Basic Logic Formulae. The Art of Proving

Costel Anghel and Mădălina Erașcu

Objectives

- Recalling basic logic formulae [1, Appendix B].
- Recalling proof techniques [2].

Remark 1 *The material in this lab is useful for understanding how the verification conditions (the logical formulae generated from the program source code) are proved/disproved internally by Dafny (or any other verifier).*

Consider the example below (see also the slides of the previous lecture):

```
method Min(x: int, y: int) returns (m: int)
    ensures m <= x && m <= y
{
    if x <= y {
        m := x;
    } else {
        m := y;
    }
}
```

In order to prove that the program is functionally correct or partially correct for all integer variables x, y (input variables), Dafny thansforms the program into 2 verification conditions, coresponding to each branch if the `if` statement and both should be True in order to show correctness.
Branch 1:

$$x \leq y \Rightarrow x \leq x \wedge x \leq y$$

Branch 2:

$$x > y \Rightarrow y \leq x \wedge y \leq y \quad \Longleftrightarrow \quad x > y \Rightarrow x > y || x = y$$

We take each of the 2 formulae and prove they are True.

- *Branch 1:*

$$x \leq y \Rightarrow \underbrace{x \leq x}_{\mathbb{T}} \wedge x \leq y \quad \Longleftrightarrow \quad x \leq y \Rightarrow x \leq y \quad \checkmark$$

- *Branch 2:*

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

  Next, we use the proof rule *disjunction in the goal* (see in the following pages) and prove $x > y \wedge x! = y \Rightarrow x > y$✓

1 Basic logic formulae

1. Negation !X. True if and only if X is false.

$$\begin{aligned} &!\mathbf{true} {=} \mathbf{false} \\ &\mathbf{true} = !\mathbf{false} \\ &!!X \quad = X \qquad (Double\ Negation) \end{aligned} \tag{1}$$

2. Conjunction X && Y ("X and Y"). True if and only if X and Y are both true.

$$\begin{aligned} &\mathbf{true}\&\&X && = X && (Unit) \\ &\mathbf{false}\&\&X && = \mathbf{false} && (Zero) \\ &X\&\&X && = X && (Idempotent) \\ &X\&\&!X && = \mathbf{false} && (Law\ of\ Excluded\ Middle) \\ &X\&\&Y && = Y\&\&X && (Commutative) \\ &X\&\&(Y\&\&Z) && = (X\&\&Y)\&\&Z && (Associative) \end{aligned} \tag{2}$$

3. Disjunction $X \parallel Y$ ("X or Y"). True if and only if at least one of X or Y is true.

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

$$!(X\&\&Y) = !X\|!Y \qquad (De\ Morgan's\ Law) \tag{3}$$

$$!(X\|Y) = !X\&\&!Y \qquad (De\ Morgan's\ Law) \tag{4}$$

$$X\|(Y\&\&Z) = (X\|Y)\&\&(X\|Z) \qquad (Distribution) \tag{5}$$

$$X\&\&(Y\|Z) = (X\&\&Y)\|(X\&\&Z) \qquad (Distribution) \tag{6}$$

4. Implication $X ==> Y$ ("if X, then Y"). False if and only if X is true and Y is false.

$$\begin{aligned}
&X ==> Y && =!X\|Y && (Implication) && (7)\\
&X\&\&(X ==> Y) && =X\&\&Y && (Modus\ Ponens) && (8)\\
&X ==> Y && =!Y ==>!X && (Contrapositive) && (9)\\
&X\&\&Y ==> Z && =X ==>!Y||Z && (Shunting) && (10)\\
&X\|Y ==> Z && =(X ==> Z)\&\&(Y ==> Z) && (Distribution) &&
\end{aligned}$$

5. Equivalence $X <==> Y$ ("if X, then Y and vice versa"). True if and only if X and Y are both true or both false.

$$X <==> Y = (X ==> Y)\&\&(Y ==> X) \quad (Equivalence)$$

6. Universal and existential quantification

Remark 2 *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.

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

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.

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

Remark 3 *A variable can be both free and bound in a single formula. For example, y is both free and bound in this formula: $(\forall x)P(x, y) \wedge (\forall y)Q(y)$.*

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:

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

Knowing that $F[x]$ and $H[x]$ are two formulas containing x, here are some other laws:

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

Remark 4 *The universal quantifier $\forall$ and the existential quantifier $\exists$ cannot distribute over $\vee$ and $\wedge$:*

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

7. Atomic formula $p(T_1, \ldots, T_n)$. True if the predicate denoted by p holds for the values of $T_1, \ldots, T_n$.

Remark 5 *When a boolean formula equals **true**, we say that it holds.*

1.1 Solved Exercises (Basic logic formulae)

1. De Morgan's Law proof:

$$!(X\|Y) \stackrel{(1)}{=} !(!!X\|!!Y) \stackrel{(3)}{=} !!(!X\&\&!Y) \stackrel{(1)}{=} !X\&\&!Y$$

