

# IMP

This is the symbolic semantics of IMP enriched with reachability logic.

This semantics receives as input programs generated from reachability formulas. Additionally, the semantics contains the circularities also generated from reachability formulas.

MODULE IMP-SYNTAX

```
SYNTAX  AExp ::= Int
          | Id
          | AExp / AExp [strict]
          | AExp + AExp [strict]
          | AExp - AExp [strict]
          | (AExp) [bracket]

SYNTAX  BExp ::= Bool
          | AExp ≤ AExp [seqstrict]
          | ! BExp [strict]
          | BExp && BExp [strict(1)]
          | (BExp) [bracket]

SYNTAX  Block ::= {}
          | {Smt}
          | Id : Block

SYNTAX  Smt ::= Block
          | Id = AExp ; [strict(2)]
          | if (BExp)Block else Block [strict(1)]
          | while (BExp)Block
          | Smt Smt
          | Id : Smt

SYNTAX  Pgm ::= int Ids ; Smt

SYNTAX  Ids ::= List{Id, ",", ""}

SYNTAX  Pgm ::= #ps (Bag)
```

K tool issues

```
SYNTAX  Int ::= #symInt (Id) [onlyLabel, klabel(#symInt)]

SYNTAX  Int ::= (Int) [bracket]

SYNTAX  X ::= symInt [dummySymInt]
```

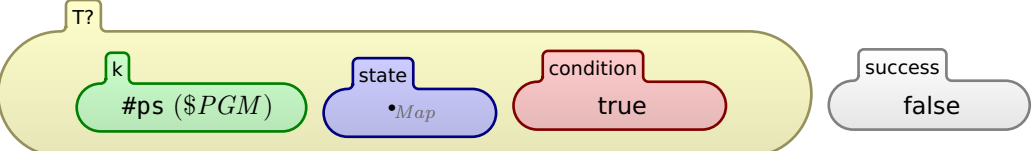
END MODULE

MODULE IMP

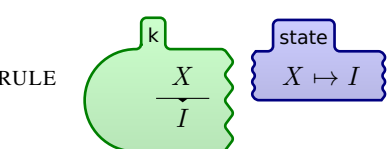
```
SYNTAX  KResult ::= Int
          | Bool
```

The configuration of IMP is enriched with cells <frozen> and <goal>. Cell <ruleConstraints> will store some labels which are meant to block the first application of the circularity rule. The cell <goal> contains the current goal. Whenever multiple rules can be applied to the same configuration, the current goal will be splitted into multiple goals.

CONFIGURATION:



The initial semantics of IMP.



RULE

$$\frac{I1 + I2}{I1 +_{Int} I2}$$

RULE

$$\frac{I1 - I2}{I1 -_{Int} I2}$$

RULE

$$\frac{I1 \leq I2}{I1 \leq_{Int} I2}$$

RULE

$$\frac{! T}{\neg_{Bool} T}$$

RULE

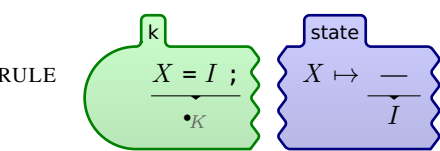
$$\frac{\{\}}{\bullet_K}$$

[structural]

RULE

$$\frac{\{S\}}{S}$$

[structural]



RULE

$$\frac{S1 \ S2}{S1 \frown S2}$$

[structural]

RULE

$$\frac{\text{while } (B)S}{\text{if } (B)\{S \ \text{while } (B)S \ \text{else } \{\}\}}$$

[transition]

RULE

$$\frac{\text{int } \bullet_{ids} \ X, Xs ; \text{---}}{Xs}$$
 requires  $\neg_{Bool}(X \text{ in keys } (\rho))$

RULE

$$\frac{\text{int } \bullet_{ids} \ X ; S}{S}$$

[structural]

Symbolic semantics - the transformed rules

RULE

$$\frac{I1 \ / \ I2}{I1 \div_{Int} I2} \quad \frac{Phi}{Phi \wedge_{Bool} I2 \neq_{Int} 0}$$
 requires  $\text{checkSat } (Phi \wedge_{Bool} (I2 \neq_{Int} 0)) \neq_K \text{"unsat"}$

[transition]

RULE

$$\frac{B1 \ \&\& \ B2}{B2} \quad \frac{Phi}{Phi \wedge_{Bool} B1 ==_{Bool} \text{true}}$$
 requires  $\text{checkSat } (Phi \wedge_{Bool} B1) \neq_K \text{"unsat"}$

[transition]

RULE

$$\frac{B1 \ \&\& \ B2}{\text{false}} \quad \frac{Phi}{Phi \wedge_{Bool} \neg_{Bool} B1}$$
 requires  $\text{checkSat } (Phi \wedge_{Bool} \neg_{Bool} B1) \neq_K \text{"unsat"}$

[transition]

RULE

$$\frac{\text{if } (B)S \ \text{else } \text{---}}{S} \quad \frac{Phi}{Phi \wedge_{Bool} B}$$
 requires  $\text{checkSat } (Phi \wedge_{Bool} B) \neq_K \text{"unsat"}$

[transition, computational]

RULE

$$\frac{\text{if } (B) \text{---} \ \text{else } S}{S} \quad \frac{Phi}{Phi \wedge_{Bool} \neg_{Bool} B}$$
 requires  $\text{checkSat } (Phi \wedge_{Bool} \neg_{Bool} B) \neq_K \text{"unsat"}$

