On Compositional safety verification with Max-SMT

Author: Fabian Böller
Supervision: David Korzeniewski

RWTH Aachen

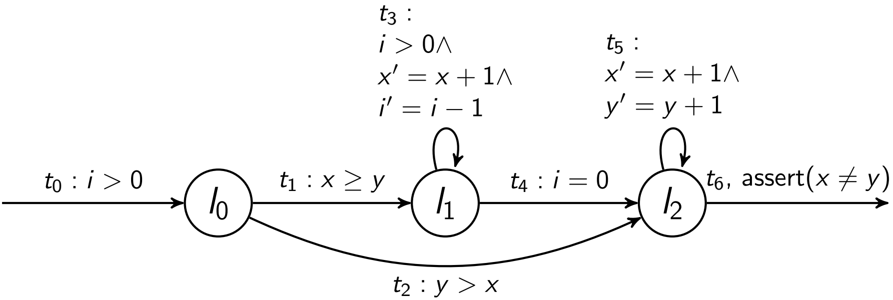
fabian.boeller@rwth-aachen.de

SS 2017

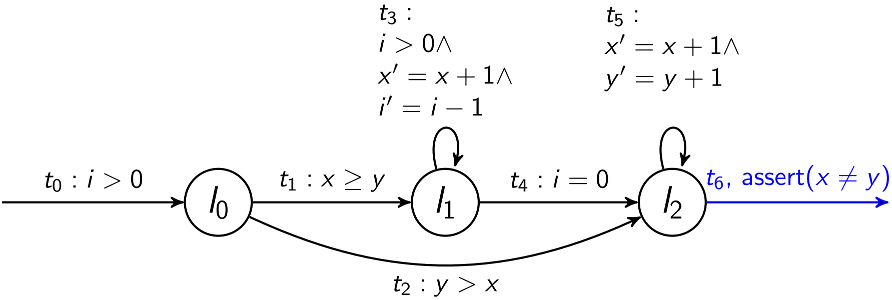
Overview

1. Example execution

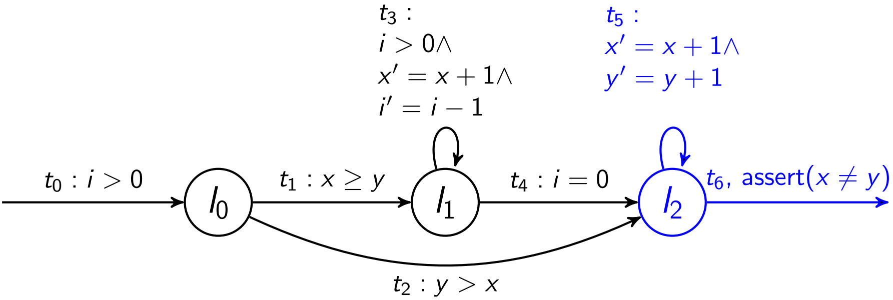
Example program



