

# Electronic Appendix to “Input Invariants”

Dominic Steinhöfel

CISPA Helmholtz Center for Information Security  
Saarbrücken, Germany  
dominic.steinhofel@cispa.de

Andreas Zeller

CISPA Helmholtz Center for Information Security  
Saarbrücken, Germany  
zeller@cispa.de

In this electronic appendix to our paper “Input Invariants” [3], we provide additional examples, formal definitions, theorems, and proof sketches. Furthermore, we show the invariants that ISLearn mined in our evaluation (RQ3). For more information on the ISLa language, we also refer to the ISLa language specification [2].

## 2 ISLa by Example

In Section 2, we discussed the semantic properties *def-use* and *redefinition* along the XML language. Apart from those, there are two other re-occurring *generic* constraints we would like to discuss: *Length* properties and complex conditions for which we need dedicated *semantic predicates*.

One of the target languages in our evaluation (Section 6) is reStructuredText (reST), a plaintext markup language used, e.g., by Python’s docutils. In reST, document (sub)titles are underlined with “=” or “\_” symbols. However, titles are only valid if the length of the underline is not smaller than the length of the title text. This property cannot be expressed in a Context-Free Grammar (CFG); however, we can easily capture it in an ISLa constraint:

```
str.len(<section-title>.<underline>) >=
str.len(<section-title>.<title-text>)
```

The corresponding Core-ISLa constraint is

```
forall <section-title> title=
  {"<title-txt> titletxt"}\n{<underline> underline}" in start:
  (>= (str.len underline) (str.len titletxt))
```

There are properties which cannot be expressed using structural predicates and SMT-LIB formulas alone. A stereotypical case are checksums occurring in many binary formats, such as in the TAR archive file format from our benchmark set. To account for such situations, we can extend the ISLa language with additional atomic assertions, so-called *semantic predicates*. In contrast to structural predicates such as *inside* or *same\_position*, which we have seen before, semantic predicates do not always evaluate to false for invalid arguments. Instead, they can suggest a *satisfying solution*. The solver logic for individual semantic predicates is implemented in Python code in our prototype. Once this logic has been implemented, we can pass such predicates as additional signature elements to both the ISLa evaluator or solver and use them in constraints. The following constraint, which is part of our constraint set for TAR files, uses a semantic predicate *tar\_checksum* computing a correct checksum value for the header of a TAR file.

```
tar_checksum(<header>, <header..<checksum>)
```

This corresponds to the Core-ISLa constraint

```
forall <header> header in start:
  forall <checksum> checksum in header:
    tar_checksum(header, checksum)
```

Another use case for semantic predicates is when the SMT solver frequently times out when looking for satisfying assignments. This happens in particular for constraints involving a complex combination of arithmetic and string (e.g., regular expression) constraints. For example, valid CSV files have the property that all rows have the same numbers of columns. Assuming that we know the number of columns in the file header, we could create a regular expression matching all CSV lines with the same number of columns. However, if we admit quoted expressions and a wide character range for contained text, these regular expressions get quite complex, and the problem exceeds the capabilities of current SMT solvers in our experience. Thus, we implemented a new semantic predicate *count* which counts the number of occurrences of some nonterminal in an input tree, and fixes trees with an insufficient number of occurrences if possible. The following ISLa constraint for the CSV property uses an additional language feature: It introduces a *numeric constant* *colno* using the **num** directive, which works similarly to let expressions in functional programming languages. It is primarily—and also in this example—used to enable information exchange between semantic predicate formulas.

```
forall <csv-header> hline:
  exists int colno: (
    str.to_int(colno) >= 3 and
    str.to_int(colno) <= 5 and
    count(hline, "<raw-field>", colno) and
    forall <csv-record> line in start:
      count(line, "<raw-field>", colno))
```

One has to be aware that the *order* of semantic predicates in a constraint matters. This is in contrast to all other language atoms: SMT formulas, in particular, are fed to an SMT solver only after all universal quantifiers have been eliminated resp. matched, and evaluated *en bloc*. Semantic predicates, on the other hand, are generally not compositional. When computing the checksum for a TAR file, for instance, it is important that all elements of the file header are already fixed at that point, i.e., all semantic predicates on header elements have to be evaluated before. Consequently, they have to occur before the checksum predicate in the overall constraint. Despite this particularity, semantic predicates are an easy way to increase both the expressiveness and solving performance of ISLa constraints, and to overcome the limits of SMT-LIB and off-the-shelf solvers.

## 3 ISLa Syntax and Semantics

We provide a more formal definition of derivation trees. We use the symbols  $<$  and  $\leq$  to denote the strict and non-strict versions of the same partial order relation, respectively; for the corresponding covering relation which only holds between parents and their *immediate* children, we write  $\prec$ .

*Definition 3.1 (Derivation Tree).* A *derivation tree* for a CFG  $G = (N, T, P, S)$  is a *rooted ordered tree*  $t = (X, \leq_V, \leq_S)$  such that (1) the vertices  $v \in X$  are *labeled* with symbols  $\text{label}(v) \in N \cup T$ , (2) the *vertical order*  $\leq_V \subseteq X \times X$  indicates the parent-child relation such that the partial order  $(X, \leq_V)$  forms an unordered tree, (3) the *sibling order*  $\leq_S \subseteq X \times X$  yields a partial order  $(X, \leq_S)$  such that two distinct nodes  $v_1, v_2$  are comparable by relation  $\leq_S$  if, and only if, they are siblings, (4) the root of  $t$  is labeled with  $S$ , and (5) each inner node  $v$  is labeled by a symbol in  $n \in N$  and, if  $v_1, \dots, v_k$  is the ordered list of all immediate children of  $v$ , i.e., all distinct nodes such that  $v \prec_V v_i$  and  $v_i \leq_S v_l$  for  $1 \leq i < l \leq k$ , there is a production  $(n, s_1, \dots, s_k) \in P$  such that  $\text{label}(v) = n$  and, for all  $v_i$ ,  $\text{label}(v_i) = s_i$ . We write  $\text{leaves}(t)$  for the set of leaves of  $t$ , and  $\text{label}(t)$  for the label of its root. A derivation tree is *closed* if  $l \in T$  for all  $l \in \text{leaves}(t)$ , and *open* otherwise. We define  $\text{closed}(t) := \forall l \in \text{leaves}(t) : l \in T$ , and  $\text{open}(t) := \neg \text{closed}(t)$ .  $\mathcal{T}(G)$  is the set of all (closed and open) derivation trees for  $G$ .