2. Associativity of $\|$ proof:

$$\begin{aligned}X\|(Y\|Z) &\stackrel{(1)}{=} !!X\|!!(Y\|Z) \stackrel{(3)}{=} !(!X\&\&!(Y\|Z)) \stackrel{(4)}{=} !(!X\&\&(!Y\&\&!Z))\\&\stackrel{(2)}{=} !((!X\&\&!Y)\&\&!Z) \stackrel{(4)}{=} !(!(X\|Y)\&\&!Z) \stackrel{(3)}{=} !!(X\|Y)\|!!Z\\&\stackrel{(1)}{=} (X\|Y)\|Z\end{aligned}$$

3. Distribution of $==>$ proof:

$$\begin{aligned}X\|Y ==> Z = (X\|Y) ==> Z &\stackrel{(7)}{=} !(X\|Y)\|Z \stackrel{(4)}{=} (!X\&\&!Y)\|Z \stackrel{(5)}{=} (!X\|Z)\&\&(!Y\|Z) \stackrel{(7)}{=}\\&\stackrel{(7)}{=} (X ==> Z)\&\&(Y ==> Z)\end{aligned}$$

2 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.

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 apparently true with respect to the given knowledge.

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 subsitutions 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).

3. Implication $F_1 ==> F_2$

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

- Goal $G_1 ==> G_2$.
  - Create one subsitution where G_2 is proved under the assumption that G_1 holds:

    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 goal K_1 and one with knowledge K_2.

    We show $K_1 ==> K_2$:
    * We show K_1: …(proof continues with goal K_1)
    * We know K_2: …(proof continues with current goal and additional knowledge K_2).

4. Equivalence $F_1 <==> F_2$

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

- 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 $K_1 <==> K_2$:
    * We show (!)K_1: ... (proof continues with goal (!)K_1)
    * We know (!)K_2: ... (proof continues with current goal and additional knowledge (!)K_2).

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 $K[x_0/x]$.
    We know $\exists x : K$. Let x_0 be such that $K[x_0/x]$. (proof continues with current goal and additional knowledge $K[x_0/x]$).

Indirect Proofs

$$\frac{K, !G \models \textbf{false}}{K \models G} \qquad \frac{K, !G \models F \quad K, !G \models !F}{K \models G} \qquad \frac{\ldots, !G \models !K}{\ldots, K \models G}$$

- Add $!G$ to the knowledge and show a contradiction.
  - Prove that "false" is true.
  - Prove that a formula F is true and also prove that it is false.
  - Prove that some knowledge K is false, i.e. that $!K$ is true.
    - Switches goal G and knowledge K (negating both).

Sometimes simpler than a direct proof.

2.1 Solved Exercises (The Art of Proving)

$$\text{We show} \quad (\exists x : \forall y : P(x,y)) \implies (\forall y : \exists x : P(x,y))$$

$$\text{We assume} \quad (\exists x : \forall y : P(x,y)) \tag{11}$$

$$\text{and show} \quad (\forall y : \exists x : P(x,y))$$

$$\text{Take arbitrary } y_0. \quad \text{We show} \quad \exists x : P(x, y_0) \tag{12}$$

$$\text{From (11) we know for some } x_0 \quad \forall y : P(x_0, y) \tag{13}$$

$$\text{From (13) we know} \quad P(x_0, y_0) \tag{14}$$

$$\text{From (14) we know (12).} \blacksquare$$

3 Homework

3.1 Topic: Basic logic formulae

1. Prove the Unit, Zero, Idempotent, Law of Excluded Middle, and Commutative properties of $\|$ stated above.

2. Prove the two additional variations of De Morgan's Law:

$$(a) \quad X \| Y = !(!X \&\& !Y)$$
$$(b)\, X \&\& Y = !(!X \| !Y)$$

3. Prove (5), and (6) defined above.

4. Prove the Modus Ponens (8), Contrapositive (9), Shunting (10), and *(a)* and *(b)* below:

$$(a) X \| (!X ==> Y) = X \| Y$$
$$(b)\ X ==> Y \&\& Z = (X ==> Y) \&\& (X ==> Z)$$

5. Prove the following formula:

$$(P(x)\&\&Q(y) ==> R(x,y))\&\&!R(x,y)\&\&P(x) \quad ==> \quad !Q(y)$$

3.2 Topic: The Art of Proving

Prove:

$$(a)(\exists x : p(x))\&\&(\forall x : p(x)) ==> \exists y : q(x,y)) ==> \quad (\exists x, y : q(x,y))$$
$$(b) \qquad (\exists x : \forall y : P(x,y)) ==> (\forall y : \exists x : P(x,y))$$

References

[1] K. R. M. Leino. *Program Proofs*. MIT Press, 2023.

[2] W. Schreiner. Lecture notes in formal methods in software development, 2023.