

# 1 CoPylot

## 1.1 Grammar

The grammar of the language to be analyzed appears in Figure 2.

We assume throughout the rest of this document that a fixed program  $\hat{S}$  is under analysis. *(TODO: describe here the idea of a bijection between labels and statements in this fixed program. – ZP)*

## 1.2 Control Flow

The grammar of control flow graphs appears in Figure 3. *(Discuss construction of initial graph. – ZP)*

We write  $\hat{o} \stackrel{?}{\blacktriangleleft} \hat{o}'$  to denote  $(\hat{o} \blacktriangleleft \hat{o}' \in \hat{G}$  when  $\hat{G}$  is understood from context. Likewise, we write  $\hat{o} \stackrel{?}{\ll} \hat{o}'$  to denote  $(\hat{o} \ll \hat{o}' \in \hat{G}$  when  $\hat{G}$  is understood from context.

We define a relation  $\longrightarrow^1$  to perform control flow graph closure.

**Definition 1.3.** Let  $\hat{G} \longrightarrow^1 \hat{G}'$  be the least relation satisfying the rules appearing in Figure 4. Throughout these rules, the predicates  $\stackrel{?}{\ll}$  and  $\stackrel{?}{\blacktriangleleft}$  refer to graph  $\hat{G}$ .

## 1.3 Value Lookup

The value lookup function uses the additional grammar in Figure 5.

**Definition 1.4.** Given a control-flow graph  $\hat{G}$ , let  $\hat{G}(\hat{o}_0, \hat{K})$  be the function returning the least set  $\hat{V}$  which satisfies the following conditions:

### 1. Value Manipulation

- (a) RESULT  
If  $\hat{K} = [\hat{v}]$ , then  $\hat{v} \in \hat{V}$ .

### 2. Variable Lookup

- (a) VALUE DISCOVERY  
If  $\hat{o}_1 \stackrel{?}{\ll} \hat{o}_0$ ,  $\hat{o}_1 = \hat{\ell}_1 : \hat{\ell}_2 : \hat{x} = \hat{v}$ , and  $\hat{K} = [\hat{x}] \parallel \hat{K}'$ , then  $\hat{G}(\hat{o}_1, [\hat{v}] \parallel \hat{K}') \subseteq \hat{V}$ .

- (b) VALUE SKIP  
If  $\hat{o}_1 \stackrel{?}{\ll} \hat{o}_0$ ,  $\hat{o}_1 = \hat{\ell}_1 : \hat{\ell}_2 : \hat{x}' = \hat{v}$ ,  $\hat{K} = [\hat{x}] \parallel \hat{K}'$ , and  $\hat{x} \neq \hat{x}'$ , then  $\hat{G}(\hat{o}_1, \hat{K}) \subseteq \hat{V}$ .

- (c) VALUE ALIASING  
If  $\hat{o}_1 \stackrel{?}{\ll} \hat{o}_0$ ,  $\hat{o}_1 = \hat{\ell}_1 : \hat{\ell}_2 : \hat{x} = \hat{x}'$ , and  $\hat{K} = [\hat{x}] \parallel \hat{K}'$ , then  $\hat{G}(\hat{o}_1, [\hat{x}'] \parallel \hat{K}) \subseteq \hat{V}$ .

$x$	$::=$	$\text{ALPHANUMERIC} \mid \star\text{ALPHANUMERIC}$	<i>variables</i>
$\ell$	$::=$	$\ell \mid \text{END}$	<i>labels</i>
$T$	$::=$	$[t, \dots]$	<i>stack</i>
$t$	$::=$	$\ell \times S$	<i>stack frames</i>
$S$	$::=$	$[s, \dots]$	<i>programs</i>
$d$	$::=$	$x = e \mid \text{def } x(x, \dots) = \{S\} \mid \text{return } x \mid \text{goto } \ell \mid \text{goto } \ell \text{ if not } x$	<i>directives</i>
$B$	$::=$	$\{x \mapsto m, \dots\}$	<i>bindings</i>
$H$	$::=$	$\{m \mapsto v, \dots\}$	<i>heap</i>
$v$	$::=$	$\mathbb{Z} \mid \langle m, \text{def } (x) \rightarrow S \rangle \mid \langle m, m, \text{def } (x) \rightarrow S \rangle \mid [m, \dots] \mid (m, \dots) \mid B \mid \mathfrak{F} \mid \langle m, \mathfrak{M} \rangle$	<i>values</i>
$e$	$::=$	$v \mid x \mid x(x, \dots) \mid [x, \dots] \mid (x, \dots)$	<i>expressions</i>
$P$	$::=$	$m \mapsto m$	<i>parental map</i>
$m$			<i>memory locations</i>
$\mathfrak{F}$			<i>magic functions</i>
$\mathfrak{M}$			<i>magic methods</i>