[transition, computational]

These rules must be generated from reachability formulas given as input and added to the semantics at runtime. Since we don't have this possibility now, we added them manually

For each reachability formula given as input we have two corresponding generated rules: - one corresponding to circularity deduction rule - one checking if the final configuration implies the righ-hand side of the formula (corresponding to consequence deduction rule).

```
SYNTAX  Id ::= Token{"a"}
          | Token{"b"}
          | Token{"x"}
          | Token{"y"}
          | Token{"ll0"}
          | Token{"ll1"}
          | Token{"ll2"}
```

```
SYNTAX  Pgm ::= check0
          | check1
          | check2
```

```
SYNTAX  Bag ::= success
```

RULE

$$\frac{(\text{ll0} : \{a = 0 ; b = x ; (\text{ll1} : \text{while } (y \leq b) \{b = b - y ; a = a + 1 ; \})\}) \frown K}{\text{---}} \quad \frac{\text{a} \mapsto A \ \text{b} \mapsto B \ \text{x} \mapsto X \ \text{y} \mapsto Y}{\text{---}} \quad \frac{Psi}{\text{---}}$$
 requires  $\text{fresh } (B') \wedge_{Bool} \text{fresh } (A') \wedge_{Bool} \text{checkSat } (Psi \wedge_{Bool} \neg_{Bool} (0 \leq_{Int} X \wedge_{Bool} 0 <_{Int} Y)) =_K \text{"unsat"}$

[transition]

RULE

$$\frac{(\text{ll1} : \text{while } (y \leq b) \{b = b - y ; a = a + 1 ; \}) \frown K}{\text{---}} \quad \frac{\text{a} \mapsto A \ \text{b} \mapsto B \ \text{x} \mapsto X \ \text{y} \mapsto Y}{\text{---}} \quad \frac{Psi}{\text{---}}$$
 requires  $\text{fresh } (B') \wedge_{Bool} \text{fresh } (A') \wedge_{Bool} \text{checkSat } (Psi \wedge_{Bool} \neg_{Bool} (X ==_{Int} A *_{Int} Y +_{Int} B \wedge_{Bool} B \geq_{Int} 0)) =_K \text{"unsat"}$

RULE

$$\frac{(\text{ll1} : \text{while } (y \leq b) \{b = b - y ; a = a + 1 ; \}) \frown K}{\text{---}} \quad \frac{\text{a} \mapsto A \ \text{b} \mapsto B \ \text{x} \mapsto X \ \text{y} \mapsto Y}{\text{---}} \quad \frac{Psi \wedge_{Bool} X ==_{Int} A' *_{Int} Y +_{Int} B' \wedge_{Bool} B' \geq_{Int} 0 \wedge_{Bool} B' <_{Int} Y}{\text{---}}$$
 requires  $\text{fresh } (B') \wedge_{Bool} \text{fresh } (A') \wedge_{Bool} \text{checkSat } (Psi \wedge_{Bool} \neg_{Bool} (X ==_{Int} A' *_{Int} Y +_{Int} B' \wedge_{Bool} B' \geq_{Int} 0)) =_K \text{"unsat"}$

[transition]

RULE

$$\frac{(\text{ll2} : \{b = b - y ; a = a + 1 ; \}) \frown K}{\text{---}} \quad \frac{\text{a} \mapsto A \ \text{b} \mapsto B \ \text{x} \mapsto X \ \text{y} \mapsto Y}{\text{---}} \quad \frac{Psi}{\text{---}}$$
 requires  $\text{fresh } (B') \wedge_{Bool} \text{fresh } (A') \wedge_{Bool} \text{checkSat } (Psi \wedge_{Bool} \neg_{Bool} (X ==_{Int} A *_{Int} Y +_{Int} B \wedge_{Bool} B \geq_{Int} 0 \wedge_{Bool} Y \leq_{Int} B)) =_K \text{"unsat"}$

RULE

$$\frac{(\text{ll2} : \{b = b - y ; a = a + 1 ; \}) \frown K}{\text{---}} \quad \frac{\text{a} \mapsto A \ \text{b} \mapsto B \ \text{x} \mapsto X \ \text{y} \mapsto Y}{\text{---}} \quad \frac{Psi \wedge_{Bool} (X ==_{Int} A' *_{Int} Y +_{Int} B' \wedge_{Bool} B' \geq_{Int} 0)}{\text{---}}$$
 requires  $\text{fresh } (B') \wedge_{Bool} \text{fresh } (A') \wedge_{Bool} \text{checkSat } (Psi \wedge_{Bool} \neg_{Bool} (X ==_{Int} A' *_{Int} Y +_{Int} B' \wedge_{Bool} B' \geq_{Int} 0)) =_K \text{"unsat"}$

[transition]

RULE

$$\frac{(\text{ll2} : \{b = b - y ; a = a + 1 ; \}) \frown K}{\text{---}} \quad \frac{\text{a} \mapsto A \ \text{b} \mapsto B \ \text{x} \mapsto X \ \text{y} \mapsto Y}{\text{---}} \quad \frac{Psi}{\text{---}}$$
 requires  $\text{checkSat } (Psi \wedge_{Bool} \neg_{Bool} (X ==_{Int} A' *_{Int} Y +_{Int} B' \wedge_{Bool} B' \geq_{Int} 0)) =_K \text{"unsat"}$

[transition]

Utils

RULE

$$\frac{\left( \frac{\text{---}}{\text{---}} \right)}{B}$$

[structural]

END MODULE