*Example 3.2.* We explain the formal definition of derivation trees (Definition 3.1) along the XML document  $\langle a \rangle x \langle /a \rangle$ , visualized in Figure 2 in our paper [3]. Formally, this tree is represented as a triple  $t = (X, \leq_V, \leq_S)$ , where  $X = \{v_1, \dots, v_{14}\}$ , with  $\text{label}(v_1) = \langle \text{xml-tree} \rangle$ ,  $\text{label}(v_2) = \langle \text{xml-open-tag} \rangle$ , etc. The *vertical order*  $\leq_V$  contains the edges in the figure: For example,  $v_1 \leq_V v_2$  and  $v_2 \leq_V v_{13}$ . This relation alone only gives us an unordered tree: When “unparsing” the tree, we could thus obtain the undesired result  $x a > < > / a$ . Thus, we define a *sibling order*  $\leq_S$  to order the immediate children of the same node. For instance, we have  $v_6 \leq_S v_8$  (and  $v_6 \leq_S v_6$ ,  $v_6 \leq_S v_8$ , and  $v_6 \prec_S v_7$ ), but not  $v_6 \leq_S v_9$  (since they have different parents) and  $v_6 \prec_S v_8$  (since they are not *immediate* siblings). The tree is not only any ordered tree, but a *derivation tree* for the XML grammar in Figure 1 in [3], since it satisfies 4 and 5 of Definition 3.4 in [3]. The root of the tree,  $v_1$ , is labeled with the grammar’s start symbol  $\langle \text{xml-tree} \rangle$  (Item (4)). The tree relations conform to the possible grammar derivations: Consider, e.g., node  $v_2$  and its immediate children  $v_6, v_7$ , and  $v_8$ . According to Item (5), there has to be a production  $(\langle \text{xml-open-tag} \rangle, '<', \langle id \rangle, '>')$  in the grammar, which is indeed the case, since  $'<' \langle id \rangle '>'$  is an expansion alternative (the first one) for the nonterminal  $\langle \text{xml-open-tag} \rangle$ . The leaf set  $\text{leaves}(t)$  is  $\{v_6, v_{13}, v_8, v_9, v_{10}, v_{14}, v_{12}\}$ . The tree  $t$  is *closed*, since all leaves are labeled with *terminal* symbols. It would be *open* if we removed the subtree rooted in any tree node (but the root).

*Standard ISLa Predicates.* ISLa offers a catalog of default supported predicates. Table 1 provides an overview of those. Structural predicates can be re-used for many different languages, while semantic predicates are mostly application-specific. For this reason, there is only one semantic predicate included in ISLa per default, which is the count predicate used in the formalization of CSV.

*Matching Match Expressions.* Match expressions are matched against derivation trees by first parsing them into *abstract* parse trees (with open leaves), and then matching these parse trees against the derivation tree in question. This process is also described in detail in the ISLa language specification [2].

We use a function  $\text{mexprTrees}(T, \text{mexpr})$  that takes a nonterminal  $T$  and a match expression  $\text{mexpr}$  and returns a set of derivation

trees. If the match expression contains *optional* elements, it is “flattened” first. That is, we compute all combinations of activated and non-activated optional expressions. If there are  $n$  optionals in the match expression, we obtain  $2^n$  flattened match expressions. Then, we parse the flattened expressions using an augmented version of the reference grammar. The augmented grammar adds expansions “ $\langle A \rangle ::= '<' \langle A' \rangle '>'$  for each nonterminal  $A$ , and similarly extends the grammar with expansions for variable binders “ $\{ \langle T \rangle \text{ var} \}$ .” Due to ambiguities in the grammar, we might obtain multiple parse trees even for flattened expressions;  $\text{mexprTrees}$  returns all of them, along with a mapping of bound variables to the positions of their matches in the respective derivation trees. After parsing the match expression, the function  $\text{matchTrees}(t, t', P)$  matches a derivation tree  $t$  against a result  $(t', P)$  from  $\text{mexprTrees}$ , where  $t'$  is a parse tree and  $P$  a mapping from bound variables to positions in  $t'$ . Figure 1 shows the definition of  $\text{mexprTrees}$ . In the definition,

- $t$  is the label of the tree  $t$ ;
- all alternatives in the definition are \*mutually exclusive\* (the first applicable one is applied);
- by  $\text{numc}(t)$  we denote the number of children of the derivation tree  $t$ ;
- by  $\text{child}(t, i)$  we denote the  $i$ -th child of  $t$ , starting with 1;
- $P_i$  is computed from a mapping  $P$  by discarding all paths in  $P$  not starting with  $i$  and taking the *tail* (discarding the first element) for all other paths; and
- we use standard set union notation  $\bigcup_{i=1}^n \beta_i$  for combining variable assignments  $\beta_i$ .

Let  $T$  be the label of the root of tree  $t$ . We define

$$\text{match}(t, \text{mexpr}) :=$$

$$\left( \bigcup_{(t', P) \in \text{mexprTrees}(T, \text{mexpr})} \{\text{matchTrees}(t, t', P)\} \right) \setminus \{\perp\}$$

## 4 Solving ISLa Constraints

We provide a formalization of our ISLa constraint solver, including two correctness theorems and proof sketches.

We formalize input generation for ISLa as a transition system between *Conditioned Derivation Trees* (CDTs)  $\Phi \triangleright t$ , where  $\Phi$  is a set of ISLa formulas (interpreted as a conjunction) and  $t$  a (possibly open) derivation tree. Intuitively,  $\wedge \Phi$  constrains the inputs represented by  $t$ , similarly as  $\llbracket \varphi \rrbracket$  constrains the language of the grammar. To make this possible, we need to relax the definition of ISLa formulas: Instead of free variables, formulas may contain references to tree nodes which they are concerned about. To that end, tree nodes are assigned unique, numeric identifiers, which may occur everywhere in ISLa formulas where a free variable might occur (variables bound by quantifiers may not be replaced with tree identifiers).

