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 30 & November 6, 2013

Example 1 (Clausification) Transform the formulas F_1, F_2, F_3, F_4, and $\neg G$ into a set of clauses, where

$$F_1: \quad \underset{x,y}{\forall}\ \underset{z}{\exists} P[x,y,z]$$

$$F_2: \quad \begin{array}{l} \underset{x,y,z,u,v,w}{\forall} (P[x,y,u] \ \wedge\ P[y,z,v] \ \wedge\ P[u,z,w] \quad \Rightarrow \quad P[x,v,w]) \\ \wedge \\ \underset{x,y,z,u,v,w}{\forall} (P[x,y,u] \ \wedge\ P[y,z,v] \ \wedge\ P[x,v,w] \quad \Rightarrow \quad P[u,z,w]) \end{array}$$

$$F_3: \quad \underset{x}{\forall} P[x,e,x] \wedge \underset{x}{\forall} P[e,x,x]$$

$$F_4: \quad \underset{x}{\forall} P[x,i[x],e] \wedge \underset{x}{\forall} P[i[x],x,e]$$

$$G: \quad \left(\underset{x}{\forall} P[x,x,e]\right) \ \Rightarrow\ \left(\underset{u,v,w}{\forall} (P[u,v,w] \ \Rightarrow\ P[v,u,w])\right)$$

Solution. F_1, F_2,F_3,F_4 can almost immediately transformed into clauses. We have

$$\begin{array}{l} P[x,y,f[x,y]] \\ \neg P[x,y,u] \ \vee\ \neg P[y,z,v] \ \vee\ \neg P[u,z,w] \ \vee\ P[x,v,w] \\ \neg P[x,y,u] \ \vee\ \neg P[y,z,v] \ \vee\ \neg P[x,v,w] \ \vee\ P[u,z,w] \\ P[x,e,x] \\ P[e,x,x] \\ P[x,i[x],e] \\ P[i[x],x,e] \end{array}$$

We transform $\neg G$ into standard form

$$\begin{aligned}
&\neg\left(\left(\underset{x}{\forall} P[x,x,e]\right) \;\Rightarrow\; \left(\underset{u,v,w}{\forall}(P[u,v,w] \;\Rightarrow\; P[v,u,w])\right)\right)\\
\Longleftrightarrow\; &\neg\left(\neg\left(\underset{x}{\forall} P[x,x,e]\right) \;\vee\; \left(\underset{u,v,w}{\forall}(\neg P[u,v,w] \;\vee\; P[v,u,w])\right)\right)\\
\Longleftrightarrow\; &\left(\underset{x}{\forall} P[x,x,e]\right) \;\wedge\; \left(\underset{u,v,w}{\exists}(P[u,v,w] \;\wedge\; \neg P[v,u,w])\right)\\
\rightsquigarrow &\underset{x}{\forall} P[x,x,e] \;\wedge\; P[a,b,c] \;\wedge\; \neg P[b,a,c]
\end{aligned}$$

which gives the following clauses

$$\begin{aligned}
&P[x,x,e]\\
&P[a,b,c]\\
&\neg P[b,a,c]
\end{aligned}$$

◀

Example 2 (Most General Unifier) Find a most general unifier for

$$W = \{P[a,x,f[g[y]]],\; P[z,f[z],f[u]]\}$$

Solution. Let $\sigma_0 = \varepsilon$ and $W_0 = W$. Since W_0 is not a singleton, σ_0 is not a mgu of W.
$D_0 = \{a, z\}$.
Let $\sigma_1 = \varepsilon \circ \{z \to a\}$, $W_1 = W_0\sigma_1 = \{P[a,x,f[g[y]]],\; P[a,f[a],f[u]]\}$.
W_1 is not a singleton. $D_1 = \{x, f[a]\}$.
Let $\sigma_2 = \{z \to a\}\{x \to f[a]\} = \{z \to a, x \to f[a]\}$. $W_2 = W_1\sigma_2 = \{P[a,f[a],f[g[y]]],\; P[a,f[a],f[u]]\}$.
W_2 is not a singleton. $D_2 = \{g[y], u\}$.
Let $\sigma_3 = \sigma_2\{u \to g[y]\} = \{z \to a, x \to f[a], u \to g[y]\}$.
$W_3 = W_2\sigma_2 = \{P[a,f[a],f[g[y]]],\; P[a,f[a],f[g[y]]]\} = \{P[a,f[a],f[g[y]]]\}$.
Since W_3 is a singleton. $\sigma_3 = \{z \to a, x \to f[a], u \to g[y]\}$ is a mgu for W. ◀

