Formal Methods in Software Development
Course 11. Recalling the Basics of Computational Logic

Mădălina Eraşcu

Content based on the book Leino, K. Rustan M. Program Proofs. MIT Press, 2023

Thanks to Costel Anghel, 3rd year Bachelor student, Applied Informatics

June 5, 2024

Contents

Motivating Example

Recall the program computing the minimum of two integer numbers from previous lecture. What are the rules which were applied in the proofs of the 2 verification conditions?

Equivalent Formulae in Logic

Let X, Y be propositional logic formulae. Let ! (or $\neg$), && (or $\wedge$), || (or $\vee$), $==>$ (or $\Rightarrow$), , $<==>$ (or $\Leftrightarrow$) be the logical connectives.
We introduce the following semantics and rewrite rules for logical connectives introduced above.
Negation. *The formula !X is True if and only if X is false.*

$$
\begin{aligned}
!\textbf{true} &= \textbf{false} \\
\textbf{true} &= !\textbf{false} \\
!!X &= X \qquad (\textit{Double Negation})
\end{aligned}
$$

Conjunction. *X && Y is True if and only if X and Y are both true.*

$$
\begin{aligned}
\textbf{true} \&\& X &= X && (\textit{Unit}) \\
\textbf{false} \&\& X &= \textbf{false} && (\textit{Zero}) \\
X \&\& X &= X && (\textit{Idempotent}) \\
X \&\& !X &= \textbf{false} && (\textit{Law\ of\ Excluded\ Middle}) \\
X \&\& Y &= Y \&\& X && (\textit{Commutative}) \\
X \&\& (Y \&\& Z) &= (X \&\& Y) \&\& Z && (\textit{Associative})
\end{aligned}
$$

Equivalent Formulae in Logic (cont'd)

Disjunction. $X \| Y$ is True if and only if at least one of X or Y is true.

$$
\begin{array}{lll}
\textbf{false} \| X & = X & (\mathit{Unit}) \\
\textbf{true} \| X & = \textbf{true} & (\mathit{Zero}) \\
X \| X & = X & (\mathit{Idempotent}) \\
X \| !X & = \textbf{true} & (\mathit{Law\ of\ Excluded\ Middle}) \\
X \| Y & = Y \| X & (\mathit{Commutative}) \\
X \| (Y \| Z) & = (X \| Y) \| Z & (\mathit{Associative}) \\
!(X \&\& Y) & = !X \| !Y & (\mathit{De\ Morgan's\ Law}) \\
!(X \| Y) & = !X \&\& !Y & (\mathit{De\ Morgan's\ Law}) \\
X \| (Y \&\& Z) & = (X \| Y) \&\& (X \| Z) & (\mathit{Distribution}) \\
X \&\& (Y \| Z) & = (X \&\& Y) \| (X \&\& Z) & (\mathit{Distribution})
\end{array}
$$

Equivalent Formulae in Logic (cont'd)

Implication. $X \implies Y$ is False if and only if X is true and Y is false.

$$
\begin{aligned}
X &\implies Y && = !X \| Y && (\textit{Implication}) \\
X \&\& (X &\implies Y) && = X \&\& Y && (\textit{Modus Ponens}) \\
X &\implies Y && = !Y \implies !X && (\textit{Contrapositive}) \\
X \&\& Y &\implies Z && = X \implies !Y \| Z && (\textit{Shunting}) \\
X \| Y &\implies Z && = (X \implies Z) \&\& (Y \implies Z) && (\textit{Distribution})
\end{aligned}
$$

Equivalence. $X \iff Y$ is True if and only if X and Y are both true or both false.

$$X \iff Y = (X \implies Y) \&\& (Y \implies X) \quad (\textit{Equivalence})$$

Example

- Which rules do you apply to show that

$$x \leq y \Rightarrow (x \leq x \wedge x \leq y)$$

- Prove the Shunting rule.

Equivalent Formulae in Logic (cont'd)

Introduce universal ($\forall$) and existential ($\exists$) quantification.

Remark

Before talking about universal and existential quantifiers, we need to talk about bound variables and free variables.

We say a variable is **bound** when it's introduced by quantifiers ($\forall$ for universal quantification, $\exists$ for existential quantification). When a variable is bound, it means that it has a restricted scope, and its value is dependent on that scope.

A variable is **free** when it's not bound by any quantifier within the formula. They are introduced from outside and are not limited by any local scope.
A variable can be both free and bound in a single formula. For example, y is both free and bound in this formula: $(\forall x)P(x, y) \wedge (\forall y)Q(y)$.

Example (Bound variables)

$(\forall x)(Q(x) \implies R(x))$, since every occurrence of x is bound, the variable x is bound.

Example (Free variables)

$(\exists x)P(x, y)$, since the only appearance of y is free, the variable y is free.

