Mathematical and Logical Foundations of Computer Science

Predicate Logic (Equivalences continued)

Vincent Rahli

(some slides were adapted from Rajesh Chitnis' slides)

University of Birmingham

Where are we?

- Symbolic logic
- Propositional logic
- **Predicate logic**
- Intuitionistic vs. Classical logic
- Type theory

Today

Equivalences:

- in Natural Deduction
- in the Sequent Calculus
- rewriting using “known” equivalences
- using semantics

Further reading:

- Chapter 8 of
  http://leanprover.github.io/logic_and_proof/

Recap: Syntax

The syntax of predicate logic is defined by the following grammar:

$$\begin{array}{lcl} t & ::= & x \mid f(t, \ldots, t) \\ P & ::= & p(t, \ldots, t) \mid \neg P \mid P \wedge P \mid P \vee P \mid P \rightarrow P \mid \forall x.P \mid \exists x.P \end{array}$$

where:

- x ranges over variables
- f ranges over function symbols
- $f(t_1, \ldots, t_n)$ is a well-formed term only if f has arity n
- p ranges over predicate symbols
- $p(t_1, \ldots, t_n)$ is a well-formed formula only if p has arity n

The pair of a collection of function symbols, and a collection of predicate symbols, along with their arities, is called a **signature**.

The scope of a quantifier extends as far right as possible. E.g., $P \wedge \forall x.p(x) \vee q(x)$ is read as $P \wedge \forall x.(p(x) \vee q(x))$

Recap: Substitution

Substitution is defined recursively on terms and formulas:

$P[x\backslash t]$ substitute all the free occurrences of x in P with t.

$$
\begin{array}{lcl}
x[x\backslash t] & = & t \\
x[y\backslash t] & = & x \\
(f(t_1,\ldots,t_n))[x\backslash t] & = & f(t_1[x\backslash t],\ldots,t_n[x\backslash t]) \\
(p(t_1,\ldots,t_n))[x\backslash t] & = & p(t_1[x\backslash t],\ldots,t_n[x\backslash t]) \\
\hline
(\neg P)[x\backslash t] & = & \neg P[x\backslash t] \\
(P_1 \wedge P_2)[x\backslash t] & = & P_1[x\backslash t] \wedge P_2[x\backslash t] \\
(P_1 \vee P_2)[x\backslash t] & = & P_1[x\backslash t] \vee P_2[x\backslash t] \\
(P_1 \rightarrow P_2)[x\backslash t] & = & P_1[x\backslash t] \rightarrow P_2[x\backslash t] \\
\hline
(\forall x.P)[x\backslash t] & = & \forall x.P \\
(\exists x.P)[x\backslash t] & = & \exists x.P \\
(\forall y.P)[x\backslash t] & = & \forall y.P[x\backslash t], \text{ if } y \notin \mathtt{fv}(t) \\
(\exists y.P)[x\backslash t] & = & \exists y.P[x\backslash t], \text{ if } y \notin \mathtt{fv}(t)
\end{array}
$$

The additional **conditions** ensure that **free variables do not get captured**.

These conditions can always be met by silently renaming bound variables before substituting.

Recap: $\forall$ & $\exists$ elimination and introduction rules

Natural Deduction rules for quantifiers:

$$\frac{P[x\backslash y]}{\forall x.P}\ [\forall I] \qquad \frac{\forall x.P}{P[x\backslash t]}\ [\forall E] \qquad \frac{P[x\backslash t]}{\exists x.P}\ [\exists I] \qquad \frac{\exists x.P \qquad \begin{matrix}\overline{P[x\backslash y]}^{\,1} \\ \vdots \\ Q\end{matrix}}{Q}\ 1\ [\exists E]$$

Condition:

- for $[\forall I]$: y must not be free in any not-yet-discharged hypothesis or in $\forall x.P$
- for $[\forall E]$: $\mathtt{fv}(t)$ must not clash with $\mathtt{bv}(P)$
- for $[\exists I]$: $\mathtt{fv}(t)$ must not clash with $\mathtt{bv}(P)$
- for $[\exists E]$: y must not be free in Q or in not-yet-discharged hypotheses or in $\exists x.P$

Recap: ∀ & ∃ left and right rules

Sequent Calculus rules for quantifiers:

$$\frac{\Gamma \vdash P[x\backslash y]}{\Gamma \vdash \forall x.P}\ [\forall R] \qquad \frac{\Gamma, P[x\backslash t] \vdash Q}{\Gamma, \forall x.P \vdash Q}\ [\forall L]$$

$$\frac{\Gamma \vdash P[x\backslash t]}{\Gamma \vdash \exists x.P}\ [\exists R] \qquad \frac{\Gamma, P[x\backslash y] \vdash Q}{\Gamma, \exists x.P \vdash Q}\ [\exists L]$$

