Logic-based Program Verification
First-Order Logic

Mădălina Eraşcu and Tudor Jebelean
Research Institute for Symbolic Computation,
Johannes Kepler University, Linz, Austria
{merascu,tjebelea}@risc.jku.at

October 23, 2013

Example 1 (Semantics) Let

$$F \quad :\Longleftrightarrow \quad \underset{x}{\forall}\,\underset{y}{\exists}\; x+y>c$$

$$I:\begin{cases} D=\{0,1\} \\ c_I=0 \\ +_I \to +_{\mathbb{Z}} \\ >_I \to >_{\mathbb{Z}} \end{cases}$$

Solution. $\langle F\rangle_I = \mathbb{T}$ iff for each $d \in D$:

$$\left\langle \underset{y}{\exists}\; x+y>c \right\rangle^I_{\sigma \uplus \{x\to d\}} = \mathbb{T}$$

- Case $x \to 0$. We have

$$\left\langle \underset{y}{\exists}\; x+y>c \right\rangle^I_{\{x\to 0\}} = \mathbb{T} \text{ iff for some } d\in D: \quad \langle x+y>c\rangle^I_{\{x\to 0\}\uplus\{y\to d\}} = \mathbb{T}$$

  - Case $y \to 0$. We have

$$\begin{aligned} & \langle x+y>c\rangle^I_{\{x\to 0,y\to 0\}} \\ \rightsquigarrow\ & >_{\mathbb{Z}} \left[\langle x+y\rangle^I_{\{x\to 0,y\to 0\}}, \langle c\rangle^I_{\{x\to 0,y\to 0\}}\right] \\ \rightsquigarrow\ & >_{\mathbb{Z}} \left[+_{\mathbb{Z}}\left[\langle x\rangle^I_{\{x\to 0,y\to 0\}}, \langle y\rangle^I_{\{x\to 0,y\to 0\}}\right], 0\right] \\ \rightsquigarrow\ & >_{\mathbb{Z}} \left[+_{\mathbb{Z}}\left[0,0\right], 0\right] \\ \rightsquigarrow\ & >_{\mathbb{Z}} \left[0,0\right] \\ \rightsquigarrow\ & \mathbb{F} \end{aligned}$$

– Case $y \to 1$. We have

$$\begin{aligned} & \langle x + y > c \rangle^I_{\{x \to 0, y \to 1\}} \\ \rightsquigarrow \quad & >_{\mathbb{Z}} \left[\langle x + y \rangle^I_{\{x \to 0, y \to 1\}}, \langle c \rangle^I_{\{x \to 0, y \to 1\}} \right] \\ \rightsquigarrow \quad & >_{\mathbb{Z}} \left[+_{\mathbb{Z}} \left[\langle x \rangle^I_{\{x \to 0, y \to 1\}}, \langle y \rangle^I_{\{x \to 0, y \to 1\}} \right], 0 \right] \\ \rightsquigarrow \quad & >_{\mathbb{Z}} \left[+_{\mathbb{Z}} [0, 1], 0 \right] \\ \rightsquigarrow \quad & >_{\mathbb{Z}} [1, 0] \\ \rightsquigarrow \quad & \mathbb{T} \end{aligned}$$

- Case $x \to 1$. We have

$$\left\langle \underset{y}{\exists}\, x + y > c \right\rangle^I_{\{x \to 1\}} = \mathbb{T} \text{ iff for some } d \in D: \quad \langle x + y > c \rangle^I_{\{x \to 1\} \uplus \{y \to d\}} = \mathbb{T}$$

  – Case $y \to 0$. We have

$$\begin{aligned} & \langle x + y > c \rangle^I_{\{x \to 1, y \to 0\}} \\ \rightsquigarrow \quad & >_{\mathbb{Z}} \left[\langle x + y \rangle^I_{\{x \to 1, y \to 0\}}, \langle c \rangle^I_{\{x \to 1, y \to 0\}} \right] \\ \rightsquigarrow \quad & >_{\mathbb{Z}} \left[+_{\mathbb{Z}} \left[\langle x \rangle^I_{\{x \to 1, y \to 0\}}, \langle y \rangle^I_{\{x \to 1, y \to 0\}} \right], 0 \right] \\ \rightsquigarrow \quad & >_{\mathbb{Z}} \left[+_{\mathbb{Z}} [1, 0], 0 \right] \\ \rightsquigarrow \quad & >_{\mathbb{Z}} [1, 0] \\ \rightsquigarrow \quad & \mathbb{T} \end{aligned}$$

  – Case $y \to 1$. We have ...

