Logic-based Program Verification
First-Order Theories. Theory of Equality

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

November 20, 2013

Example 1 Prove that F is T_E valid where

$$F \quad :\Longleftrightarrow \quad a = b \;\wedge\; b = c \;\Longrightarrow\; g[f[a], b] = g[f[c], a]$$

Solution.

$a = b \;\wedge\; b = c \;\Longrightarrow\; a = c$	(transitivity)
$a = b \;\Longrightarrow\; f[a] = f[b]$	(function congruence)
$b = c \;\Longrightarrow\; f[b] = f[c]$	(function congruence)
$a = c \;\Longrightarrow\; f[a] = f[c]$	(function congruence)
$f[a] = f[c] \;\wedge\; b = a \;\Longrightarrow\; g[f[a], b] = g[f[c], a]$	(function congruence)

◀

Example 2 Determine if the following formula is satisfiable or not

$$F_1 \quad :\Longleftrightarrow \quad f[a, b] = a \;\wedge\; f[f[a, b], b] \neq a$$

Solution. We construct the initial partition by letting each member of the subterm set S_{F_1} be its own class:

$$S_{F_1} = \{\{a\},\ \{b\},\ \{f[a, b]\},\ \{f[f[a, b], b]\}\}$$

From the first conjunct of F_1 we have

$$S_{F_1} = \{\{a,\ f[a, b]\},\ \{b\},\ \{f[f[a, b], b]\}\}$$

Further we have

$$a \sim f[a, b] \;\wedge\; b \sim b \;\Longrightarrow\; f[f[a, b], b] \sim f[a, b] \qquad \text{(function congruence)}$$

Hence

$$S_{F_1} = \{\{a,\ f[a, b],\ f[f[a, b], b]\},\ \{b\}\} \quad \text{(congruence closure of } S_{F_1}\text{)}$$

From here we have that F_1 is unsatisfiable, since by S_{F_1} we have $f[f[a, b], b] \sim a$ and F_1 asserts that $f[f[a, b], b] \neq a$. ◀

Example 3 Determine if the following formula is satisfiable or not

$$F_2 \quad :\iff \quad f[x] = f[y] \ \wedge \ x \neq y$$

Solution. We construct the initial partition by letting each member of the subterm set S_{F_2} be its own class:

$$S_{F_2} = \{\{x\},\ \{y\},\ \{f[x]\},\ \{f[y]\}\}$$

From the first conjunct of F_2 we have

$$S_{F_2} = \{\{x\},\ \{y\},\ \{f[x], f[y]\}\}$$

From here we have that F_2 is satisfiable, since by S_{F_2} we have $x \not\sim y$ and F_1 asserts that $x \neq y$. ◀