Definition of Safety

Günther Wullaert

May 2022

1 Language

1.1 Term and Pools

We inductively define *terms*, *tuples of terms*, and *pools*:

- all numerals, symbolic constants, and variables are terms,[1]
- $f(\boldsymbol{t})$ is a term, if f is a symbolic constant and $\boldsymbol{t}$ is a pool,
- $t_1 \star t_2$ is a term, if $\star$ is among the symbols $+$, $-$, $\times$, $/$ or $..$ and t_1, t_2 are terms,
- $\langle \boldsymbol{t} \rangle$ is a term, if $\boldsymbol{t}$ is a pool,
- $t_1, \dots, t_n$ is a tuple of terms, if $n \geq 0$ and t_i is a term,
- $\dot{t_1}; \dots; \dot{t_n}$ is a pool, if $n \geq 1$ and each $\dot{t_i}$ is a tuple of terms.[2]

[1] R: Define those things.

[2] R: Why not empty?

We inductively define a term to be *numeric* if

- it is a numeral, or
- it has form $t \star u$ where t and u are constant and $\star$ is among the symbols $+$, $-$, $\times$ or $/$.

We define function *eval* to evaluate numeric terms to sets of numerals:

$$
\begin{aligned}
\mathit{eval}(c) &= \{c\} \\
\mathit{eval}(a+b) &= \{x+y \mid x \in \mathit{eval}(a), y \in \mathit{eval}(b)\} \\
\mathit{eval}(a-b) &= \{x-y \mid x \in \mathit{eval}(a), y \in \mathit{eval}(b)\} \\
\mathit{eval}(a*b) &= \{x*y \mid x \in \mathit{eval}(a), y \in \mathit{eval}(b)\} \\
\mathit{eval}(a/b) &= \{x/y \mid x \in \mathit{eval}(a), y \in \mathit{eval}(b), y \neq 0\}
\end{aligned}
$$

We say that a numeric term c is *nonzero* if $0 \notin \mathit{eval}(c)$.

1.2 Atoms and Literals

An *atom* has form $p(\boldsymbol{t})$ where p is a predicate symbol and $\boldsymbol{t}$ is a pool.[3]

[3] R: Define predicate symbols.

A *comparison* has form $t_1 \prec t_2$, where t_1, t_2 are terms and $\prec$ is among the symbols $\leq$, $\geq$, $<$, $>$ or $\neq$.

A *literal* is either an atom or a comparison optionally preceded by the *default negation* symbol $\neg$.

A *conditional literal* has form $l : \dot{l}$, where l is a literal and $\dot{l}$ is a (possibly empty) tuple of literals.

1.3 Aggregates

An *aggregate* has the form

$$\alpha\{\dot{t_1} : \dot{l_1}; \dots ; \dot{t_n} : \dot{l_n}\} \prec s \tag{1}$$

where

- $n \geq 0$,
- α is an aggregate name,
- each $\dot{t_i}$ is a tuple of terms,
- each $\dot{l_i}$ is a tuple of literals,
- $\prec$ is among the symbols $\leq$, $\geq$, $<$, $>$, $=$ or $\neq$, and
- s is a term.

1.4 Rules

A *rule* has form

$$a_1 \vee \dots \vee a_m \leftarrow l_1 \wedge \dots \wedge l_n \tag{2}$$

where $m, n \geq 0$, each a_i is a literal and each l_i is a literal, conditional literal or aggregate.

A *choice rule* has form

$$\{a_1; \dots ; a_m\} \leftarrow l_1 \wedge \dots \wedge l_n \tag{3}$$

where $m, n \geq 0$, each e_i is an atom and each l_i is a literal, conditional literal or aggregate.

2 Safety

The $vars(e)$ function returns all variables for an expression e.
For Example:

$$vars(a(X) = b(Y)) = \{X, Y\}$$

2.1 Terms

2.1.1 Constants

For any numeral n and symbolic constant f

$$pt(n) = pt(f) = dt(n) = dt(f) = \emptyset$$

2.1.2 Variables

For any variable X

$$pt(X) = \{X\}$$
$$dt(X) = \emptyset$$

2.1.3 Tuples

For any tuple of terms $t_1, ..., t_n$

$$pt(t_1, ..., t_n) = pt(t_1) \cup \cdots \cup pt(t_n)$$
$$dt(t_1, ..., t_n) = dt(t_1) \cup \cdots \cup dt(t_n)$$

2.1.4 Pools

For any pool of terms $\dot{t_1}; ...; \dot{t_n}$

$$pt(\dot{t_1}; ...; \dot{t_n}) = pt(\dot{t_1}) \cap \cdots \cap pt(\dot{t_n})$$
$$dt(\dot{t_1}; ...; \dot{t_n}) = dt(\dot{t_1}) \cup \cdots \cup dt(\dot{t_n})$$

2.1.5 Functions

For a term of form $f(\boldsymbol{t})$, where f is a function and $\boldsymbol{t}$ a pool

$$pt(f(\boldsymbol{t})) = pt(\boldsymbol{t})$$
$$dt(f(\boldsymbol{t})) = dt(\boldsymbol{t})$$

2.1.6 Arithmetics

For a term of form $a \star b$, where a, b are terms and one of them is a *constant* and $\star$ is among the symbols +, - or a and b are both *constant* and $\star$ is among the symbols +, -, / or ..

$$pt(a \star b) = pt(a) \cup pt(b)$$
$$dt(a \star b) = dt(a) \cup dt(b)$$

Otherwise for a term of form $a \star b$, where a, b are terms and none of them are *constant* and $\star$ is among the symbols +, -, $\times$, / or ..

