E-ACSL
Executable ANSI/ISO C Specification Language
Version 1.17
## Contents

1 Introduction
   1.1 Organization of this document ........................................ 11
   1.2 Generalities about Annotations ........................................ 11
   1.3 Notations for grammars ................................................. 11

2 Specification language
   2.1 Lexical rules ............................................................ 13
   2.2 Logic expressions ....................................................... 13
      2.2.1 Operators precedence .............................................. 17
      2.2.2 Semantics .......................................................... 17
      2.2.3 Typing .............................................................. 19
      2.2.4 Integer arithmetic and machine integers ....................... 19
      2.2.5 Real numbers and floating point numbers ....................... 19
      2.2.6 C arrays and pointers .......................................... 19
      2.2.7 Structures, Unions and Arrays in logic ....................... 20
   2.3 Function contracts .................................................... 20
      2.3.1 Built-in constructs `old` and `result` ......................... 20
      2.3.2 Simple function contracts ...................................... 20
      2.3.3 Contracts with named behaviors ................................ 21
      2.3.4 Memory locations and sets of terms ......................... 21
      2.3.5 Default contracts, multiple contracts ....................... 22
   2.4 Statement annotations ................................................ 22
      2.4.1 Assertions ......................................................... 22
      2.4.2 Loop annotations ................................................. 22
      2.4.3 Built-in construct `at` ......................................... 25
      2.4.4 Statement contracts ............................................. 26
   2.5 Termination ............................................................ 26
      2.5.1 Integer measures ................................................. 26
      2.5.2 General measures ................................................. 26
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5.3</td>
<td>Recursive function calls</td>
<td>26</td>
</tr>
<tr>
<td>2.5.4</td>
<td>Non-terminating functions</td>
<td>26</td>
</tr>
<tr>
<td>2.6</td>
<td>Logic specifications</td>
<td>27</td>
</tr>
<tr>
<td>2.6.1</td>
<td>Predicate and function definitions</td>
<td>27</td>
</tr>
<tr>
<td>2.6.2</td>
<td>Lemmas</td>
<td>28</td>
</tr>
<tr>
<td>2.6.3</td>
<td>Inductive predicates</td>
<td>28</td>
</tr>
<tr>
<td>2.6.4</td>
<td>Axiomatic definitions</td>
<td>28</td>
</tr>
<tr>
<td>2.6.5</td>
<td>Polymorphic logic types</td>
<td>28</td>
</tr>
<tr>
<td>2.6.6</td>
<td>Recursive logic definitions</td>
<td>28</td>
</tr>
<tr>
<td>2.6.7</td>
<td>Higher-order logic constructions</td>
<td>28</td>
</tr>
<tr>
<td>2.6.8</td>
<td>Concrete logic types</td>
<td>30</td>
</tr>
<tr>
<td>2.6.9</td>
<td>Hybrid functions and predicates</td>
<td>31</td>
</tr>
<tr>
<td>2.6.10</td>
<td>Memory footprint specification: \texttt{reads} clause</td>
<td>31</td>
</tr>
<tr>
<td>2.6.11</td>
<td>Specification Modules</td>
<td>31</td>
</tr>
<tr>
<td>2.7</td>
<td>Pointers and physical addressing</td>
<td>31</td>
</tr>
<tr>
<td>2.7.1</td>
<td>Memory blocks and pointer dereferencing</td>
<td>31</td>
</tr>
<tr>
<td>2.7.2</td>
<td>Separation</td>
<td>32</td>
</tr>
<tr>
<td>2.7.3</td>
<td>Dynamic allocation and deallocation</td>
<td>32</td>
</tr>
<tr>
<td>2.8</td>
<td>Sets and lists</td>
<td>32</td>
</tr>
<tr>
<td>2.8.1</td>
<td>Finite sets</td>
<td>32</td>
</tr>
<tr>
<td>2.8.2</td>
<td>Finite lists</td>
<td>33</td>
</tr>
<tr>
<td>2.9</td>
<td>Abrupt termination</td>
<td>33</td>
</tr>
<tr>
<td>2.10</td>
<td>Dependencies information</td>
<td>33</td>
</tr>
<tr>
<td>2.11</td>
<td>Data invariants</td>
<td>34</td>
</tr>
<tr>
<td>2.11.1</td>
<td>Semantics</td>
<td>34</td>
</tr>
<tr>
<td>2.11.2</td>
<td>Model variables and model fields</td>
<td>34</td>
</tr>
<tr>
<td>2.12</td>
<td>Ghost variables and statements</td>
<td>34</td>
</tr>
<tr>
<td>2.12.1</td>
<td>Volatile variables</td>
<td>34</td>
</tr>
<tr>
<td>2.13</td>
<td>Initialization and undefined values</td>
<td>36</td>
</tr>
<tr>
<td>2.14</td>
<td>Dangling pointers</td>
<td>36</td>
</tr>
<tr>
<td>2.15</td>
<td>Well-typed pointers</td>
<td>36</td>
</tr>
<tr>
<td>2.16</td>
<td>Logic attribute annotations</td>
<td>36</td>
</tr>
<tr>
<td>2.17</td>
<td>Preprocessing for ACSL</td>
<td>36</td>
</tr>
<tr>
<td>3</td>
<td>Libraries</td>
<td>37</td>
</tr>
<tr>
<td>4</td>
<td>Conclusion</td>
<td>39</td>
</tr>
</tbody>
</table>
This document describes version 1.17 of the E-ACSL specification language. It is based on the ACSL specification language [2]. Features of both languages may still evolve in the future, even if we do our best to preserve backward compatibility. In particular, some features are considered experimental, meaning that their syntax and semantics is not yet fixed. These features are marked with EXPERIMENTAL.

**Acknowledgements**

We gratefully thank all the people who contributed to this document: Patrick Baudin, Bernard Botella, Thibaut Benjamin, Loïc Correnson, Pascal Cuq, Basile Desloges, Johannes Kanig, André Maroneze, Fonenantsoa Maurica, David Mentré, Benjamin Monate, Yannick Moy and Virgile Prevosto.
Chapter 1

Introduction

This document is a reference manual for E-ACSL. E-ACSL is an acronym for “Executable ANSI/ISO C Specification Language”. It is an “executable” subset of ACSL [2] implemented [3] in the FRAMA-C platform [7]. Contrary to ACSL, each E-ACSL specification is executable: it may be evaluated at runtime.

In this document, we assume that the reader has a good knowledge of both ACSL [2] and the ANSI C programming language [8, 9].