Consider, for example, the ISLa constraint

$$\varphi = \textbf{forall } \langle id \rangle id \text{ in start: } (= (\text{str.len } id) 17)$$

constraining the XML grammar in Figure 1 in [3] to identifiers of length 17, where  $id$  is a bound variable of type  $\langle ID \rangle$  and  $\text{start}$  is a free variable of type  $\langle \text{start} \rangle$ . Let  $t$  be a tree consisting of a single

**Table 1: Standard ISLa predicates. The predicate count is a semantic predicate; all other predicates are structural predicates.**

Predicate	Explanation
after( $node_1, node_2$ )	$node_1$ occurs after $node_2$ (not below) in the parse tree.
before( $node_1, node_2$ )	$node_1$ occurs before $node_2$ (not below) in the parse tree.
consecutive( $node_1, node_2$ )	$node_1$ and $node_2$ are consecutive leaves in the parse tree.
different_position( $node_1, node_2$ )	$node_1$ and $node_2$ occur at different positions (cannot be the same node).
direct_child( $node_1, node_2$ )	$node_1$ is a direct child of $node_2$ in the derivation tree.
inside( $node_1, node_2$ )	$node_1$ is a subtree of $node_2$ .
level(PRED, NONTERMINAL, $node_1, node_2$ )	$node_1$ and $node_2$ are related relatively to each other as specified by PRED and NONTERMINAL (see below). PRED and NONTERMINAL are strings.
nth(N, $node_1, node_2$ )	$node_1$ is the N-th occurrence of a node with its nonterminal symbol within $node_2$ . N is a numeric String.
same_position( $node_1, node_2$ )	$node_1$ and $node_2$ occur at the same position (have to be the same node).
count(in_tree, NEEDLE, NUM)	There are NUM occurrences of the NEEDLE nonterminal in in_tree. NEEDLE is a string, NUM a numeric string or int variable.

$$matchTrees(t, t', P) := \begin{cases} \perp & \text{if } l(t) \neq l(t') \vee (numc(t') > 0 \wedge numc(t) \neq numc(t')) \\ [v \mapsto t] & \text{if } P = [v \mapsto ()] \text{ for some } v \\ \perp & \text{if } matchTrees(child(t, i), child(t', i), P_i) = \perp \\ & \quad \text{for any } i \in [1, \dots, numc(t)] \\ \bigcup_{i=1}^{numc(t)} \left( \begin{array}{l} matchTrees(child(t, i), \\ child(t', i), P_i) \end{array} \right) & \text{otherwise} \end{cases}$$

**Figure 1: Recursive Definition of  $matchTrees$ .**

(root) node with identifier 1, and labeled with  $\langle start \rangle$ . Then,  $\llbracket \varphi \rrbracket$  is identical to the strings represented by the CDT

```
{forall <id> id in 1: (= (str.len id) 17)} ▷ t.
```

Our CDT transition system relates an input CDT to a set of output CDTs. We define two properties of such transitions: A transition is *precise* if the input represents *at most* the set of all strings represented by all outputs together; conversely, it is *complete* if the input represents *at least* the set of all strings represented by all outputs. Precision is mandatory for the ISLa producer, since we have to avoid generating system inputs which do not satisfy the specified constraints.

To define the semantics of CDTs, we first define the closed trees represented by (the language of) *open* derivation trees. We need the concept of a *tree substitution*: The tree  $t[v \mapsto t']$  results from  $t = (X, \leq_V, \leq_S)$  by replacing the subtree rooted in node  $v \in X$  by  $t'$ , updating  $X$ ,  $\leq_V$  and  $\leq_S$  accordingly.

**Definition 4.1 (Semantics of Open Derivation Trees).** Let  $t \in \mathcal{T}(G)$  be a derivation tree for a grammar  $G = (N, T, P, S)$ . We define the set  $\mathcal{T}(t) \subseteq \mathcal{T}(G)$  of closed derivation trees represented by

$t$  as

$$\begin{aligned} \mathcal{T}(t) := \{ & t[l_1 \mapsto t_1] \cdots [l_k \mapsto t_k] \mid \\ & l_i \in \text{leaves}(t) \wedge k = |\text{leaves}(t)| \\ & \wedge (\forall j, m \in 1 \dots k : l \neq m \rightarrow l_j \neq l_m) \\ & \wedge n_i = \text{label}(t_i) = \text{label}(l_i) \\ & \wedge G_{n_i} = (N, T, P, n_i) \wedge t_i \in \mathcal{T}(G_{n_i}) \} \end{aligned}$$

Observe that for the tree consisting of a single node labeled with the start symbol  $S$ ,  $\mathcal{T}(t)$  is identical to  $\mathcal{T}(S)$ . Furthermore, for any *closed* tree  $t'$ , it holds that  $\mathcal{T}(t') = \{t'\}$ .

We re-use the validity judgment defined from Definition 3.6 in our paper [3] for the semantics definition for CDTs by interpreting tree identifiers in formulas similarly to variables. Furthermore, the special variable assignment  $\beta_t$  for the derivation tree  $t$  associates with each tree identifier in  $t$  the subtree rooted in the node with that identifier. Then, the definition is a straightforward specialization of Definition 3.8 from [3]:

**Definition 4.2 (Semantics of CDTs).** Let  $\Phi \subseteq 2^{\text{Fml}}$  be a set of ISLa formulas for the signature  $\Sigma = (G, \text{PSym}, \text{VSym})$ ,  $t \in \mathcal{T}(G)$  be a derivation tree, and  $\pi, \sigma$  be interpretations for predicates and SMT formulas. We define the semantics  $\llbracket \Phi \triangleright t \rrbracket$  of the CDT  $\Phi \triangleright t$  as

$$\llbracket \Phi \triangleright t \rrbracket := \{ \text{str}(t') \mid t' \in \mathcal{T}(t) \wedge \text{closed}(t') \wedge \pi, \sigma, \beta_{t'} \models \bigwedge \Phi \}.$$

A CDT Transition System (CDTTS) is simply a transition system between CDTs.

**Definition 4.3 (CDT Transition System).** A CDTTS for a signature  $\Sigma = (G, \text{PSym}, \text{VSym})$  is a transition system  $(C, \rightarrow)$ , where, for  $\Phi \in 2^{\text{Fml}}$  and  $t \in \mathcal{T}(G)$ ,  $C$  consists of CDTs  $\Phi \triangleright t$ , and  $\rightarrow \subseteq C \times C$ . We write  $cdt \rightarrow cdt'$  if  $(cdt, cdt') \in \rightarrow$ .

Intuitively, one applies CDTTS transitions to an initial constraint with a trivial tree only consisting of a root node labeled with the start nonterminal, and collects “output” CDTs  $\emptyset \triangleright t$  with an empty constraint. The trees  $t$  of such outputs are solutions to the initial problem. We call a CDTTS *globally precise* if all such trees  $t$  are actual solutions, i.e., the system does not produce wrong outputs; we call it *globally complete* if the entirety of trees  $t$  from result CDTs represents the full semantics of the input CDT.

**Definition 4.4 (Global Precision and Completeness).** Let  $(C, \rightarrow)$  be a CDTTS, and  $R_{cdt}$  be the set of all closed trees  $t$  such that  $cdt \rightarrow \dots \rightarrow \emptyset \triangleright t$  is a derivation in  $(C, \rightarrow)$ . Then,  $(C, \rightarrow)$  is *globally precise* if, for each CDT  $cdt$  in the domain of  $\rightarrow$ , it holds that  $\llbracket cdt \rrbracket \supseteq \{str(t) | t \in R_{cdt}\}$ . The CDTTS is *globally complete* if it holds that  $\llbracket cdt \rrbracket \subseteq \{str(t) | t \in R_{cdt}\}$ .