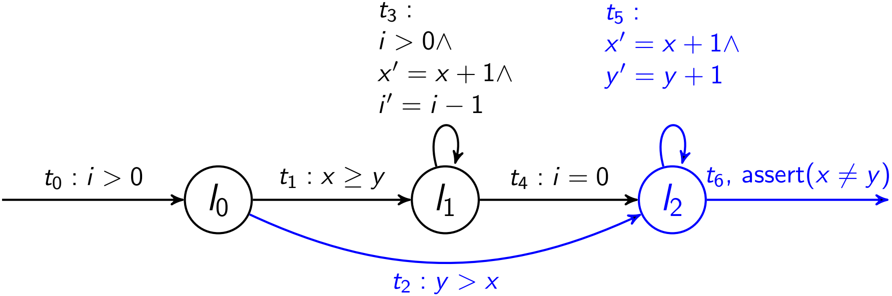
Example execution



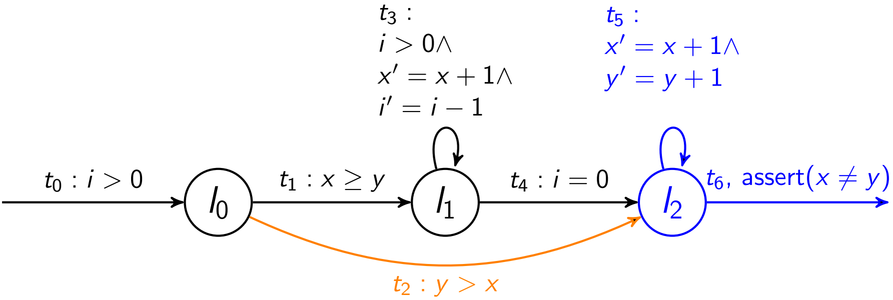
Example execution



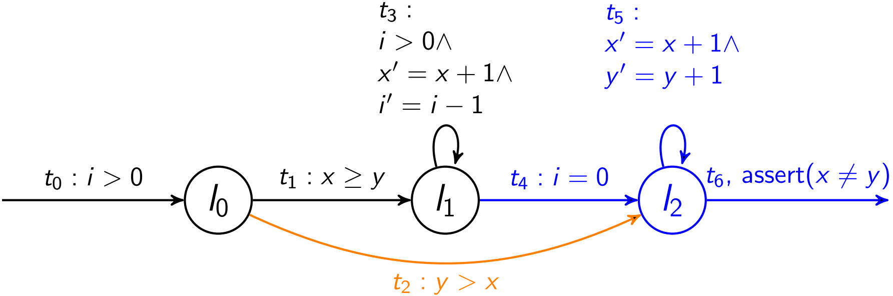
Example execution



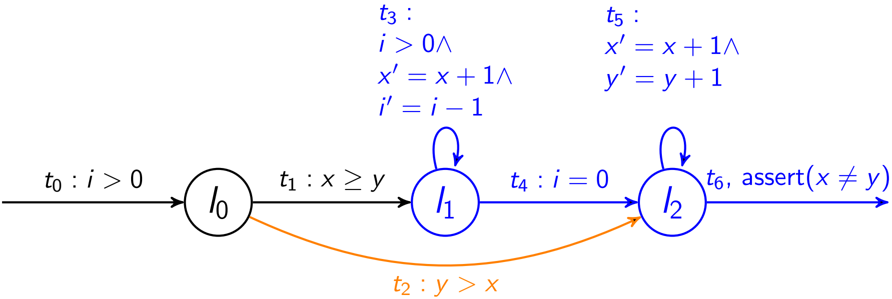
Example execution



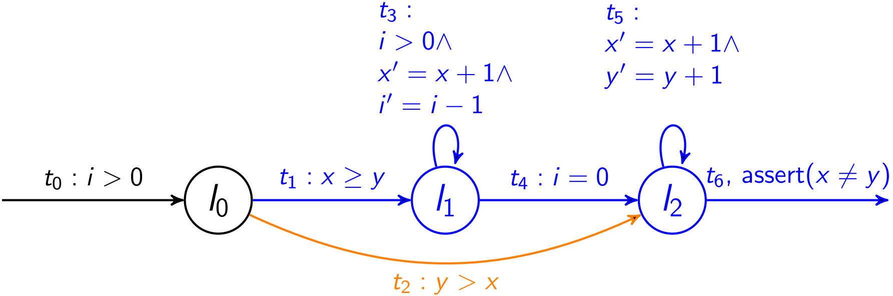
Example execution



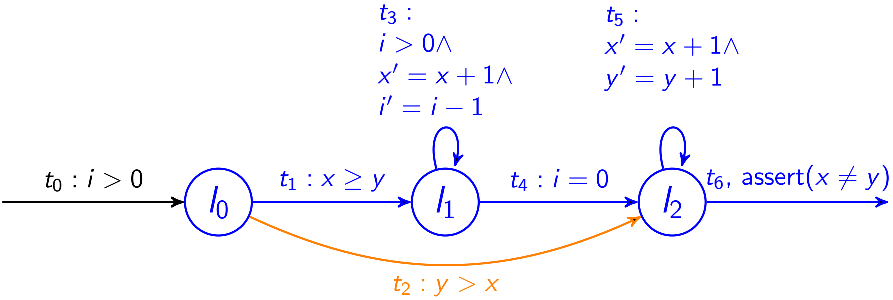
