# Revisions

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td></td>
<td>Initial version</td>
</tr>
</tbody>
</table>
INDEX

Revisions........................................................................................................... 2
Index................................................................................................................... 3
I Introduction...................................................................................................... 6
II Usage.............................................................................................................. 7
II.1 Usage with AtelierB tool............................................................................ 7
II.2 Advanced users – Bart command line..................................................... 7
   II.2.1 Command usage................................................................................. 8
   II.2.2 Input files........................................................................................... 8
   II.2.3 Visibility for loaded components...................................................... 8
   II.2.4 Bart standard output verbosity................................................................. 9
   II.2.5 Bart rule trace.................................................................................. 10
III Automatic refinement principles............................................................. 11
   III.1 Refined elements............................................................................... 11
      III.1.1 Abstract variables...................................................................... 11
      III.1.2 Operations.................................................................................. 11
      III.1.3 Initialisation.............................................................................. 12
      III.1.4 Process...................................................................................... 12
   III.2 Pattern-Matching............................................................................... 12
      III.2.1 Jokers syntax............................................................................. 13
      III.2.2 Pattern matching...................................................................... 13
   III.3 Refinement rules................................................................................ 14
      III.3.1 Introduction............................................................................... 14
      III.3.2 Constraints............................................................................... 14
      III.3.3 Guards..................................................................................... 15
      III.3.4 Rule checking process................................................................. 16
      III.3.5 Jokers use in result.................................................................... 16
   III.4 Hypothesis stack – Environment analysis........................................... 17
   III.5 Result production and writing............................................................ 18
IV Bart guards - Predicate synonyms............................................................ 19
   IV.1 Guards............................................................................................. 19
      IV.1.1 Expression guards..................................................................... 19
      IV.1.2 Predicate guards....................................................................... 20
      IV.1.3 Substitution guards................................................................... 21
   IV.2 Predicate synonyms........................................................................ 21
V Pragmas and comments............................................................................ 23
   V.1 EMPILE_PRE, DEPILE_PRE............................................................... 23
   V.2 Magic.................................................................................................. 24
      V.2.1 For variables............................................................................... 24
      V.2.2 For substitutions.......................................................................... 24
   V.3 CAND.................................................................................................. 24
VI Rule files...........................................................................................................26
   VI.1 Syntax...........................................................................................................26
   VI.2 Using rule files.............................................................................................27
      VI.2.1 Providing rule files on command line....................................................27
      VI.2.2 Rule file associated to the component..................................................27
      VI.2.3 BART refinement rule base....................................................................27
VII Variables refinement........................................................................................28
   VII.1 Variable theories syntax............................................................................28
   VII.2 Variable rule research...............................................................................29
   VII.3 Storing information predicates about found variable rules.......................31
   VII.4 Invariant for refined abstract variables....................................................31
   VII.5 Specifying variable refinement results......................................................32
      VII.5.1 Using CONCRETE_VARIABLES clause..............................................32
      VII.5.2 Using REFINEMENT_VARIABLES clause.........................................33
VIII Substitution refinement...............................................................................35
   VIII.1 Rule syntax...............................................................................................35
   VIII.2 Rule research............................................................................................36
   VIII.3 Refinement process..................................................................................37
   VIII.4 Default refinement behaviours...............................................................41
   VIII.5 Special refinement substitutions.............................................................43
      VIII.5.1 Iterators...............................................................................................43
      VIII.5.2 Using operations from seen machines - SEEN_OPERATION...............49
      VIII.5.3 Defining imported operations - IMPORTED_OPERATION.................50
      VIII.5.4 Controlling the refinement process.....................................................53
      VIII.5.5 Local variable declarations.................................................................55
   VIII.6 Declaring operation refinement variables..............................................56
   VIII.7 Usage of substitution rules.......................................................................56
      VIII.7.1 Structural and operation rules - Operation refinement......................57
      VIII.7.2 Initialisation rules................................................................................60
IX Tactic and user pass theories.................................................................63
   IX.1 User pass theory.........................................................................................63
      IX.1.1 Syntax....................................................................................................63
      IX.1.2 Usage.....................................................................................................63
   IX.2 Tactic theory...............................................................................................64
      IX.2.1 Syntax....................................................................................................64
      IX.2.2 Usage.....................................................................................................64
   IX.3 Priority of Tactic and User pass theories....................................................65
X Result production and writing......................................................................67
   X.1 Formatting the result.....................................................................................67
   X.2 Implementing results.....................................................................................68
      X.2.1 Splitting operations in output components.............................................68
      X.2.2 Resolving deadlocks..............................................................................69
XI Appendix A – Figures table.........................................................................73
XII Appendix B – Syntax elements table............................................................75
XIII Appendix C – Rule files complete syntax....................................................76
   XIII.1 Rule files...................................................................................................76
   XIII.2 Variables refinement rules.......................................................................76
# Introduction

BART is a tool that can be used to automatically refine B components. This process is rule based so that the user can drive refinement. Its own rule language has been defined in this purpose.
II Usage

This section describes different ways to launch Bart for processing automatic refinement.

Note: For all launching methods, Bart is supposed to work on type-checkable components. So user should ensures, if it is not automatically done (as with AtelierB, which does not allow launching refinement on a component that is not type-checked), that components are correct.

II.1 Usage with AtelierB tool

Usual way to use automatic refiner Bart is to launch it from the AtelierB GUI. It integrates automatic refinement in the whole B development process. Components generated by automatic refinement are added to project component list, and can then be type-checked and proved.

In AtelierB 4, automatic refinement can be simply launched by selecting a component and choosing “Automatic refinement” in menu “Component”. AtelierB then uses Bart executable, with suitable values for parameters described in section II.2).

Settings used for launching Bart from AtelierB are:

- Automatic setting of directories containing component to refine environment (seen machines)
- Automatic selection of Bart rule file associated to the component if any (file with same name as the component and the .rmf extension, which must be present in source directory)
- Automatic selection of Bart predefined rule base which comes with AtelierB (file PatchRaffiner.rmf)
- Generation of the trace file with rs extension, but no generation of rule trace inside generated component
- Displaying errors messages coming from Bart output

II.2 Advanced users – Bart command line

Besides launching automatic refiner from the AtelierB GUI, it is also possible to use directly the Bart executable in command line. It gives the user more possibilities, as providing more rule files, customizing the way to look for seen machines, using trace modes...

This section describes how the command should be used.
II.2.1 Command usage

The Bart command syntax is as follow (help message displayed by command launching without parameters):

Bart { -r rule_file } -m machine_file

Options:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>-h</td>
<td>Displays this help message</td>
</tr>
<tr>
<td>-d</td>
<td>Debug. This forces Bart to display back all the loaded data</td>
</tr>
<tr>
<td>-I dir</td>
<td>Adds the given directory to the list of directories searched for machine files</td>
</tr>
<tr>
<td>-v</td>
<td>Displays more information</td>
</tr>
<tr>
<td>-V</td>
<td>Displays more information than -v</td>
</tr>
<tr>
<td>-s machine_name</td>
<td>Adds a seen machine</td>
</tr>
<tr>
<td>-o operation_name</td>
<td>Only refine the given operation</td>
</tr>
<tr>
<td>-a file_name</td>
<td>Visibility file</td>
</tr>
<tr>
<td>-e</td>
<td>Handles duplicate names in rmf files as error instead of warning</td>
</tr>
<tr>
<td>-p project</td>
<td>Name of the project that should be loaded (requires -b)</td>
</tr>
<tr>
<td>-b path</td>
<td>Path to the bdp of the project</td>
</tr>
<tr>
<td>-H file</td>
<td>Indicates a file containing the header that should be inserted in the generated machines</td>
</tr>
<tr>
<td>-t</td>
<td>Writes rule trace in the result</td>
</tr>
<tr>
<td>-g file</td>
<td>Writes the list of generated files to file</td>
</tr>
<tr>
<td>-0 dir</td>
<td>Writes the generated files to the given directory</td>
</tr>
<tr>
<td>-x</td>
<td>Displays output as xml</td>
</tr>
<tr>
<td>-X file</td>
<td>Writes input machine as xml</td>
</tr>
<tr>
<td>-l</td>
<td>Displays guards list</td>
</tr>
<tr>
<td>-f name</td>
<td>Use given resolving information for finding path of given component file</td>
</tr>
</tbody>
</table>

**Figure 1** : Bart command line parameters

II.2.2 Input files

As an input, Bart must be given at least the machine or refinement (.mch or .ref file) to refine. This file path must be given to Bart using –m parameter. This given file path can be relative or absolute. There must be exactly one component to refine.

Furthermore, user may provide rule files to process refinement of given component. These files are .rmf suffixed, and are given using –r parameter. User can provide zero, one or more rule files. Their path can be relative or absolute.

II.2.3 Visibility for loaded components

When Bart must load seen machines, given component abstraction or definition files, it must be able to find their associated files on the file system. So at the command launching user must provide necessary information. There are three ways to do this:
• **-I dir:** This option allows the user to directly specify directories components to load must be searched in. So there can be several –I parameters on command line.

• **-a file_name:** This is used to give Bart a visibility file. Each line of this file is a research directory. This option could be used together with –I option, in this case file directories and command line directories are added.

• **-b path and –p project:** With these options, information about an AtelierB project is provided for searching components. –p option indicates the project name, and –b is the project bdp path. –b and –p must be present together.

All these options can not be used at the same time. Only AtelierB project resolving is used if all these parameters are given on command line.

### II.2.4 Bart standard output verbosity

In standard output mode, Bart prints result of variables, operations and initialisation refinement on standard output.

Variable refinement result is the list of found rules associated to their variables. In standard output mode, operation and initialisation refinement result is symbolized with "+" (rule found) and "-" (no rule could be found) characters. For example:

```
Refining operation operation_test
++++++
Refinement of operation_test finished
```

**Figure 2 : Example of Bart standard output**

On the command line, the detail level of output can be increased with –v (verbose mode) and –V (very verbose mode) options.

In verbose mode, the output for previous operation refinement would be as follow:

```
Refining operation operation_test
Rule found: theory1.rule1
Rule found: theory1.rule2
Rule found: theory1.rule3
Rule found: theory2.rule1
Rule found: theory2.rule2
Rule found: theory2.rule3
Refinement of operation_test finished
```

---

**Ce document est la propriété de ClearSy - Toute reproduction ou utilisation partielle ou totale de celui-ci est interdite sans son accord préalable.**
Figure 3: Example of Bart verbose output mode

The failure character “-” is replaced by a “No rule could be found” message when launching Bart in verbose mode.

II.2.5 Bart rule trace

There are two ways to keep a trace of rules applied by Bart.

Each time a component is refined with Bart, the tool generates a file with same name as the component with a .rs extension (example: machine.rs for machine.mch or machine_r.ref). This file contains name of the rules used to refine each element.

Furthermore, user may add –t parameter on command line. This option indicates to Bart that it must write used rule names in comments in generated components.
III Automatic refinement principles

Automatic refinement is a rule based refinement process for B components (abstractions or refinements). The tool is given a component, and it searches, for each element to refine, some rules that specify how it must be treated.

This section describes basic principles of automatic refinement.

III.1 Refined elements

III.1.1 Abstract variables

First elements treated by Bart tool are abstract variables of component to refine (content of the ABSTRACT_VARIABLE clause). The tool must produce, for each one of them, one or more abstract or concrete variables that implement it.

III.1.2 Operations

Bart processes operations of given component in order to refine them. It must produce, for each operation, a substitution body concrete enough to be put in the component implementation.

Refined operations are considered for the whole component abstraction. It means that Bart refines most concrete version of each operation. Here is an example of this process:

![Diagram](image)

**Figure 4 : Example of selection of operations to refine**

For this example, if the given component to refine is Machine_2r, operations processed by Bart will be:

- *Op1* from *Machine*
- *Op2* from *Machine_r*
- *Op3* from *Machine_2r*
III.1.3 Initialisation

Bart also refines content of initialisation clause of given component. Typically, it produces a concrete result by specifying initialisation substitutions for concrete variables refining content of ABSTRACT_VARIABLES clause.

III.1.4 Process

The following draw presents the order of previously described refinement steps.

![Diagram of refinement process order]

**Figure 5 : Refinement process order**

Abstract variables are refined first, as other parts of the process need its output to find suitable rules for operations and initialisation. It is necessary at these steps to know how variables have been refined.

This variable information is stored as predicates in Bart hypothesis stack (cf. III.4).

As it will be described later, refinement process uses rules to determine how each element is refined. A same rule can apply for several elements, so it must be general. In this purpose, the rule language uses jokers, so that rules can contain variable parts.

III.2 Pattern-Matching

A large part of the refinement process uses the concept of pattern-matching. In Bart rule language, user can define patterns, containing jokers, which will be matched against real B elements.
III.2.1 Jokers syntax

In Bart, jokers are ‘@’ character followed by a single letter. For example, @a, @x and @t are valid Bart jokers.

@_ is a special joker, used for special treatments in pattern-matching.

III.2.2 Pattern matching

Bart jokers can be used to write general expression, predicate or substitution patterns. These patterns can be matched against B elements.

Each pattern-matching action has a result status, as it may be either a success or a failure, and instantiates jokers that it contains.

A simple joker matches with any B element. A complex pattern matches a B element if each of its contained jokers can be instantiated with a subpart of the element. If a joker appears several times in a pattern, it has the same value in a unique instantiation.

If the pattern-matching is a success, jokers contain element subparts that made the match successful. The @_ joker is a special one, as it means that its instantiation has not to be stored. So @_ joker can stand for different elements in a same pattern if it appears several times.

The following table shows examples of successful or failed pattern-matching, with their status and associated jokers instantiation.