To enable transition-local reasoning about precision and completeness, we define notions of local precision and completeness. Local precision is the property that *at each transition step, no “wrong” inputs are added*, and local completeness the property that no transition step loses information.

**Definition 4.5 (Local Precision and Completeness).** A CDTTS  $(C, \rightarrow)$  is *precise* if, for each CDT  $cdt$  in the domain of  $\rightarrow$ , it holds that  $\llbracket cdt \rrbracket \supseteq \bigcup_{cdt \rightarrow cdt'} (\llbracket cdt' \rrbracket)$ . The CDTTS is *complete* if it holds that  $\llbracket cdt \rrbracket \subseteq \bigcup_{cdt \rightarrow cdt'} (\llbracket cdt' \rrbracket)$ .

As for “soundness” in first-order logic (see, e.g., [4]), local precision implies global precision, i.e., it suffices to show that the individual transitions are precise to obtain the property for the whole system. This is demonstrated by the following Lemma 4.6. Note that the opposite direction does not hold, since a CDTTS could in theory lose precision locally and recover it globally, although it is unclear how (and why) such a system should be designed.

**LEMMA 4.6.** *A locally precise CDTTS is also globally precise.*

**PROOF.** The lemma trivially holds if  $R_{cdt} = \emptyset$ . Otherwise, let  $cdt_0 \rightarrow cdt_1 \rightarrow \dots \rightarrow \emptyset \triangleright t$  be any transition chain s.t.  $cdt_0 = cdt$  and  $t \in R_{cdt}$ . Then, it follows from local precision that  $\llbracket cdt_k \rrbracket \supseteq \llbracket cdt_{k+1} \rrbracket$  for  $k = 0, \dots, n-1$ , and by transitivity of  $\supseteq$  also  $\llbracket cdt_k \rrbracket \supseteq \llbracket cdt_l \rrbracket$  for  $0 \leq k < l \leq n$ . Since  $\llbracket \emptyset \triangleright t' \rrbracket = str(t')$  for closed  $t'$ , the lemma follows.  $\square$

Global completeness cannot easily be reduced to local completeness: It includes the “termination” property that all derivations end in CDTs with empty constraint set; furthermore, one has to show that there is an applicable transition for each CDT with non-empty semantic.

Our ISLa solver prototype implements the CDTTS in Fig. 2. It solves SMT and semantic predicate constraints by querying the

SMT solver or the predicate oracle, and eliminates existential constraints by inserting new subtrees into the current conditioned tree. Only when the complete constraint has been eliminated, we finish off the remaining incomplete tree by replacing open leaves with suitable concrete subtrees. This is in principle a complete procedure; yet, our implementation only considers a finite subset of all solutions in solver queries and when performing tree insertion. Consequently, it usually misses some solutions, but outputs *more diverse results more quickly* compared, e.g., to a naive search-based approach filtering out wrong solutions.

**Transition Rules.** In the ISLa CDTTS, we use *indexed* CDTs  $\Phi \triangleright^I t$ . In the index set  $I$ , we track previous matches of universal quantifiers to make sure that we do not match the same trees over and over. Since SMT formulas can now also contain variables, evaluating them can result in a *model*  $\beta$  (an assignment). Note that we can obtain different assignments by repeated solver calls (negating previous solutions). We divide the set PSym of predicate symbols into two disjoint sets PSym<sub>st</sub> and PSym<sub>sem</sub> of *structural* and *semantic* predicates. Structural predicates address constraints such as *before* or *within*, and they evaluate to  $\top$  or  $\perp$ . Semantic predicates formalize constraints such as specific checksum implementations. They may additionally evaluate to a set of assignments, as in the case of satisfiable SMT expressions, or to the special value “not ready” (denoted by  $\cup$ ). Intuitively, an evaluation results in  $\top$  ( $\perp$ ) if all of (not any of) the derivation trees represented by an abstract tree satisfy the predicate. Assignments are returned if the given tree can be completed or “fixed” to a satisfying solution. One may obtain  $\cup$  if the constrained tree lacks sufficient information for such a computation (e.g., the inputs of a checksum predicate are not yet determined).

We explain the individual transition rules of the CDTTS from Fig. 2. Rule (1) uses a function  $inv : \text{Fml} \rightarrow 2^{\text{Fml}}$  to enforce the invariant that all formulas  $\varphi \in \Phi$  are in Negation Normal Form (NNF) and do not contain top-level conjunctions and disjunctions. Basically,  $inv$  converts its input into Disjunctive Normal Form and returns the disjunctive elements. It is only applicable to CDTs whose constraints do not satisfy the invariant. Rule (2) eliminates satisfied structural predicate formulas from a constraint set. Existential quantifiers over numbers are eliminated in Rule (3) by introducing a fresh (not occurring in the containing CDT) variable symbol with the special nonterminal type int for natural numbers.

Rules (4) and (5) eliminate universal formulas that have already been matched with all applicable subtrees, and which cannot possibly be matched against *any* extension of the (open) tree. This is the case if the nonterminal type of the quantified variable is not reachable from any leaf and, if there is a match expression, the current tree cannot be completed to a matching one.

Universal formulas with and without match expressions are subject of Rules (6) and (7). First, matching subtrees of the tree  $\beta_t(id)$  identified with  $id$  are collected in a set  $T$ . We only consider subtrees that are not already matched, i.e., where  $(\psi, t')$  is not yet in the index set  $I$ . If  $T$  is empty, the rules are not applicable. Otherwise, the set  $\Phi$  of all instantiations of  $\varphi$  according to the discovered matches is added to the constraint set. We record the instantiations  $(\psi, t')$ , for all matched trees  $t'$ , in the index set. The output of these rules is a singleton.