Example execution



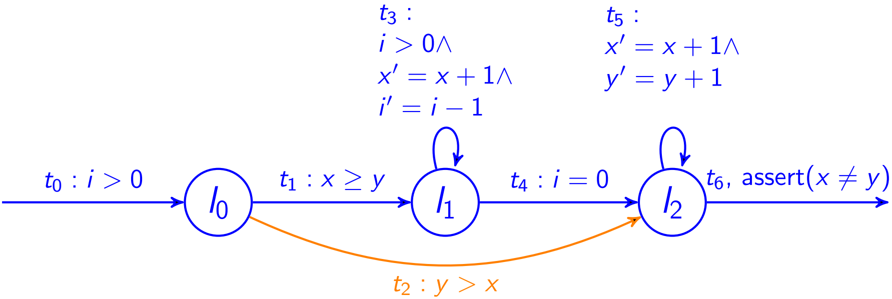
Example execution



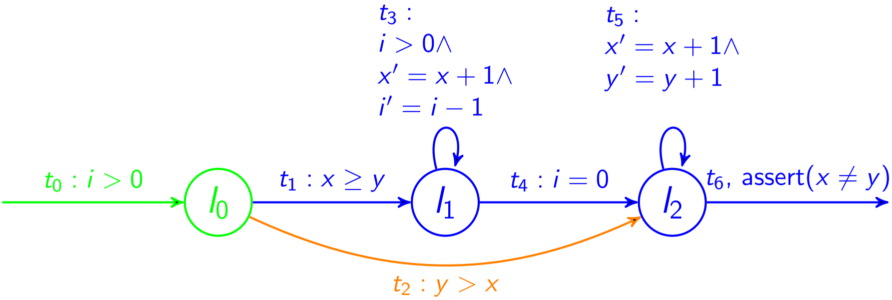
Example execution



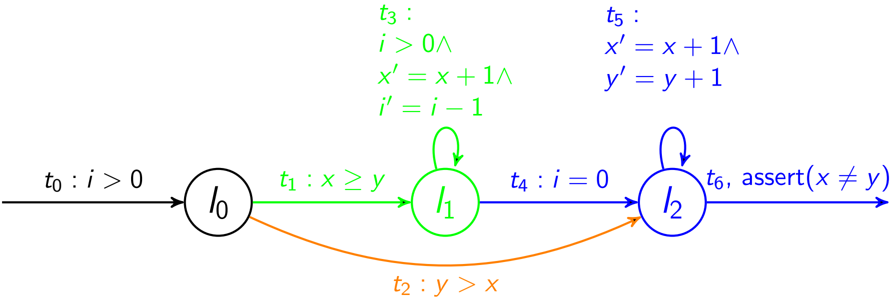
Example execution



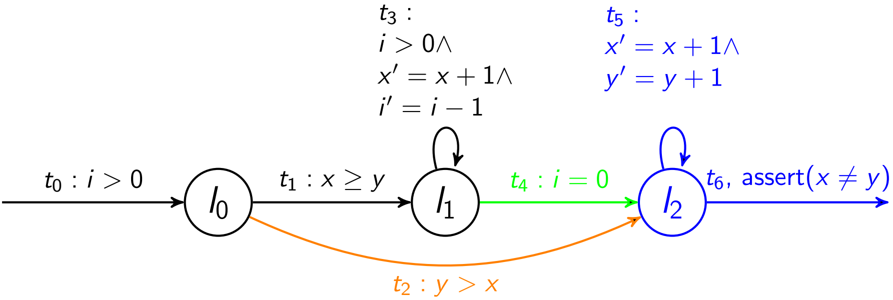
Example execution



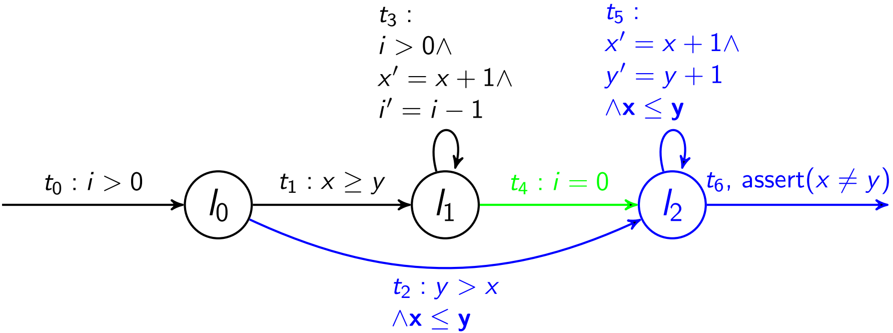
Example execution