1.1 Organization of this document

This document is organized in the very same way that the reference manual of ACSL [2]. Instead of being a fully new reference manual, this document points out the differences between E-ACSL and ACSL. Each E-ACSL construct which is not pointed out must be considered to have the very same semantics than its ACSL counterpart. For clarity, each relevant grammar rules are given in BNF form in separate figures like the ACSL reference manual does. In these rules, constructs with semantic changes are displayed in blue.

1.2 Generalities about Annotations

No difference with ACSL.

1.3 Notations for grammars

No difference with ACSL.
2.1 Lexical rules

No difference with ACSL.

2.2 Logic expressions

No difference with ACSL, but the quantifications must be guarded.

More precisely, the grammars of terms and binders presented respectively Figures 2.1 and 2.3 are the same than the ones of ACSL, while Figure 2.2 presents the grammar of predicates. The only differences introduced by E-ACSL with respect to ACSL are the fact that the quantifications that must be guarded and the introduction of iterators.

Quantification

The general form of quantifications (called generalized quantifications below), as described in Fig. 2.2, is restricted to a few finite enumerable types: the types of bound variables must be C integer types, enum types, pointer types, or their aliases.

Generalized quantification over large types (for instance, types containing $2^{32}$ elements) are unlikely evaluated efficiently at runtime.

In addition to generalized quantifications, a restricted form of guarded quantifications described in Fig. 2.4 is also recognized for (possibly infinite) enumerable types (typically, integer). In guarded quantifications, each bound variable must be guarded exactly once and, if its bounds depend on other bound variables, these variables must be guarded earlier or guarded by the same guard. Additionnally, guards are limited to bound variables, meaning that the only allowed identifiers id are variable identifiers enclosed in the binder list.

Example 2.1 The following predicates are (labeled) guarded quantifications:

- sorted: $\forall integer\ i, j; 0 <= i <= j < \text{len} \Rightarrow a[i] <= a[j]$
- is_c: $\exists u8 \ast q; p <= q < p + \text{len} \& \& \ast q == (u8)c$
### Figure 2.1: Grammar of terms. The terminals \textit{id}, \textit{C-type-name}, and various literals are the same as the corresponding C lexical tokens.
### 2.2. LOGIC EXPRESSIONS

<table>
<thead>
<tr>
<th>rel-op</th>
<th>::=</th>
<th>==</th>
<th>!=</th>
<th>&lt;=</th>
<th>&gt;=</th>
<th>&gt;</th>
<th>&lt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>pred</td>
<td>::=</td>
<td>\true</td>
<td>\false</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>term (rel-op term)† comparisons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>id (term (, term)* ) predicate application</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>( pred ) parentheses</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pred &amp;&amp; pred conjunction</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pred</td>
<td></td>
<td>pred disjunction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pred ==&gt; pred implication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pred &lt;==&gt; pred equivalence</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>! pred negation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pred ^^ pred exclusive or</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>term ? pred : pred ternary condition</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>pred ? pred : pred</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>\let id = term ; pred local binding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>\let id = pred ; pred</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>\forall binders ; univ. integer quantification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>integer-guards ==&gt; pred</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>\exists binders ; exist. integer quantification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>integer-guards &amp;&amp; pred</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>\forall binders ; univ. iterator quantification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>iterator-guard ==&gt; pred</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>\exists binders ; exist. iterator quantification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>iterator-guard &amp;&amp; pred</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>\forall binders ; pred univ. quantification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>\exists binders ; pred exist. quantification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>id : pred syntactic naming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>string : pred syntactic naming</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>integer-guards</td>
<td>::=</td>
<td>interv (&amp;&amp; interv)*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>interv</td>
<td>::=</td>
<td>(term integer-guard-op)†</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>id (integer-guard-op term)*</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>integer-guard-op</td>
<td>::=</td>
<td>&lt;=</td>
<td>&lt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iterator-guard</td>
<td>::=</td>
<td>id ( term , term )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 2.2:** Grammar of predicates
CHAPTER 2. SPECIFICATION LANGUAGE

binders ::= binder (, binder)*

binder ::= type-expr variable-ident
          (,variable-ident)*

type-expr ::= logic-type-expr | C-type-name

logic-type-expr ::= built-in-logic-type
                  | id

built-in-logic-type ::= boolean | integer | real

variable-ident ::= id | * variable-ident
                 | variable-ident []
                 | ( variable-ident )

Figure 2.3: Grammar of binders and type expressions

guarded-quantif ::= \forall binders ; (guards ==>)+ pred
                  | \exists binders ; guards && pred

guards ::= interv (&& interv)*

interv ::= term (guard-op id)+ guard-op term

guard-op ::= <= | <

Figure 2.4: Grammar of guarded quantifications.

Iterator quantification

For iterating over other data structures, E-ACSL introduces a notion of iterators over types that are introduced by a specific construct which attaches two sets — namely nexts and guards — to a binary predicate over a type \( \tau \). This construct is described by the grammar of Figure 2.5. For a type \( \tau \), nexts is a set of terms, and guards a set of predicates of the

iterator ::= \forall binders ; iterator-guard ==> pred
           | \exists binders ; iterator-guard && pred

iterator-guard ::= id ( term , term )

declaration ::= //@ iterator id ( wildcard-param , wildcard-param ) :
               nexts terms ; guards predicates ;

wildcard-param ::= parameter
                 | _

terms ::= term (, term)*

predicates ::= predicate (, predicate)*

Figure 2.5: Grammar of iterator declarations

same cardinal. Each term in nexts is a function taking an argument of type \( \tau \) and returning a value of type \( \tau \) which is a successor of its argument. Each predicate in the set guards takes an element of type \( \tau \), and is valid (resp. invalid) to indicate that the iteration should
continue on the corresponding successor (resp. stop at the given argument).

Furthermore, the guard of a quantification using an iterator must be the predicate given in the definition of the iterator. This abstract binary predicate takes two arguments of the same type. One of them must be unnamed by using a wildcard (character underscore `_`). The unnamed argument must be bound to the quantifier, while the other corresponds to the term from which the iteration begins.

**Example 2.2** The following example introduces binary trees and a predicate which is valid if and only if each value of a binary tree is even.

```c
struct btree {
    int val;
    struct btree *left, *right;
};

/*@ iterator access(_, struct btree *t):
@ nexts t->left, t->right;
@ guards \valid(t->left), \valid(t->right); */

/*@ predicate is_even(struct btree *t) =
@ \forall struct btree *tt; access(tt, t) ==> tt->val % 2 == 0; */
```

### 2.2.1 Operators precedence

*No difference with ACSL.*

Figure 2.6 summarizes operator precedences.

### 2.2.2 Semantics

*No difference with ACSL, but undefinedness and same laziness than C.*

More precisely, while ACSL is a 2-valued logic with only total functions, E-ACSL is a 3-valued logic with partial functions since terms and predicates may be “undefined”.