Example 3 (Most General Unifier) Find a most general unifier for

$$W = \{Q[a],\; Q[b]\}$$

Solution. Let $\sigma_0 = \varepsilon$ and $W_0 = W$. Since W_0 is not a singleton, σ_0 is not a mgu of W.
$D_0 = \{a, b\}$. Since none of the elements of D_0 is a variable we conclude that W is not unifiable. ◀

Example 4 (Resolution 1) Prove by resolution the following

$$\underset{x}{\forall} F[x] \;\vee\; \underset{x}{\forall} H[x] \quad\not\equiv\quad \underset{x}{\forall}(F[x] \;\vee\; H[x])$$

Solution. Direction "⇒". Let

$$\begin{aligned} F \quad &:\Longleftrightarrow \quad \underset{x}{\forall} F[x] \;\vee\; \underset{x}{\forall} H[x] \\ G \quad &:\Longleftrightarrow \quad \underset{x}{\forall} (F[x] \;\vee\; H[x]) \end{aligned}$$

We prove that G is a logical consequence of F by resolution. We have

$$\begin{aligned} F \quad &:\Longleftrightarrow \quad \underset{x}{\forall} F[x] \;\vee\; \underset{x}{\forall} H[x] \\ &\Longleftrightarrow \quad \underset{x,y}{\forall} F[x] \;\vee\; H[y] \\ \neg G \quad &:\Longleftrightarrow \quad \neg \left(\underset{x}{\forall} (F[x] \;\vee\; H[x]) \right) \\ &\Longleftrightarrow \quad \underset{x}{\exists} (\neg F[x] \;\wedge\; \neg H[x]) \\ &\rightsquigarrow \quad \neg F[a] \;\wedge\; \neg H[a] \end{aligned}$$

By transforming them into a set of clauses we have

$$\begin{array}{ll} (1) & F[x] \;\vee\; H[y] \\ (2) & \neg F[a] \\ (3) & \neg H[a] \end{array}$$

By applying resolution we obtain the following clauses

$$\begin{array}{lll} (4) & H[a] & (1) \wedge (2), \{x \to a, y \to a\} \\ (5) & \emptyset & (3) \wedge (4) \end{array}$$

Direction "⇐". Let

$$\begin{aligned} F \quad &:\Longleftrightarrow \quad \underset{x}{\forall} (F[x] \;\vee\; H[x]) \\ G \quad &:\Longleftrightarrow \quad \underset{x}{\forall} F[x] \;\vee\; \underset{x}{\forall} H[x] \end{aligned}$$

We prove that G is a logical consequence of F by resolution. We have

$$\begin{aligned} F \quad &:\Longleftrightarrow \quad \underset{x}{\forall} (F[x] \;\vee\; H[x]) \\ \neg G \quad &:\Longleftrightarrow \quad \neg \left(\underset{x}{\forall} F[x] \;\vee\; \underset{x}{\forall} H[x] \right) \\ &\Longleftrightarrow \quad \underset{x}{\exists} \neg F[x] \;\wedge\; \underset{x}{\exists} \neg H[x] \\ &\rightsquigarrow \quad \neg F[a] \;\wedge\; \neg H[b] \end{aligned}$$

By transforming them into a set of clauses we have

$$\begin{array}{ll} (1) & F[x] \vee H[x] \\ (2) & \neg F[a] \\ (3) & \neg H[b] \end{array}$$

By applying resolution we obtain the following clauses

$$\begin{array}{lll} (4) & H[a] & (1) \wedge (2), \{x \to a\} \\ (5) & F[b] & (1) \wedge (3), \{x \to b\} \end{array}$$

◄

Example 5 (Resolution 2) Prove by resolution that G is a logical consequence of F_1 and F_2 where

$$\begin{array}{ll} F_1 : & \underset{x}{\forall}\,(C[x] \;\Rightarrow\; (W[x] \;\wedge\; R[x])) \\ F_2 : & \underset{x}{\exists}(C[x] \wedge O[x]) \\ G : & \underset{x}{\exists}(O[x] \wedge R[x]) \end{array}$$