<table>
<thead>
<tr>
<th>Pattern</th>
<th>Element</th>
<th>Status</th>
<th>Jokers instantiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>@a</td>
<td>aa</td>
<td>Success</td>
<td>{@a = aa}</td>
</tr>
<tr>
<td>@a</td>
<td>aa + bb</td>
<td>Success</td>
<td>{@a = aa + bb}</td>
</tr>
<tr>
<td>@a + @c</td>
<td>yy + 2</td>
<td>Success</td>
<td>{@a = yy, @c = 2}</td>
</tr>
<tr>
<td>@a + @c</td>
<td>yy - 2</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>@a + @c</td>
<td>(aa + 1) + f(3)</td>
<td>Success</td>
<td>{@a = aa + 1, @b = f(3)}</td>
</tr>
<tr>
<td>@a + @b * @a</td>
<td>aa + bb * 2</td>
<td>Failure</td>
<td></td>
</tr>
<tr>
<td>not(@p)</td>
<td>not(vv &lt; 0)</td>
<td>Success</td>
<td>{@p = vv &lt; 0}</td>
</tr>
<tr>
<td>@a</td>
<td>IF val THEN aa := 0 ELSE aa := 1 END</td>
<td>Success</td>
<td>{@a = IF val THEN aa := 0 ELSE aa := 1 END}</td>
</tr>
<tr>
<td>IF @p THEN @t ELSE @e END</td>
<td>IF val THEN aa := 0 ELSE aa := 1 END</td>
<td>Success</td>
<td>{@p = val, @t = aa :=0, @e = aa := 1}</td>
</tr>
<tr>
<td>IF @_ THEN @t ELSE @e END</td>
<td>IF val THEN aa := 0 ELSE aa := 1 END</td>
<td>Success</td>
<td>{@t = aa :=0, @e = aa := 1}</td>
</tr>
</tbody>
</table>
Figure 6: Examples of pattern-matching without previous instantiation

In some cases, some jokers may already be instantiated when the pattern matching is done. An instantiated joker matches an element if its stored value is equal to the element.

For example, if pattern is \( @a + @b \), following table shows how pattern-matching is done if some jokers are already instantiated.

<table>
<thead>
<tr>
<th>Element</th>
<th>Original instantiation</th>
<th>Status</th>
<th>Result instantiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>( 1 + 3 )</td>
<td>{@a = 2}</td>
<td>Failure</td>
<td>-</td>
</tr>
<tr>
<td>( 1 + 3 )</td>
<td>{@a = 1}</td>
<td>Success</td>
<td>{@a = 1, @b = 3}</td>
</tr>
<tr>
<td>( aa + (1 + bb) )</td>
<td>{@b = bb}</td>
<td>Failure</td>
<td>-</td>
</tr>
<tr>
<td>( aa + (1 + bb) )</td>
<td>{@b = 1 + bb}</td>
<td>Success</td>
<td>{@b = 1 + bb, @a = aa}</td>
</tr>
<tr>
<td>( var1 + (var2 - 1) )</td>
<td>{@a = var1, @b = var2 - 1}</td>
<td>Success</td>
<td>{@a = var1, @b = var2 - 1}</td>
</tr>
</tbody>
</table>

Figure 7: Examples of \( @a + @b \) pattern-matching with previous instantiation

III.3 Refinement rules

III.3.1 Introduction

Bart uses rules for refining variables, operations and substitutions. These rules belong to different types: variables rules, or substitution rules, which can be used for both operations and initialisation. Rules of same type are gathered in theories.

Rules usually contain a pattern, and may contain a constraint. These two elements are used to know if a rule can be applied to refine a certain element. Rules also contain clauses that express the refinement result.

III.3.2 Constraints

Rules may have constraints, expressed in their WHEN clause. A constraint is a predicate, which may contain jokers. It may be a complex predicate, built with “&” and “or” operators.

Bart contains a stack of hypothesis (cf. III.4), which is built from the machine to refine and its environment. A constraint is successfully checked if its elementary elements (element not containing “&” or “or”) can be pattern-matched with a predicate of the stack so that the complex constraint is true. According to operators, Bart uses backtracking to try every combination of instantiation that should be a success.

If several instantiations can make the constraint be successfully checked, Bart uses one of them. In this case, it is better to write a more detailed constraint to have only one result. If there are several results, Bart could choose one which is not what the user had planned.
Usually, when checking a constraint, some jokers have already been instantiated.

Here are some examples of constraint checking, if the hypothesis stack contains the following predicates:

<table>
<thead>
<tr>
<th>Constraint</th>
<th>Original instantiation</th>
<th>Status</th>
<th>Result instantiation</th>
</tr>
</thead>
<tbody>
<tr>
<td>@a &lt;= 0</td>
<td>{}</td>
<td>Success</td>
<td>{@a = bb}</td>
</tr>
<tr>
<td>@a &lt;= 0</td>
<td>{@a = cc}</td>
<td>Failure</td>
<td>-</td>
</tr>
<tr>
<td>@a = 0 &amp; (@b = 0 OR @b = @a)</td>
<td>@a = bb</td>
<td>Success</td>
<td>@a = bb, @b = var</td>
</tr>
<tr>
<td>@a : INT &amp; @a = 2</td>
<td>{}</td>
<td>Success</td>
<td>@a = nn, (Bart tries mm but it fails, so the joker is instantiated with nn)</td>
</tr>
</tbody>
</table>

**Figure 8 : Hypothesis stack for constraint checking examples**

**Figure 9 : Examples of constraint checking**

### III.3.3 Guards

Guards are special predicates which may be present in rule constraint clauses. They allow checking some properties on elements to refine and their environment.

There are two kinds of guards: some are simply present in the predicate stack. They are added at the environment loading. For instance ABCON (abstract constant), ABVAR (abstract variable) belong to this kind of guards.

The other kind is calculated guards. For these ones, during constraint checking, Bart doesn’t try to match them with the stack, but directly calculates if the guard is true or false. This kind of guards may also have side effects. For example bnum (numeric test) or bident (identifier test) are calculating guards.

Guards are simply put in the constraint as regular predicates.

Example: @a <= @b & ABVAR(@b) & bnum(@a), with @b instantiated.
III.3.4 Rule checking process

The following figure presents how Bart determines if a rule can be used to refine an element:

![Rule checking process diagram](image)

**Figure 10: Bart testing rule process**

This process is used for variables, operations and initialisation refinement, although it is simpler for variables.

Every rule contains a pattern. First Bart tries to match it with the element to refine. If it succeeds, it tries, if the rule has a constraint clause, to check it against hypothesis. When checking the constraint, some jokers have already been instantiated by pattern matching. If the constraint checking is a success or the rule had no constraint, then it will be used to refine current element.

Variable process is simpler as variable rules have simple pattern, which is a single joker (cf. IV). Variable rule patterns are only matched in order to instantiate the joker representing currently refined abstract variable. This joker is reused in WHEN or result clauses.

III.3.5 Jokers use in result

Once a rule has been chosen to refine an element, Bart must build refinement results. These results are specified in dedicated clauses of variable or substitution rules.

Jokers that have been instantiated by the rule selecting process are reused in the result specification. Those which have been instantiated with identifiers...
can be reused to build new identifiers. For instance, if @i joker was present in pattern and its value is “ident”’, user can provide @i_r value in the result. This value will be “ident_r” after instantiation.

For substitution rules, result pattern is a substitution. For variable rules, it is a list of refinement variables identifiers, invariant and initialisation. For building the result, Bart replaces in this pattern all joker occurrences with their values previously calculated.

### III.4 Hypothesis stack – Environment analysis

At launch, Bart builds an hypothesis stack with predicates coming from the machine to refine and its environment, and with guards, which are predicates giving more information about environment.

This section shows which parts of the environment are analysed to fill the predicate stack.

<table>
<thead>
<tr>
<th>Machine</th>
<th>Predicate stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>All machines (component to refine, abstraction, seen machines)</td>
<td>I &amp; A &amp;</td>
</tr>
<tr>
<td>INARIANT</td>
<td></td>
</tr>
<tr>
<td>I assertions</td>
<td></td>
</tr>
<tr>
<td>Seen Machines only</td>
<td>P &amp;</td>
</tr>
<tr>
<td>Properties</td>
<td></td>
</tr>
<tr>
<td>Sets</td>
<td>SET(S) &amp;</td>
</tr>
<tr>
<td>E = {v1, …. , vn}</td>
<td>ENUM(E) &amp; v1 : E &amp; &amp; vn : E &amp;</td>
</tr>
<tr>
<td>Concrete constants</td>
<td>COCON(C1) &amp; COCON(C2) &amp;</td>
</tr>
<tr>
<td>CC1, CC2</td>
<td></td>
</tr>
<tr>
<td>Concrete variables</td>
<td>COVAR(CV1) &amp; COVAR(CV2) &amp;</td>
</tr>
<tr>
<td>CV1, CV2</td>
<td></td>
</tr>
<tr>
<td>Abstract variables</td>
<td>ABVAR(AV1) &amp; ABVAR(AV2) &amp;</td>
</tr>
<tr>
<td>AV1, AV2</td>
<td></td>
</tr>
<tr>
<td>Abstract constants</td>
<td>ABCON(AC1) &amp; ABCON(AC2) &amp;</td>
</tr>
<tr>
<td>AC1, AC2</td>
<td></td>
</tr>
<tr>
<td>Operations</td>
<td>DECL_OPERATION(par1 ← op1(par2) = body1)</td>
</tr>
<tr>
<td>Component to refine only</td>
<td></td>
</tr>
<tr>
<td>Abstract variables</td>
<td>REFVAR(AV3) &amp; REFVAR(AV4)</td>
</tr>
<tr>
<td>AV3, AV4</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 11 : Hypothesis stack filling with environment**

This table presents only how parts of given component environment are used to fill the stack. Bart doesn’t necessarily add predicates in this exact order. Some others stack guards will be added to the stack during refinement process. These guards will be only presented in IV, as they are not a part of the
initial environment analysis. Variables refinement also adds type predicates to the stack (cf. VII.3).

III.5 Result production and writing

Once every element (variables, operations and initialisation) has been refined, Bart must write the result. For a unique component, there may be several output components.

Operation refinement process may define new operations called in original ones refinement results. Furthermore, sometimes some operations can’t be implemented in the same component. So Bart output is actually a chain of output components, each implementation importing the following machine. Original variables and operations, and new operations, are implemented along the chain.

For instance, following figure shows what could be a Bart output, when refining the component “Machine”:

![Diagram](image)

Figure 12: Example of Bart output components

Thinnest arrows are importation links, and thick ones are refinement links.

If an operation refinement result calls a new imported operation, the new one must be defined and implemented further in the chain.
## IV Bart Guards – Predicate Synonyms

### IV.1 Guards

Following tables describe Bart predefined guards, with their name, type (stack guard or calculated guard) and short descriptions of their meaning and side effects.

Guards description is available on command-line using the –l parameter with bart executable. Users can add new guards, by adding suitable classes to Bart library. Using the command line will display all registered guards, so it may print more information than this section.

Calculated guards usually must have all their joker instantiated to be used, except if the description explicitly says not. Most of stack guards should have their joker instantiated, although it is not mandatory.

For example, user could write a simple constraint as `ABVAR(@a)` where @a joker is not instantiated by rule pattern matching. This means the constraint checks if at least one abstract variable is present in seen machines, and @a is instantiated with one of seen machines abstract variables identifiers, if any.

#### IV.1.1 Expression guards

<table>
<thead>
<tr>
<th>Guard</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABCON(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an identifier of a seen machine abstract constant</td>
</tr>
<tr>
<td>ABVAR(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an identifier of a seen machine abstract variable</td>
</tr>
<tr>
<td>B0EXPR(expr)</td>
<td>Calculated</td>
<td>Checks if given expression is a B0 expression</td>
</tr>
<tr>
<td>bident(expr)</td>
<td>Calculated</td>
<td>Checks if given parameter is an identifier</td>
</tr>
<tr>
<td>bnum(expr)</td>
<td>Calculated</td>
<td>Checks if given expression is a numeric literal</td>
</tr>
<tr>
<td>bpattern(expr1,expr2)</td>
<td>Calculated</td>
<td>Tries to make expr2 match with expr1. expr2 may be not fully instantiated If the match is successful, jokers of expr2 are instantiated</td>
</tr>
<tr>
<td>COCON(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an identifier of a seen machine concrete constant</td>
</tr>
<tr>
<td>COVAR(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an identifier of a seen machine concrete variable</td>
</tr>
<tr>
<td>ENUM(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an enumerated set identifier from a seen machine</td>
</tr>
<tr>
<td>match(joker,expr)</td>
<td>Calculated</td>
<td>“joker” must be a single joker. This guard makes</td>
</tr>
</tbody>
</table>
### Guard Description

<table>
<thead>
<tr>
<th>Guard</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>joker match with expr. Joker may be uninstantiated. If joker is not instantiated, the guard is true and joker value is now expr. If joker is instantiated, guard is true if g can match with joker instantiation.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PAR_IN(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an identifier of a currently refined operation input parameter. These guards are added to the stack when a new operation refinement begins.</td>
</tr>
<tr>
<td>PAR_OUT(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an identifier of a currently refined operation output parameter. These guards are added to the stack when a new operation refinement begins.</td>
</tr>
<tr>
<td>Refined(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an identifier of a variable introduced by another variable refinement. These guards are added after variables refinement phase.</td>
</tr>
<tr>
<td>REFVAR(expr)</td>
<td>Stack</td>
<td>Checks if given expression is an abstract variable of the component to refine.</td>
</tr>
<tr>
<td>SET(expr)</td>
<td>Stack</td>
<td>Checks if parameter is a non-enumerated set identifier from seen machines.</td>
</tr>
<tr>
<td>VAR_G(expr)</td>
<td>Stack</td>
<td>Checks if given parameter is a concrete variable introduced by the operation refinement process. Added when the concrete variable is introduced.</td>
</tr>
<tr>
<td>VAR_LOC(expr)</td>
<td>Stack</td>
<td>Checks if given parameter is a local variable introduced by current operation refinement. Added when the local variable is introduced.</td>
</tr>
</tbody>
</table>

**Figure 13: Bart expression guards**

### IV.1.2 Predicate guards

<table>
<thead>
<tr>
<th>Guard</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PR(pred)</td>
<td>Calculated</td>
<td>Checks if given predicate is true using AtelierB prover. pred must be a simple predicate with no guards.</td>
</tr>
<tr>
<td>bistrue(pred)</td>
<td>Calculated</td>
<td>Checks if pred constraint can be matched against. pred must be a simple predicate with no guards.</td>
</tr>
<tr>
<td>bisfalse(pred)</td>
<td>Calculated</td>
<td>Checks if not(pred) is present within the hypothesis stack. pred must be a simple predicate with no guards.</td>
</tr>
</tbody>
</table>
### IV.1.3 Substitution guards

Some of following guards are called substitution guards because their parameter is internally represented as substitution by the tool.