$$\begin{aligned}
& \{\dots, \varphi, \dots\} \triangleright^I t \rightarrow \{\{\dots, \varphi' \dots\} \triangleright^I t \mid \\
& \quad \varphi' \in \text{inv}(\varphi) \wedge \varphi \neq \varphi'\} \neq \emptyset & (1) \\
& \Phi \triangleright^I t \rightarrow \{\Phi \setminus \varphi \triangleright^I t \mid \varphi \in \Phi \cap \text{PSym}_{st} \wedge \pi(\varphi) = \top\} & (2) \\
& \{\dots, \text{forall int } n \text{ in } \varphi: \dots\} \triangleright^I t \rightarrow & (3) \\
& \quad \{\dots, \{n \mapsto c\}(\varphi), \dots\} \triangleright^I t \\
& \quad \text{where } c \in \text{VSym} \text{ is fresh and } \text{vtype}(c) = \text{int} \\
& \quad \overbrace{\dots, \text{forall type } v \text{ in id: } \varphi, \dots}^\psi \triangleright^I t \rightarrow \{\{\dots, \dots\} \triangleright^I t\} & (4) \\
& \quad \text{if } \forall \text{ subrees } t' \text{ of } \mathcal{T}(\beta_t(id)) : \\
& \quad \quad (\psi, t') \in I \vee \text{label}(t') \neq \text{type} \\
& \quad \quad \overbrace{\dots, \text{forall type } v = "mexpr" \text{ in id: } \varphi, \dots}^\psi \triangleright^I t \rightarrow & (5) \\
& \quad \quad \{\{\dots, \dots\} \triangleright^I t\} \text{ if } \forall \text{ subrees } t' \text{ of } \mathcal{T}(\beta_t(id)) : \\
& \quad \quad \quad (\psi, t') \in I \vee \text{label}(t') \neq \text{type} \vee \\
& \quad \quad \quad \text{there is no } m = \text{match}(t', \text{mexpr}) \\
& \quad \quad \quad \overbrace{\dots, \text{forall type } v \text{ in id: } \varphi, \dots}^\psi \triangleright^I t \rightarrow & (6) \\
& \quad \quad \quad \{\{\dots, \psi, \dots\} \cup \bigcup_{\xi \in \Psi} \Psi \triangleright^{I \cup (\{\psi\} \times T)} t\} \text{ where} \\
& \quad \quad \quad \Psi = \{\beta_t[v \mapsto t'](\varphi) \mid t' \in T\} \wedge \\
& \quad \quad \quad T = \{t' \mid t' = \beta_t(id) \wedge (\psi, t') \notin I \wedge \\
& \quad \quad \quad \text{label}(t') = \text{type}\} \neq \emptyset \\
& \quad \quad \quad \overbrace{\dots, \text{forall type } v = "mexpr" \text{ in id: } \varphi, \dots}^\psi \triangleright^I t \rightarrow & (7) \\
& \quad \quad \quad \{\{\dots, \psi, \dots\} \cup \bigcup_{\xi \in \Psi} \Psi \triangleright^{I \cup (\{\psi\} \times T)} t\} \text{ where} \\
& \quad \quad \quad \Psi = \{\beta_t[v \mapsto t'][m](\varphi) \mid (t', m) \in T\} \wedge \\
& \quad \quad \quad T = \{(t', m) \mid t' = \beta_t(id) \wedge (\psi, t') \notin I \wedge \\
& \quad \quad \quad \text{label}(t') = \text{type} \wedge \\
& \quad \quad \quad \text{there is an } m = \text{match}(t, \text{mexpr})\} \neq \emptyset \\
& \quad \quad \quad \Phi \triangleright^I t \rightarrow \{\Phi \setminus \varphi \triangleright^I \beta(t) \mid \varphi \in \Phi \cap \text{Trm}_{\text{bool}}(\text{VSym}) \wedge \beta \in \sigma(\varphi) \neq \perp\} & (8) \\
& \quad \quad \quad \Phi \triangleright^I t \rightarrow \{\Phi \setminus \varphi \triangleright^I \beta(t) \mid \varphi \text{ is first } \varphi \in \Phi \cap \text{PSym}_{\text{sem}} \wedge \beta \in \pi(\varphi) \notin \{\perp, \cup\}\} & (9) \\
& \quad \quad \quad \overbrace{\dots, \text{exists type } v \text{ in id: } \varphi, \dots}^\psi \triangleright^I t \rightarrow & (10) \\
& \quad \quad \quad \bigcup_{\xi \in \Psi} \{\{\dots, \xi, \dots\} \triangleright^I t\} \text{ where} \\
& \quad \quad \quad \Psi = \{\beta_t[v \mapsto t'](\varphi) \mid t' \in T\} \wedge \\
& \quad \quad \quad T = \{t' \mid t' = \beta_t(id) \wedge (\psi, t') \notin I \wedge \\
& \quad \quad \quad \text{label}(t') = \text{type}\} \neq \emptyset \\
& \quad \quad \quad \overbrace{\dots, \text{exists type } v = "mexpr" \text{ in id: } \varphi, \dots}^\psi \triangleright^I t \rightarrow & (11) \\
& \quad \quad \quad \bigcup_{\xi \in \Psi} \{\{\dots, \xi, \dots\} \triangleright^I t\} \text{ where} \\
& \quad \quad \quad \Psi = \{\beta_t[v \mapsto t'][m](\varphi) \mid (t', m) \in T\} \wedge \\
& \quad \quad \quad T = \{(t', m) \mid t' = \beta_t(id) \wedge (\psi, t') \notin I \wedge \\
& \quad \quad \quad \text{label}(t') = \text{type} \wedge \\
& \quad \quad \quad \text{there is an } m = \text{match}(t, \text{mexpr})\} \neq \emptyset \\
& \quad \quad \quad \overbrace{\dots, \text{exists type } v \text{ in id: } \varphi, \dots}^\psi \triangleright^I t \rightarrow & (12) \\
& \quad \quad \quad \{\{\dots, \{v \mapsto nid\}(\varphi), \dots\} \cup \Phi_{\text{orig}} \triangleright^I \{id \mapsto t'\}(t) \mid \\
& \quad \quad \quad (nid, t') \in \text{insert}(\text{makeTree}(v), \beta_t(id))\} & (13) \\
& \quad \quad \quad \{\{\dots, \{v \mapsto nid\}(\varphi), \dots\} \cup \Phi_{\text{orig}} \triangleright^I \{id \mapsto t'\}(t) \mid \\
& \quad \quad \quad (nid, t') \in \text{insert}(\text{makeTree}(v, \text{mexpr}), \beta_t(id))\} & (14) \\
& \emptyset \triangleright^I t \rightarrow \{\emptyset \triangleright^I t' \mid t' \in \mathcal{T}(t)\} \neq \{\emptyset \triangleright^I t\} & (15) \\
& \Phi \triangleright^I t \rightarrow \{\Phi \triangleright^I t' \mid t' \in \mathcal{T}(t)\} \neq \{\Phi \triangleright^I t\} & (16) \\
& \quad \text{if } \Phi \subseteq \{p(\dots) \mid p \in \text{PSym}_{\text{sem}}\}
\end{aligned}$$

Figure 2: Efficient ISLa CDTTS Transition Relation

If universal quantifiers remain which cannot be matched or eliminated, we expand the current tree in Rule (8). The function  $\text{expand}_\Phi^\vee(t)$  returns all possible trees  $t'$  in which each open leaf has been expanded *one step* according to the grammar. However, we only expand leaves which are bound by a universal quantifier, that is, which represent possible subtrees that could be unified with a universally quantified formula. For this reason, we pass  $\Phi$  as an argument. We call the remaining, unbound grammar symbols *free nonterminals*. For example, the XML constraint in Listing 2 from our paper [3] does not restrict the instantiation of  $\langle \text{text} \rangle$  nonterminals. Thus,  $\langle \text{text} \rangle$  is a free nonterminal which we will not expand

with Rule (8). Instead, such nonterminals are instantiated to concrete closed subtrees in a single step by Rules (15) and (16). In our implementation, we use a standard coverage-based fuzzer to that end. Thus, we avoid producing many strings which only differ, e.g., in identifier names or text passages within XML tags.

