Limitation-I-Flowsto-Overapproxi

Friday, May 20, 2022 10:28 AM

inthe CFG Analysis: in $x = y - y$.

Semantic dependency $Dep(x^i, y^j, c)$ is traditionally

① over-approximated syntactically by VAR(Ae). and VAR(b).

we can improve by normolize the expression syntactically.

$$VAR(a_1 - a_2) = \{y \mid y \in VAR(a_1) \cup VAR(a_2) \wedge NF(a_1) \neq NF(a_2)\}.$$

$$VAR(b(a_1 = a_2)) = \{y \mid y \in VAR(a_1) \cup VAR(a_2) \wedge NF(a_1) \neq NF(a_2)\}.$$

$x = 1$

if $x = x$

then $y = 1$

else $y = 2$.

or

$x = 1$

if $x = 1$:

then $y = 1$

else $y = 2$

② also over-approximated syntactically by conditional commands:

$x = 2$

if $x > 0$

then $y = 1$

else $y = 1$.