◀

Example 2 (CNF) Prove the following by bringing the formulas into CNF

$$\left(\underset{x}{\forall} P[x] \right) \Rightarrow Q \quad \equiv \quad \underset{x}{\exists} \left(P[x] \Rightarrow Q \right).$$

Solution. We have

$$\left(\underset{x}{\forall} P[x] \right) \Rightarrow Q \quad \equiv \quad \neg \left(\underset{x}{\forall} P[x] \right) \vee Q \quad \equiv \quad \left(\underset{x}{\exists} \neg P[x] \right) \vee Q \quad \equiv \quad \underset{x}{\exists} \left(\neg P[x] \vee Q \right)$$

Further we have

$$\underset{x}{\exists} \left(P[x] \Rightarrow Q \right) \quad \equiv \quad \underset{x}{\exists} \left(\neg P[x] \vee Q \right)$$

◀

Example 3 (Skolem Standard Form) Bring the following formula into Skolem Standard Form

$$\underset{x}{\forall}\ \underset{y,z}{\exists} \left((\neg P[x, y] \ \wedge \ Q[x, z]) \ \vee \ R[x, y, z] \right)$$

Solution.

$$\begin{aligned}
& \underset{x}{\forall}\ \underset{y,z}{\exists}\ ((\neg P[x,y]\ \wedge\ Q[x,z])\ \vee\ R[x,y,z]) \\
\Longleftrightarrow\ & \underset{x}{\forall}\ \underset{y,z}{\exists}\ ((\neg P[x,y]\ \vee\ R[x,y,z])\ \wedge\ (Q[x,z]\ \vee\ R[x,y,z])) \\
\rightsquigarrow\ & \underset{x}{\forall}((\neg P[x,f[x]]\ \vee\ R[x,f[x],g[x]])\ \wedge\ (Q(x,g[x])\ \vee\ R[x,f[x],g[x]]))
\end{aligned}$$

◀

Example 4 (Skolem Standard Form) Bring the following formula into Skolem Standard Form

$$\underset{x,y}{\forall}\left(\underset{z}{\exists}P[x,z]\wedge P[y,z]\right)\ \Rightarrow\ \underset{u}{\exists}Q[x,y,u]$$

Solution.

$$\begin{aligned}
& \underset{x,y}{\forall}\left(\underset{z}{\exists}P[x,z]\wedge P[y,z]\right)\ \Rightarrow\ \underset{u}{\exists}Q[x,y,u] \\
\Longleftrightarrow\ & \underset{x,y}{\forall}\neg\left(\underset{z}{\exists}P[x,z]\wedge P[y,z]\right)\ \vee\ \underset{u}{\exists}Q[x,y,u] \\
\Longleftrightarrow\ & \underset{x,y}{\forall}\left(\underset{z}{\forall}\neg P[x,z]\vee\neg P[y,z]\right)\ \vee\ \underset{u}{\exists}Q[x,y,u] \\
\Longleftrightarrow\ & \underset{x,y,z}{\forall}\ (\neg P[x,z]\vee\neg P[y,z])\ \vee\ \underset{u}{\exists}Q[x,y,u] \\
\Longleftrightarrow\ & \underset{x,y,z}{\forall}\ \underset{u}{\exists}\ (\neg P[x,z]\vee\neg P[y,z])\ \vee\ Q[x,y,u] \\
\rightsquigarrow\ & \underset{x,y,z}{\forall}\ \neg P[x,z]\vee\neg P[y,z]\ \vee\ Q[x,y,f[x,y,z]]
\end{aligned}$$

◀

Example 5 ((Un)Satisfiability & (In)Validity) Prove that the formula

$$\underset{x}{\forall}P[x]\ \wedge\ \underset{y}{\exists}\neg P[y]$$

is inconsistent.

Solution. We have

$$\underset{x}{\forall}P[x]\wedge\underset{y}{\exists}\neg P[y]\ \equiv\ \underset{x}{\forall}P[x]\wedge\neg\left(\underset{y}{\forall}P[y]\right)\ \equiv\ \equiv\ \underset{x}{\forall}P[x]\wedge\neg\left(\underset{x}{\forall}P[x]\right)\ \equiv\ \mathbb{F}$$

◀

Example 6 Prove that the formula

$$\underset{x}{\forall}P[x]\ \Rightarrow\ \underset{y}{\exists}P[y]$$

is valid.

Solution. We assume that the formula is invalid and derive a contradiction. Hence, it exists an interpretation I under which the formula is false. That is

$$\left\langle \underset{x}{\forall} P[x] \right\rangle^I = \mathbb{T}$$
$$\wedge$$
$$\left\langle \underset{y}{\exists} P[y] \right\rangle^I = \mathbb{F} \;\; \rightsquigarrow \;\; \left\langle \underset{y}{\forall} \neg P[y] \right\rangle^I = \mathbb{T}$$

From the above we obtain that

$$\left\langle \underset{x}{\forall} P[x] \right\rangle^I = \left\langle \underset{y}{\forall} \neg P[y] \right\rangle^I \text{ which is a contradiction}$$

◀