Rules (9) and (10) eliminate *satisfiable* SMT or semantic predicate formulas by querying  $\sigma$  or  $\pi$  (there is no transition for unsatisfiable or “not ready” formulas). The transition result consists of one instantiation per returned assignment  $\beta$ .

The only remaining constraints—in satisfiable constraint sets—are existential formulas, and semantic predicate formulas that are

not yet ready to provide a solution. Existential formulas can be matched just like universal ones; but instead of returning one result with all matches, Rules (11) and (12) return a *set* of solutions with one match each.

In addition to matching, we provide two rules Rules (13) and (14) to eliminate existential formulas using *tree insertion*. Note that, as exception to the general principle that the rules in the CDTTS are mutually exclusive, we can apply Rules (11) and (12) and Rules (13) and (14) wherever possible. The insertion routine *insert(newTree, t)* guarantees that all returned results contain all nodes from the original tree  $t$  as well as the complete tree  $newTree$ . Nevertheless, tree insertion is an aggressive operation that may violate constraints that were satisfied before. For this reason, we have to add the original constraint  $\Phi_{orig}$ , from which we started solving, again to the constraint set; if the tree insertion did not violate structural constraints, the original constraint can usually be quickly eliminated. However, tree insertion can also entail the necessity of subsequent tree insertions, e.g., if a new identifier was added that needs to be declared. Our implemented insertion routine prioritizes structurally simple solutions, for which this is usually not necessary. In the appendix, we provide details on tree insertion.

Finally, Rules (15) and (16) “finish off” the remaining open derivation trees by replacing all open leaves with suitable concrete subtrees. In the case of Rule (15), this yields a decisive result of the CDTTS. Rule (16) addresses residual “not ready” semantic predicate formulas. We compute the represented closed subtrees such that all information for evaluating the semantic predicates is present. After this step, Rule (10) must be applicable.

In the appendix, we argue for the correctness of the subsequent precision and completeness theorems.

**THEOREM 4.7. (Precision)** *The ISLa CDTTS in Fig. 2 is globally precise.*

**PROOF SKETCH.** By Lemma 4.6, we prove global precision by showing that each individual transition rule is *locally* precise, i.e., that the produced states do not represent derivation trees that were not originally in the semantics of the inputs CDT.

Rule (1) is precise since conversion to Disjunctive Normal Form is equivalence-preserving. Elimination of structural predicates (Rule (2)) is trivially precise (removing a true element from a conjunction does not change the semantics).

Rules (4) and (5) are precise because a universal quantifier that does not match any tree element evaluates to true according to Definition 3.6 in our paper [3], and we only remove it if we can be sure that no possible extension of an open tree will ever match the quantifier. If a match is already in the index set, we can be sure that it already has been considered due to the definition of Rules (6) and (7), which are the only rules ever adding to that set.

Rules (6) and (7) are precise because we only *add* the matching instantiations of the inner formula to the (conjunctive) constraint set.

Tree expansion (Rule (8)) is precise since by considering *more concrete* trees, the set of concrete trees represented by the input CDT is only ever *decreased* in the outputs (cf. Definition 4.1).

The elimination of SMT formulas (Rule (9)) is precise since their semantics is defined via the interpretation function  $\sigma$ , which we

query to produce valid output states. The same holds for Rule (10) for semantic predicates.

Existential quantifier matching (Rules (11) and (12)) is precise since it conforms to Definition 3.6 in our paper [3] inasmuch it creates one instantiated CDT for each match in the input CDT. The original formula is removed from these results, but the instantiation retained.

The tree insertion rules (Rules (13) and (14)) (the most complicated ones in our system due to the complexity of tree tree insertion itself) are trivially to prove, because we add the additional constraint again to the constraint set.

Finally, Rules (15) and (16) consider more concrete trees and are therefore precise for the same reasons as Rule (8).  $\square$

**THEOREM 4.8. (Completeness)** *The ISLa CDTTS in Fig. 2 is globally complete.*

**PROOF SKETCH.** To prove the global completeness of our system, we have to show that the semantics of each input CDT is contained in the semantics of all reachable CDTs with empty constraint set. We reduce this problem as follows. First, we show *local* completeness, i.e., that no information is lost by applying any transition rule of our CDTTS. Second, we argue that for each *valid* CDT, there is an applicable rule in the CDTTS. Third, we argue that for each input CDT, there is *one* output CDT which is *closer* to a state with empty constraint set in the CDTTS than the inputs. From this, we conclude global completeness as follows: Since for each valid state, there is a transition step from which get closer to an output state with empty constraint set, this also holds for each valid state produced by this step. By additionally requiring that the individual steps do not lose information, we conclude global completeness.

We argue for the local completeness of a chosen set of CDTTS rules.

The expansion and finishing rules are locally complete if *all* expansions are considered. This is the case in our CDTTS, although our actual implementation can only ever consider a finite set of solutions.

The same holds for solving SMT formulas. Note that if we only consider a finite solution set as in our prototype, it is crucial that *there remain no universal quantifiers* in the constraint set. Otherwise, we could obtain instantiations that conflict with formulas obtained from later quantifier instantiation. This is not a problem in the theoretic framework, though, since there we consider *all possible* solutions, of which at least some will not conflict with atoms nested in remaining universal quantifiers.

Tree insertion, which is easy to show precise, is more problematic to show locally complete, since we add the original constraint set. However, since we consider *all* possible insertions, there have to be some satisfying that constraint, since the input CDT is valid.

Since we defined one rule for each syntactic construct in ISLa, there is one rule for each valid input state. Rule (8), for example, only expands nonterminals with potential concrete subtrees matching existing existential quantifiers; for all other nonterminals, the finishing rules will be applicable.