Equivalent Formulae in Logic (cont'd)

Let F be a formula that contains a free variable x. To show that, we write F by $F[x]$. Let G be a formula that doesn't contain variable x. Q stands for "quantifier" type so it can be either $\forall$ or $\exists$. Then we have the following laws:

$$\begin{aligned}
(Qx)F[x] \vee G &= (Qx)(F[x] \vee G) \\
(Qx)F[x] \wedge G &= (Qx)(F[x] \wedge G) \\
\neg((\forall x)F[x]) &= (\exists x)(\neg F[x]) \\
\neg((\exists x)F[x]) &= (\forall x)(\neg F[x])
\end{aligned}$$

Other equivalent formulae. Let $F[x]$ and $H[x]$ are two formulas containing x, here are some other laws:

$$\begin{aligned}
(\forall x)F[x] \wedge (\forall x)H[x] &= (\forall x)(F[x] \wedge H[x]) \\
(\exists x)F[x] \vee (\exists x)H[x] &= (\exists x)(F[x] \vee H[x]) \\
(\forall x)F[x] \vee (\forall x)H[x] &\neq (\forall x)(F[x] \vee H[x]) \\
(\exists x)F[x] \wedge (\exists x)H[x] &\neq (\exists x)(F[x] \wedge H[x])
\end{aligned}$$

Contents

The Art of Proving

A **proof** is a structured argument that a formula is true. Each proof consists of *knowledge* and a *goal*.

$$K_1, \ldots, K_n \models G$$

- Knowledge $K_1, \ldots, K_n$: formulae assumed to be true.
- Goal G: formula to be proved relative to knowledge.

A **proof rules** describes how a proof situation can be reduced to zero, one, or more subsituations.

$$\frac{\ldots \models \ldots \quad \ldots \models \ldots}{K_1, \ldots, K_n \models G}$$

Rule may or may not close the (sub)proof:

- Zero subsituations: G has been proved, (sub)proof is closed.
- One or more subsituations: G is proved, if all subgoals are proved.

Top-down rules: focus on G i.e. G is decomposed into simpler goals $G_1, G_2, \ldots$.
Bottom-up rules: focus on $K_1, \ldots, K_n$. Knowledge is extended to $K_1, \ldots, K_n, K_{n+1}$.
In each proof situation, we aim at showing that the goal is true with respect to the given knowledge.

Example

How do you apply top-down/bottom-up rules for the examples below?

- $x \leq y \Rightarrow \underbrace{x \leq x}_{\mathbb{T}} \wedge x \leq y \quad \Longleftrightarrow \quad x \leq y \Rightarrow x \leq y \quad \checkmark$
- $x > y \Rightarrow y \leq x \wedge \underbrace{y \leq y}_{\mathbb{T}} \quad \Longleftrightarrow \quad \underbrace{x > y}_{K} \Rightarrow \underbrace{x > y}_{G_2} || \underbrace{x = y}_{G_1}$. ...

The Art of Proving (cont'd)

1. Conjunction $F_1 \&\& F_2$

$$\frac{K \models G_1 \quad K \models G_2}{K \models G_1 \&\& G_2} \qquad \frac{\ldots, K_1 \&\& K_2, K_1, K_2 \models G}{\ldots, K_1 \&\& K_2 \models G}$$

- Goal $G_1 \&\& G_2$.
  - Create two subsituations with goals G_1 and G_2.
    We have to show $G_1 \&\& G_2$.
  - We show G_1: …(proof continues with goal G_1)
  - We show G_2: …(proof continues with goal G_2)
- Knowledge $K_1 \&\& K_2$.
  - Create one subsituation with K_1 and K_2 in knowledge.
    We know $K_1 \&\& K_2$. We thus also know K_1 and K_2 (proof continues with current goal and additional knowledge K1 and K2).

2. Disjunction $F_1 \| F_2$

$$\frac{K, !G_1 \models G_2}{K \models G_1 \| G_2} \qquad \frac{\ldots, K_1 \models G \quad \ldots, K_2 \models G}{\ldots, K_1 \| K_2 \models G}$$

- Goal $G_1 \| G_2$.
  - Create one subsituation where G_2 is proved under the assumption that G_1 does not hold (or vice versa):
    We have to show $G_1 \| G_2$. We assume $!G_1$ and show $!G_2$. (proof continues with goal G_2 and additional knowledge $!G_1$)
- Knowledge $K_1 \| K_2$.
  - Create two subsituations, one with K_1 and one with K_2 in knowledge.
    We know $K_1 \| K_2$. We thus proceed by case distinction:
  - Case K_1: …(proof continues with current goal and additional knowledge K_1).
  - Case K_2: …(proof continues with current goal and additional knowledge K_2).

The Art of Proving (cont'd)

3. Implication $F_1 \implies F_2$

$$\frac{K, G_1 \models G_2}{K \models G_1 \implies G_2} \qquad \frac{\ldots \models K_1 \quad \ldots, K_2 \models G}{\ldots, K_1 \implies K_2 \models G}$$

- Goal $G_1 \implies G_2$.
  - Create one subsituation where G_2 is proved under the assumption that G_1 holds:

    We have to show $G_1 \implies G_2$. We assume G_1 and show G_2. (proof continues with goal G_2 and additional knowledge G_1).
- Knowledge $K_1 \implies K_2$.
  - Create two subsituations, one with goal K_1 and one with knowledge K_2.