<table>
<thead>
<tr>
<th>Guard</th>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECL_OPERATION(oper)</td>
<td>Stack</td>
<td>“oper” must be an operation description that can contain jokers. The shape of the parameter is prototype separated of operation body with a “</td>
</tr>
<tr>
<td></td>
<td></td>
<td>A guard of this type is added for each operation of machines seen by the component to refine.</td>
</tr>
<tr>
<td>bhasflow(sub)</td>
<td>Calculated</td>
<td>Checks if given substitution contains flow (i.e. branch structures as IF or SELECT substitutions)</td>
</tr>
<tr>
<td>bsearch(pattern</td>
<td>list</td>
<td>result)</td>
</tr>
</tbody>
</table>

**Figure 15 : Bart substitution guards**

### IV.2 Predicate synonyms

In addition to Bart guard extensibility, which requires code writing and recompilation, Bart provides a mechanism to the user allowing to custom predicates that can be used in rule constraints.

This is done using a special theory, which must be put in rule files (cf. VI).

Syntax of the predicate theory is:

```plaintext
PredicateTheory =

    "THEORY_PREDICATES"
    "IS"
    PredicateDefinition { "|" PredicateDefinition}
```
“END”

PredicateDefinition

ident "(" JokerList ")" " <==> " Predicate

Syntax 1 : Predicate theory

Here is an example of this special theory:

THEORY_PREDICATES IS
    test(@a) <=> bnum(@a) |
    NumOrIdent(@a) <=> bident(@a) or test(@a) |
    belongs(@a,@b) <=> (@a : @b) |
    ElementOfSet(@d) < => @d : @s
END

Figure 16 : Predicate theory example

Left part of each line is a synonym. It is a predicate identifier with a list of jokers between parentheses. Right part is the value, it’s a predicate containing jokers. When these keywords are found in a rule file, they are replaced by predicates described on the right part. Jokers present in the value and in the synonym are replaced by the element given at use. Others jokers are left unchanged.

For example, if the preceding predicate theory is used and a rule has the following constraint:

belongs(@c,INT) & 0 <= @c & ElementOfSet(@e)

, the following predicate will be actually loaded by Bart:

@c: INT & 0 <= @c & @e: @s

Every synonym predicate defined in the rule file must have been defined before. If, for example, Bart finds test(@a) before the predicate theory that defines test, it will load this predicate as a type predicate (predicates to be matched with hypothesis added by variable refinement, cf. VII.3).

A synonym can use another one previously defined (as NumOrIdent uses test in the example).

A predicate theory is local to its definition rule file. Definitions from a particular file can not be used in another one.
V Pragmas and Comments

In most cases, Bart tries to keep comments from original B component elements, and to rewrite them beside suitable refinement results.

Pragmas are special comments that the user writes in the B component to refine in order to impact the refinement process. These elements are not processed by AtelierB, but only by Bart. AtelierB processes them as simple comments. Each pragma begins with /* pragma_b.

V.1 EMPILE_PRE, DEPILE_PRE

These two pragmas are used to modify the top of Bart predicate stack. They must be written before a substitution of an operation from the machine to refine. They are used when the refinement of the substitution they are written before begins.

/* pragma_b EMPILE_PRE(predicate) */ is used to add predicate at the top of the hypothesis stack.
/* pragma_b DEPILE_PRE */ is used to remove last predicates added to the stack.

For example, if Bart must refines following substitution:

```
IF valeur > 100 THEN
  /* pragma_b EMPILE_PRE(valeur > 0) */
  Substitution1
ELSE
  /* pragma_b DEPILE_PRE */
  Substitution2
END
```

Figure 17: Substitution for EMPILE_PRE and DEPILE_PRE example

Let’s assume that Bart adds the if condition for refining the THEN branch, and the negation of the condition for refining the ELSE branch. Following table presents the stack state depending on pragmas presence.

<table>
<thead>
<tr>
<th>Branch</th>
<th>Without pragma</th>
<th>With pragma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Then branch</td>
<td>valeur &gt; 100 &amp; Previous predicates</td>
<td>valeur &gt; 0 &amp; valore &gt; 100 &amp; Previous predicates</td>
</tr>
<tr>
<td>Else branch</td>
<td>Not(valeur &gt; 100) &amp; Previous predicates</td>
<td>Previous predicates</td>
</tr>
</tbody>
</table>
V.2 Magic

Pragma MAGIC can be used to directly specify in B components which rules must be used to refine certain elements (variables or substitutions). It is useful to force use of a certain rule. The given one is used even if suitable rules could be found before it in a regular rule research. Bart checks that the given rule can be applied to the element (pattern matching and constraint checking).

V.2.1 For variables

Magic pragma is used to specify which rule should be used to refine a certain variable. The syntax is /* pragma_b MAGIC(theory.rule,variable) */. It means that given rule from given theory will be used to refine the variable.

Variable magic pragmas must be put at the machine beginning. There can be several magic pragmas at the machine beginning. As the rule file is not specified, Bart processes rule files in the classic rule research order to find the rule in the suitable theory. If no such rule is found, a refinement error occurs.

V.2.2 For substitutions

Magic pragma can also be used for refining substitutions. The pragma must be written directly before the involved substitution in the B model. The syntax is /* pragma_b MAGIC(theory.rule) */

For example:

/* pragma_b MAGIC(theory_operation.r_affect_bool) */
bool_value := TRUE

will refine the substitution using r_affect_bool rule in theory theory_operation.

V.3 CAND

This pragma has a particular shape. It must be written /* CAND *//, and be put just before a “&” operator in B model.

It means that this operator is a conditional and (right part is not evaluated if left part is false).
A “&” operator from B model that has a /* CAND */ pragma will match with cand operator of Bart rule files.
VI Rule files

VI.1 Syntax

Rule files are files containing theories, each theory containing one or several rules used to refine a given component. Rule file extension is usually .rmf. A rule file can contain variable, operation, structure and initialisation theories. It can also contain utility theories such as tactic, user pass, or definition of predicates synonyms.

Syntax of rule files is:

```
RuleFile = [ Theory { "&" Theory } ].
Theory
= VariableTheory
| OperationTheory
| StructureTheory
| InitialisationTheory
| UserPassTheory
| TacticTheory
| PredicateTheory
```

Syntax 2 : Rule files

The rule file syntax must also respect certain constraints:

- User pass can be present at most once
- Tactic can be present at most once
- Predicate theory can be present at most once

Order between theories has no syntactical impact, except for predicates theory: it must be defined before its elements are used in the rule.

Order between theories has an impact on the rule research, as the standard process (no user pass or tactic) reads theories from bottom to top.

User pass and tactic can be defined anywhere in the file, even before theories they refer to have been defined.
VI.2 Using rule files

VI.2.1 Providing rule files on command line

As it was previously described, user provides rules files when launching Bart by using \(-r\) parameter. This parameter can be present several times, and is not mandatory.

When it searches for rules, Bart processes rule files from right to left, according to command line order.

Let’s consider following command line:

```
./bart -m machine.mch -r rule2.rmf -r rule1.rmf
```

For a given element to refine, the tool will search first in rule1.rmf, and then in rule2.rmf if the first file did not contain a suitable rule.

VI.2.2 Rule file associated to the component

If directory that contains the given machine file also contains a rule file with same name, it has not to be specified on the command line, Bart will automatically load it.

If such a file is present, it will be used in priority (as it had been given last using \(-r\) parameter on command line).

For this command line:

```
./bart -m machine.mch -r rule.rmf
```

, Bart will look for machine.rmf in current directory. If it is present, rule files will be used in this order: machine.rmf, then rule.rmf.

VI.2.3 Bart refinement rule base

The tool comes with a set of predefined rule base, contained in the file PatchRaffiner.rmf present in Bart distribution. It provides rules that permit to refine most of the classical B substitutions.

When Bart is used on command line, the rule base must be provided using \(-r\) parameter.

The classical automatic refinement scheme is the following: most elements of given component can be refined using the rule base. If an element can not be refined with it, or needs a more specific treatment, user should write suitable rules in rmf files that will be provided after the rule base on command line, or in the component associated rule file.
VII VARIABLES REFINEMENT

VII.1 Variable theories syntax

```plaintext
VariableTheory
  =  "THEORY_VARIABLE" ident
     "IS"
        VariableRule { ";" VariableRule } 
     "END" ident

VariableRule
  =  "RULE" ident ["(" JokerList ")" ]
     "VARIABLE" JokerList
     [ "TYPE" ident ["(" JokerList ")" ]
     [ "WHEN" Predicate ]
     "IMPORT_TYPE" Predicate
     (VariableImplementation | VariablesRefinement )
     "END"

VariableImplementation
  =  "CONCRETE_VARIABLES" JokerList
     [ "DECLARATION" Predicate ]
     "INVARIANT" Predicate

VariablesRefinement
  =  "REFINEMENT_VARIABLES"
     VariableRefinement { "," VariableRefinement } 
     "GLUING_INVARIANT" Predicate

VariableRefinement
  =  "CONCRETE_VARIABLE" joker
     "WITH_INV" Predicate
     "END"
     |
     "ABSTRACT_VARIABLE" joker
     "REFINED_BY" ident ";" ident ["(" Expression ")" ]
     "WITH_INV" Predicate
     "END"
```

Syntax 3 : Variable rule theories

Each theory has an identifier, which must be repeated after the END keyword. A theory can contain several rules, each rule having its own unique identifier. Each following subsection will associate a variable refinement functionality with one or more clauses of variable rules.
VII.2 Variable rule research

Variable rule research is different from rule research for operations and initialisation. Instead of processing each variable and finding a suitable rule for it, it processes each rule of considered theories (all variable theories or a subset if tactic or user pass is used, cf. IX) and checks if it can be used to refine some variables.

This is necessary because a single variable rule can be used to refine several variables. Once a rule has been selected for one (or several) variable, resulting refinement variables can be calculated from its clauses.

The principle of rule research is the following:

- At the beginning the tool considers the set of abstract variables to refine
- It processes every theory that could be used (according to tactic, user pass or neither) from bottom to top. For each theory:
  - The tool processes all rules of theory from bottom to top. For each variable rule:
    - Bart determines which variables can be refined by current rule
    - Refined variables are removed from the set of remaining variables

This process stops when there are not variables to refine anymore, or when all variable rules to consider have been treated. Variable refinement is successful if all variables have been associated with a rule. It is a failure if all rules have been treated and some variables could not be refined.

For a certain rule, Bart determines which variables it can refine as follow:

- The tool tries every combination of values to instantiate joker list of VARIABLE clause. For each instantiation:
  - Bart checks constraint expressed in WHEN clause against hypothesis stack, with jokers of VARIABLE clause instantiated
    - If WHEN constraint could be checked, variables used to instantiate VARIABLE clause can be refined by this rule
    - Variable refined by the rule are removed from set of remaining variables, to be sure they won’t be used in following tried instantiation

If current rule has several jokers in VARIABLE clause, there are more combinations to try than for simple variable rules.

Following example presents results of a variable rule research, with given theories and predicates stacks. Variable to refine are \{aa, bb, cc, dd, ee\}.
RULE r1
VARIABLE
  @a
WHEN
  @a : INT & @b < @a & ABCON(@b)
[...]
END;

RULE r2
VARIABLE
  @a, @b
WHEN
  @a : INT & @b : NAT
  & @a < 0 & 0 <= @b
[...]
END

END t1 &

THEORY_VARIABLE t2 IS

RULE r3
VARIABLE
  @a
WHEN
  @a : NAT & 1 <= @a
[...]
END

END t2

c : NAT    &
dd : NAT    &
ee : NAT    &
value < aa      &
bb < 0      &
0 <= cc      &
1 <= dd      &
1 <= ee      &
ABCON(value)

Figure 21: Theories and stack for variable rule research example

For this stack, the rule research process is the following:

- Trying theory t2
  - Trying rule r3
    - Possible instantiations of VARIABLE clause: {aa}, {bb}, {cc}, {dd}, {ee}
    - dd and ee can be refined by the rule
    - Set of variables to refine is now {aa, bb, cc}
  - Trying theory t1
    - Trying rule r2
      - Possible instantiations of VARIABLE clause: {aa, bb}, {bb, cc}, {aa, cc}, {bb, aa}, {cc, bb}, {cc, aa}
      - Only {bb,cc} instantiation makes the WHEN clause be checked. bb and cc can be refined by the rule
      - Set of variables to refine is now {aa}
    - Trying rule r1
      - aa can be refined by current rule

Figure 22: Variable rule research example

For this example, variable refinement is successful, as each variable has been refined.
VII.3 Storing information predicates about found variable rules

Bart allows specifying, in variable rules, predicates that will be added in the stack if the rule is selected. These predicates will be called “Type predicates” and are specified in TYPE clause of variable rules.

Type predicates are constituted of an identifier and a joker list between parentheses. They are added to the stack after variables refinement, to be reused in operations and initialisation refinement (in substitution rules constrains). Jokers of the joker list must be have been present in VARIABLE or WHEN clauses, because they have to be instantiated for the type predicate to be added to the stack.