Conditions:

- for $[\forall R]$: y must not be free in Γ or $\forall x.P$
- for $[\forall L]$: $\mathtt{fv}(t)$ must not clash with $\mathtt{bv}(P)$
- for $[\exists R]$: $\mathtt{fv}(t)$ must not clash with $\mathtt{bv}(P)$
- for $[\exists L]$: y must not be free in Γ, Q, or $\exists x.P$

Recap: Models

Models: a model provides the interpretation of all symbols

Given a **signature** $\langle\langle f_1^{k_1}, \ldots, f_n^{k_n}\rangle, \langle p_1^{j_1}, \ldots, p_m^{j_m}\rangle\rangle$

- of function symbols f_i of arity k_i, for $1 \leqslant i \leqslant n$
- of predicate symbols p_i of arity j_i, for $1 \leqslant i \leqslant m$

a **model** is a structure $\langle D, \langle \mathcal{F}_{f_1}, \ldots, \mathcal{F}_{f_n}\rangle, \langle \mathcal{R}_{p_1}, \ldots, \mathcal{R}_{p_m}\rangle\rangle$

- of a non-empty domain D
- interpretations $\mathcal{F}_{f_i}$ for function symbols f_i
- interpretations $\mathcal{R}_{p_i}$ for function symbols p_i

Models of predicate logic replace **truth assignments** for propositional logic

Variable valuations:

- a partial function v
- that map variables to D
- i.e., a mapping of the form $x_1 \mapsto d_1, \ldots, x_n \mapsto d_n$

Recap: Semantics of Predicate Logic

Given a **model** M with domain D and a **variable valuation** v:

- $[\![t]\!]^M_v$ gives meaning to the term t w.r.t. M and v
- $\models_{M,v} P$ gives meaning to the formula P w.r.t. M and v

Meaning of terms:

- $[\![x]\!]^M_v = v(x)$
- $[\![f(t_1, \ldots, t_n)]\!]^M_v = \mathcal{F}_f(\langle [\![t_1]\!]^M_v, \ldots, [\![t_n]\!]^M_v \rangle)$

Meaning of formulas:

- $\models_{M,v} p(t_1, \ldots, t_n)$ iff $\langle [\![t_1]\!]^M_v, \ldots, [\![t_n]\!]^M_v \rangle \in \mathcal{R}_p$
- $\models_{M,v} \neg P$ iff $\neg \models_{M,v} P$
- $\models_{M,v} P \land Q$ iff $\models_{M,v} P$ and $\models_{M,v} Q$
- $\models_{M,v} P \lor Q$ iff $\models_{M,v} P$ or $\models_{M,v} Q$
- $\models_{M,v} P \to Q$ iff $\models_{M,v} Q$ whenever $\models_{M,v} P$
- $\models_{M,v} \forall x.P$ iff for every $d \in D$ we have $\models_{M,(v,x\mapsto d)} P$
- $\models_{M,v} \exists x.P$ iff there exists a $d \in D$ such that $\models_{M,(v,x\mapsto d)} P$

Recap: Logical equivalences for Propositional Logic

The same equivalences hold as in Propositional Logic:

- De Morgan's law (I): $\neg(A \vee B) \leftrightarrow (\neg A \wedge \neg B)$
- De Morgan's law (II): $\neg(A \wedge B) \leftrightarrow (\neg A \vee \neg B)$
- Implication elimination: $(A \rightarrow B) \leftrightarrow (\neg A \vee B)$
- Commutativity of $\wedge$: $(A \wedge B) \leftrightarrow (B \wedge A)$
- Commutativity of $\vee$: $(A \vee B) \leftrightarrow (B \vee A)$
- Associativity of $\wedge$: $((A \wedge B) \wedge C) \leftrightarrow (A \wedge (B \wedge C))$
- Associativity of $\vee$: $((A \vee B) \vee C) \leftrightarrow (A \vee (B \vee C))$
- Distributivity of $\wedge$ over $\vee$: $(A \wedge (B \vee C)) \leftrightarrow ((A \wedge B) \vee (A \wedge C))$
- Distributivity of $\vee$ over $\wedge$: $(A \vee (B \wedge C)) \leftrightarrow ((A \vee B) \wedge (A \vee C))$
- Double negation elimination: $(\neg\neg A) \leftrightarrow A$
- Idempotence: $(A \wedge A) \leftrightarrow A$ and $(A \vee A) \leftrightarrow A$