    We show $K_1 \implies K_2$:
  - We show K_1: . . . (proof continues with goal K_1)
  - We know K_2: . . . (proof continues with current goal and additional knowledge K_2).

The Art of Proving (cont'd)

4. Equivalence $F_1 <==> F_2$

$$\frac{K \models G_1 ==> G_2 \quad K \models G_2 ==> G_1}{K \models G_1 <==> G_2} \qquad \frac{\ldots \models K_1, \ldots, K_2 \models G}{\ldots, K_1 <==> K_2 \models G} \text{ or } \frac{\ldots \models !K_1, \ldots, !K_2 \models G}{\ldots, K_1 <==> K_2 \models G}$$

- Goal $G_1 <==> G_2$. Create two subsituations with implications in both directions as goals. We have to show $G_1 <==> G_2$.
- We show $G_1 ==> G_2$: ... (proof continues with goal $G_1 ==> G_2$).
- We show $G_2 ==> G_1$: ... (proof continues with goal $G_2 ==> G_1$).
- Knowledge $K_1 <==> K_2$. Create two subsituations, one with goal K_1 and one with knowledge K_2. We show G:
- We show K_1: ... (proof continues with goal K_1)
- We know K_2: ... (proof continues with current goal and additional knowledge K_2).

Remark

Simmilar for $\frac{\ldots \models !K_1, \ldots, !K_2 \models G}{\ldots, K_1 <==> K_2 \models G}$

The Art of Proving (cont'd)

5. Universal Quantification $\forall x : F$

$$\frac{K \models G[x_0/x]}{K \models \forall x : G}(x_0 \text{ new for } K, G) \qquad \frac{\ldots, \forall x : K, K[T/x] \models G}{\ldots, \forall x : K \models G}$$

- Goal $\forall x : G$.
- Introduce new (arbitrarily named) constant x_0 and create one subsituation with goal $G[x_0/x]$.

  We have to show $\forall x : G$. Take arbitrary x_0.

  We show $G[x_0/x]$. (proof continues with goal $G[x_0/x]$).
- Knowledge $\forall x : K$.
- Choose term T to create one subsituation with formula $K[T/x]$ added to the knowledge.

  We know $\forall x : K$ and thus also $K[T/x]$. (proof continues with current goal and additional knowledge $K[T/x]$).

6. Existential Quantification $\exists x : F$

$$\frac{K \models G[T/x]}{K \models \exists x : G} \qquad \frac{\ldots, K[x_0/x] \models G}{\ldots, \exists x : K \models G}(x_0 \text{ new for } K, G)$$

- Goal $\exists x : G$.
- Choose term T to create one subsituation with goal $G[T/x]$.

  We have to show $\exists x : G$. It suffices to show $G[T/x]$. (proof continues with goal $G[T/x]$).
- Knowledge $\exists x : K$.
- Introduce new (arbitrarily named constant) x_0 and create one subsituation with additional knowledge $K[x_0/x]$.

Examples

- Prove $x > y \Rightarrow y \leq x \wedge \underbrace{y \leq y}_{\mathbb{T}}$.

- $(\exists x : \forall y : P(x, y)) ==> (\forall y : \exists x : P(x, y))$

Examples

- Prove $x > y \Rightarrow y \leq x \wedge \underbrace{y \leq y}_{\mathbb{T}}$. We have $x > y \Rightarrow y \leq x \wedge \underbrace{y \leq y}_{\mathbb{T}}$

- $(\exists x : \forall y : P(x, y)) ==> (\forall y : \exists x : P(x, y))$

Examples

- Prove $x > y \Rightarrow y \leq x \wedge \underbrace{y \leq y}_{\mathbb{T}}$. We have $x > y \Rightarrow y \leq x \wedge \underbrace{y \leq y}_{\mathbb{T}}$ which is equivalent to $\underbrace{x > y}_{K} \Rightarrow \underbrace{x > y}_{G_2} || \underbrace{x = y}_{G_1}$.

- $(\exists x : \forall y : P(x, y)) ==> (\forall y : \exists x : P(x, y))$

Examples

- Prove $x > y \Rightarrow y \leq x \wedge \underbrace{y \leq y}_{\mathbb{T}}$. We have $x > y \Rightarrow y \leq x \wedge \underbrace{y \leq y}_{\mathbb{T}}$ which is equivalent to $\underbrace{x > y}_{K} \Rightarrow \underbrace{x > y}_{G_2} || \underbrace{x = y}_{G_1}$. We apply the proof rule *disjunction in the goal* so we prove
  $x > y \wedge x! = y \Rightarrow x > y \checkmark$
- $(\exists x : \forall y : P(x, y)) ==> (\forall y : \exists x : P(x, y))$