In this logic, the semantics of a term denoting a C expression $e$ is undefined if $e$ leads to a runtime error. Consequently the semantics of any term $t$ (resp. predicate $p$) containing a C expression $e$ leading to a runtime error is undefined if $e$ has to be evaluated in order to evaluate $t$ (resp. $p$).

**Example 2.3** The semantics of all the below predicates are undefined:

- $1/0 == 1/0$
- $f(*p)$ for any logic function $f$ and invalid pointer $p$

Furthermore, C-like operators `&&`, `||`, and `_ ? _ : _` are lazy like in C: their right members are evaluated only if required. Thus the amount of undefinedness is limited. Consequently, predicate $p == q$ is also lazy since it is equivalent to $1p || q$. It is also the case for guarded quantifications since guards are conjunctions and for ternary condition since it is equivalent to a disjunction of implications.
Example 2.4 All the predicates below are well defined. The first, second and fourth predicates are invalid, whereas the third one is valid:

- \( \false \land 1/0 == 1/0 \)
- \( \forall \text{ integer } x, -1 <= x <= 1 ==> 1/x > 0 \)
- \( \forall \text{ integer } x, 0 <= x <= 0 ==> \false ==> -1 <= 1/x <= 1 \)
- \( \exists \text{ integer } x, 1 <= x <= 0 \land -1 <= 1/0 <= 1 \)

In particular, the second one is invalid since the quantification is in fact an enumeration over a finite number of elements, it amounts to \( 1/-1 > 0 \land 1/0 > 0 \land 1/1 > 0 \). The first atomic proposition is invalid, so the rest of the conjunction (and in particular \( 1/0 \)) is not evaluated. The fourth one is invalid since it is an existential quantification over an empty range.

A contrario the semantics of the predicates below is undefined:

- \( 1/0 == 1/0 \land \false \)
- \( -1 <= 1/0 <= 1 ==> \true \)
- \( \exists \text{ integer } x, -1 <= x <= 1 \land -1 <= 1/x <= 0 \)

Furthermore, casting a term denoting a C expression \( e \) to a smaller type \( \tau \) is undefined if \( e \) is not representable in \( \tau \).
Example 2.5 Below, the first term is well-defined, while the second one is undefined.

- (char)127
- (char)128

Handling undefinedness in tools It is the responsibility of each tool which interprets E-ACSL to ensure that an undefined term is never evaluated. For instance, it may exit with a proper error message or, if it generates C code, it may guard each generated undefined C expression in order to be sure that they are always safely used. This behavior is consistent with both ACSL [2] and mainstream specification languages for runtime assertion checking like JML [10]. Consistency means that, if it exists and is defined, the E-ACSL predicate corresponding to a valid (resp. invalid) ACSL predicate is valid (resp. invalid). Thus it is possible to reuse tools interpreting ACSL (e.g., FRAMA-C’s Eva [4] or WP [1] in order to interpret E-ACSL, and it is also possible to perform runtime assertion checking of E-ACSL predicates in the same way than JML predicates. Reader interested by the implications (especially issues) of such a choice may read the articles of Patrice Chalin on that topic [5, 6].

2.2.3 Typing

No difference with ACSL.

2.2.4 Integer arithmetic and machine integers

No difference with ACSL.

2.2.5 Real numbers and floating point numbers

No difference with ACSL, but no quantification over real numbers and floating point numbers. Exact real numbers and even operations over floating point numbers are usually difficult to implement. Thus, most tools may not support them (or may support them partially).

More precisely, most real numbers are not representable at runtime with an infinite precisions. Consequently, most operations over them (e.g., equality) cannot be computed at runtime with an arbitrary precision. In such cases, it is the responsibility of each tool which interprets E-ACSL to specify the level of precision (e.g., $1e^{-6}$) up to which it is sound, and/or to emit undefined verdicts (e.g., “unknown”).

2.2.6 C arrays and pointers

No difference with ACSL.

Ensuring validity of memory accesses is usually difficult to implement, since it requires the implementation of a memory model. Thus, most tools may not support it (or may support it partially).
2.2.7 Structures, Unions and Arrays in logic

No difference with ACSL.
Logic arrays without an explicit length are usually difficult to implement. Thus, most tools may not support them (or may support them partially).

2.3 Function contracts

No difference with ACSL, but no clause terminates.

Figure 2.7 shows the grammar of function contracts. This is a simplified version of ACSL one without terminates clauses. Section 2.5 explains why E-ACSL has no terminates clause.

```
function-contract ::= requires-clause* decreases-clause? simple-clause* named-behavior* completeness-clause*
clause-kind ::= check | admit
requires-clause ::= clause-kind? requires pred ;
decreases-clause ::= decreases term (for ident)? ;
simple-clause ::= assigns-clause | ensures-clause | allocation-clause | abrupt-clause
assigns-clause ::= assigns locations ;
locations ::= locations-list | \nothing
locations-list ::= location (, location)*
location ::= tset
ensures-clause ::= clause-kind? ensures pred ;
named-behavior ::= behavior id : behavior-body
behavior-body ::= assumes-clause* requires-clause* simple-clause*
assumes-clause ::= assumes pred ;
completeness-clause ::= complete behaviors (id (, id)*)? ;
| disjoint behaviors (id (, id)*)? ;
```

Figure 2.7: Grammar of function contracts

2.3.1 Built-in constructs \old and \result

No difference with ACSL.

Figure 2.8 summarizes the grammar extension of terms with \old and \result.

2.3.2 Simple function contracts

No difference with ACSL.
2.3 FUNCTION CONTRACTS

\begin{align*}
term & ::= \text{\old ( term )} \quad \text{old value} \\
     & \mid \text{\result} \quad \text{result of a function} \\
pred & ::= \text{\old ( pred )} \\
\end{align*}

Figure 2.8: \old and \result in terms

assigns is usually difficult to implement, since it requires the implementation of a memory model. Thus, most tools may not support it (or may support it partially).

2.3.3 Contracts with named behaviors

No difference with ACSL.