If we reuse previous example and complete rules with these TYPE clauses:

\[
\begin{align*}
\text{RULE } \text{r1} & \quad \text{VARIABLE } \quad @a \\
& \quad \text{TYPE } \quad \text{COMP}(@a,@b) \\
& \quad \text{WHEN } \\
& \quad \text{ } \quad @a : \text{INT} \ & \ & @b < @a \\
& \quad \text{ } \quad & \quad \ & \quad \ & \ & \ & \ & \ & \ & \ & \ & ABCON(@b) \\
& \quad \text{ } \quad & \quad \ & \quad \ & \ & \ & \ & \ & \ & [...] \\
& \quad \text{END} \\
\quad \text{RULE } \text{r2} & \quad \text{VARIABLE } \quad @a, @b \\
& \quad \text{TYPE } \quad \text{DOUBLE}(@a,@b) \\
& \quad \text{WHEN } \\
& \quad \text{ } \quad @a : \text{INT} \ & \ & @b : \text{NAT} \\
& \quad \text{ } \quad & \quad \ & \quad \ & \ & \ & \ & \ & @a < 0 \ & \ & 0 \leq \ & \ & @b \\
& \quad \text{ } \quad & \quad \ & \quad \ & \ & \ & \ & \ & [...] \\
& \quad \text{END} \\
\quad \text{RULE } \text{r3} & \quad \text{VARIABLE } \quad @a \\
& \quad \text{TYPE } \quad \text{SCALAR}(@a) \\
& \quad \text{WHEN } \\
& \quad \text{ } \quad @a : \text{NAT} \ & \ & 1 \leq \ & @a \\
& \quad \text{ } \quad & \quad \ & \quad \ & \ & \ & \ & \ & [...] \\
& \quad \text{END}
\end{align*}
\]

These predicates will be added after variable refinement previously described:

\[
\{\text{SCALAR}(ee) \ & \ \text{&} \\
\text{SCALAR}(dd) \ & \ \text{&} \\
\text{DOUBLE}(bb,cc) \ & \ \text{&} \\
\text{COMP}(aa,value)\}
\]

VII.4 Invariant for refined abstract variables

In the output chain components, refined abstract variables won’t be necessarily implemented in the first one. It is necessary to provide the invariant that must be copied in component in which variables refined by the rule have not been implemented yet.

This is done within the clause IMPORT_TYPE of the rule. This clause is a predicate which may contain jokers. These jokers must have been present in VARIABLE or WHEN clauses, because they have to be instantiated for the predicate to be copied in output components.
VII.5 Specifying variable refinement results

Refinement results for abstract variables are specified in REFINEMENT_VARIABLES or CONCRETE_VARIABLES clauses of variables rules. These two clauses can not be used at the same time.

VII.5.1 Using CONCRETE_VARIABLES clause

Using CONCRETE_VARIABLES clause is simpler than using REFINEMENT_VARIABLES, but it is less powerful as it is impossible to specify abstract refinement variables. This clause corresponds to the VariableImplementation element of the syntax presented in VII.1.

This clause contains a list of jokerized identifiers (CONCRETE_VARIABLES clause), which will be concrete variables refining abstract variable treated by the rule, and the invariant that will be added for these concrete variables (INVARIANT clause). Jokers in the invariant must have been instantiated during the rule selection. Expressions designating new concrete variable must be built on previously instantiated jokers.

As the result is a joker list, and not a single joker, it is possible to specify several refinement variables for a unique rule.

For example, if the rule:

```plaintext
RULE r_ens
VARIABLE @a
TYPE raffinement_ensemble(@a, @b, @c)
WHEN SET(@c) & @a <: @c
IMPORT_TYPE @a <: @c
CONCRETE_VARIABLES @a_r
INVARIANT
  @a_r : @c --> BOOL & @a = @a_r~[{TRUE}]
END
```

**Figure 25 : Example of variable refinement rule with variable implementation**

is used to refine the abstract variable “ee”, this variable will be refined by “ee_r”. If we suppose that @c joker value determined by constraint checking was “set”, the following predicate will be added to the invariant of the output implementation it will be implemented in: ee_r : set --> BOOL & ee = ee_r~[{TRUE}].
VII.5.2 Using REFINEMENT_VARIABLES clause

Using this clause allows specifying both concrete and abstract variable to refine the abstract variable treated by the rule. It corresponds to VariablesRefinement element of syntax described in VII.1.

This clause must contain a list of VariableRefinement elements as described in the syntax in VII.1. Each one of these elements specify a refinement variable (abstract or concrete), and its associated invariant. For refinement abstract variables, rule that will be used to refine it must also be provided, with its parameters (cf. example). Jokers contained in subparts of these elements must all have been previously instantiated.

After the list of refinement variables, the GLUING_INVARIANT clause must be written. This predicate is the invariant that will be put in output components when all refinement variables will have been implemented. This predicate must only contain previously instantiated jokers.

Following rule using REFINEMENT_VARIABLES clause is equivalent to the previously described one:

```
RULE r_ens
  VARIABLE @a
  TYPE raffinement_ensemble(@a, @b, @c)
  WHEN
    SET(@c) &
    @a <: @c
  IMPORT_TYPE
    @a <: @c
  REFINEMENT_VARIABLES
    CONCRETE_VARIABLE
      @a_r
    WITH_INV
      @a_r : @c --> BOOL &
    END
  GLUING_INVARIANT
    @a = @a_r~[TRUE]
END
```

**Figure 26 : Variable refinement rule with concrete variable**

If we need to refine the variable with another abstract variable, the rule should be:

```
RULE r_ens
  VARIABLE @a
  TYPE raffinement_ensemble(@a, @b, @c)
  WHEN
    SET(@c) &
    @a <: @c
END
```
Here we directly specify which rule will be used to refine the new variable in the `REFINED_BY` clause. The syntax is `theory.rule(parameters)`. Values specified between parentheses after the rule name are parameters. This means that the given rule must have parameters, like this:

```
RULE abstract_rule(@a)
  VARIABLE @a
  [...] @a
END
```

When a rule is given for a new refinement variable, the `VARIABLE` and `WHEN` clause jokers are instantiated with the variable name and the parameters. Then the regular rule checking process goes on as the `WHEN` constraint is verified.

If new abstract variables are introduced, a `REFINEMENT` component will be introduced in output chain.

**Figure 27: Variable refinement rule with abstract variable**
VIII Substitution Refinement

Substitution refinement gathers operation, initialisation and structural rules. Operation and structure rules are identical. Initialisation rules are simpler versions of operation rules.

Syntax and principles of substitution refinement will be presented through operations rules. A further section will be dedicated to the different kind of substitution rules, their usage and differences. So in first sections of this chapter, “refining a substitution” will stand for “refining a substitution from an operation”.

Substitution refinement is more complex than variable refinement, as it can be recursive, i.e. result of refinement for a given substitution may have to be refined too. Furthermore, for a given substitution, refinement may need several sub-processes (cf. SUB_REFINEMENT clause or default refinement behaviours for parallel or semicolon). So refinement sub-branches are created and the underlying structure that can be used to represent substitution refinement is in fact a tree.

VIII.1 Rule syntax

Here is the syntax of operation theories:

```
OperationTheory
= "THEORY_OPERATION" ident
  "IS" OperationRule { ";" OperationRule } "END" ident
  .

OperationRule
= "RULE" ident
  "REFINES" Substitution
  [ "WHEN" Predicate ]
  [ "SUB_REFINEMENT" SubRefinementRule { "," SubRefinementRule } ]
  ( "REFINEMENT" | "IMPLEMENTATION" )
    { RefinementVarDecl }
    Substitution
  ["IMPLEMENT" IdentOrJokerList ]
  "END"
  .

RefinementVarDecl
= ( "VARIABLE" | "ABSTRACT_VARIABLE" | "CONCRETE_VARIABLE" ) joker
  [ "REFINED_BY" ident "(" Expression ")" ]
```
"WITH_INV" Predicate
"WITH_INIT" Substitution
"IN"

SubRefinementRule =
"{" Substitution "}" "->" "{" Joker "}"

Syntax 4 : Operation rule theories

Syntax for others kinds of substitution rules will be presented further.

As for variable theories, an identifier must be present after THEORY_OPERATION keyword and repeated after the END keyword.

VIII.2 Rule research

The substitution rule research process is simpler than for variables.

- For a substitution to refine, Bart processes each rule file as long as he could not find a rule.
- For each rule file it processes operation theories to consider (all theories, or a subset if tactic or user pass is used, cf. IX) from bottom to top.
- For each theory it processes operation rules from bottom to top
- For each rule, Bart checks if it can be used to refine currently treated substitution.

If each rule file was processed by Bart and no rule could be found for a certain substitution, an operation refinement may occur (cf. VIII.3).

Each operation rule has a pattern (REFINES clause) and may have a constraint (WHEN clause). The process used to check if a rule can be applied to a substitution is as described in III.3.4.

First the tool tries to match the rule pattern with the substitution. If it is successful, the rule can be applied under the condition it has no WHEN constraint or its WHEN constraint can be checked against hypothesis stack.

For example, if par_out := par_in1 + par_in2 must be refined, with following theories and stack:

<table>
<thead>
<tr>
<th>Theories</th>
<th>Stack</th>
</tr>
</thead>
<tbody>
<tr>
<td>THEORY_OPERATION assign_plus IS</td>
<td></td>
</tr>
<tr>
<td>RULE r_assign_plus_par_in</td>
<td></td>
</tr>
<tr>
<td>REFINES</td>
<td></td>
</tr>
<tr>
<td>WHEN</td>
<td></td>
</tr>
<tr>
<td>@a := @b + @c</td>
<td></td>
</tr>
<tr>
<td>PAR_OUT(@a) &amp; PAR_IN(@b) &amp; PAR_IN(@c)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>PAR_OUT(par_out) &amp; PAR_IN(par_in1) &amp; PAR_IN(par_in2)</td>
</tr>
</tbody>
</table>
RULE r_assign_plus_const
  REFINES
  \@a := \@b + \@c
  WHEN PAR_OUT(@a) & ABCON(@b) & ABCON(@c)
  [...] END
END assign_plus &
THEORY VARIABLE assign_minus IS
RULE assign_minus_1
  REFINES
  \@a := \@b - \@c
  [...] END
END assign_minus

**Figure 28 : Theories and stack for operation rule research**

Let's suppose that for this rule file there is no tactic or user pass. The rule research will be as follow:

- First tried rule is assign_minus.assign_minus_1. Its pattern doesn’t match the substitution, so it can not be used
- Second tried rule is assign_plus.assign_plus_const. Its pattern matches the substitution, but its WHEN constraint can not be checked, so it can not be used
- Third tried rule is assign_plus.assign_plus_par_in. Its pattern matches the substitution, and its WHEN constraint can be checked, so this rule is selected.

**Figure 29 : Example of operation rule research**

**VIII.3 Refinement process**

The substitution refinement process depends, for given rule and substitution, on the presence and content of SUB_REFINEMENT, IMPLEMENTATION and REFINEMENT clauses.

SUB_REFINEMENT clause corresponds to SubRefinementRule element of syntax described in VIII.1. It contains a ",," separated list of sub-elements.

Each sub-element left part is a substitution that may contain jokers. These jokers must all have been instantiated by pattern matching and constraint checking. Right part of the sub-element must be a single and still uninstantiated joker.

This clause is used to refine the given substitution and store the result in given joker. This is done before calculation of the rule substitution result, so the sub-refinement can be used to express the result.

IMPLEMENTATION clause expresses the result of current rule. It contains a substitution which may contain jokers. All these jokers must have been
instantiated during pattern matching, constraint checking or sub-refinement processing. IMPLEMENTATION clause may also contain concrete operation refinement variable declaration (cf. VIII.6).

Using IMPLEMENTATION clause means that given result is the final result of current branch and doesn’t need to be refined again.

REFINEMENT clause expresses the result of current rule. It contains a substitution which may contain jokers. All these jokers must have been instantiated during pattern matching, constraint checking or sub-refinement processing. REFINEMENT clause may also contain abstract or concrete operation refinement variable declaration (cf. VIII.6).

Using REFINEMENT clause means that given result is not the final result of current branch. The result of rule must be refined.

IMPLEMENTATION and REFINEMENT clause can not be both used in a same rule. When a rule has been selected (and eventual sub-refinements have been processed), the rule result is calculated by instantiating jokers of its result clause.

A rule can contain both SUB_REFINEMENT and REFINEMENT clauses. In this case, each subrefinement is calculated and stored in its joker. Then content of REFINEMENT clause is instantiated and refined.

For a substitution to refine, if no rule could be found, Bart will check if it can be refined using a “predefined behaviour”. For some kinds of substitutions, Bart may know how to refine them if no rule is present. Predefined behaviour can be the end of current branch (skip substitution refinement) or a simple node of refinement tree. In this case, Bart may create one (BEGIN substitution refinement) or several (semicolon refinement) subnodes in refinement tree for current substitution. For each new subnode created by predefined refinement behaviour, the recursive refinement process is restarted as a rule or predefined behaviour will be searched for each one.

Following figure summarizes the process:
Rectangles are actions processed by Bart. Ellipses are decisions. Error and success boxes represent error and success for current branch (an error in current branch means error in the whole refinement process).

Subrefinement computations are represented aside because they must be calculated for the result to be instantiated, but refinement of substitutions contained in left part of SUB_REFINEMENT clauses sub-elements uses the same process.

For example, if we consider following substitution to refine:

```plaintext
IF in < 0 THEN
    aa := aa + 1
ELSE
    aa := 0
END
```

and the following theories:

```plaintext
THEORY_OPERATION theory IS
    RULE assign
    REFINES
        @a := @b
IMPLEMENTATION
```
@a := @b
END;

RULE r_assign_plus_2
REFINES
    @a := @b + @c
IMPLEMENTATION
    @a := @b + @c
END;

RULE r_assign_plus
REFINES
    @a := @b + @c
WHEN
    bnot(B0EXPR(@a))
REFINEMENT
    #1 := @b + @c ;
    @a := #1
END ;

RULE r_if
REFINES
    IF @a THEN @b ELSE @c END
SUB_REFINEMENT
    (@b) -> (@d),
    (@c) -> (@e)
IMPLEMENTATION
    #1 := bool(@a);
    IF #1 = TRUE THEN @d ELSE @e END
END
END theory

Figure 31: Substitution and theories for rule tree example

#x expressions written in rules result clauses are used to introduce local variables (cf. VIII.5.5).