$$pt(a \star b) = \emptyset$$
$$pt(a \star b) = vars(a \star b)$$

For a term of form $a \times b$, where a, b are terms and one of them is a *constant* and $0 \in eval(a)$ or $0 \in eval(b)$

$$
\begin{aligned}
pt(a \times b) &= \emptyset \\
dt(a \times b) &= \emptyset
\end{aligned}
$$

Otherwise if $0 \notin eval(a) \cup eval(b)$

$$
\begin{aligned}
pt(a \times b) &= pt(a) \cup pt(b) \\
dt(a \times b) &= dt(a) \cup dt(b)
\end{aligned}
$$

For a term of form $-t$, where t is a term

$$
\begin{aligned}
pt(-t) &= pt(t) \\
dt(-t) &= dt(t)
\end{aligned}
$$

2.2 Atoms and Literals

2.2.1 Atoms and Literals

For an literal of form *not* a, where a is an atom

$$dep(not\ a) = \{(\emptyset, vars(a))\}$$

For an atom of form $p(\boldsymbol{t})$, where $\boldsymbol{t}$ is a pool

$$dep(p(\boldsymbol{t})) = \{(pt(\boldsymbol{t}), \emptyset), (\emptyset, dt(\boldsymbol{t}))\}$$

2.2.2 Comparison Literals

For an comparison literal of form $a \prec b$, where a and b are terms and $\prec$ is among the symbols $\leq, \geq, <, >, \neq$

$$dep(a \prec b) = \{(\emptyset, vars(a \prec b))\}$$

For an comparison literal of form $a = b$, where a and b are terms

$$dep(a = b) = \{(pt(a), vars(b)), (pt(b), vars(a)), (\emptyset, dt(a) \cup dt(b))\}$$

For an literal of form *not* $a \prec b$, where a and b are terms

$$
\begin{aligned}
dep(not\ a = b) &= dep(a \neq b) \\
dep(not\ a \neq b) &= dep(a = b) \\
dep(not\ a \leq b) &= dep(a > b) \\
dep(not\ a > b) &= dep(a \leq b) \\
dep(not\ a \geq b) &= dep(a < b) \\
dep(not\ a < b) &= dep(a \geq b)
\end{aligned}
$$

2.2.3 Conditional Literals

For a conditional literal of form $\dot{t} : \dot{c}$, where t is a tuple of terms and c is a tuple of comparison literals and atoms, where G is the set of variables occuring globally in it.

$$dep(\dot{t} : \dot{c}) = \{(\emptyset, G \cup vars(s))\}$$

For an conditional literal of form $\dot{t} : \dot{c}$, where t is a tuple of terms and c is a tuple of comparison literals and atoms in a local context

$$dep_l(\dot{t} : \dot{c}) = \{(\emptyset, vars(\dot{t}))\} \cup \bigcup_{e \in \dot{c}} dep(e)$$

2.3 Aggregates

For a aggragate a occuring in a rule, where G is the set of variables occuring globally in it. We define $elem(a)$ to return a set of elements in a as

$$elem(a) = \{\dot{t_1} : \dot{L_1}, \ldots, \dot{t_n} : \dot{L_n}\}$$

For an aggregate element of form $\dot{t_1} : \dot{L_1}$, where t_1 is a tuple of terms and $\dot{L_1}$ is a tuple of comparison literals and atoms

$$dep(\dot{t_1} : \dot{L_1}) = \{(\emptyset, vars(\dot{t_1}))\} \cup \bigcup_{l \in \dot{L_1}} dep(l)$$

For an aggregate a, where $\prec$ is $=$

$$dep(a) = \{(pt(s), G), (\emptyset, dt(s) \cup G)\}$$

Otherwise

$$dep(a) = \{(\emptyset, G \cup vars(s))\}$$

2.4 Rule

For a rule r in the form of (2) the following holds:

$$dep(r) = \{(\emptyset, vars(H_1 \vee ... \vee H_k))\} \cup dep(B_1) \cup ... \cup dep(B_m)$$

2.5 Choice Rule

For a choice rule r in the form of (3) the following holds:

$$dep(r) = \{(\emptyset, vars(e_1 \vee ... \vee e_k))\} \cup dep(B_1) \cup ... \cup dep(B_m)$$

2.6 Safety Definition

We define operator C_r for a rule r applied to a set of variables V as

$$C_r(V) = \bigcup_{(P,D)\in dep(r), D\subseteq V} P.$$

A rule r is globally safe if $vars(r)$ is the least fixed point of C_r and each aggregate and conditional literal is locally safe.
We define operator $C_{e,G}$ for an element e of an aggregate a applied to a set of variables V as

$$C_{e,G}(V) = G \cup \bigcup_{(P,D)\in dep(e), D\subseteq V} P.$$

a is locally safe if for each element $e \in elem(a)$, $vars(e)$ is the least fixed point of $C_{e,G}$
We define operator $C_{l,G}$ for an conditional literal l applied to a set of variables V as

$$C_{l,G}(V) = G \cup \bigcup_{(P,D)\in dep_l(l), D\subseteq V} P.$$

l is locally safe if $vars(l)$ is the least fixed point of $C_{l,G}$

3 Other Examples

$$\begin{aligned}
dep(p(X, Y+Y)) &= \{(pt(X, Y+Y), \emptyset), (\emptyset, dt(X, Y+Y))\} \\
&= \{(pt(X) \cup pt(Y+Y), \emptyset), (\emptyset, dt(X) \cup dt(Y+Y))\} \\
&= \{(\{X\} \cup \emptyset, \emptyset), (\emptyset, \emptyset \cup vars(Y+Y))\} \\
&= \{(\{X\}, \emptyset), (\emptyset, \{Y\})\}
\end{aligned}$$

This article was processed using the comments style on July 12, 2022.
There remain 3 comments to be processed.