2.3.4 Memory locations and sets of terms

No difference with ACSL, but ranges and set comprehensions are limited in order to be finite. Figure 2.9 describes the grammar of sets of terms. There are two differences with ACSL:

- ranges necessarily have lower and upper bounds;
- a guard for each binder is required when defining set comprehension. The requested constraints for guards are the very same than the ones for quantifications.

\begin{align*}
\text{range} & ::= \text{term} \ldots \text{term} \\
\text{tset} & ::= \text{\emptyset} \quad \text{empty set} \\
     & \mid \text{tset } \to \text{id} \\
     & \mid \text{tset } \ldots \text{id} \\
     & \mid \ast \text{tset} \\
     & \mid \& \text{tset} \\
     & \mid \text{tset } [ \text{tset } ] \\
     & \mid \text{tset } [ \text{range } ] \\
     & \mid ( \text{range } ) \quad \text{a range as a set of integers} \\
     & \mid \text{\union ( tset , tset)*} \quad \text{union of location sets} \\
     & \mid \text{\inter ( tset , tset)*} \quad \text{intersection of location sets} \\
     & \mid \text{tset } + \text{tset} \\
     & \mid \{ \text{tset } \mid \text{binders ; constraints } \} \quad \text{set comprehension} \\
     & \mid \{ ( \text{term } (, \text{term})^* ) \} \quad \text{explicit set} \\
     & \mid \text{term} \quad \text{implicit singleton} \\
pred & ::= \text{\subset ( tset , tset )} \quad \text{set inclusion} \\
     & \mid \text{term } \text{\in tset} \quad \text{set membership} \\
\text{constraints} & ::= \text{\guard} (\&\& \text{pred}) \\
\end{align*}

Figure 2.9: Grammar for sets of terms

Example 2.6 The set \{ x \mid \text{integer } x; 0 <= x <= 10 \&\& x \% 2 == 0\} denotes the set of even integers between 0 and 10.
CHAPTER 2. SPECIFICATION LANGUAGE

2.3.5 Default contracts, multiple contracts

No difference with ACSL.

2.4 Statement annotations

2.4.1 Assertions

No difference with ACSL.

Figure 2.10 summarizes the grammar for assertions.

\[
C\text{-}\text{compound}\text{-}\text{statement} ::= \{ C\text{-}\text{declaration}^* \}
\]

\[
C\text{-}\text{statement} ::= \text{assertion} \quad \text{C\text{-}\text{statement}}
\]

\[
\text{assertion\text{-}kind} ::= \text{assert} \quad \text{assertion} \quad \text{non-blocking assertion}
\]

\[
\text{assertion} ::= /*@ \text{assertion\text{-}kind} \text{pred} ; */ \quad \text{for id (, id)* : \text{assertion\text{-}kind} \text{pred} ; */}
\]

Figure 2.10: Grammar for assertions

2.4.2 Loop annotations

No difference with ACSL, but loop invariants lose their inductive nature.

Figure 2.11 shows the grammar for loop annotations. There is no syntactic difference with ACSL.

Loop allocation and loop assigns are usually difficult to implement, since they require the implementation of a memory model. Thus, most tools may not support them (or may support them partially).

Loop invariants

The semantics of loop invariants is the same than the one defined in ACSL, except that they are not inductive. More precisely, if one does not take care of side effects (the semantics of specifications about side effects in loop is the same in E-ACSL than the one in ACSL), a loop invariant \( I \) is valid in ACSL if and only if:

- \( I \) holds before entering the loop; and

- if \( I \) is assumed true in some state where the loop condition \( c \) is also true, and if the execution of the loop body in that state ends normally at the end of the body or with a 'continue' statement, \( I \) is true in the resulting state.
In E-ACSL, the same loop invariant $I$ is valid if and only if:

- $I$ holds before entering the loop; and
- if the execution of the loop body in that state ends normally at the end of the body or with a 'continue' statement, $I$ is true in the resulting state.

Thus the only difference with ACSL is that E-ACSL does not assume that the invariant previously holds when one checks that it holds at the end of the loop body. In other words a loop invariant $I$ is equivalent to putting an assertion $I$ just before entering the loop and at the very end of the loop body.

**Example 2.7** In the following, `bsearch(t,n,v)` searches for element $v$ in array $t$ between indices 0 and $n-1$.

```c
/*@ requires n > = 0 && \valid(t+(0..n-1)); @
@ assigns \nothing;
@ ensures -1 <= \result <= n-1;
@ behavior success:
  @ ensures \result >= 0 ==> t[\result] == v;
@ behavior failure:
  @ assumes t_is_sorted : \forallall integer k1, int k2;
  @ 0 <= k1 <= k2 <= n-1 ==> t[k1] <= t[k2];
  @ ensures \result == -1 ==>
  @ \forallall integer k; 0 <= k < n ==> t[k] != v;
/*@*/
int bsearch(double t[], int n, double v) { int l = 0, u = n-1;
 /*@ loop invariant 0 <= l && u <= n-1;
  @ for failure: loop invariant
  @ \forallall integer k; 0 <= k < n ==> t[k] == v ==> 1 <= k <= u;
  @*/
  while (l < u) {
    int m = l + (u-l)/2; // better than (l+u)/2
```
In E-ACSL, this annotated function is equivalent to the following one since loop invariants are not inductive.

```c
int bsearch(double t[], int n, double v) {
    int l = 0, u = n-1;
    /*@ assert 0 <= l && u <= n-1; @*/
    while (l <= u) {
        int m = l + (u-l)/2; // better than (l+u)/2
        if (t[m] < v) l = m + 1;
        else if (t[m] > v) u = m - 1;
        else return m;
        /*@ assert 0 <= l && u <= n-1; @*/
    }
    return -1;
}
```

**General inductive invariant**

The syntax of this kind of invariant is shown Figure 2.12.

```plaintext
assertion ::=
    /*@ clause-kind invariant pred ; */
    | /*@ for id (, id)* : clause-kind invariant pred ; */
```

Figure 2.12: Grammar for general inductive invariants

In E-ACSL, a general inductive invariant may be written everywhere in a loop body, and is exactly equivalent to writing an assertion.
2.4. STATEMENT ANNOTATIONS

2.4.3 Built-in construct \at

No difference with ACSL, but no forward references.

The construct \at(t, id) (where id is a regular C label, a label added within a ghost statement or a default logic label) follows the same rule than its ACSL counterpart, except that a more restrictive scoping rule must be respected in addition to the standard ACSL scoping rule:

- when evaluating \at(t, id) at a program point p, the program point p' denoted by id must be reached before p in the program execution flow; and

- when evaluating \at(t, id), for each C left-value x that contributes to the definition of a (non-ghost) logic variable involved in t, the equality \at(x, id) == \at(x, Here) must hold, i.e. the value of x must not be modified between the program points id and Here.

Below, the first example illustrates the first constraint, whereas the second example illustrates the second constraint.