Recap: Logical Equivalences

In addition, the following hold (some hold only classically):

- $(\forall x.A \land B) \leftrightarrow ((\forall x.A) \land (\forall x.B))$
- $(\exists x.A \lor B) \leftrightarrow ((\exists x.A) \lor (\exists x.B))$
- $(\neg\forall x.A) \leftrightarrow (\exists x.\neg A)$
- $(\neg\exists x.A) \leftrightarrow (\forall x.\neg A)$
- $(\forall x.A) \leftrightarrow A$ if $x \notin \texttt{fv}(A)$
- $(\exists x.A) \leftrightarrow A$ if $x \notin \texttt{fv}(A)$
- $(\forall x.A \lor B) \leftrightarrow ((\forall x.A) \lor B)$ if $x \notin \texttt{fv}(B)$
- $(\exists x.A \land B) \leftrightarrow ((\exists x.A) \land B)$ if $x \notin \texttt{fv}(B)$
- $(\forall x.A \rightarrow B) \leftrightarrow ((\exists x.A) \rightarrow B)$ if $x \notin \texttt{fv}(B)$
- $(\exists x.A \rightarrow B) \leftrightarrow ((\forall x.A) \rightarrow B)$ if $x \notin \texttt{fv}(B)$
- $(\forall x.A \rightarrow B) \leftrightarrow (A \rightarrow \forall x.B)$ if $x \notin \texttt{fv}(A)$
- $(\exists x.A \rightarrow B) \leftrightarrow (A \rightarrow \exists x.B)$ if $x \notin \texttt{fv}(A)$

Recap: Logical Equivalences

As before: if ($P \leftrightarrow Q$ or $Q \leftrightarrow P$) and P occurs in A, then replacing P by Q in A leads to a formula B, such that $A \leftrightarrow B$

Also,

Semantical equivalence: two formulas P and Q are equivalent if for all models M and valuations v, $\models_{M,v} P$ iff $\models_{M,v} Q$

Logical Equivalences

As before to prove a logical equivalence $A \leftrightarrow B$, we will prove:

- that we can derive B form A
- that we can derive A form B

We will start by proving:

- $(\forall x.A) \leftrightarrow A$ if $x \notin \texttt{fv}(A)$
- $(\exists x.A) \leftrightarrow A$ if $x \notin \texttt{fv}(A)$
- $(\forall x.A \vee B) \leftrightarrow ((\forall x.A) \vee B)$ if $x \notin \texttt{fv}(B)$
- $(\exists x.A \wedge B) \leftrightarrow ((\exists x.A) \wedge B)$ if $x \notin \texttt{fv}(B)$

We will use the following result:

Lemma (L1): if $x \notin \texttt{fv}(A)$ then $A[x \backslash t] = A$

Logical Equivalences

Prove $(\forall x.A) \leftrightarrow A$ if $x \notin \mathtt{fv}(A)$ in Natural Deduction

Here is a proof of the right-to-left implication (constructive):

$$\dfrac{A[x\backslash y]A}{\forall x.A}\ [\forall I]$$

- pick y such that it does not occur in A
- by L1, because $x \notin \mathtt{fv}(A)$ then $A[x\backslash y] = A$

Here is a proof of the left-to-right implication (constructive):

$$\dfrac{\forall x.A}{AA[x\backslash y]}\ [\forall E]$$

- by L1, because $x \notin \mathtt{fv}(A)$ then $A[x\backslash y] = A$
- pick y such that it does not occur in A

Logical Equivalences

Prove $(\exists x.A) \leftrightarrow A$ if $x \notin \texttt{fv}(A)$ in Natural Deduction

Here is a proof of the right-to-left implication (constructive):

$$\dfrac{A[x\backslash y]A}{\exists x.A}\ [\exists I]$$

- pick y such that it does not occur in A
- by L1, because $x \notin \texttt{fv}(A)$ then $A[x\backslash y] = A$

Here is a proof of the left-to-right implication (constructive):

$$\dfrac{\exists x.A \quad A\overline{A[x\backslash y]}^{\,1}}{A}\ 1\ [\exists E]$$

- by L1, because $x \notin \texttt{fv}(A)$ then $A[x\backslash y] = A$
- pick y such that it does not occur in A

Logical Equivalences

Prove that $(\forall x.A \vee B) \leftrightarrow ((\forall x.A) \vee B)$ if $x \notin \mathtt{fv}(B)$ in the Sequent Calculus