Solution. We show that $F_1 \wedge F_2 \wedge \neg G$ is unsatisfiable by resolution. We transform F_1, F_2, $\neg G$ into Skolem standard form. We have

$$\begin{array}{ll} & F_1 : \; \underset{x}{\forall}\,(C[x] \;\Rightarrow\; (W[x] \;\wedge\; R[x])) \\ \iff & \underset{x}{\forall}\,(\neg C[x] \;\vee\; (W[x] \;\wedge\; R[x])) \\ \iff & \underset{x}{\forall}\,(\neg C[x] \;\vee\; W[x]) \;\wedge\; (\neg C[x] \;\vee\; R[x]) \end{array}$$

$$\begin{array}{l} F_2 : \; \underset{x}{\exists}(C[x] \wedge O[x]) \\ \rightsquigarrow \; C[a] \wedge O[a] \end{array}$$

$$\begin{array}{ll} & \neg G : \; \neg\left(\underset{x}{\exists}(O[x] \wedge R[x])\right) \\ \iff & \underset{x}{\forall}(\neg O[x] \vee \neg R[x]) \end{array}$$

We have the following set of clauses

$$\begin{array}{ll} (1) & \neg C[x] \;\vee\; W[x] \\ (2) & \neg C[x] \;\vee\; R[x] \\ (3) & C[a] \\ (4) & O[a] \\ (5) & \neg O[x] \vee \neg R[x] \end{array}$$

By resolution we obtain also the following clauses

$$\begin{array}{lll} (6) & \neg R[a] & (4) \wedge (5), \{x \to a\} \\ (7) & \neg C[a] & (6) \wedge (2), \{x \to a\} \\ (8) & \emptyset & (7) \wedge (3) \end{array}$$

◄

Example 6 (Resolution 3) Prove by resolution that G is a logical consequence of F_1 and F_2 where

$$
\begin{aligned}
F_1 : &\quad \underset{x}{\exists}\Big(P[x] \;\wedge\; \underset{y}{\forall}(D[y] \;\Rightarrow\; L[x,y])\Big) \\
F_2 : &\quad \underset{x}{\forall}\Big(P[x] \;\Rightarrow\; \underset{y}{\forall}(Q[y] \;\Rightarrow\; \neg L[x,y])\Big) \\
G : &\quad \underset{x}{\forall}(D[x] \;\Rightarrow\; \neg Q[x])
\end{aligned}
$$

Solution. We show that $F_1 \wedge F_2 \wedge \neg G$ is unsatisfiable by resolution. We transform F_1, F_2, $\neg G$ into Skolem standard form. We have

$$
\begin{aligned}
F_1 : &\quad \underset{x}{\exists}\Big(P[x] \;\wedge\; \underset{y}{\forall}(D[y] \;\Rightarrow\; L[x,y])\Big) \\
\Longleftrightarrow &\quad \underset{x}{\exists}\Big(P[x] \;\wedge\; \underset{y}{\forall}(\neg D[y] \;\vee\; L[x,y])\Big) \\
\Longleftrightarrow &\quad \underset{x}{\exists}\underset{y}{\forall}(P[x] \;\wedge\; (\neg D[y] \;\vee\; L[x,y])) \\
\rightsquigarrow &\quad \underset{y}{\forall}(P[a] \;\wedge\; (\neg D[y] \;\vee\; L[a,y]))
\end{aligned}
$$

$$
\begin{aligned}
F_2 : &\quad \underset{x}{\forall}\Big(P[x] \;\Rightarrow\; \underset{y}{\forall}(Q[y] \;\Rightarrow\; \neg L[x,y])\Big) \\
\Longleftrightarrow &\quad \underset{x}{\forall}\Big(P[x] \;\Rightarrow\; \underset{y}{\forall}(\neg Q[y] \;\vee\; \neg L[x,y])\Big) \\
\Longleftrightarrow &\quad \underset{x}{\forall}\Big(\neg P[x] \;\vee\; \underset{y}{\forall}(\neg Q[y] \;\vee\; \neg L[x,y])\Big) \\
\Longleftrightarrow &\quad \underset{x}{\forall}\underset{y}{\forall}(\neg P[x] \;\vee\; \neg Q[y] \;\vee\; \neg L[x,y])
\end{aligned}
$$

$$
\begin{aligned}
\neg G : &\quad \neg\Big(\underset{x}{\forall}(D[x] \;\Rightarrow\; \neg Q[x])\Big) \\
\Longleftrightarrow &\quad \neg\Big(\underset{x}{\forall}(\neg D[x] \;\vee\; \neg Q[x])\Big) \\
\Longleftrightarrow &\quad \underset{x}{\exists}(D[x] \;\wedge\; Q[x]) \\
\rightsquigarrow &\quad D[a] \;\wedge\; Q[a]
\end{aligned}
$$

We have the following set of clauses

$$
\begin{aligned}
&(1) \quad P[a] \\
&(2) \quad \neg D[y] \;\vee\; L[a,y] \\
&(3) \quad \neg P[x] \;\vee\; \neg Q[y] \;\vee\; \neg L[x,y] \\
&(4) \quad D[a] \\
&(5) \quad Q[a]
\end{aligned}
$$