Example 2.8 In the following example, both assertions are accepted and valid in ACSL, but only the first one is accepted and valid in E-ACSL since evaluating the term \at(*p+\at(*q, Here)),L1) at L2 requires to evaluate the term \at(*q, Here) at L1: that is forbidden since L1 is executed before L2.

```c
/*@ requires \valid(p+(0..1));
@ requires \valid(q);
@*/
void f(int *p, int *q) {
    *p = 0;
    *(p+1) = 1;
    *q = 0;
    L1: *p = 2;
    *(p+1) = 3;
    *q = 1;
    L2:
    /*@ assert \let k = m + 1;
    \exists integer u; 9 <= u < 21 &&
    @*/
    return;
}
```

Example 2.9 In the following example, the first assertion is supported, while the second one is not supported. Indeed, in the second assertion, the guard defining the logic variable u depends on n whose value is modified between L1 and L2.

```c
main(void) {
    int m = 2;
    int n = 7;;
    L1: ;
    n = 4;
    L2:
    /*@ assert
    \let k = m + 1;
    \exists integer u; 9 <= u < 21 &&
    */
    return;
}
```
2.4.4 Statement contracts

No difference with ACSL.

Figure 2.13 shows the grammar of statement contracts.

2.5 Termination

No difference with ACSL, but no terminates clauses.

2.5.1 Integer measures

No difference with ACSL.

2.5.2 General measures

No difference with ACSL.

2.5.3 Recursive function calls

No difference with ACSL.

2.5.4 Non-terminating functions

No such feature in E-ACSL: whether a function is guaranteed to terminate if some predicate p holds is not a monitorable property.
2.6 Logic specifications

No difference with ACSL.

Figure 2.14 presents the grammar of logic definitions.

```
C-external-declaration ::= /*@ logic-def+ */
logic-def ::= logic-const-def
| logic-function-def
| logic-predicate-def
| lemma-def
| data-inv-def

type-var ::= id

type-expr ::= type-var  type variable
| id
| < type-expr
| (, type-expr)∗ > polymorphic type

type-var-binders ::= < type-var
| (, type-var)∗ >

poly-id ::= id type-var-binders polymorphic object identifier

logic-const-def ::= logic
| type-expr
| poly-id
= term ;

logic-function-def ::= logic
| type-expr
| poly-id
| parameters
= term ;

logic-predicate-def ::= predicate
| poly-id
| parameters?
= pred ;

parameters ::= ( parameter
| (, parameter)∗ )
	parameter ::= type-expr id

lemma-def ::= clause-kind
| lemma poly-id :
| pred ;
```

Figure 2.14: Grammar for global logic definitions

2.6.1 Predicate and function definitions

No difference with ACSL.
2.6.2 Lemmas

*No difference with ACSL.*

Lemmas are verified before running the function `main` but after initializing global variables.

2.6.3 Inductive predicates

*Experimental*

*No difference with ACSL.*

Figure 2.15 presents the grammar of inductive predicates.

```
logic-def ::= inductive-def
inductive-def ::= inductive
               poly-id parameters? { indcase* }
indcase ::= case poly-id : pred ;
```

Figure 2.15: Grammar for inductive predicates

Inductive predicates in all their generality are not monitorable. Therefore, future versions of this document will restrict them syntactically (e.g., to definite Horn clauses ([http://en.wikipedia.org/wiki/Horn_clause](http://en.wikipedia.org/wiki/Horn_clause)) and/or through semantic criteria.

2.6.4 Axiomatic definitions

*Experimental*

*No difference with ACSL.*

Figure 2.16 presents the grammar of axiomatic definitions.

Axiomatic definitions in all their generality are not monitorable. Therefore, future versions of this document will restrict them syntactically and/or through semantic criteria.

2.6.5 Polymorphic logic types

*No difference with ACSL.*

2.6.6 Recursive logic definitions

*No difference with ACSL.*

2.6.7 Higher-order logic constructions

*Experimental*

*No difference with ACSL.*

Figure 2.17 introduces new term constructs for higher-order logic.
2.6. LOGIC SPECIFICATIONS

\[
\begin{align*}
\text{logic-def} & ::= \text{axiomatic-decl} \\
\text{axiomatic-decl} & ::= \text{axiomatic id \{ logic-decl\* \}} \\
\text{logic-decl} & ::= \text{logic-def} \\
& \quad | \text{logic-type-decl} \\
& \quad | \text{logic-const-decl} \\
& \quad | \text{logic-predicate-decl} \\
& \quad | \text{logic-function-decl} \\
& \quad | \text{axiom-def} \\
\text{logic-type-decl} & ::= \text{type logic-type ;} \\
\text{logic-type} & ::= \text{id} \\
& \quad | \text{id type-var-binders polymorphic type} \\
\text{logic-const-decl} & ::= \text{logic type-expr poly-id ;} \\
\text{logic-function-decl} & ::= \text{logic type-expr} \\
& \quad \text{poly-id parameters ;} \\
\text{logic-predicate-decl} & ::= \text{predicate} \\
& \quad \text{poly-id parameters? ;} \\
\text{axiom-def} & ::= \text{axiom poly-id : pred ;}
\end{align*}
\]

Figure 2.16: Grammar for axiomatic declarations

\[
\begin{align*}
\text{term} & ::= \lambda \text{binders ; term} \quad \text{abstraction} \\
& \quad | \text{ext-quantifier ( term , term , term )} \\
& \quad | \{ \text{term \ with [ range ] = term } \\
\text{ext-quantifier} & ::= \max | \min | \sum \\
& \quad | \text{product | numof}
\end{align*}
\]

Figure 2.17: Grammar for higher-order constructs
### 2.6.8 Concrete logic types

**Experimental**

*No difference with ACSL.*

Figure 2.18 introduces new constructs for defining logic types and the associated new terms.

---

**logic-def** ::= type logic-type = logic-type-def ;

**logic-type-def** ::= record-type
                             | sum-type
                             | product-type
                             | function-type
                             | type-expr

**record-type** ::= { type-expr id ( ; type-expr id)* ;? }

**function-type** ::= ( ( type-expr (, type-expr )*? ) ? ) -> type-expr

**sum-type** ::= |? constructor ( | constructor)*

**constructor** ::= id constant constructor
                        | id
                                ( type-expr
                                (, type-expr)*
                                ) non-constant constructor

**product-type** ::= ( type-expr
                        (, type-expr)+
                        ) product type

**term** ::= term . id record field access
               | \match term
                    { match-cases } pattern-matching
                    | ( term (, term)+ ) tuples
                    | { (. id = term ;)* } records
                    | \let ( id (, id)+ ) = term ; term

**match-cases** ::= match-case+

**match-case** ::= case pat : term

**pat** ::= id constant constructor
             | id ( pat (, pat)* ) non-constant constructor
             | pat | pat or pattern
             | _ any pattern
             | literal | \{ (. id = pat)* \} record pattern
             | ( pat (, pat)* ) tuple pattern
             | pat as id pattern binding

---

Figure 2.18: Grammar for concrete logic types and pattern-matching
2.6.9 Hybrid functions and predicates

_No difference with ACSL._

Hybrid functions and predicates are usually difficult to implement, since they require the implementation of a memory model (or at least to support `at`). Thus, most tools may not support them (or may support them partially).