For this example the resulting rule tree will be:
Figure 32: Example of refinement rule tree

Each rectangle (except the first one which shows only the first found rule) shows the substitution to refine at current node, and the found rule.

First rule (r_if) has its result described in an IMPLEMENTATION clause but the refinement goes on as it contains SUB_REFINEMENT clauses. The refinement of r_assign_plus_rule_2 rule result uses the predefined refinement behaviour for semicolon.

For the refinement of this substitution, the result will be:

```plaintext
l_1 := bool(in < 0);
IF l_1 = TRUE THEN
  l_2 := bb + 1;
  aa := l_2
ELSE
  aa := 0
END
```

**VIII.4 Default refinement behaviours**

When a substitution must be refined and no rule could be found for it, Bart may apply a predefined behaviour to process refinement further.

If both a rule and a predefined behaviour are suitable for a substitution, the rule will be applied. For example Bart knows by default how to refine a semicolon substitution. But if a rule is present with @a;@b pattern and a WHEN constraint that can be checked for current substitution, Bart will use the rule.
Following table show which kind of substitutions can be refined by Bart even if no rule could be found in rule files. Here are only shown regular B substitutions that can be refined by predefined behaviours. Some Bart specific substitutions use this mechanism to control the refinement process, they will be described later.

In this table result(sub) means refinement result of substitution sub.

<table>
<thead>
<tr>
<th>Substitution</th>
<th>Refinement result</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Semicolon: sub1 ; sub2</td>
<td>result(sub1); result(sub2)</td>
<td></td>
</tr>
<tr>
<td>Parallel: sub1</td>
<td></td>
<td>sub2</td>
</tr>
<tr>
<td>Bloc substitution:</td>
<td>BEGIN result(sub) END</td>
<td></td>
</tr>
<tr>
<td>Guarded substitution:</td>
<td>BEGIN result(sub) END</td>
<td>“predicate” is added to the hypothesis stack for refining “sub”</td>
</tr>
<tr>
<td>Assertion substitution:</td>
<td>ASSERT predicate THEN result(sub) END</td>
<td>“predicate” is added to the hypothesis stack for refining “sub”</td>
</tr>
<tr>
<td>Operation call</td>
<td>Refined by itself</td>
<td></td>
</tr>
<tr>
<td>Skip</td>
<td>Refined by itself</td>
<td></td>
</tr>
<tr>
<td>Local variables:</td>
<td>VAR list result(sub) END</td>
<td>VAR_LOC hypothesis is added to the stack for each element of “list”</td>
</tr>
<tr>
<td>Loop substitution:</td>
<td>WHILE condition DO result(sub) INARIANT I VARIANT V END</td>
<td>“condition” is added to the hypothesis stack for refining “body”</td>
</tr>
</tbody>
</table>

**Figure 33 : Bart predefined refinement behaviours**
As described in the table, a sequentialization is done when a parallel substitution is refined. For example if \( aa := bb \mid cc := aa \) must be refined and each branch is refined by itself, result without sequentialization would be \( aa := bb \mid cc := aa \), which is incorrect. So Bart makes sequentialization, and the real produced result will be \( l_1 := aa ; aa := bb ; cc := l_1 \), where \( l_1 \) is a local variable declared for the sequentialization. The local variable will be declared with others ones coming from \# declaration in rules (cf. VIII.5.5).

**VIII.5 Special refinement substitutions**

In operation rules result clauses, it is possible to use Bart specific substitutions to control the refinement process or add elements to the produced result.

These substitutions don’t exist in regular B models, and they can only be written in REFINEMENT or IMPLEMENTATION clauses of substitution rules and used to express the rule result. As they are present only in result clauses, all jokers contained in these substitutions must have been instantiated before. They are presented in following sections.

**VIII.5.1 Iterators**

Several substitutions can be used in Bart to manage iterators. These substitutions become WHILE loops when the result of rule they are written in is calculated. At the same time, some of them generate iterator machines that contains operations called in generated while loops. These generated machines are then refined by Bart using predefined rules.

**VIII.5.1.1 TYPE_ITERATION**

TYPE_ITERATION substitution allows specifying loops iterating on all elements of a set. In the produced implementation, this substitution is replaced by an automatically built WHILE loop which calls operations from an iteration machine created by Bart.

TYPE_ITERATION substitution syntax is as follow:

```
"TYPE ITERATION" "(" [ ("tant que" | "while") "=>$" IdentOrJokerOrVarDecl "," ] "index" "=>$" Expression "," "type" "=>$" Expression "," "body" "=>$" "(" Substitution ")" "," "invariant" "=>$" Predicate ")"
```

Syntax 5 : Type iteration

The different clauses meaning is:
- **while**: It must be given a variable (instantiated or not). This clause may be used if the iteration might be stopped before all elements of the set have been processed. If while clause is present, the loop continues as long as there are still more elements in the set, and given variable is TRUE. Given variable should be set to FALSE in the user defined loop body part to stop the loop.
- **index**: Name of the variable that will contain each element of the given set.
- **type**: Set the loop is iterating on.
- **body**: User defined part of the loop body.
- **invariant**: User defined part of the loop invariant.

This shows how Bart generates the WHILE loop for a TYPE_ITERATION substitution (with no while clause):

```
vg_loop <-- init_iteration_TYPE;
WHILE vg_loop = TRUE DO
  vg_loop, index <-- continue_iteration_TYPE;
  body;
INVARIANT
  vg_loop= bool(TYPE_remaining /= {}) &
  TYPE_remaining \ TYPE_done = TYPE &
  TYPE_remaining /\ TYPE_done = {} &
  invariant
VARIANT
  card(TYPE_remaining)
END
```

**Figure 34 : Type iteration generated loop, without while parameter**

In this example, vg_loop is the automatically generated variable used to iterate on elements of the set. If a while clause is added to the TYPE_ITERATION substitution, generated loop becomes:

```
vg_loop <-- init_iteration_TYPE;
WHILE vg_loop = TRUE DO
  vg_loop, index <-- continue_iteration_TYPE;
  body;
  vg_loop := bool(vg_loop = TRUE & while = TRUE)
INVARIANT
  vg_loop= bool(TYPE_remaining /= {}) &
  TYPE_remaining \ TYPE_done = TYPE &
  TYPE_remaining /\ TYPE_done = {} &
  invariant
VARIANT
  card(TYPE_remaining)
```
Figure 35: Type iteration generated loop, with while parameter

In these generated loops, called operations are defined in the following generated machine:

```plaintext
MACHINE iterator_name
ABSTRACT VARIABLES
  TYPE_remaining, TYPE_done
INVARIANT
  TYPE_remaining <: TYPE &
  TYPE_done <: TYPE &
  TYPE_remaining \ TYPE_done = {}
INITIALISATION
  TYPE_remaining := {} ||
  TYPE_done := {} 
OPERATIONS
continue <-- init_iteration_TYPE =
  BEGIN
    TYPE_done := {} ||
    TYPE_remaining := TYPE ||
    continue := bool(TYPE /= {})
  END;
continue, elt <-- continue_iteration_TYPE =
  PRE
    TYPE_remaining /= {}
  THEN
    ANY
      nn
    WHERE
      nn : TYPE &
      nn : TYPE_remaining
    THEN
      TYPE_done := TYPE_done \ {nn} ||
      TYPE_remaining := TYPE_remaining - {nn} ||
      elt := nn ||
      continue := bool(TYPE_remaining /= {nn})
  END
END
```

Figure 36: Type iteration generated machine

This is a simple example in which a single iterator is generated for a given refined component. Generated machines can be more complex (cf. VIII.5.1.4)
**VIII.5.1.2 INVARIANT_ITERATION**

As TYPE_ITERATION, this substitution allows to automatically generate loops. But here, iteration is done on the image of a relation element.

INVARIANT_ITERATION syntax is:

```
"INVARIANT ITERATION" "("
  [ ("tant que"|"while") "\=>" IdentOrJokerOrVardecl ",," ]
  "1st" "index" "\=>" Expression ","
  "2nd" "index" "\=>" Expression ","
  "constant" "\=>" Expression ","
  "1st" "type" "\=>" Expression ","
  "2nd" "type" "\=>" Expression ","
  "body" "\=>" "(" Substitution ")" ","
  "invariant" "\=>" "(" Predicate ")"
")"
```

**Syntax 6 : Invariant iteration syntax**

Clauses meaning is:
- **while**: If present, provides a variable which permits to interrupt the loop before its natural ending
- **constant**: Defines the relation which will be used to iterate
- **1st index**: Defines original element of iteration. Iteration will be done on constant[\{1st index\}]
- **2nd index**: Element storing current element of the loop
- **1st type**: Type of constant domain elements
- **2nd type**: Type of constant range elements
- **body**: User defined part of the loop body
- **invariant**: User defined part of the loop invariant

Generated loop for an INVARIANT substitution is:

```
v_g_loop <-- init_iteration_CONSTANT(index1);
WHILE v_g_loop = TRUE DO
  v_g_loop, index2 <-- continue_iteration_CONSTANT(index1);
  body
INVARIANT
  v_g_loop = bool(CONSTANT_remaining /= \{\} &
                 CONSTANT_remaining \(/\) CONSTANT_done = CONSTANT[\{index1\}]
                 CONSTANT_remaining \(/\) CONSTANT_done = \{\} &
                 invariant
VARIANT
  cardCONSTANT_remaining
END
```

**Figure 37 : Invariant iteration generated loop**
As for TYPE_ITERATION, \(\text{vg\_loop} := \text{bool}(\text{vg\_loop} = \text{TRUE} \& \text{while} = \text{TRUE})\) will be added to the loop body if a while substitution is added.

Generated iteration machine for a single INVARIANT_ITERATION is:

\[
\begin{align*}
\text{MACHINE} & \quad \text{iterator\_name} \\
\text{ABSTRACT\_VARIABLES} & \quad \text{CONSTANT}\_\text{remaining}, \quad \text{CONSTANT}\_\text{done} \\
\text{INVARIANT} & \quad \text{CONSTANT}\_\text{remaining} <: \text{ran(CONSTANT)} \& \\
& \quad \text{CONSTANT}\_\text{remaining} <: \text{TYPE2} \& \\
& \quad \text{CONSTANT}\_\text{done} <: \text{TYPE2} \& \\
& \quad \text{CONSTANT}\_\text{remaining} \setminus \text{CONSTANT}\_\text{done} = \{\} \\
\text{INITIALISATION} & \quad \text{CONSTANT}\_\text{remaining} := \{\} || \\
& \quad \text{CONSTANT}\_\text{done} := \{\} \\
\text{OPERATIONS} & \\
& \quad \text{continue} \leftarrow \text{init\_iteration\_CONSTANT(elt)} = \\
& \quad \text{PRE} \\
& \quad \text{elt} : \text{TYPE1} \\
& \quad \text{THEN} \\
& \quad \text{CONSTANT}\_\text{done} := \{\} || \\
& \quad \text{CONSTANT}\_\text{remaining} := \text{CONSTANT}\{\text{elt}\} || \\
& \quad \text{continue} := \text{bool(\text{CONSTANT}\{\text{elt}\} /= \{\})} \\
& \quad \text{END}; \\
& \quad \text{continue, elt} \leftarrow \text{continue\_iteration\_CONSTANT=} \\
& \quad \text{PRE} \\
& \quad \text{CONSTANT}\_\text{remaining} /= \{\} \\
& \quad \text{THEN} \\
& \quad \text{ANY} \\
& \quad \text{nn} \\
& \quad \text{WHERE} \\
& \quad \text{nn} : \text{TYPE2} \& \\
& \quad \text{nn} : \text{CONSTANT}\_\text{remaining} \\
& \quad \text{THEN} \\
& \quad \text{CONSTANT}\_\text{done} := \text{CONSTANT}\_\text{done} \setminus \{\text{nn}\} || \\
& \quad \text{CONSTANT}\_\text{remaining} := \text{CONSTANT}\_\text{remaining} - \{\text{nn}\} || \\
& \quad \text{elt} := \text{nn} || \\
& \quad \text{continue} := \text{bool(\text{CONSTANT}_\text{remaining} /= \{\text{nn}\})} \\
& \quad \text{END} \\
& \quad \text{END} \\
\end{align*}
\]

\textbf{Figure 38 : Invariant iteration generated machine}
VIII.5.1.3 CONCRETE_ITERATION

CONCRETE_ITERATION substitution also produces automatically generated WHILE loops. Unlike TYPE_ITERATION or INARIANT_ITERATION, these loops don’t use any iteration machine.

Syntax for CONCRETE_ITERATION substitution is:

```
"CONCRETE_ITERATION" "(" "init_while" "=>" "(" Substitution ")" ")" "," 
("tant_que"|"while") "=>" Expression "," 
"body" "=>" "(" Substitution ")" "," 
"invariant" "=>" "(" Predicate ")" "," 
"variant" "=" Expression "," 
"flag" "=" IdentOrJoker
```

Syntax 7: Concrete iteration

The generated loop for this substitution is:

```
init_while;
vg_loop := bool( while );
WHILE vg_loop = TRUE DO
  \/*? Flag iteration: flag ?*/
  body ;
  vg_loop := bool( while )
INVARIANT
  invariant
VARIANT
  variant
END
```

Figure 39: Concrete iteration generated loop

VIII.5.1.4 Iteration components

During refinement process, Bart stores information about iteration machines used by operations refinement and defined by TYPE_ITERATION or INARIANT_ITERATION substitutions.