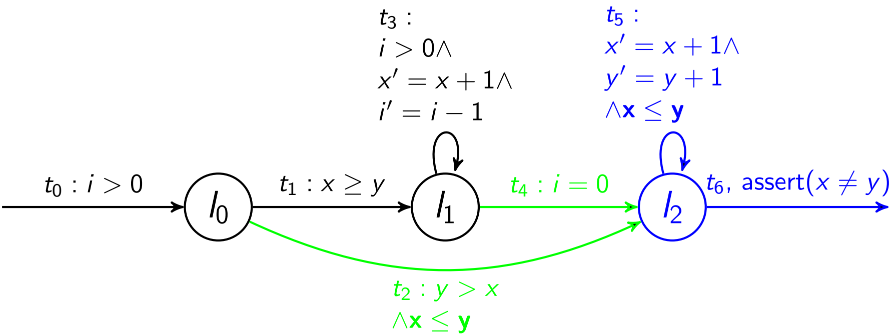
Example execution



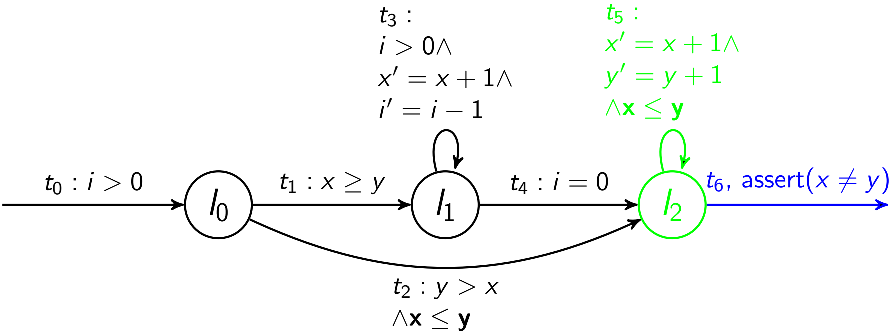
Example execution



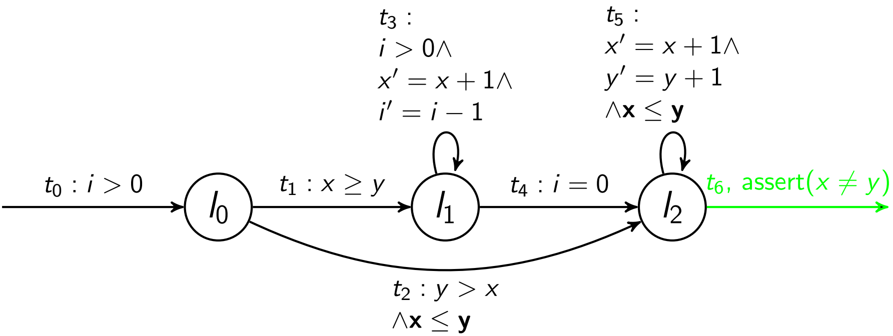
Example execution

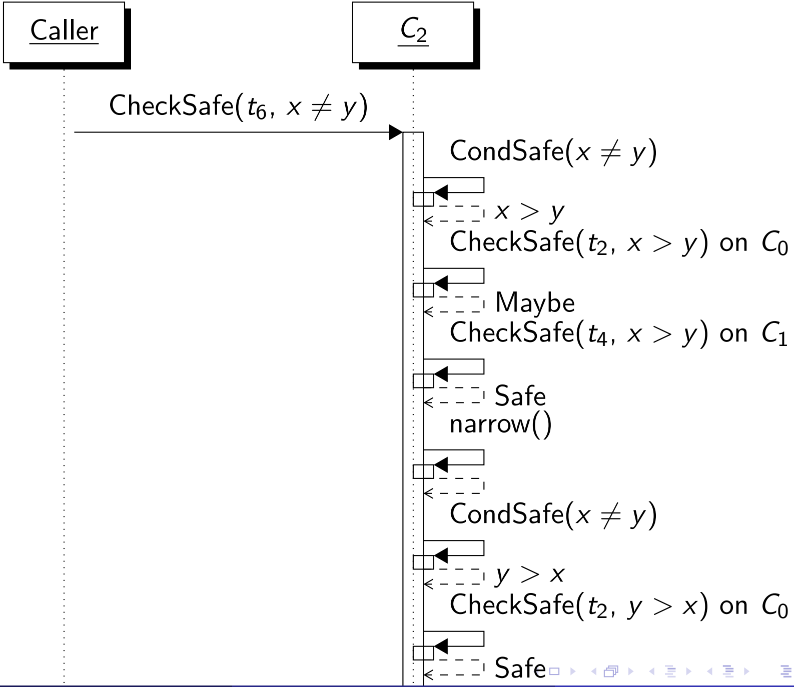


Example execution



Example execution





Caller

C_2

CheckSafe(t_6, $x \neq y$)

CondSafe($x \neq y$)