2.6.10 Memory footprint specification: reads clause

_Experimental_

_No difference with ACSL._

Figure 2.19 introduces reads clauses.

```plaintext
logic-function-decl ::= logic type-expr poly-id
parameters reads-clause ;
logic-predicate-decl ::= predicate poly-id
parameters? reads-clause ;
reads-clause ::= reads locations
logic-function-def ::= logic type-expr poly-id
parameters reads-clause = term ;
logic-predicate-def ::= predicate poly-id
parameters? reads-clause = pred ;
```

Figure 2.19: Grammar for logic declarations with reads clauses

Read clauses are usually difficult to implement, since they require the implementation of a memory model. Thus, most tools may not support them (or may support them partially).

2.6.11 Specification Modules

_No difference with ACSL._

2.7 Pointers and physical addressing

_No difference with ACSL._

Figure 2.20 shows the additional constructs for terms and predicates which are related to memory location.

2.7.1 Memory blocks and pointer dereferencing

_No difference with ACSL._

All memory-related built-in functions and predicates are usually difficult to implement, since they require the implementation of a memory model. Thus, most tools may not support them (or may support them partially).
2.7.2 Separation

No difference with ACSL.
\texttt{\textbackslash separated} is usually difficult to implement, since it requires the implementation of a memory model. Thus, most tools may not support it (or may support it partially).

2.7.3 Dynamic allocation and deallocation

No difference with ACSL.
All these constructs are usually difficult to implement, since they require the implementation of a memory model. Thus, most tools may not support them (or may support them partially).

Figure 2.21 introduces grammar for dynamic allocations and deallocations.

2.8 Sets and lists

2.8.1 Finite sets

No difference with ACSL.
2.9. ABRUPT TERMINATION

Figure 2.22: Notations for built-in list datatype

### Finite lists

*No difference with ACSL.*

Figure 2.22 shows the notations for built-in lists.

#### Abrupt termination

*No difference with ACSL.*

Figure 2.23 shows the grammar of abrupt terminations.

$$
\begin{align*}
\text{term} &::= [ \mid ] \quad \text{empty list} \\
& \mid [ \mid \text{term} , \text{term}\mid ]^* \mid ] \quad \text{list of elements} \\
& \mid \text{term} \ ^\wedge \text{term} \quad \text{list concatenation (overloading bitwise-xor operator)} \\
& \mid \text{term} \ ^\ast \text{term} \quad \text{list repetition}
\end{align*}
$$

Figure 2.23: Grammar of contracts about abrupt terminations

2.10 Dependencies information

*Experimental

*No difference with ACSL.*

Figure 2.24 shows the grammar for dependencies information.

$$
\begin{align*}
\text{assigns-clause} &::= \text{assigns locations-list (from locations)}^2 ; \\
& \mid \text{assigns term (from locations = term)} ;
\end{align*}
$$

Figure 2.24: Grammar for dependencies information
2.11 Data invariants

No difference with ACSL.

Figure 2.25 summarizes grammar for declarations of data invariants.

\[
\begin{align*}
\text{data-inv-def} & ::= \text{data-invariant} \mid \text{type-invariant} \\
\text{data-invariant} & ::= \text{inv-strength} ? \text{global invariant} \\
& \quad \quad \text{id} : \text{pred} ; \\
\text{type-invariant} & ::= \text{inv-strength} ? \text{type invariant} \\
& \quad \quad \text{id} (\ C\text{-type-name} \text{id} ) = \text{pred} ; \\
\text{inv-strength} & ::= \text{weak} \mid \text{strong}
\end{align*}
\]

Figure 2.25: Grammar for declarations of data invariants

Strong invariants are unlikely evaluated efficiently at runtime.

2.11.1 Semantics

No difference with ACSL.

2.11.2 Model variables and model fields

No difference with ACSL.

Figure 2.26 summarizes the grammar for declarations of model variables and fields.

\[
\begin{align*}
\text{logic-def} & ::= \text{model parameter} ; \quad \text{model variable} \\
& \quad \quad \text{model C-type-name} \{ \text{parameter} ; ? \} ; \quad \text{model field}
\end{align*}
\]

Figure 2.26: Grammar for declarations of model variables and fields

2.12 Ghost variables and statements

No difference with ACSL.

Figure 2.27 summarizes the grammar for ghost statements which is the same than the one of ACSL.

2.12.1 Volatile variables

Figure 2.28 summarizes the grammar for volatile constructs.
2.12. GHOST VARIABLES AND STATEMENTS

\[
\begin{align*}
C\text{-type-qualifier} &::= \text{ghost} & \text{only in ghost} \\
C\text{-type-specifier} &::= \text{logic-type} \\
\text{logic-def} &::= \text{ghost } C\text{-declaration} \\
C\text{-direct-declarator} &::= \text{C-direct-declarator} \quad \text{function declarator} \\
\text{C-parameter-type-list} &\quad \text{(C-parameter-type-list)?} \\
\text{ghost (} &\text{C-parameter-type-list} \quad \text{with ghost params} \\
\text{C-parameter-type-list} &\text{)} */ \\
C\text{-postfix-expression} &::= \text{C-postfix-expression} \quad \text{function call} \\
\text{C-argument-expression-list} &\quad \text{(C-argument-expression-list)?} \\
\text{ghost (} &\text{C-argument-expression-list} \quad \text{with ghost args} \\
\text{C-argument-expression-list} &\text{)} */ \\
C\text{-statement} &::= \text{/*\ ghost} \quad \text{function code} \\
\text{C-statement}^+ \quad \text{ghost code} \\
\text{C-statement}^* &\quad \text{unconditional ghost code} \\
| &\quad \text{if (C-expression )} \\
\text{C-statement} &\quad \text{ghost alternative} \\
\text{C-statement}^* &\quad \text{unconditional ghost code} \\
\text{C-struct-declaration} &::= \text{/*\ ghost} \quad \text{ghost field} \\
\text{C-struct-declaration}^* &\quad \text{ghost field} \\
\end{align*}
\]

Figure 2.27: Grammar for ghost statements

\[
\begin{align*}
\text{logic-def} &::= //\@ \text{volatile } \text{locations (reads ident)? (writes ident)? ;}
\end{align*}
\]

Figure 2.28: Grammar for volatile constructs

35
2.13 Initialization and undefined values

No difference with ACSL.

\texttt{initialized} is usually difficult to implement, since it requires the implementation of a memory model. Thus, most tools may not support it (or may support it partially).

2.14 Dangling pointers

No difference with ACSL.

\texttt{dangling} is usually difficult to implement, since it requires the implementation of a memory model. Thus, most tools may not support it (or may support it partially).

