String Constants Abstract Domain

Ben Hardekopf

1 Constants Lattice

Let Σ be an alphabet and $\Sigma*$ be the set of all strings using that alphabet. Define $S = \{\top, \bot\} \cup \Sigma*$. The constants lattice is $(S, \sqsubseteq, \sqcup, \sqcap)$ where for $s_1, s_2 \in S$ and $str_1, str_2 \in \Sigma*$ s.t. $str_1 \neq str_2$:

- $\sqcup$ is defined as
  - $\bot \sqcup s_1 = s_1 \sqcup \bot = s_1$
  - $\top \sqcup s_1 = s_1 \sqcup \top = \top$
  - $str_1 \sqcup str_1 = str_1$
  - $str_1 \sqcup str_2 = \top$
- $\sqcap$ is defined as
  - $\bot \sqcap s_1 = s_1 \sqcap \bot = \bot$
  - $\top \sqcap s_1 = s_1 \sqcap \top = s_1$
  - $str_1 \sqcap str_1 = str_1$
  - $str_1 \sqcap str_2 = \bot$
- $\sqsubseteq$ is defined as $s_1 \sqsubseteq s_2$ iff $s_1 \sqcup s_2 = s_2$.

1.1 Lattice Properties

The lattice is infinitely wide because it contains all possible strings, but has a finite height (at most three elements in a chain) and thus is noetherian.

2 Abstraction and Concretization Functions

$$\alpha : \mathcal{P}(\Sigma*) \to S$$

$$\alpha(x) = \begin{cases} \bot & \text{if } x = \{\} \\ str & \text{if } x = \{str\} \\ \top & \text{otherwise} \end{cases}$$

$$\gamma : S \to \mathcal{P}(\Sigma *)$$

$$\gamma(x) = \begin{cases} \{\} & \text{if } x = \bot \\ \{str\} & \text{if } x = str \\ \Sigma * & \text{if } x = \top \end{cases}$$

3 Abstract + Operator

Define $\widehat{+}$ as:

$\widehat{+}$	$\bot$	str_2	$\top$
$\bot$	$\bot$	$\bot$	$\bot$
str_1	$\bot$	$str_1 + str_2$	$\top$
$\top$	$\bot$	$\top$	$\top$

$\widehat{+}$ is monotone if $a \sqsubseteq a'$ and $b \sqsubseteq b'$ implies $a \widehat{+} b \sqsubseteq a' \widehat{+} b'$. Consider the following cases in order (i.e., if multiple cases apply use the first case listed below):

Case 1. a' or b' is $\bot$. Then because $a \sqsubseteq a'$ and $b \sqsubseteq b'$, at least one of a and b are $\bot$. By definition of $\widehat{+}$, both $a \widehat{+} b$ and $a' \widehat{+} b'$ are $\bot$. QED.

Case 2. a' or b' is $\top$. By definition of $\widehat{+}$, $a' \widehat{+} b' = \top$. QED.

Case 3. $a' = str_1$, $b' = str_2$, $a, b \neq \bot$. Then $a = a'$ and $b = b'$, hence $a \widehat{+} b = a' \widehat{+} b'$. QED.

4 Abstract ≤ Operator

Define $\widehat{\leq}$ as:

$\widehat{\leq}$	$\bot$	str_2	$\top$
$\bot$	$\bot$	$\bot$	$\bot$
str_1	$\bot$	$str_1 \leq str_2$	$\top$
$\top$	$\bot$	$\top$	$\top$

$\widehat{\leq}$ is monotone if $a \sqsubseteq a'$ and $b \sqsubseteq b'$ implies $a \widehat{\leq} b \sqsubseteq a' \widehat{\leq} b'$. The proof is the same as for $\widehat{+}$ above, except substituting $\widehat{\leq}$ for $\widehat{+}$.