After splitting refinement results in output components (cf. X), Bart creates an iteration machine associated to each generated implementation, if necessary. Each iteration machine generated contains variables and operations for all iterators defined and used by refinement of operations implemented in associated implementation.

Following table presents which abstract variables and operations are generated in iteration machines for the refinement of a component “Machine”, according to TYPE_ITERATION and INARIANT_ITERATION substitutions used during refinement.
<table>
<thead>
<tr>
<th>Iterators used by operations refinement</th>
<th>Associated iteration machine</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Machine_i</strong></td>
<td>-</td>
</tr>
<tr>
<td><strong>Operation1</strong></td>
<td>No iterator defined</td>
</tr>
<tr>
<td><strong>Machine1_i</strong></td>
<td><strong>Machine1_it</strong></td>
</tr>
<tr>
<td><strong>Operation2</strong></td>
<td>Abstract variables:</td>
</tr>
<tr>
<td>type iterator on type 1</td>
<td>type1_remaining, type1_done,</td>
</tr>
<tr>
<td>Invariant iterator on const1</td>
<td>const1_remaining, const1_done,</td>
</tr>
<tr>
<td><strong>Operation3</strong></td>
<td>type2_remaining, type2_done</td>
</tr>
<tr>
<td>type iterator on type2</td>
<td><strong>Operations:</strong></td>
</tr>
<tr>
<td><strong>Operation4</strong></td>
<td>init_iteration_type1;</td>
</tr>
<tr>
<td>Invariant iterator on const1</td>
<td>continue_iteration_type1;</td>
</tr>
<tr>
<td><strong>Machine2_i</strong></td>
<td><strong>Machine2_it</strong></td>
</tr>
<tr>
<td><strong>Operation5</strong></td>
<td>Abstract variables:</td>
</tr>
<tr>
<td>type iterator on type2</td>
<td>type2_remaining, type2_done,</td>
</tr>
<tr>
<td><strong>Operation6</strong></td>
<td>const2_remaining, const2_done</td>
</tr>
<tr>
<td>Invariant iterator on const2</td>
<td><strong>Operations:</strong></td>
</tr>
<tr>
<td></td>
<td>init_iteration_type2;</td>
</tr>
<tr>
<td></td>
<td>continue_iteration_type2;</td>
</tr>
<tr>
<td></td>
<td>init_iteration_const2;</td>
</tr>
<tr>
<td></td>
<td>continue_iteration_const2;</td>
</tr>
</tbody>
</table>

Figure 40: Example of generated iterators

If a same iterator is used by several operations of implementation, it is only created once in iteration machine. Bart gathers all iteration variables and operations necessary for all refinement results written in the implementation. Invariant and initialisation are generated according to defined variables. Real iteration machines are actually merges of iteration machines presented in VIII.5.1.1 and VIII.5.1.2.

VIII.5.2 Using operations from seen machines - SEEN_OPERATION

SEEN_OPERATION substitution is used to insert a call to an operation from a seen machine in the rule result. Its syntax is:

```
"SEEN_OPERATION" "(" 

 "name" "=" IdentOrJoker "," 

 "out" "=" "(" [ IdentJokerVardeclList ] ")" "," 

 "in" "=" "(" [ IdentJokerVardeclList ] ")" "," 

 "body" "=" "(" Substitution ")" 

")" 
```

Syntax 8: Seen operation

- name: Name of the operation to use
- out: Output parameters of the operation call
• in : Input parameters of the operation call
• body: Substitution that may be used by Bart to control in seen machines that it corresponds to the given identifier. For now the control is not done, so the clause can be filled with @_ joker

For example,

\[
\text{SEEN\_OPERATION}(
\quad \text{name} => \text{operation},
\quad \text{out} => \text{(out1)},
\quad \text{in} => \text{(in1)},
\quad \text{body} => \text{(_@) }
\)
\]

will be converted in \( \text{out1} \leftarrow \text{operation(in1)} \) operation call.

When SEEN\_OPERATION is used, Bart doesn’t check if the operation exists or if the user has provided the correct number of parameters. The operation is supposed to exist.

If the operation existence must be checked, it is better to use the DECL\_OPERATION guard in the WHEN clause of the rule, and then express the result using jokers instantiated by constraint checking.

**VIII.5.3 Defining imported operations - IMPORTED\_OPERATION**

IMPORTED\_OPERATION substitution lets the user create a new operation that will be called in this one refinement and inserts a call to it. The newly created operation will be declared further in the output components chain. For example, if currently refined operation is implemented in Machine1\_i, the new one will be first declared in Machine2, and implemented in Machine2\_i or a further implementation.

In the generated implementation, IMPORTED\_OPERATION will be replaced by a call to the created operation.

**IMPORTED\_OPERATION substitution syntax is:**

```
"IMPORTED\_OPERATION" "("
    [ "name" "=>" ident "," ]
    "out" "=>" "(" [ IdentJokerVardeclList ] ")" ",",
    "in" "=>" "(" [ IdentJokerVardeclList ] ")" ",",
    "pre" "=>" "(" Predicate ")" ",",
    "body" "=>" "(" Substitution ")"
"
```

**Syntax 9 : Imported operation**

• **name**: This facultative clause can contain a base for generating the name of the new operation. If it is given, Bart may add number suffixes to the identifier to distinguish between different generated operation (as a rule can be selected several times)
• **output**: Output call parameters. Formal output parameters for the operation definition will also be generated from this list
- **input**: Input call parameters. Formal input parameters for the operation definition will also be generated from this list
- **pre**: User defined part of the precondition for the new operation
- **body**: The new operation body

### VIII.5.3.1 Naming new operations

If a name clause is given in IMPORTED_OPERATION, Bart will generate a unique name from it by adding a number suffix to the identifier. Else, Bart will use current operation name as a base, and will add number suffix to it. For example, IMPORTED_OPERATION substitution used in refinement of operation1 may generate operation1_1, operation1_2, etc.

As there can be several layers of overlapped operations (ex: operation generates operation1 which generates other operations), Bart may add several numbers to an original pattern. To avoid conflicts in naming, it adds underscore after the first counter and before each counter greater than 10.

For example:

```
operation -> operation1 -> operation1_1 -> operation1_1_11
operation -> operation1 -> operation1_1 -> operation1_11 -> operation1_111
```

**Figure 41**: Imported operation naming example

### VIII.5.3.2 Operation parameters

The user can provide input or output parameters for the operation.

Following table presents an IMPORTED_OPERATION treatment in a simple case where instantiation is \{@a = aa, @b = bb, @c = cc\}. For this example we do not consider operation abstraction and hypothesis stack (cf. VIII.5.3.3).

<table>
<thead>
<tr>
<th>Rule</th>
<th>Operation call</th>
<th>Generated operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPORTED_OPERATION(</td>
<td>aa &lt;- add1(bb, cc)</td>
<td>out &lt;- add1(in1, in2) =</td>
</tr>
<tr>
<td>name =&gt; add</td>
<td></td>
<td>PRE in1 : INT &amp;</td>
</tr>
<tr>
<td>out =&gt; (@a),</td>
<td></td>
<td>in2 : INT</td>
</tr>
<tr>
<td>in =&gt; (@b, @c),</td>
<td></td>
<td>THEN out &lt;- in1 + in2</td>
</tr>
<tr>
<td>pre =&gt; (@b : INT &amp;</td>
<td></td>
<td>END</td>
</tr>
<tr>
<td>@c : INT),</td>
<td></td>
<td></td>
</tr>
<tr>
<td>body =&gt; (@a := @b +</td>
<td></td>
<td></td>
</tr>
<tr>
<td>@c)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
In these cases, generated operation would be incorrect, as these identifiers would be unknown in the machine the new operation will be declared in. So in these particular cases, Bart automatically adds inputs (for read ones) or output (modified ones) parameters to give these values to the newly defined operation.

Let's consider a new example with instanciation \{@a = aa, @e = bb + cc\}, in which bb and cc are input parameters of current refined operation, and without considering the hypothesis stack or operation abstraction:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Operation call</th>
<th>Generated operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPORTED_OPERATION(</td>
<td>aa &lt;-- add1(bb, cc)</td>
<td>out &lt;-- add1(in1,in2) =</td>
</tr>
<tr>
<td>name =&gt; add</td>
<td></td>
<td>BEGIN</td>
</tr>
<tr>
<td>out =&gt; (@a),</td>
<td></td>
<td>out &lt;-- in1 + in2</td>
</tr>
<tr>
<td>body =&gt; (@a := @e) )</td>
<td></td>
<td>END</td>
</tr>
</tbody>
</table>

Figure 43: Imported operation example with parameters adding

As bb and cc are local parameters that can not be directly exported in new operation body, two input parameters are automatically added to new defined operation.

If bb and cc had been global variables, Bart would not have added input parameters, as they could have been directly exported.

Functionality of automatically adding parameters is used to avoid typecheck errors when a parameter is missing, when local parameters can not be identified because they are contained in a joker (as in the example, @e = bb + cc), or to help the user when the instantiated body clause is huge and contains a lot of identifiers.

However, it is still better when every parameter that should be present in "in" or "out" clauses is, so that user can have a better control of the refinement.

VIII.5.3.3 Imported operation preconditions

As it has been said before, user can provide to Bart a piece of invariant that will be added to the generated operation. But Bart also automatically adds predicates to the operation invariant.

These added predicates are:
- Preconditions of abstractions of currently refined operation
- Predicates added by the refinement process while refining current operation (LH substitution, guarded substitution)

These predicates correspond in fact to every predicates added to the stack since the beginning of current operation refinement. When they are added, they are filtered with identifiers appearing in the new operation body, so that only relevant predicates are added.
Bart, when adding those predicates, doesn’t check if user has put some of them in its “pre” clause, so sometimes predicates can appear several times. Basic typing predicates are often automatically added as they are normally present in previous abstractions. “pre” clause of the substitution should better be used for more complex and specific predicates.

Here is an example of Bart automatic predicate adding. The instantiation is \{@a = aa, @b = bb, @c = cc\}. bb and cc are input parameters of current operation, and the stack contains bb : INTEGER & cc : INTEGER (coming for example from operation precondition).

<table>
<thead>
<tr>
<th>Rule</th>
<th>Operation call</th>
<th>Generated operation</th>
</tr>
</thead>
</table>
| IMPORTED_OPERATION(  
  name => add  
  out => (@a),  
  in => (@b, @c),  
  body => (@a := @b + @c) ) | aa <-- add1(bb, cc) | out <-- add1(in1, in2) = PRE  
  in1 : INTEGER &  
  in2 : INTEGER  
THEN  
out <-- in1 + in2  
END |

**Figure 44 : Example of imported operation precondition adding**

### VIII.5.3.4 Imported operations refinement

Refinement of given component operations may introduce new imported operations.

Once all original operations have been refined, Bart processes new imported operations to refine them. If their refinement introduces new operations, the process goes on until there are no new operations.

### VIII.5.4 Controlling the refinement process

Some substitution that user can write in result clauses are not really expressing the result but permits to control the following refinement.

#### VIII.5.4.1 IMPLEMENT

IMPLEMENT syntax is:

```
ImplementSubstitution = "IMPLEMENT" "(" Substitution ")".
```

**Syntax 10 : Implement**

When IMPLEMENT is present in a result clause it means that its content will be written in the result without being more refined.
Usage of IMPLEMENT only makes sense in a REFINEMENT clause, as refinement stops when result is expressed in an IMPLEMENTATION one.

For example if IMPLEMENT(aa := 1) is present in a rule clause, aa := 1 will be written without being more refined, while others parts of the result clause may have their refinement processed further.

**VIII.5.4.2 LH**

LH stands for “Local Hypothesis” substitution. Its syntax is:

```
"LH" Predicate "THEN" Substitution "END"
```

**Syntax 11 : LH**

It is not translated in B substitution by Bart when the result clause is instantiated, but it allows the user to add a hypothesis for refining given substitution.

As IMPLEMENT, LH usage doesn’t make sense in IMPLEMENTATION clause. It can be used in REFINEMENT, and, unlike other substitutions presented in this section, in SUB_REFINEMENT clause.

For example, with the following elements:

<table>
<thead>
<tr>
<th>Substitution to refine</th>
<th>Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>IF val &gt; 0 THEN</td>
<td>RULE r_if</td>
</tr>
<tr>
<td>aa := TRUE</td>
<td>REFINES</td>
</tr>
<tr>
<td>ELSE</td>
<td>IF @a THEN @b ELSE @c END</td>
</tr>
<tr>
<td>aa := FALSE</td>
<td>SUB_REFINEMENT</td>
</tr>
<tr>
<td>END</td>
<td>(LH @a THEN @b END) -&gt; (@d),</td>
</tr>
<tr>
<td></td>
<td>(LH not(@a) THEN @c END) -&gt; (@e)</td>
</tr>
<tr>
<td>END</td>
<td>IMPLEMENTATION</td>
</tr>
<tr>
<td>#1 := bool(@a) ;</td>
<td>IF #1 = TRUE THEN @d ELSE @e END</td>
</tr>
<tr>
<td>END</td>
<td>END</td>
</tr>
</tbody>
</table>

**Figure 45 : Substitution and rule for LH example**

Following figure shows the evolution of the stack, if we suppose it is empty before applying the rule.
VIII.5.5 Local variable declarations

In Bart result clauses, it is possible to declare local variables and use them to express the result substitution.

The syntax is a “#” character followed by a number. If the same “#” declaration appears several times in the clause, it designates the same variable. Same declaration can be used in different rules, they will stand for different local variables.