**Definition 1.1.**

$$\text{BIND}(H, m_0, x, m) = H' \text{ such that } B = H.B' = B[x \mapsto m], H' = H[m_0 \mapsto B']$$

**Definition 1.2.**

$$\text{BIND}(H, m_0, x_1, m_1, \dots, x_n, m_n) = H' \text{ such that } B = H.B' = B[x \mapsto m], H' = H[m_0 \mapsto B']$$

LITERAL ASSIGNMENT

$$\frac{S(\ell) = \ell : \ell' : x = v \quad B_{\text{obj}} = \{\star x_{\text{value}} \mapsto m\} \quad H' = H[m \mapsto v, m' \mapsto B_{\text{obj}}] \quad m, m' \notin H \quad \text{BIND}(H', m_0, x, m') = H'' \quad \ell \stackrel{S}{\blacktriangleleft} \ell''}{[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S \rangle] \parallel T, H'', P, m_0}$$

NAME ASSIGNMENT

$$\frac{S(\ell) = \ell : \ell' : x_1 = v_2 \quad m = \text{LOOKUP}(m_0, P, H, x_2) \quad \text{BIND}(H, m_0, x_1, m) = H' \quad \ell \stackrel{S}{\blacktriangleleft} \ell''}{[\langle \ell, S \rangle] \parallel T, H, \text{oparent}, m_0 \longrightarrow^1 [\langle \ell'', S \rangle] \parallel T, H', \text{oparent}, m_0}$$

LIST ASSIGNMENT

$$\frac{S(\ell) = \ell : \ell' : x = [x_1, \dots, x_n] \quad \forall i \in \{1, \dots, n\}, m_i = \text{LOOKUP}(m_0, P, H, x_i) \quad v = [m_1, \dots, m_2] \quad B_{\text{obj}} = \{\star x_{\text{value}} \mapsto m\} \quad H' = H[m \mapsto v, m' \mapsto B_{\text{obj}}] \quad m, m' \notin H \quad \text{BIND}(H', m_0, x, m') = H'' \quad \ell \stackrel{S}{\blacktriangleleft} \ell''}{\langle \ell, S \rangle \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S \rangle] \parallel T, H'', P, m_0}$$

TUPLE ASSIGNMENT

$$\frac{S(\ell) = \ell : \ell' : x = (x_1, \dots, x_n) \quad \forall i \in \{1, \dots, n\}, m_i = \text{LOOKUP}(m_0, P, H, x_i) \quad v = (m_1, \dots, m_2) \quad B_{\text{obj}} = \{\star x_{\text{value}} \mapsto m\} \quad H' = H[m \mapsto v, m' \mapsto B_{\text{obj}}] \quad m, m' \notin H \quad \text{BIND}(H', m_0, x, m') = H'' \quad \ell \stackrel{S}{\blacktriangleleft} \ell''}{\langle \ell, S \rangle \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S \rangle] \parallel T, H'', P, m_0}$$

FUNCTION ASSIGNMENT

$$\frac{S(\ell) = \ell : \ell' : x_1 = \text{def } (x_2, \dots, x_n) = \{S\} \quad v = \langle \eta, \text{def } (x_2, \dots, x_n) \rightarrow S \rangle \quad B_{\text{obj}} = \{\star x_{\text{value}} \mapsto m\} \quad H' = H[m \mapsto v, m' \mapsto B_{\text{obj}}] \quad m, m' \notin H \quad \text{BIND}(H', m_0, x_1, m') = H'' \quad \ell \stackrel{S}{\blacktriangleleft} \ell''}{[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S \rangle] \parallel T, H'', P, m_0}$$

FUNCTION CALL ASSIGNMENT

$$\begin{array}{c}
S(\ell) = \ell : \ell' : x_1 = x_2(x_3, \dots, x_n) \\
m = \text{LOOKUP}(m_0, P, H, x_2) \quad H[m] = \langle m'_0, \text{def } (x'_3, \dots, x'_n) \mapsto S' \rangle \\
m'_0 \notin H \quad H' = H[m'_0 \mapsto \{ \}] \quad \forall i, 3 \leq i \leq n, m' = \text{LOOKUP}(m_0, P, H, x_i) \\
\text{BIND}(H', m'_0, x_i, m_i, \dots, x_n, m_n) = H'' \\
P' = P \cup \{m'_0 \mapsto m'_0\} \quad S' = [\ell'' : \ell''' : d] \\
\hline
[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S' \rangle, \langle l, S \rangle] \parallel T, H'', P', m''_0
\end{array}$$