2.15 Well-typed pointers

No such feature in E-ACSL: it would require the implementation of a C type system at runtime.

2.16 Logic attribute annotations

No such feature in E-ACSL: logic attributes are implementation dependent; therefore their meaning cannot be guessed by a general-purpose (runtime) verification tool.

2.17 Preprocessing for ACSL

No difference with ACSL.
Chapter 3

Libraries

Disclaimer: this chapter is empty on purpose. It is left here to be consistent with the ACSL reference manual [2].
Chapter 4

Conclusion

This document presents an Executable ANSI/ISO C Specification Language. It provides a subset of ACSL [2] implemented [3] in the FRAMA-C platform [7] in which each construct may be evaluated at runtime. The specification language described here is intended to evolve in the future in two directions. First it is based on ACSL which is itself still evolving. Second the considered subset of ACSL may also change.
Appendix A

Appendices
A.1 Changes

Version 1.17

- **Section 2.2**: xor \(^{\wedge}\) is not lazy.
- **Section 2.2**: new extended syntax for quantifications.
- **Section 2.2.5**: additional remark about real numbers and operations over them.
- **Section 2.3.4**: new extended syntax for set comprehensions.
- **Section 2.4.3**: more restrictive scoping rule for \(\text{at}\) constructs.
- **Section 2.6**: add lemmas and data invariants.
- **Section 2.6.3**: add inductive predicates experimentally: the accepted subset will be refined in a future version.
- **Section 2.6.4**: add axiomatic declarations experimentally: the accepted subset will be refined in a future version.
- **Section 2.6.5**: add polymorphic logic types.
- **Section 2.6.7**: add higher-order logic constructions.
- **Section 2.6.8**: add concrete logic types.
- **Section 2.6.10**: add \texttt{read} clauses.
- **Section 2.10**: add dependencies information.
- **Section 2.12.1**: add volatile constructs.

Version 1.16

- Update according to ACSL 1.16
  - **Section 2.3**: add the \texttt{check} and \texttt{admit} clause kinds.
  - **Section 2.4.1**: add the \texttt{check} and \texttt{admit} clause kinds.
  - **Section 2.4.2**: add the \texttt{check} and \texttt{admit} clause kinds.

Version 1.15

- Update according to ACSL 1.15:
  - **Section 2.12**: add the \texttt{ghost} qualifier.

Version 1.14

- Update according to ACSL 1.14:
  - **Section 2.4.1**: add the keyword \texttt{check}. 
A.1. CHANGES

Version 1.13

- Update according to ACSL 1.13:
  - Section 2.3.4: add syntax for set membership.

Version 1.12

- Update according to ACSL 1.12:
  - Section 2.3.4: add subsections for build-in lists.
  - Section 2.4.4: fix syntax rule for statement contracts in allowing completeness clauses.
  - Section 2.7.1: add syntax for defining a set by giving explicitly its element.
  - Section 2.15: new section.

Version 1.9

- Section 2.7.3: new section.
- Update according to ACSL 1.9.

Version 1.8

- Section 2.3.4: fix example 2.6.
- Section 2.7: add grammar of memory-related terms and predicates.

Version 1.7

- Update according to ACSL 1.7.
- Section 2.7.2: no more absent.

Version 1.5-4

- Fix typos.
- Section 2.2: fix syntax of guards in iterators.
- Section 2.2.2: fix definition of undefined terms and predicates.
- Section 2.2.3: no user-defined types.
- Section 2.3.1: no more implementation issue for \old.
- Section 2.4.3: more restrictive scoping rule for label references in \at.
Version 1.5-3

- Fix various typos.
- Warn about features known to be difficult to implement.
- Section 2.2: fix semantics of ternary operator.
- Section 2.2: fix semantics of cast operator.
- Section 2.2: improve syntax of iterator quantifications.
- Section 2.2.2: improve and fix example 2.4.
- Section 2.4.2: improve explanations about loop invariants.
- Section 2.6.9: add hybrid functions and predicates.

Version 1.5-2

- Section 2.2: remove laziness of operator $\Leftarrow$.
- Section 2.2: restrict guarded quantifications to integer.
- Section 2.2: add iterator quantifications.
- Section 2.2: extend unguarded quantifications to char.
- Section 2.3.4: extend syntax of set comprehensions.
- Section 2.4.2: simplify explanations for loop invariants and add example.

Version 1.5-1

- Fix many typos.
- Highlight constructs with semantic changes in grammars.
- Explain why unsupported features have been removed.
- Indicate that experimental ACSL features are unsupported.
- Add operations over memory like $\texttt{\valid}$.
- Section 2.2: lazy operators $\&\&, \mid\mid$, $\wedge\wedge$, $\Rightarrow$ and $\Leftarrow$.
- Section 2.2: allow unguarded quantification over boolean.
- Section 2.2: revise syntax of $\exists$.
- Section 2.2.2: better semantics for undefinedness.
- Section 2.3.4: revise syntax of set comprehensions.
- Section 2.4.2: add loop invariants, but they lose their inductive ACSL nature.
- Section 2.5.2: add general measures for termination.
- Section 2.6.11: add specification modules.
Version 1.5-0