Here is a proof of the left-to-right implication (classical):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A[x\backslash y] \vdash A[x\backslash y]}[Id] \quad \dfrac{}{B[x\backslash y] \vdash B B \vdash B}[Id]}{A[x\backslash y] \vee B[x\backslash y] \vdash A[x\backslash y], B}[\vee L]}{\forall x.A \vee B \vdash A[x\backslash y], B}[\forall L]}{\forall x.A \vee B \vdash (\forall x.A), B}[\forall R]}{\forall x.A \vee B \vdash (\forall x.A) \vee B}[\vee R]$$

- pick y such that it does not occur in A or B
- by L1, because $x \notin \mathtt{fv}(B)$ then $B[x\backslash y] = B$

Logical Equivalences

Prove that $(\forall x.A \vee B) \leftrightarrow ((\forall x.A) \vee B)$ if $x \notin \mathtt{fv}(B)$ in the Sequent Calculus

Here is a proof of the right-to-left implication (constructive):

$$
\dfrac{
\dfrac{
\dfrac{
\dfrac{}{A[x\backslash y] \vdash A[x\backslash y]}\;[Id]
}{\forall x.A \vdash A[x\backslash y]}\;[\forall L]
}{\forall x.A \vdash A[x\backslash y] \vee B[x\backslash y]}\;[\vee R_1]
\qquad
\dfrac{
\dfrac{}{B \vdash B[x\backslash y] B \vdash B}\;[Id]
}{B \vdash A[x\backslash y] \vee B[x\backslash y]}\;[\vee R_2]
}{
\dfrac{(\forall x.A) \vee B \vdash A[x\backslash y] \vee B[x\backslash y]}{(\forall x.A) \vee B \vdash \forall x.A \vee B}\;[\forall R]
}\;[\vee L]
$$

- pick y such that it does not occur in A or B
- by L1, because $x \notin \mathtt{fv}(B)$ then $B[x\backslash y] = B$

Logical Equivalences

Prove that $(\exists x.A \wedge B) \leftrightarrow ((\exists x.A) \wedge B)$ if $x \notin \texttt{fv}(B)$ in the Sequent Calculus

Here is a proof of the left-to-right implication (constructive):

$$\dfrac{\dfrac{\dfrac{\dfrac{}{A[x\backslash y], B[x\backslash y] \vdash A[x\backslash y]}[Id]}{A[x\backslash y], B[x\backslash y] \vdash \exists x.A}[\exists R] \quad \dfrac{}{A[x\backslash y], B[x\backslash y] \vdash B A[x\backslash y], B \vdash B}[Id}{A[x\backslash y], B[x\backslash y] \vdash (\exists x.A) \wedge B}[\wedge}{\dfrac{A[x\backslash y] \wedge B[x\backslash y] \vdash (\exists x.A) \wedge B}{\exists x.A \wedge B \vdash (\exists x.A) \wedge B}[\exists L]}[\wedge L]$$

- pick y such that it does not occur in A or B
- by L1, because $x \notin \texttt{fv}(B)$ then $B[x\backslash y] = B$

Logical Equivalences

Prove that $(\exists x.A \wedge B) \leftrightarrow ((\exists x.A) \wedge B)$ if $x \notin \texttt{fv}(B)$ in the Sequent Calculus

Here is a proof of the right-to-left implication (constructive):

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{A[x\backslash y], B \vdash A[x\backslash y]}\,[Id] \qquad \dfrac{}{A[x\backslash y], B \vdash B[x\backslash y] A[x\backslash y], B \vdash B}\,[Id]}{A[x\backslash y], B \vdash A[x\backslash y] \wedge B[x\backslash y]}\,[\wedge R]}{A[x\backslash y], B \vdash \exists x.A \wedge B}\,[\exists R]}{(\exists x.A), B \vdash \exists x.A \wedge B}\,[\exists L]}{(\exists x.A) \wedge B \vdash \exists x.A \wedge B}\,[\wedge L]$$

- pick y such that it does not occur in A or B
- by L1, because $x \notin \texttt{fv}(B)$ then $B[x\backslash y] = B$

Logical Equivalences

We will now prove the following using the other equivalences:

- $(\forall x.A \to B) \leftrightarrow ((\exists x.A) \to B)$ if $x \notin \mathtt{fv}(B)$
- $(\exists x.A \to B) \leftrightarrow ((\forall x.A) \to B)$ if $x \notin \mathtt{fv}(B)$

Prove that $(\forall x.A \to B) \leftrightarrow ((\exists x.A) \to B)$ if $x \notin \mathtt{fv}(B)$ using the other equivalences