ATTRIBUTE ASSIGNMENT

$$\begin{array}{c}
S(\ell) = \ell : obl' : x_1 = x_2.x_3 \quad m = \text{LOOKUP}(m_0, P, H, x_2) \\
m[x_3] = m' \quad m' \notin H \quad H[m'] = B \quad \text{BIND}(H, m_0, x_1, m') = H' \quad \ell \stackrel{s}{\blacktriangleleft} \ell^{*'} \\
\hline
[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell^{*'}, S \rangle] \parallel T, H', P, m_0
\end{array}$$

METHOD ASSIGNMENT

$$\begin{array}{c}
S(\ell) = \ell : obl' : x_1 = x_2.x_3 \quad m = \text{LOOKUP}(m_0, P, H, x_2) \\
m[x_3] = m' \quad H[m'] = \langle m_0, m, \text{def } x_4(x_5, \dots) \rightarrow S' \rangle \\
B_{\text{obj}} = \{ \star x_{\text{value}} \mapsto m' \} \quad H' = H[m'' \mapsto B_{\text{obj}}] \\
m', m', m \notin H \quad \text{BIND}(H', m_0, x_1, m'') = H'' \quad \ell \stackrel{s}{\blacktriangleleft} \ell^{*'} \\
\hline
[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell^{*'}, S \rangle] \parallel T, H'', P, m_0
\end{array}$$

MAGIC METHOD ASSIGNMENT

$$\begin{array}{c}
S(\ell) = \ell : obl' : x_1 = x_2.x_3 \quad m = \text{LOOKUP}(m_0, P, H, x_2) \quad m[x_3] = m' \\
H[m'] = \langle m'', \mathfrak{M} \rangle \quad B_{\text{obj}} = \{ \star x_{\text{value}} \mapsto m' \} \quad H' = H[m'' \mapsto B_{\text{obj}}] \\
m', m', m \notin H \quad \text{BIND}(H', m_0, x_1, m'') = H'' \quad \ell \stackrel{s}{\blacktriangleleft} \ell^{*'} \\
\hline
[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell^{*'}, S \rangle] \parallel T, H'', P, m_0
\end{array}$$

RAISE EXCEPTION CAUGHT

$$\begin{array}{c}
S(\ell) = \ell : \ell' : \text{raise } x \quad T = [\langle \ell_1, S_1 \rangle, \dots, \langle \ell_n, S_n \rangle] \\
\ell_1 = \ell' \quad \forall i, 1 \leq i \leq k, k \leq n, \text{CATCH}(\langle \ell_i, S_i \rangle) = \text{undefined} \\
\text{CATCH}(\langle \ell_{k+1}, S_{k+1} \rangle) = \ell', x' \\
m = \text{LOOKUP}(m_0, P, H, x) \quad \text{BIND}(H, m_0, x', m) = H' \quad \ell_{k+1}' \stackrel{s_{k+1}}{\blacktriangleleft} \ell^{*''} \\
\hline
[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell^{*''}, S_{k+1} \rangle] \parallel T, H', P, m_0
\end{array}$$

RAISE EXCEPTION ESCAPED

$$\begin{array}{c}
S(\ell) = \ell : \ell' : \text{raise } x \quad T = [\langle \ell_1, S_1 \rangle, \dots, \langle \ell_n, S_n \rangle] \\
\ell_1 = \ell' \quad \forall i, 1 \leq i \leq n, \text{CATCH}(\langle \ell_i, S_i \rangle) = \text{undefined} \\
\hline
[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [ \, , H, P, m_0
\end{array}$$

PASS

$$\begin{array}{c}
S(\ell) = \ell : \ell' : \text{pass} \quad \ell \stackrel{s}{\blacktriangleleft} \ell^{*''} \\
\hline
[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell^{*''}, S \rangle] \parallel T, H, P, m_0
\end{array}$$