If local variables are used by found rules during the whole operation refinement process, they will all be declared in a local variables (VAR...IN) substitution which will embrace the operation refinement result. For more information on formatting operation refinement results, see X.1.
Here is an example (we suppose that subrefinements are refinement by themselves):

<table>
<thead>
<tr>
<th>Operation body</th>
<th>Rule</th>
<th>Operation refinement result</th>
</tr>
</thead>
<tbody>
<tr>
<td>BEGIN IF value &gt; 0 THEN Aa := TRUE ELSE Aa := FALSE END IF value2 &gt; 0 THEN Bb := TRUE END</td>
<td>RULE r_if REFINES IF @a THEN @b ELSE @c END SUB_REFINEMENT (LH @a THEN @b END) -&gt; (@d), (LH not(@a) THEN @c END) -&gt; (@e) IMPLEMENTATION #1 := bool(@a); IF #1 = TRUE THEN @d ELSE @e END END</td>
<td>VAR l_1,l_2 L_1 := bool(value &gt; 0); IF l_1 = TRUE THEN Aa := TRUE ELSE Aa := FALSE END; L_2 := bool(value2 &gt; 0); IF l_2 = TRUE THEN Bb := TRUE ELSE Bb := FALSE END</td>
</tr>
</tbody>
</table>

Figure 47: Local variable declaration example

VIII.6 Declaring operation refinement variables

Besides declaring local variables during operation refinement, it is also possible to declare new abstract or concrete variables that can be used in REFINEMENT clauses of rules.

This kind of declaration corresponds to RefinementVarDecl element of syntax described in VIII.1.

If VARIABLE or ABSTRACT_VARIABLE keyword is used, it means that the new variable is an abstract one. In this case, RENIED_BY clause may be present to specify which rule must be used. Syntax is RENIED_BY(theory.rule(parameters)). Parameters usage is identical as for abstract variable refinement. If RENIED_BY clause is not present, the rule for the variable will be simply searched in rule files.

If CONCRETE_VARIABLE is used, the new variable is a concrete one. In this case, usage of RENIED_BY clause doesn’t make sense.

Invariant and initialisation for new variable are expressed in WITH_INV and WITH_INIT clauses.

If new abstract variables are introduced, a REFINEMENT component will be introduced in output chain.

VIII.7 Usage of substitution rules
VIII.7.1 Structural and operation rules - Operation refinement

VIII.7.1.1 Structural rules

Structural rules are exactly identical to operation rules, but they are gathered in theories called structure theories. So structure theories syntax is:

```plaintext
StructureTheory = "THEORY_STRUCTURE" ident "IS" OperationRule { ";" OperationRule } "END" ident .
```

**Syntax 12: Structure theories**

Structural rules are only used in certain cases for refining operations of the given component to refine. Newly introduced imported operations are only refined with operation rules from operation theories.

VIII.7.1.2 Operation refinement process

Structural rules are used to refine operations from given component that contains control structures, i.e. at least one following substitutions: IF, SELECT. They are usually used to split IF and SELECT structure branches into several operation calls. Bart rule base contains structure theories allowing to treat these substitutions. But structure rules researching process is exactly identical to operation rules one, so user can define his own rules in his rule files.

Following figure shows how Bart uses structure and operation theories to refine operations of given component. This process is not used for refinement of created imported operations.
Figure 48: Usage of structure and operation rules

Bart tries structural refinement if current operation contains structure substitution. A structural refinement error occurs if Bart can not find structure rules to completely refine the operation. If such an error occurs, Bart will try to refine the operation with operation rules from the beginning.

Consequently, an operation rule tree can contain only one kind of rules: structure rules (for operation containing structure that could be structurally refined) or operation rules (for operations without structure, or operations with structure that could not be structurally refined).

Once all original operations have been refined using structure or operation rules, imported operations introduced by this process are refined using exclusively operation rules.

Here is an example of refinement using structure and operation rules.

<table>
<thead>
<tr>
<th>Rules</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>THEORY_STRUCTURE structure IS</td>
<td>operation(val) =</td>
</tr>
<tr>
<td></td>
<td>PRE</td>
</tr>
<tr>
<td></td>
<td>val : INTEGER</td>
</tr>
<tr>
<td></td>
<td>THEN</td>
</tr>
<tr>
<td></td>
<td>IF val &gt; 0 THEN</td>
</tr>
<tr>
<td></td>
<td>aa := TRUE</td>
</tr>
<tr>
<td>RULE default</td>
<td></td>
</tr>
<tr>
<td>REFINES @a</td>
<td></td>
</tr>
<tr>
<td>WHEN</td>
<td></td>
</tr>
</tbody>
</table>
bnot(bhasflow(@a))
IMPLEMENTATION
IMPORTED_OPERATION( 
  out => (),
  in => (),
  pre => (0=0),
  body => (@a))
END;

RULE if_then_else
  REFINES
    IF @a THEN @b
    ELSE @c
    END
  REFINEMENT
    #1 := bool(@a);
    IF #1 = TRUE THEN LH @a THEN @b END ELSE LH not(@a) THEN @c END
END
END structure &

THEORY_OPERATION operation IS

RULE r_affect_bool_2
  REFINES
    @a := @b
  WHEN
    match(@b,TRUE) or match(@b,FALSE)
  IMPLEMENTATION
    @a := @b
END;

RULE r_affect_bool_1
  REFINES
    @a := @b
  WHEN
    (match(@b,TRUE) or match(@b,FALSE)) & bnot(B0EXPR(@a))
  IMPLEMENTATION
    #1 := @b
    @a := #1
END;

END operation

ELSE
  aa := FALSE
END
END;

out <-- affect_true =
BEGIN
  out := TRUE
END

Figure 49: Theories and operation for operation refinement example

For these rules and operations, refinement results are:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Found rules</th>
<th>Produced result</th>
</tr>
</thead>
</table>
| operation | - Guarded substitution refinement - LH refinement - structure.default | operation(val) = VAR l_1 IN l_1 := bool(val > 0);
     | - IF l_1 = TRUE THEN operation1 ELSE operation2 END |
Here we supposed hypothesis stack did not contain any predicates concerning aa variable, so that generated imported operation don’t have preconditions.

VIII.7.2 Initialisation rules

For refining the initialisation of treated component, Bart uses special substitution rules called initialisation rules, gathered in initialisation theories. Initialisation rules are restricted substitution rules.

Initialisation rules syntax is presented hereafter:

```
InitialisationTheory
  =
    "THEORY_INITIALISATION" ident
    "IS"
    InitialisationRule { ";" InitialisationRule }
    "END" ident
  .

InitialisationRule
  =
    "RULE" ident
    "REFINES" Substitution
    [ "WHEN" Predicate ]
    "IMPLEMENTATION" Substitution
    "END"
  .
```

Syntax 13 : Initialisation theories

Bart refines the given component initialisation as it would refine an operation body, but with using initialisation rules instead of structure and operation rules.

Restrictions in initialisation rules in comparison to other substitution rules are:
- Initialisation rule result can only be specified in an IMPLEMENTATION clause. So an initialisation rule is always terminal.
- Usage of subrefinements (SUB_REFINEMENT clause) is not allowed in initialisation rules.
- Introduction of new global variables is not allowed in initialisation rules.
- Introduction of local variables is not allowed in initialisation rules.

When Bart refines initialisation, it usually goes down in the substitution by applying parallel predefined refinement behaviour, and searches for rules for each atomic initialisation element. So result of initialisation refinement is often a semicolon separated list of atomic substitutions.

When output components are generated, Bart splits initialisation in elementary elements. Each elementary element is an initialisation for a given variable. When a refinement variable is implemented in an output component, its associated initialisation element is also written.

As it is split and dispatched along output components, initialisation of given component to refine must be a parallel or semicolon separated list of elementary elements, each elementary element initialising a unique abstract variable.

Let’s consider following initialisation and rules:

<table>
<thead>
<tr>
<th>Initialisation</th>
<th>Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>aa := 1</td>
<td></td>
</tr>
<tr>
<td>bb :: INTEGER</td>
<td></td>
</tr>
<tr>
<td>cc :: BOOL</td>
<td></td>
</tr>
<tr>
<td></td>
<td>WHEN</td>
</tr>
<tr>
<td></td>
<td>IMPLEMENTATION</td>
</tr>
<tr>
<td></td>
<td>END;</td>
</tr>
<tr>
<td></td>
<td>RULE scalar_ini2</td>
</tr>
<tr>
<td></td>
<td>WHEN</td>
</tr>
<tr>
<td></td>
<td>IMPLEMENTATION</td>
</tr>
<tr>
<td></td>
<td>END;</td>
</tr>
<tr>
<td></td>
<td>RULE scalar_ini3</td>
</tr>
<tr>
<td></td>
<td>WHEN</td>
</tr>
<tr>
<td></td>
<td>IMPLEMENTATION</td>
</tr>
<tr>
<td></td>
<td>END</td>
</tr>
</tbody>
</table>

Figure 51: Substitution and theories for initialisation refinement example
where aa, bb, cc are abstract variables refined with a variable rule adding SCALAR predicate. Following table shows the results:

<table>
<thead>
<tr>
<th>Found rule</th>
<th>Initialisation elementary element</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parallel refinement</td>
<td></td>
</tr>
<tr>
<td>Parrallel refinement</td>
<td></td>
</tr>
<tr>
<td>Init.scalar_ini1</td>
<td>aa := 1</td>
</tr>
<tr>
<td>Init.scalar_ini2</td>
<td>bb := 0</td>
</tr>
<tr>
<td>Init.scalar_ini3</td>
<td>cc := FALSE</td>
</tr>
</tbody>
</table>

**Figure 52 : Initialisation refinement example**
IX TACTIC AND USER PASS THEORIES

Tactics and user passes should be used in Bart rule files to control the rule research process, and to avoid a processing of all rules from all theories. These theories are local to their rule files. Bart processes each rule file to find rules. For the rule file currently processed, it may use tactic or user pass to filter its theories to use.

IX.1 User pass theory

IX.1.1 Syntax

```
UserPassTheory = "USER_PASS" "IS"
[ ("VARIABLE"|"OPERATION"|"INITIALISATION") ":" "(" IdentList ")" ]
{ ";" ("VARIABLE"|"OPERATION"|"INITIALISATION") ":" "(" IdentList ")" }
"END"
```

Syntax 14 : User pass theory

IX.1.2 Usage

User pass theory is used to specify, for different types of elements to be refined, which theories must be considered by Bart. There must be at most one user pass theory in a rule file.

Theories of a particular user pass element are considered from right to left.

For example, if following user pass is used:

```
USER_PASS IS
  VARIABLE : (tv1,tv2);
  OPERATION : (to1)
  INITIALISATION : (ti1, ti2)
END
```

Figure 53 : User pass theory example

Bart will search variable rules only in theories tv1 and tv2, operation rules only in theory to1, and initialisation rules in theories ti1 and ti2.

At least one element (variable, initialisation or operation pass) must be present in user pass theory. At most one pass must be present for each kind of element.
If there are several user passes for a same kind of element, an error or a warning will be raised.

**IX.2 Tactic theory**

**IX.2.1 Syntax**

```plaintext
TacticTheory =
   "THEORY" "TACTICS" "IS"
   { Tactic }
   "END".

Tactic =
   "VARIABLE" ":" VariableTactic { ":" VariableTactic }
   | "INITIALISATION" ":" SubstitutionTactic { ":" SubstitutionTactic }
   | "OPERATION" ":" SubstitutionTactic { ":" SubstitutionTactic }

SubstitutionTactic =
   IdentList "=>" "( Substitution )"
.

VariableTactic =
   IdentList "=>" "( Predicate )"
.
```

**Syntax 15 : Tactic theory**

**IX.2.2 Usage**

Tactics allow indicating which theories must be used for elements by using patterns. There must be at most one tactic theory in a rule file.

There are several sections for different elements to refine (variables, initialisation, and operations). At least one section must be present in the tactic, and each section should be present at most one time.

Each section contains a list of tactic elements, each one containing a theory list associated with a pattern. When an element must be refined by using the tactic theory, Bart processes the suitable tactic section from bottom to top, and tries to match the element with the pattern. If the variable or substitution to refine matches a tactic element pattern, rules for refining it are searched in the associated list of theories.

When a tactic pattern is selected, its theories are processed from right to left.

For example, if following tactic is used:
THEORY TACTICS IS
VARIABLE :
  standard => (@a)
INITIALISATION :
  iterateur_i, standard_i => (@a)
OPERATION :
  assign_a_b, assign_a_b_2 => (@a := @b);
  assign_a_b_plus => (@a := @b + @c);
  assign_a_union_b_c => (@a := @b / @c);
END

Figure 54: Tactic theory example

, when Bart must refine a variable, it will search for rules in theory standard. When it must refine initialisation, it will search for rules in iterateur_i and standard_i theories.

If $aa := \text{set1} \setminus \text{set2}$ must be refined in an operation, assign_a_union_b_c theory will be used.

Note: If a pattern is selected and no rule is found (and no predefined behaviour), there will be a refinement error. Bart won’t process the tactic further to check if the element to refine matches with other patterns. For example, with previous tactic, if $aa := bb + cc$ must be refined, and no rule is found in assign_a_b_plus, it won’t search for rules in assign_a_b and assign_a_b_2 theories.

IX.3 Priority of Tactic and User pass theories

This section presents which theory will be used for a rule file according to the presence of tactic or user pass theories.

Figure 55: Usage of tactics and user passes

This means that if tactic and user pass theory are both present, the tactic will be used.
When Bart has determined which kind of rule research (tactic, user pass or regular) will be used, it will only use this one, even if a refinement error occurs because no rule and predefined behaviour could be found. For example, if Bart uses user pass theory and a variable couldn’t be refined, it won’t try to find a rule in variable theories that were not included in the variable user pass.
X  RESULT PRODUCTION AND WRITING

X.1 Formatting the result

To refine an operation, Bart launches its recursive rule research process on the operation substitution body.

At the end, the tool may apply a certain treatment on the produced result to write it as an operation body of output components. Furthermore, formatting process may also include introduction of a local variable substitution to declare local variables from this operation refinement (declared with the # syntax).

Following table shows how refinement results are formatted depending on the presence of new local variables. Generic elements are expressed with jokers here.