The general measure to show that each transition produces a state that is closer to an empty constraint set is the size of the

constraint set together with the nesting depth of contained quantifiers. If either of these measures decreases in each step, we eventually reach an empty constraint set. That we get closer to an empty constraint set is clear to see for all elimination rules. In case of the matching rules, we reduce the complexity of the constraint set by peeling off the outer quantifier. Again, tree insertion is most problematic: It peels off the existential quantifier, but adds the original constraint set. Here, it is important to see that there are some insertions for which we can remove the existential constraint we eliminated by tree insertion by *matching*, and that we thus do not have to keep re-inserting.  $\square$

We explain the main building blocks used in our ISLa CDTTS (Fig. 2) in more detail.

*Tracking Instantiations.* Our CDTTS stepwise expands open trees and checks if existing universal quantifiers match the expanded tree. Expansion does not eliminate a universal quantifier, since it might apply to not yet generated subtrees. To avoid endlessly instantiating universal quantifiers with the *same* trees, we track already performed universal quantifier instantiations. To that end, we augment CDTs with an *index set*  $I$  consisting of pairs of universal formulas and trees with which they already have been unified; we write  $\Phi \triangleright^I t$  for the enhanced structures.

*Invariant.* We maintain the invariant that all formulas  $\varphi \in \Phi$  in CDTTs  $\Phi \triangleright t$  are in NNF, i.e., negations only occur directly before predicate formulas and within SMT expressions, and are free of conjunctions and disjunctions (on top level; they are allowed inside of quantifiers and within SMT formulas). The function  $inv : Fml \rightarrow 2^{Fml}$  first converts its argument into NNF by pushing negations inside (e.g., **not exists** type  $v$  in  $w$ :  $\varphi$  gets **forall** type  $v$  in  $w$ : **not**  $\varphi$ , and, for  $\psi \in \text{Trm}_{\text{bool}}(V)$ , **not**  $\psi$  gets  $(\text{not } \psi) \in \text{Trm}_{\text{bool}}(V)$ ). Then, it converts the result into Disjunctive Normal Form by applying distributivity laws, which yields a set of disjunction-free formulas in NNF. Finally, it splits all top-level conjunctions outside SMT expressions in the result set into multiple formulas.

*SMT Models.* In Fig. 2, we apply the interpretation  $\sigma$  for SMT expressions to Boolean terms  $\text{Trm}_{\text{bool}}(V)$  with a non-empty variable set  $V$ , i.e., the evaluated expressions may contain uninterpreted String constants. In this case, the SMT solver will *either* return  $\perp$  in case of an unsatisfiable constraint (or time out, which we interpret as  $\perp$ ), or an assignment  $\beta$  (a *model*). Since we can call the solver repeatedly and ask for different solutions (by adding the negated previous solutions as assumptions), we assume that we get a set of assignments of tree identifiers to new subtrees from  $\sigma$ .

*Semantic Predicates.* We divide the set PSym of predicate symbols into two disjoint sets PSym<sub>st</sub> and PSym<sub>sem</sub> of *structural* and *semantic* predicates. Structural predicates address structural constraints, such as *before* or *within*. They evaluate to  $\top$  or  $\perp$ . *Semantic* predicates formalize more complex constraints, such as specific checksum implementations. In addition to  $\top$  or  $\perp$ , semantic predicate formulas may evaluate to a set of assignments, as in the case of satisfiable SMT expressions, or to the special value “not ready” (denoted by  $\cup$ ). Intuitively, an evaluation results in  $\top$  ( $\perp$ ) if all of (not any of) the concrete derivation trees represented by an abstract

tree satisfy the predicate. A set of assignments is returned if there are reasonable “fixes” of the tree (e.g., all elements relevant for a checksum computation are determined, such that the checksum can be computed by the predicate). One may obtain  $\cup$  if the constrained tree lacks sufficient information for such a computation; for instance, we cannot compute a checksum if the summarized fields are still abstract.

In contrast to all other constraint types, the *order of semantic predicate formulas within a conjunction matters* (we use ordered sets in the implementation of our CDTs). The reason is that each semantic predicate comes with its own, atomic solver. Consider, for example, a binary format which requires a semantic predicate for the computation of a data field (e.g., requiring a specific compression algorithm) and another one for a checksum which also includes the data field. Then, one must *first* compute the value of the data field, and *then* the value of the checksum. Changing this order would result in an invalid checksum. Since SMT formulas are composable, we recommend using semantic predicates only if the necessary computation can either not be expressed in SMT-LIB, or the solver frequently times out when searching for solutions.

*Tree Insertion.* Existential constraints can occasionally be solved by matching them against the indicated subtree, similarly to universal quantifiers. In general, though, we have to manipulate the tree to enforce the existence of the formalized structure. If a successful match is not possible, we therefore constructively *insert* a new tree into the existing one. The function  $makeTree(v)$  creates a new derivation tree consisting of a single root node of type  $vtype(v)$ . When passing it a match expression  $mexpr$  as additional argument, it creates a minimal open tree rooted in a node of type  $label(v)$  and matching  $mexpr$ . The function  $insert(t', t)$  tries to inserts the tree  $t'$  into  $t$ . Whether this is possible entirely depends on  $t$ ,  $t'$  and the grammar. In the simplest case,  $t$  has an open leaf from which the nonterminal  $label(t')$  is reachable. Then, we create a suitable tree connecting the leaf and the root of  $t'$  and glue these components together.

If this is not possible, we attempt to exploit recursive definitions in the grammar. Consider, for example, a partial XML document according to the grammar in Figure 1 in our paper [3] and the constraint **exists**  $\langle \text{xml-open-tag} \rangle$  optag **in** tree: (= optag " $<\!\!a\!\!>$ "), where and tree points to a node with root of type  $\langle \text{xml-tree} \rangle$ . If there is some opening tag of form  $<\!\!a\!\!>$  in tree, we can eliminate the constraint. Otherwise, we observe that the nonterminal  $\langle \text{xml-tree} \rangle$  is *reachable from itself* in the grammar graph. Thus, we can replace an existing  $\langle \text{xml-tree} \rangle$  node in tree by a number of possible alternatives, comprising  $\langle \text{a} \rangle \langle \text{xml-tree} \rangle \langle \text{xml-close-tag} \rangle$ , which allows to insert both the already existing  $\langle \text{xml-tree} \rangle$  and the new opening tag  $<\!\!a\!\!>$  into the expanded result.

*Cost Function.* The choice of the right cost function is crucial for the performance of the solver, both in terms of generation speed (number of outputs per time) and output diversity (e.g., creation of deep nestings in the case of XML, or coverage of combinations of language constructs in the case of C).