3  
Figure 1: Operation Semantics (cont.)

$$\begin{array}{c}
\text{RETURN} \\
\frac{S(\ell) = \ell : \ell' : \text{return} \quad T = [t, \langle \ell'', S' \rangle] \parallel T' \quad m'_0 = P[m_0] \quad \ell'' \overset{S'}{\blacktriangleleft} \ell'''}{[t, \langle \ell'', S' \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S' \rangle] \parallel T', H, P, m'_0} \\
\\
\text{RETURN WITH ARGUMENTS} \\
\frac{S(\ell) = \ell : \ell' : \text{return } x \quad T = [t, \langle \ell'', S' \rangle] \parallel T' \quad m = \text{LOOKUP}(m_0, P, H, x) \quad m'_0 = P[m_0] \quad \text{BIND}(H, m'_0, x_1, m) = H' \quad \ell'' \overset{S'}{\blacktriangleleft} \ell'''}{[t, \langle \ell'', S' \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S' \rangle] \parallel T, H', P, m'_0} \\
\\
\text{GOTO} \\
\frac{S(\ell) = \ell : \ell' : \text{goto } \ell'' \quad S = [\ell'' : \ell''' : d] \parallel S'}{[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S \rangle] \parallel T, H, P, m_0} \\
\\
\text{GOTOIFNOT} \\
\frac{S(\ell) = \ell : \ell' : \text{goto } \ell'' \text{ if not } x \quad m = \text{LOOKUP}(m_0, P, H, x) \quad H[m] = \text{FALSE} \quad S = [\ell'' : \ell''' : d] \parallel S'}{[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell'', S \rangle] \parallel T, H, P, m_0} \\
\\
\text{NAME STATEMENT} \\
\frac{S(\ell) = \ell : \ell' : e \quad \forall x \in e \exists B[x] \quad \ell \overset{S'}{\blacktriangleleft} \ell''}{[\langle \ell, S \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell', S \rangle] \parallel T, H, P, m_0} \\
\\
\text{END OF FUNCTION} \\
\frac{T = [\langle \text{END}, S \rangle, \langle \ell, S' \rangle] \parallel T' \quad m'_0 = P[m_0] \quad \ell \overset{S'}{\blacktriangleleft} \ell'}{[\langle \text{END}, S \rangle, \langle \ell, S' \rangle] \parallel T, H, P, m_0 \longrightarrow^1 [\langle \ell', S' \rangle] \parallel T', H, P, m'_0} \\
\\
\text{END OF PROGRAM} \\
\frac{T = [(\text{END}, t)]}{T, H, P, m_0 \longrightarrow^1 [], H, P, m_0}
\end{array}$$

Figure 1: Operation Semantics (cont.)

$$\begin{array}{lll}
\hat{S} & ::= & [\hat{s}, \dots] & \text{abstract programs} \\
\hat{s} & ::= & \hat{\ell} : \hat{\ell} : \hat{d} & \text{abstract statements} \\
\hat{d} & ::= & \hat{x} = \hat{v} \mid \hat{x} = \hat{x} & \text{abstract directives} \\
\hat{v} & ::= & \text{int}^+ \mid \text{int}^- \mid \text{int}^0 & \text{abstract values} \\
\hat{x} & & & \text{abstract variables} \\
\hat{\ell} & & & \text{abstract labels}
\end{array}$$

Figure 2: Normalized Python Language Grammar

$$\begin{array}{lll}
\hat{G} & ::= & \{\hat{g}, \dots\} & \text{control flow graphs} \\
\hat{g} & ::= & \hat{o} \blacktriangleleft^? \hat{o} \mid \hat{o} \ll \hat{o} & \text{control flow graph edge} \\
\hat{o} & ::= & \text{START} \mid \text{END} \mid \hat{s} & \text{control flow graph nodes}
\end{array}$$

Figure 3: Control Flow Graph Grammar

$$\begin{array}{ll}
\text{LEXICAL START} & \text{LITERAL ASSIGNMENT} \\
\frac{\text{START} \blacktriangleleft^? \hat{o}}{\hat{G} \longrightarrow^1 \hat{G} \cup \{\text{START} \ll \hat{o}\}} & \frac{\hat{o}_1 = (\hat{x} = \hat{v}) \quad \hat{o}_1 \blacktriangleleft^? \hat{o}_2}{\hat{G} \longrightarrow^1 \hat{G} \cup \{\hat{o}_1 \ll \hat{o}_2\}} \\
\\
\text{VARIABLE ACCESSIBLE} & \\
\frac{\hat{o}_1 = (\hat{x} = \hat{x}') \quad \hat{o}_1 \blacktriangleleft^? \hat{o}_2 \quad \hat{v} \in \hat{G}(\hat{o}_1, [\hat{x}']) \quad \hat{v} \neq \text{UNDEFINED}}{\hat{G} \longrightarrow^1 \hat{G} \cup \{\hat{o}_1 \ll \hat{o}_2\}} & 
\end{array}$$

Figure 4: Control Flow Graph Closure

$$\begin{array}{lll}
\hat{K} & ::= & [\hat{k}, \dots] & \text{lookup stacks} \\
\hat{k} & ::= & \hat{x} \mid \hat{v} \mid \text{CAPTURE}(\mathbb{N}) \mid \text{JUMP}(\hat{o}) & \text{lookup stack elements}
\end{array}$$

Figure 5: Value Lookup Grammar