- $\forall x.A \to B$
- $\leftrightarrow \forall x.\neg A \vee B$ – using implication elimination
- $\leftrightarrow (\forall x.\neg A) \vee B$ – using $(\forall x.A \vee B) \leftrightarrow ((\forall x.A) \vee B)$ if $x \notin \mathtt{fv}(B)$
- $\leftrightarrow (\neg\exists x.A) \vee B$ – using $(\neg\exists x.A) \leftrightarrow (\forall x.\neg A)$
- $\leftrightarrow (\exists x.A) \to B$ – using implication elimination

Logical Equivalences

Prove that $(\exists x.A \to B) \leftrightarrow ((\forall x.A) \to B)$ if $x \notin \mathtt{fv}(B)$ using the other equivalences

- $\exists x.A \to B$
- $\leftrightarrow \exists x.\neg A \vee B$ – using implication elimination
- $\leftrightarrow (\exists x.\neg A) \vee (\exists x.B)$ – using $(\exists x.A \vee B) \leftrightarrow ((\exists x.A) \vee (\exists x.B))$
- $\leftrightarrow (\exists x.\neg A) \vee B$ – using $(\exists x.A) \leftrightarrow A$ if $x \notin \mathtt{fv}(A)$
- $\leftrightarrow (\neg\forall x.A) \vee B$ – using $(\neg\forall x.A) \leftrightarrow (\exists x.\neg A)$
- $\leftrightarrow (\forall x.A) \to B$ – using implication elimination

Logical Equivalences

We will now prove the following using semantics:

- $(\forall x.A \to B) \leftrightarrow (A \to \forall x.B)$ if $x \notin \texttt{fv}(A)$
- $(\exists x.A \to B) \leftrightarrow (A \to \exists x.B)$ if $x \notin \texttt{fv}(A)$

We will use following result:

Lemma (L2): if $x \notin \texttt{fv}(A)$, then $\models_{M,v,x\mapsto d} A$ iff $\models_{M,v} A$

Logical Equivalences

Prove $(\forall x.A \rightarrow B) \leftrightarrow (A \rightarrow \forall x.B)$ if $x \notin \mathtt{fv}(A)$ using the semantics method

Assume $x \notin \mathtt{fv}(A)$, M is a model with domain D and v a valuation

Left-to-right implication:

- if $\models_{M,v} \forall x.A \rightarrow B$ then $\models_{M,v} A \rightarrow \forall x.B$
  - to prove: $\models_{M,v} A \rightarrow \forall x.B$, i.e., $\models_{M,v} \forall x.B$ whenever $\models_{M,v} A$
  - assume $\models_{M,v} A$ and prove $\models_{M,v} \forall x.B$, i.e., for all $d \in D$, $\models_{M,v,x\mapsto d} B$
  - assumption: $\models_{M,v} \forall x.A \rightarrow B$, i.e., for all $e \in D$, $\models_{M,v,x\mapsto e} B$ whenever $\models_{M,v,x\mapsto e} A$
  - because $\models_{M,v} A$ by L2, $\models_{M,v,x\mapsto d} A$
  - instantiating this assumption with d gives us: $\models_{M,v,x\mapsto d} B$ whenever $\models_{M,v,x\mapsto d} A$
  - therefore, because $\models_{M,v,x\mapsto d} A$ is true, $\models_{M,v,x\mapsto d} B$ is also true

Logical Equivalences

Right-to-left implication:

- if $\models_{M,v} A \to \forall x.B$ then $\models_{M,v} \forall x.A \to B$
  - to prove: $\models_{M,v} \forall x.A \to B$, i.e., for all $d \in D$, $\models_{M,v,x\mapsto d} B$ whenever $\models_{M,v,x\mapsto d} A$
  - assume $d \in D$ and $\models_{M,v,x\mapsto d} A$, and prove $\models_{M,v,x\mapsto d} B$
  - by L2, we can assume $\models_{M,v} A$
  - assumption: $\models_{M,v} A \to \forall x.B$, i.e., $\models_{M,v} \forall x.B$ whenever $\models_{M,v} A$
  - because $\models_{M,v} A$, we can assume $\models_{M,v} \forall x.B$, i.e., for all $e \in D$, $\models_{M,v,x\mapsto e} B$
  - instantiating this assumption using d, we get to assume $\models_{M,v,x\mapsto d} B$, which is what we wanted to prove

Conclusion

What did we cover today?

- Equivalence using Natural Deduction
- Equivalence using the Sequent Calculus
- Rewriting using “known” equivalences
- Equivalences using semantics

Further reading:

- Chapter 8 of
  http://leanprover.github.io/logic_and_proof/

Next time?

- Theorem Proving