Our cost function computes the weighted geometric mean of *cost factors*  $cf_i$  and corresponding *weights*  $w_i$  as

$$\text{cost} = \left( \prod_{i=1,\dots,n}^{w_i \neq 0} (cf_i + 1)^{w_i} \right)^{\left( \sum_{i=1,\dots,n}^{w_i \neq 0} w_i \right)} - 1$$

We filter out pairs of cost factors and weights where the weight is 0; in this case, the corresponding cost factor is deactivated. Furthermore, we avoid the case that the final cost value is 0 if one of the factors is 0 by incrementing each factor by 1, and finally decrementing the result by 1 again.

We chose the following cost factors:

**Tree closing cost.** We precompute, for each nonterminal in the grammar, an approximation of the instantiation effort of that nonterminal, roughly by instantiating it several times randomly with a fuzzer, and then summing up the sizes of the possible grammar expansion alternatives in the resulting tree. The closing cost for a derivation tree is defined as the sum of the costs of each nonterminal symbol in all open leaves of the tree.

**Constraint cost.** Certain constraints are more expensive to solve than others. In particular, solving existential quantifiers by tree insertion is computationally costly. This cost factor assigns higher cost for constraints with existential and deeply nested quantifiers.

**Derivation depth penalty.** As the solver's queue fills up, it becomes more improbable for individual queue elements to be selected next. If we assign a cost to the derivation depth, it becomes more likely that the solver eventually comes back to partial solutions discovered earlier, avoiding starvation of such inputs.

**k-path coverage.** When choosing between different partial trees, we generally want to generate those exercising more language features at once. The k-path coverage metric [1] computes all paths of length k in a grammar and derivation tree; the proportion of such paths covered by a tree is then the coverage value. We penalize trees which cover only few k-paths. The concrete value of k is configurable; the default is 3.

**Global k-path coverage.** For each final result produced by the solver, we record the covered k-paths and from then on prefer solutions covering *additional* language features. Once all k-paths in a grammar have been covered, we erase the record.

The influence of these cost factors can be controlled by passing a tuple of weights to the solver. We provide a reasonable default vector ((11, 3, 5, 20, 10)), but in certain cases, a problem-specific tuning might be necessary to improve the performance. Our implementation provides an evolutionary parameter tuning mechanism, which runs the solver with randomly chosen weights, and then computes several generations of weight vectors using crossover and mutation. The fitness value of a weight vector is determined by the generation speed, a vacuity estimator, and a k-path-based coverage measure.

## 6 Evaluation

### 6.3 RQ3: ISLearn

In the subsequent Listings 1 to 5, we list the constraints that ISLearn mined in our case study for our third research question.

```
((forall <graph_type> container in start:
  exists <DIGRAPH> elem in container:
    (= elem "digraph") or
  forall <edge_stmt> container_0 in start:
    exists <edgeop> elem_0 in container_0:
      (= elem_0 "--")) and
(forall <graph> container_1 in start:
  exists <GRAPH> elem_1 in container_1:
    (= elem_1 "graph") or
forall <edge_stmt> container_2 in start:
  exists <edgeop> elem_2 in container_2:
    (= elem_2 "->")))
```

**Listing 1: Constraint mined by ISLearn for DOT**

```
(forall <expr> attribute=
  "<maybe_comments><MWSS>{<name> prefix_use}" in start:
  ((= prefix_use "sqrt") or
  (= prefix_use "string-append") or
  ...
  exists <definition> outer_tag="(<MWSS>define<MWSS>(<MWSS><
    ↪ name>{<WSS_NAMES> cont_attribute}<MWSS>)<MWSS><
    ↪ expr><MWSS>)" in start:
    (inside(attribute, outer_tag) and
    exists <NAME> def_attribute="{<NAME_CHARS> prefix_def}"
      ↪ in cont_attribute:
      (= prefix_use prefix_def)))
```

**Listing 2: Constraint mined by ISLearn for Racket based on the XML def-use pattern for prefixes in attributes**

```
(forall <expr> use_ctxt="<maybe_comments><MWSS>(<MWSS>{<name>
  ↪ use}<wss_exprs><MWSS>)" in start:
  ((= use "sqrt") or
  (= use "string-append") or
  ...
  exists <definition> def_ctxt=
    "<MWSS>define<MWSS>(<MWSS>{<name> def}<WSS_NAMES><
      ↪ MWSS>)<MWSS><expr><MWSS>)" in start:
    (before(def_ctxt, use_ctxt) and
    (= use def)))) and
  forall <expr> attribute=
    "<maybe_comments><MWSS>{<name> prefix_use}" in start:
    ((= prefix_use "sqrt") or
    (= prefix_use "string-append") or
    ...
    exists <definition> outer_tag="(<MWSS>define<MWSS>(<MWSS><
      ↪ name>{<WSS_NAMES> cont_attribute}<MWSS>)<MWSS><
      ↪ expr><MWSS>)" in start:
      (inside(attribute, outer_tag) and
      exists <NAME> def_attribute="{<NAME_CHARS> prefix_def}"
        ↪ in cont_attribute:
```

```
(= prefix_use prefix_def))))
```

**Listing 3:** Racket constraint based on the XML *def-use* pattern in addition to an extended reST *def-use* pattern

```
((forall <icmp_message> container in start:
  exists <type> elem in container:
    (= elem "00 ") or
  forall <icmp_message> container_0 in start:
    exists <type> elem_0 in container_0:
      (= elem_0 "08 ")))
```

**Listing 4:** ISLearn constraint for ICMP Echo type fields

```
((forall <icmp_message> container in start:
  exists <type> elem in container:
    (= elem "00 ") or
  forall <icmp_message> container_0 in start:
    exists <type> elem_0 in container_0:
```

```
(= elem_0 "08 ")))) and
forall <icmp_message> container in start:
  exists <checksum> checksum in container:
    internet_checksum(container, checksum)
```

**Listing 5:** Constraint learned by ISLearn for ICMP Echo after adding a predicate for Internet Checksums

## REFERENCES

- [1] Nikolai Havrikov and Andreas Zeller. 2019. Systematically Covering Input Structure. In *34th IEEE/ACM International Conference on Automated Software Engineering (ASE)*. IEEE, 189–199. <https://doi.org/10.1109/ASE.2019.00027>
- [2] Dominic Steinböfel. 2022. The ISLa Language Specification. <https://rindphi.github.io/isla/islaspec/> Accessed: 2022-08-23.
- [3] Dominic Steinböfel and Andreas Zeller. 2022. Input Invariants. In *Proceedings of the 30th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (ESEC/FSE ’22), November 14–18, 2022, Singapore*. ACM. To appear..
- [4] Dirk van Dalen. 1994. *Logic and Structure* (3rd ed.). Springer.