By resolution we obtain also the following clauses

(6)	$L[a,a]$	$(2) \wedge (4), \{y \to a\}$
(7)	$\neg P[a] \ \vee \ \neg Q[a]$	$(3) \wedge (6), \{x \to a, y \to a\}$
(8)	$\neg Q[a]$	$(1) \wedge (7)$
(9)	$\emptyset$	$(5) \wedge (8)$

◀

Example 7 (Resolution 4) Prove by resolution that G is a logical consequence of F where

$$F: \ \underset{x}{\forall}\underset{y}{\exists}\,(S[x,y] \ \wedge \ M[y]) \quad \Rightarrow \quad \underset{y}{\exists}\,(I[y] \ \wedge \ E[x,y])$$
$$G: \ \neg\underset{x}{\exists} I[x] \quad \Rightarrow \quad \underset{x,y}{\forall}\,(S[x,y] \Rightarrow \neg M[y])$$

Solution. We show that $F \wedge \neg G$ is unsatisfiable. First we transform the formulas into standard form. We have

$$\begin{aligned}
F: \ & \underset{x}{\forall}\left(\underset{y}{\exists}\,(S[x,y] \ \wedge \ M[y])\right) \quad \Rightarrow \quad \underset{y}{\exists}\,(I[y] \ \wedge \ E[x,y]) \\
\Longleftrightarrow \quad & \underset{x}{\forall}\neg\left(\underset{y}{\exists}\,(S[x,y] \ \wedge \ M[y])\right) \ \vee \ \underset{y}{\exists}\,(I[y] \ \wedge \ E[x,y]) \\
\Longleftrightarrow \quad & \underset{x}{\forall}\left(\underset{y}{\forall}\,(\neg S[x,y] \ \vee \ \neg M[y])\right) \ \vee \ \underset{y}{\exists}\,(I[y] \ \wedge \ E[x,y]) \\
\Longleftrightarrow \quad & \underset{x}{\forall}\left(\underset{y}{\forall}\,(\neg S[x,y] \ \vee \ \neg M[y])\right) \ \vee \ (I[f[x]] \ \wedge \ E[x,f[x]]) \\
\Longleftrightarrow \quad & \underset{x}{\forall}\underset{y}{\forall}\,(\neg S[x,y] \ \vee \ \neg M[y]) \ \vee \ (I[f[x]] \ \wedge \ E[x,f[x]]) \\
\Longleftrightarrow \quad & \underset{x}{\forall}\underset{y}{\forall}\,((\neg S[x,y] \ \vee \ \neg M[y] \ \vee \ I[f[x]]) \ \wedge \ (\neg S[x,y] \ \vee \ \neg M[y] \ \vee \ E[x,f[x]]))
\end{aligned}$$

$$\begin{aligned}
\neg G: \neg & \left(\neg\underset{x}{\exists} I[x] \quad \Rightarrow \underset{x,y}{\forall}(S[x,y] \Rightarrow \neg M[y])\right) \\
\Longleftrightarrow \quad & \neg\left(\neg\underset{x}{\exists} I[x] \quad \Rightarrow \underset{x,y}{\forall}(\neg S[x,y] \vee \neg M[y])\right) \\
\Longleftrightarrow \quad & \neg\left(\underset{x}{\exists} I[x] \quad \vee \underset{x,y}{\forall}(\neg S[x,y] \vee \neg M[y])\right) \\
\Longleftrightarrow \quad & \left(\underset{x}{\forall}\neg I[x] \quad \wedge \underset{x,y}{\exists}(S[x,y] \wedge M[y])\right) \\
\Longleftrightarrow \quad & \underset{z}{\forall}\neg I[z] \quad \wedge \underset{x,y}{\exists}(S[x,y] \wedge M[y]) \\
\rightsquigarrow \quad & \underset{z}{\forall}\neg I[z] \quad \wedge \ S[a,b] \wedge M[b]
\end{aligned}$$

We have the following set of clauses

$$\begin{array}{ll} (1) & \neg S[x,y] \ \vee \ \neg M[y] \ \vee \ I[f[x]] \\ (2) & \neg S[x,y] \ \vee \ \neg M[y] \ \vee \ E[x,f[x]] \\ (3) & \neg I[z] \\ (4) & S[a,b] \\ (5) & M[b] \end{array}$$

By resolution we obtain also the following clauses

$$\begin{array}{lll} (6) & \neg S[x,y] \ \vee \ \neg M[y] & (1) \wedge (3), \{z \to f[x]\} \\ (7) & \neg M[b] & (4) \wedge (6), \{x \to a, y \to b\} \\ (8) & \emptyset & (5) \wedge (7) \end{array}$$