- Initial version.
Bibliography


<table>
<thead>
<tr>
<th>Figure</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1</td>
<td>Grammar of terms. The terminals <em>id</em>, <em>C-type-name</em>, and various literals are the same as the corresponding C lexical tokens.</td>
<td>14</td>
</tr>
<tr>
<td>2.2</td>
<td>Grammar of predicates</td>
<td>15</td>
</tr>
<tr>
<td>2.3</td>
<td>Grammar of binders and type expressions</td>
<td>16</td>
</tr>
<tr>
<td>2.4</td>
<td>Grammar of guarded quantifications.</td>
<td>16</td>
</tr>
<tr>
<td>2.5</td>
<td>Grammar of iterator declarations</td>
<td>16</td>
</tr>
<tr>
<td>2.6</td>
<td>Operator precedence</td>
<td>18</td>
</tr>
<tr>
<td>2.7</td>
<td>Grammar of function contracts</td>
<td>20</td>
</tr>
<tr>
<td>2.8</td>
<td><code>\old</code> and <code>\result</code> in terms</td>
<td>21</td>
</tr>
<tr>
<td>2.9</td>
<td>Grammar for sets of terms</td>
<td>21</td>
</tr>
<tr>
<td>2.10</td>
<td>Grammar for assertions</td>
<td>22</td>
</tr>
<tr>
<td>2.11</td>
<td>Grammar for loop annotations</td>
<td>23</td>
</tr>
<tr>
<td>2.12</td>
<td>Grammar for general inductive invariants</td>
<td>24</td>
</tr>
<tr>
<td>2.13</td>
<td>Grammar for statement contracts</td>
<td>26</td>
</tr>
<tr>
<td>2.14</td>
<td>Grammar for global logic definitions</td>
<td>27</td>
</tr>
<tr>
<td>2.15</td>
<td>Grammar for inductive predicates</td>
<td>28</td>
</tr>
<tr>
<td>2.16</td>
<td>Grammar for axiomatic declarations</td>
<td>29</td>
</tr>
<tr>
<td>2.17</td>
<td>Grammar for higher-order constructs</td>
<td>29</td>
</tr>
<tr>
<td>2.18</td>
<td>Grammar for concrete logic types and pattern-matching</td>
<td>30</td>
</tr>
<tr>
<td>2.19</td>
<td>Grammar for logic declarations with <code>reads</code> clauses</td>
<td>31</td>
</tr>
<tr>
<td>2.20</td>
<td>Grammar extension of terms and predicates about memory</td>
<td>32</td>
</tr>
<tr>
<td>2.21</td>
<td>Grammar for dynamic allocations and deallocations</td>
<td>32</td>
</tr>
<tr>
<td>2.22</td>
<td>Notations for built-in list datatype</td>
<td>33</td>
</tr>
<tr>
<td>2.23</td>
<td>Grammar of contracts about abrupt terminations</td>
<td>33</td>
</tr>
<tr>
<td>2.24</td>
<td>Grammar for dependencies information</td>
<td>33</td>
</tr>
<tr>
<td>2.25</td>
<td>Grammar for declarations of data invariants</td>
<td>34</td>
</tr>
<tr>
<td>2.26</td>
<td>Grammar for declarations of model variables and fields</td>
<td>34</td>
</tr>
<tr>
<td>2.27</td>
<td>Grammar for ghost statements</td>
<td>35</td>
</tr>
<tr>
<td>2.28</td>
<td>Grammar for volatile constructs</td>
<td>35</td>
</tr>
</tbody>
</table>
Index

abrupt termination, 31
admit, 18
\allocable, 30
allocates, 30
\allocation, 30
annotation, 20
as, 28
assert, 20
assigns, 18, 21, 31
assumes, 18
\at, 23
axiom, 27
axiomatic, 27
\base_addr, 30
behavior, 19
behavior, 18, 24
behaviors, 18
\block_length, 30
boolean, 14
breaks, 31
case, 26, 28
check, 18
complete, 18
continues, 31
contract, 18, 24
data invariant, 32
decreases, 18
\decreases, 24
disjoint, 18
else, 33
\empty, 19
ensures, 18
\exists, 13, 14
\exit_status, 31
exits, 31
\false, 12, 13
for, 18, 20–22, 24
\forall, 13, 14
\freeable, 30
frees, 30
\fresh, 30
\from, 31
function behavior, 19
function contract, 18
ghost, 32
ghost, 33
\ghost, 33
global, 32
global invariant, 32
grammar entries
  C-compound-statement, 20
  C-direct-declarator, 33
  C-external-declaration, 25
  C-postfix-expression, 33
  C-statement, 20, 33
  C-struct-declaration, 33
  C-type-qualifier, 33
  C-type-specifier, 33
  abrupt-clause-stmt, 31
  abrupt-clause, 31
  allocation-clause, 30
  assertion-kind, 20
  assertion, 20, 22
  assigns-clause, 18, 31
  assumes-clause, 18
  axiom-def, 27
  axiomatic-decl, 27
  behavior-body-stmt, 24
  behavior-body, 18
  bin-op, 12
  binders, 14
  binder, 14
  breaks-clause, 31
  built-in-logic-type, 14
  clause-kind, 18

? 12, 13
_ 14, 28

51
completeness-clause, 18
constraints, 19
constructor, 28
continues-clause, 31
data-inv-def, 32
data-invariant, 32
declaration, 14
decreases-clause, 18
dyn-allocation-addresses, 30
ensures-clause, 18
exits-clause, 31
ext-quantifier, 27
function-contract, 18
function-type, 28
guard-op, 14
guarded-quantif, 14
guards, 14
ident, 12
indcase, 26
inductive-def, 26
integer-guard-op, 13
integer-guards, 13
interv, 13, 14
inv-strength, 32
iterator-guard, 13, 14
iterator, 14
lemma-def, 25
literal, 12
locations-list, 18
locations, 18
location, 18
logic-const-decl, 27
logic-const-def, 25
logic-decl, 27
logic-def, 25–28, 32, 33
logic-function-decl, 27, 29
logic-function-def, 25, 29
logic-predicate-decl, 27, 29
logic-predicate-def, 25, 29
logic-type-decl, 27
logic-type-def, 28
logic-type-expr, 14
logic-type, 27
loop-allocation, 30
loop-annot, 21
loop-assigns, 21
loop-behavior, 21
loop-clause, 21
loop-invariant, 21
loop-variant, 21
match-cases, 28
match-case, 28
named-behavior-stmt, 24
named-behavior, 18
one-label, 30
parameters, 25
parameter, 25
pat, 28
poly-id, 12, 25
predicates, 14
pred, 13, 25
product-type, 28
range, 19
reads-clause, 29
record-type, 28
rel-op, 13
requires-clause, 18
returns-clause, 31
simple-clause-stmt, 24
simple-clause, 18
statement-contract, 24
statement, 21, 24
sum-type, 28
terms, 14
term, 12, 19, 27, 28, 30, 31
tset, 19
two-labels, 30
type-expr, 14, 25
type-invariant, 32
type-var-binders, 25
type-var, 25
unary-op, 12
variable-ident, 14
 wildcard-param, 14
guards, 14

hybrid
  function, 29
  predicate, 29
if, 33
\in, 19
inductive, 26
inductive predicates, 26
integer, 14
\inter, 19
invariant, 20
data, 32
global, 32
INDEX

type, 32
invariant, 21, 22, 32
iterator, 14
\lambda, 27
lemma, 25
\let, 12, 13, 28
location, 30
logic, 25, 27, 29
logic specification, 25
loop, 21, 30
\match, 28
\max, 27
\min, 27
model, 32
model, 32
nexts, 14
\nothing, 18
\null, 30
\numof, 27

\offset, 30
\old, 19

polymorphism, 26
predicate, 25, 27, 29
\product, 27
reads, 29, 33
real, 14
recursion, 26
requires, 18
\result, 19
returns, 31

\separated, 30
sizeof, 12
specification, 25
statement contract, 24
strong, 32
\subset, 19
\sum, 27
termination, 24
\true, 12, 13
type
canonical, 28
polymorphic, 26
record, 28
sum, 28

\union, 19
\valid, 30
\valid_read, 30
variant, 21
\variant, 24
volatile, 32, 33
weak, 32
\with, 12, 27
\writes, 33