p(y)] \qquad \dfrac{\dfrac{[p(y)]}{p(y) \vee q(y)}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))} \qquad \dfrac{[\exists z, q(z)] \qquad \dfrac{\dfrac{[q(z)]}{p(z) \vee q(z)}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))} \star
$$

  since $p(y) \vee q(y)$ is $(p(x) \vee q(x))\{x \mapsto y\}$

  and $p(z) \vee q(z)$ is $(p(x) \vee q(x))\{x \mapsto z\}$

  Again, the two $\exists$-elim are correct: the bound variable y (resp. z) is not free in the conclusion $\exists x, (p(x) \vee q(x))$ & no open assumption

Example of theorem

- $(\exists y, p(y)) \vee (\exists z, q(z)) \vdash \exists x, (p(x) \vee q(x))$

  Proof:

$$
\dfrac{(\exists y, p(y)) \vee (\exists z, q(z)) \quad \dfrac{[\exists y, p(y)] \quad \dfrac{\dfrac{[p(y)]}{p(y) \vee q(y)}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))} \quad \dfrac{[\exists z, q(z)] \quad \dfrac{\dfrac{[q(z)]}{p(z) \vee q(z)}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))}}{\exists x, (p(x) \vee q(x))} \star
$$

  since $p(y) \vee q(y)$ is $(p(x) \vee q(x))\{x \mapsto y\}$

  and $p(z) \vee q(z)$ is $(p(x) \vee q(x))\{x \mapsto z\}$

  Again, the two $\exists$-elim are correct: the bound variable y (resp. z) is not free in the conclusion $\exists x, (p(x) \vee q(x))$ & no open assumption

Questions?