$x > y$

CheckSafe(t_2, $x > y$) on C_0

Maybe

CheckSafe(t_4, $x > y$) on C_1

Safe

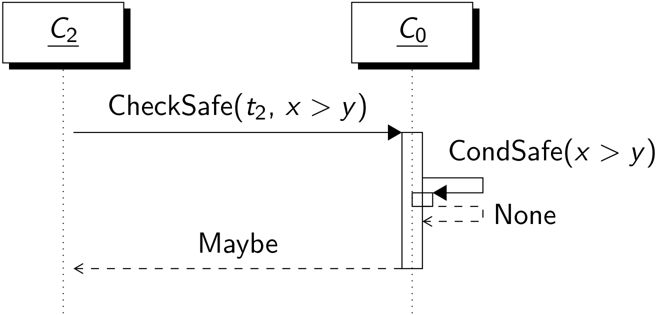
narrow()

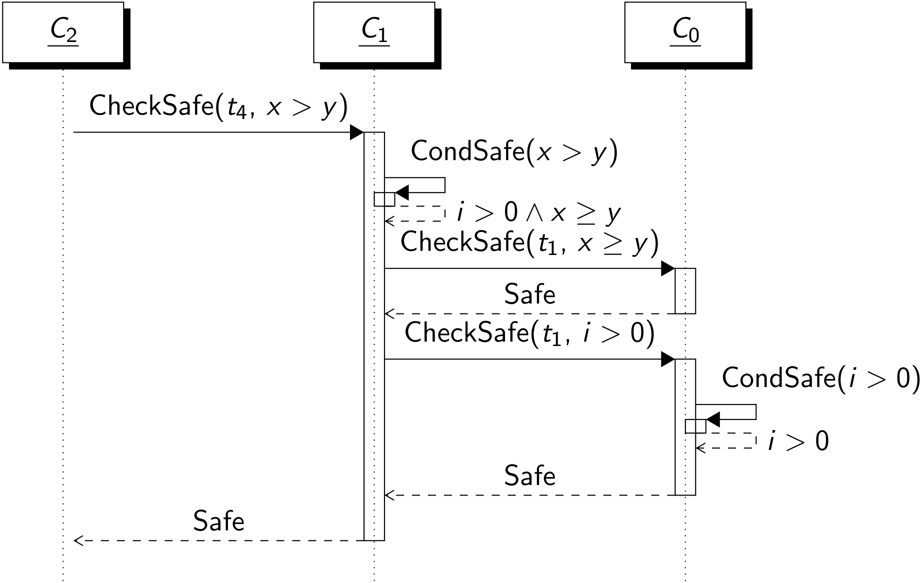
CondSafe($x \neq y$)

$y > x$

CheckSafe(t_2, $y > x$) on C_0

Safe


C_2
C_0
CheckSafe(t_2, $x > y$)
CondSafe($x > y$)
None
Maybe



$\underline{C_2}$

$\underline{C_1}$

$\underline{C_0}$

$\text{CheckSafe}(t_4,\ x > y)$

$\text{CondSafe}(x > y)$

$i > 0 \wedge x \geq y$

$\text{CheckSafe}(t_1,\ x \geq y)$

Safe

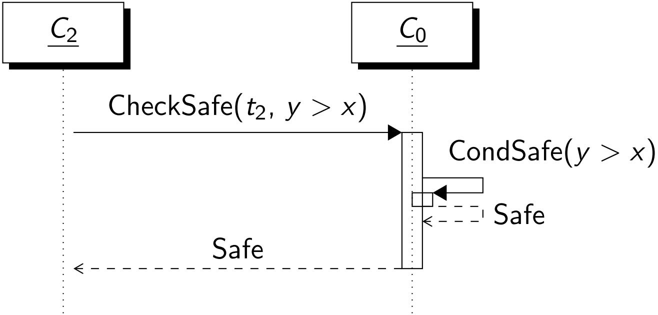
$\text{CheckSafe}(t_1,\ i > 0)$

$\text{CondSafe}(i > 0)$

$i > 0$

Safe

Safe


$\underline{C_2}$
$\underline{C_0}$
CheckSafe(t_2, $y > x$)
CondSafe($y > x$)
Safe
Safe

References

Brockschmidt, Marc and Larraz, Daniel and Oliveras, Albert and Rodriguez-Carbonell, Enric and Rubio, Albert (2015)

Compositional Safety Verification with Max-SMT

Proceedings of FMCAD'15

The End