◀

Example 8 (Resolution 5) Prove by resolution that G is a logical consequence of F_1, F_2, and F_3 where

$$\begin{array}{ll} F_1: & \underset{x}{\forall} (Q[x] \ \Rightarrow \ \neg P[x]) \\ F_2: & \underset{x}{\forall} \Big((R[x] \ \wedge \ \neg Q[x]) \quad \Rightarrow \quad \underset{y}{\exists} (T[x,y] \ \wedge \ S[y]) \Big) \\ F_3: & \underset{x}{\exists} \Big(P[x] \ \wedge \ \underset{y}{\forall} (T[x,y] \ \Rightarrow \ P[y]) \ \wedge \ R[x] \Big) \\ G: & \underset{x}{\exists} (S[x] \wedge P[x]) \end{array}$$

Solution. We show that $F_1 \wedge F_2 \wedge F_3 \wedge \neg G$ is unsatisfiable. First we transform the formulas into standard form.

$$F_1: \underset{x}{\forall}(Q[x] \Rightarrow \neg P[x]) \quad \Longleftrightarrow \quad \underset{x}{\forall}(\neg Q[x] \vee \neg P[x])$$

$$F_2: \underset{x}{\forall}\Big((R[x] \wedge \neg Q[x]) \Rightarrow \underset{y}{\exists}(T[x,y] \wedge S[y])\Big)$$

$$\Longleftrightarrow \underset{x}{\forall}\Big(\neg(R[x] \wedge \neg Q[x]) \vee \underset{y}{\exists}(T[x,y] \wedge S[y])\Big)$$

$$\Longleftrightarrow \underset{x}{\forall}\Big(\neg R[x] \vee Q[x] \vee \underset{y}{\exists}(T[x,y] \wedge S[y])\Big)$$

$$\Longleftrightarrow \underset{x}{\forall}\underset{y}{\exists}(\neg R[x] \vee Q[x] \vee (T[x,y] \wedge S[y]))$$

$$\Longleftrightarrow \underset{x}{\forall}\underset{y}{\exists}((\neg R[x] \vee Q[x] \vee T[x,y]) \wedge (\neg R[x] \vee Q[x] \vee S[y]))$$

$$\rightsquigarrow \underset{x}{\forall}((\neg R[x] \vee Q[x] \vee T[x,f[x]]) \wedge (\neg R[x] \vee Q[x] \vee S[f[x]]))$$

$$F_3: \underset{x}{\exists}\Big(P[x] \wedge \underset{y}{\forall}(T[x,y] \Rightarrow P[y]) \wedge R[x]\Big)$$

$$\Longleftrightarrow \underset{x}{\exists}\Big(P[x] \wedge \underset{y}{\forall}(\neg T[x,y] \vee P[y]) \wedge R[x]\Big)$$

$$\Longleftrightarrow \underset{x}{\exists}\underset{y}{\forall}(P[x] \wedge (\neg T[x,y] \vee P[y]) \wedge R[x])$$

$$\rightsquigarrow \underset{y}{\forall}(P[a] \wedge (\neg T[a,y] \vee P[y]) \wedge R[a])$$

$$\neg G: \neg\Big(\underset{x}{\exists}(S[x] \wedge P[x])\Big)$$

$$\Longleftrightarrow \underset{x}{\forall}(\neg S[x] \vee \neg P[x])$$

We have the following set of clauses

(1)	$\neg Q[x] \vee \neg P[x]$	
(2)	$\neg R[x] \vee Q[x] \vee T[x,f[x]]$	
(3)	$\neg R[x] \vee Q[x] \vee S[f[x]]$	
(4)	$P[a]$	
(5)	$\neg T[a,y] \vee P[y]$	
(6)	$R[a]$	
(7)	$\neg S[x] \vee \neg P[x]$	
(8)	$\neg Q[a]$	$(1) \wedge (4), \{x \to a\}$
(9)	$\neg R[a] \vee T[a,f[a]]$	$(8) \wedge (2), \{x \to a\}$
(10)	$\neg R[a] \vee P[f[a]]$	$(9) \wedge (5), \{y \to f[a]\}$
(11)	$P[f[a]]$	$(10) \wedge (6)$
(12)	$\neg S[f[a]]$	$(11) \wedge (7)$
(13)	$\neg R[a] \vee Q[a]$	$(12) \wedge (3)$
(14)	$Q[a]$	$(13) \wedge (6)$
(15)	$\emptyset$	$(14) \wedge (8)$

◀