<table>
<thead>
<tr>
<th>Refinement result</th>
<th>Declaration of local variables</th>
<th>Formatted result</th>
</tr>
</thead>
<tbody>
<tr>
<td>PRE @p THEN @s END</td>
<td>No</td>
<td>PRE @p THEN @s END</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>PRE @p THEN VAR @v IN @s END END</td>
</tr>
<tr>
<td>ASSERT @p THEN @s END</td>
<td>No</td>
<td>ASSERT @p THEN @s END</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>ASSERT @p THEN VAR @v IN @s END END</td>
</tr>
<tr>
<td>BEGIN @b END</td>
<td>No</td>
<td>BEGIN @b END</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>VAR @v IN @b END</td>
</tr>
<tr>
<td>VAR @l IN</td>
<td>No</td>
<td>VAR @l IN</td>
</tr>
</tbody>
</table>
Here are examples of Bart result formatting:

<table>
<thead>
<tr>
<th>Operation</th>
<th>Refinement result</th>
<th>Declared local variables</th>
<th>Formatted result</th>
</tr>
</thead>
<tbody>
<tr>
<td>affect_sum(in1,in2) =</td>
<td>BEGIN</td>
<td></td>
<td>affect_sum(in1,in2) =</td>
</tr>
<tr>
<td>pre</td>
<td>l_1 := in1 + in2;</td>
<td></td>
<td>VAR l_1</td>
</tr>
<tr>
<td>in1 : INTEGER &amp; in2 : INTEGER</td>
<td>abvar := l_1</td>
<td></td>
<td>IN VAR l_1</td>
</tr>
<tr>
<td>then</td>
<td>END</td>
<td></td>
<td>IN abvar := l_1</td>
</tr>
<tr>
<td>abvar := in1 + in2;</td>
<td>END</td>
<td></td>
<td>END</td>
</tr>
<tr>
<td>out := lire_abvar =</td>
<td>out := abvar</td>
<td></td>
<td>BEGIN</td>
</tr>
<tr>
<td>out := abvar</td>
<td></td>
<td></td>
<td>END</td>
</tr>
</tbody>
</table>

**Figure 57: Refinement result formatting example**

### X.2 Implementing results

Once all variables, operations and initialisation have been successfully refined, Bart must produce output components and implement variables, operations and initialisation parts in these components.

Bart output splitting process is driven by operation refinement results and by variables used by those. Once the tool has decided how operations must be implemented along the output chain, variables and initialisations parts are dispatched according to operation arrangement.

#### X.2.1 Splitting operations in output components
For each operation to implement, Bart considers two sets of variables:

- **Variables to implement**: This set contains all variables present in IMPLEMENT clauses of substitution rules found for this operation. These are variables that must be implemented in the machine for the operation to be implemented.

- **Exported variables**: These are abstract variables used in specifications of imported operations generated for this one refinement. These variables must not be implemented as long as the operation is not implemented.

In the following, exported\( (op) \) are variables exported by operation \( op \), and implement\( (op) \) are variables to implement for operation \( op \). Term “before” and “further” refers to the order of the output chain.

Bart chooses operations arrangement by generating iteratively output components with respect of following constraints:

- An operation must be implemented before imported operations defined for its refinement.
- If the operation \( op \) is implemented in current component, other operations \( opX \) have to be implemented further if intersection of exported\( (op) \) and implement\( (opX) \) is not empty.

**X.2.2 Resolving deadlocks**

**X.2.2.1 Bart splitting algorithm**

This section presents the algorithm used by Bart to split operations with respect for constraints exposed in X.2.1.

First, the set of operations to implement is filled with operations of original component to refine. Then Bart repeats following process as long as no error occurs and there are still operations to implement:

- The tool builds the set \( E \) containing variables exported by all operation that must be currently implemented.
- Each operation “\( op \)” such as intersection of implement\( (op) \) and \( E \) is empty is implemented in current component, and is removed of set of operations to implement.
- Operation of the set that could not be implemented in current component will be promoted in the implementation.
- Once every operation has been tried, imported operations eventually defined by refinement of the ones implemented in current component are added to the set of operations to implement.
- If the set of operations to implement is not empty, process goes on with a new generated output component.
Following figure shows some example operations and their generated imported operations:

---

Figure 58: Operations to implement for splitting example

For these operations, Bart may generate following machines:

---

Figure 59: Result machines for splitting example

The generation process is as follow:

- **Step 1**, operations to implement are \{OpA, OpB, OpC, OpD\}
  - Variables exported by all operations are \{bb, cc\}
  - OpA and OpB don’t contain those in their variables to implement, they can be implemented
  - OpC and OpD can not be implemented, they will be promoted
- **Step 2**, operations to implement are \{OpA1, OpA2, OpC, OpD\}
  - Exported variables are \{cc\}
OpA1 and OpC can be implemented
- OpA2 and OpD are promoted
- Step 3, operations to implement are \{OpA2, OpC1, OpD\}
  - There are no exported variables anymore, all operations can be implemented

Figure 60: Splitting process example

X.2.2.2 What is a splitting deadlock?

A splitting deadlock is an error in the process previously described in X.2.2.1.
It occurs when, at a certain splitting step, no operation can be implemented by Bart in current component. It means that every operation has one of its variables to implement contained in another one exported variables.

For example, following draw shows a deadlock case:

![Splitting deadlock example](image)

Figure 61: Splitting deadlock example

Each operation to be implemented in current component needs another to be implemented further. So no operation can be implemented at current step and an error occurs.

X.2.2.3 Solving a deadlock case

When a deadlock occurs, Bart tries some processes to automatically solve it. It checks whether splitting conflicting operation bodies in several parts and
putting them in imported operations may solve the problem. If so, the result is generated and the operation is transparent to the user.

But in some cases, Bart is not able to solve automatically the problem. Then it generates a deadlock.xml file in the component directory. This file contains a XML description of the conflicting situation (operations, exported variables and variables to implement). It can be provided to the Bart GUI, which will display a draw representing the deadlock.

A deadlock is often caused by cycle as described in the example of X.2.2.2. In this case, the user should modify used rules to split more operation bodies and not have operations needing at the same time to implement and export variables.


**APPENDIX A – FIGURES TABLE**

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Bart command line parameters</td>
<td>8</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Example of Bart standard output</td>
<td>9</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Example of Bart verbose output mode</td>
<td>10</td>
</tr>
<tr>
<td>Figure 4</td>
<td>Example of selection of operations to refine</td>
<td>11</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Refinement process order</td>
<td>12</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Examples of pattern-matching without previous instantiation</td>
<td>14</td>
</tr>
<tr>
<td>Figure 7</td>
<td>Examples of @a + @b pattern-matching with previous instantiation</td>
<td>14</td>
</tr>
<tr>
<td>Figure 8</td>
<td>Hypothesis stack for constraint checking examples</td>
<td>15</td>
</tr>
<tr>
<td>Figure 9</td>
<td>Examples of constraint checking</td>
<td>15</td>
</tr>
<tr>
<td>Figure 10</td>
<td>Bart testing rule process</td>
<td>16</td>
</tr>
<tr>
<td>Figure 11</td>
<td>Hypothesis stack filling with environment</td>
<td>17</td>
</tr>
<tr>
<td>Figure 12</td>
<td>Example of Bart output components</td>
<td>18</td>
</tr>
<tr>
<td>Figure 13</td>
<td>Bart expression guards</td>
<td>20</td>
</tr>
<tr>
<td>Figure 14</td>
<td>Bart predicate guards</td>
<td>21</td>
</tr>
<tr>
<td>Figure 15</td>
<td>Bart substitution guards</td>
<td>21</td>
</tr>
<tr>
<td>Figure 16</td>
<td>Predicate theory example</td>
<td>22</td>
</tr>
<tr>
<td>Figure 17</td>
<td>Substitution for EMPILE_PRE and DEPILE_PRE example</td>
<td>23</td>
</tr>
<tr>
<td>Figure 18</td>
<td>Example of stack evolution with EMPILE_PRE and DEPILE_PRE</td>
<td>24</td>
</tr>
<tr>
<td>Figure 19</td>
<td>Processing variable theories to find rules</td>
<td>29</td>
</tr>
<tr>
<td>Figure 20</td>
<td>Searching variables refined by a particular rule</td>
<td>29</td>
</tr>
<tr>
<td>Figure 21</td>
<td>Theories and stack for variable rule research</td>
<td>30</td>
</tr>
<tr>
<td>Figure 22</td>
<td>Variable rule research example</td>
<td>30</td>
</tr>
<tr>
<td>Figure 23</td>
<td>Rules for type predicate example</td>
<td>31</td>
</tr>
<tr>
<td>Figure 24</td>
<td>Example of type predicates adding</td>
<td>31</td>
</tr>
<tr>
<td>Figure 25</td>
<td>Example of variable refinement rule with variable implementation</td>
<td>32</td>
</tr>
<tr>
<td>Figure 26</td>
<td>Variable refinement rule with concrete variable</td>
<td>33</td>
</tr>
<tr>
<td>Figure 27</td>
<td>Variable refinement rule with abstract variable</td>
<td>34</td>
</tr>
<tr>
<td>Figure 28</td>
<td>Theories and stack for operation rule research</td>
<td>37</td>
</tr>
<tr>
<td>Figure 29</td>
<td>Example of operation rule research</td>
<td>37</td>
</tr>
<tr>
<td>Figure 30</td>
<td>Process of substitution refinement</td>
<td>39</td>
</tr>
<tr>
<td>Figure 31</td>
<td>Substitution and theories for rule tree example</td>
<td>40</td>
</tr>
<tr>
<td>Figure 32</td>
<td>Example of refinement rule tree</td>
<td>41</td>
</tr>
<tr>
<td>Figure 33</td>
<td>Bart predefined refinement behaviours</td>
<td>42</td>
</tr>
<tr>
<td>Figure 34</td>
<td>Type iteration generated loop, without while parameter</td>
<td>44</td>
</tr>
<tr>
<td>Figure 35</td>
<td>Type iteration generated loop, with while parameter</td>
<td>45</td>
</tr>
<tr>
<td>Figure 36</td>
<td>Type iteration generated machine</td>
<td>45</td>
</tr>
<tr>
<td>Figure 37</td>
<td>Invariant iteration generated loop</td>
<td>46</td>
</tr>
<tr>
<td>Figure 38</td>
<td>Invariant iteration generated machine</td>
<td>47</td>
</tr>
<tr>
<td>Figure 39</td>
<td>Concrete iteration generated loop</td>
<td>48</td>
</tr>
<tr>
<td>Figure 40</td>
<td>Example of generated iterators</td>
<td>49</td>
</tr>
<tr>
<td>Figure 41</td>
<td>Imported operation naming example</td>
<td>51</td>
</tr>
</tbody>
</table>
Figure 42: Simple imported operation example ........................................... 51
Figure 43: Imported operation example with parameters adding ................. 52
Figure 44: Example of imported operation precondition adding ................. 53
Figure 45: Substitution and rule for LH example ....................................... 54
Figure 46: Example of stack filling with LH substitutions ......................... 55
Figure 47: Local variable declaration example ........................................ 56
Figure 48: Usage of structure and operation rules .................................... 58
Figure 49: Theories and operation for operation refinement example ............ 59
Figure 50: Operation refinement example ............................................... 60
Figure 51: Substitution and theories for initialisation refinement example ...... 61
Figure 52: Initialisation refinement example .......................................... 62
Figure 53: User pass theory example ...................................................... 63
Figure 54: Tactic theory example .......................................................... 65
Figure 55: Usage of tactics and user passes ............................................ 65
Figure 56: Bart refinement result formatting ........................................... 68
Figure 57: Refinement result formatting example .................................... 68
Figure 58: Operations to implement for splitting example ......................... 70
Figure 59: Result machines for splitting example .................................... 70
Figure 60: Splitting process example ..................................................... 71
Figure 61: Splitting deadlock example .................................................. 71
# Appendix B - Syntax Elements Table

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Syntax 1</td>
<td>Predicate theory</td>
<td>22</td>
</tr>
<tr>
<td>Syntax 2</td>
<td>Rule files</td>
<td>26</td>
</tr>
<tr>
<td>Syntax 3</td>
<td>Variable rule theories</td>
<td>28</td>
</tr>
<tr>
<td>Syntax 4</td>
<td>Operation rule theories</td>
<td>36</td>
</tr>
<tr>
<td>Syntax 5</td>
<td>Type iteration</td>
<td>44</td>
</tr>
<tr>
<td>Syntax 6</td>
<td>Invariant iteration syntax</td>
<td>46</td>
</tr>
<tr>
<td>Syntax 7</td>
<td>Concrete iteration</td>
<td>48</td>
</tr>
<tr>
<td>Syntax 8</td>
<td>Seen operation</td>
<td>49</td>
</tr>
<tr>
<td>Syntax 9</td>
<td>Imported operation</td>
<td>50</td>
</tr>
<tr>
<td>Syntax 10</td>
<td>Implement</td>
<td>53</td>
</tr>
<tr>
<td>Syntax 11</td>
<td>LH</td>
<td>54</td>
</tr>
<tr>
<td>Syntax 12</td>
<td>Structure theories</td>
<td>57</td>
</tr>
<tr>
<td>Syntax 13</td>
<td>Initialisation theories</td>
<td>60</td>
</tr>
<tr>
<td>Syntax 14</td>
<td>User pass theory</td>
<td>63</td>
</tr>
<tr>
<td>Syntax 15</td>
<td>Tactic theory</td>
<td>64</td>
</tr>
</tbody>
</table>
XIII APPENDIX C — RULE FILES COMPLETE SYNTAX

This section presents the complete Bart rule files syntax.

XIII.1 Rule files

RuleFile = [ Theory { "&" Theory } ].

Theory =
  VariableTheory
   | OperationTheory
   | StructureTheory
   | InitialisationTheory
   | UserPassTheory
   | TacticTheory
   | PredicateTheory
.

XIII.2 Variables refinement rules

VariableTheory =
  "THEORY_VARIABLE" ident
  "IS"
     VariableRule { ":;" VariableRule } 
  "END" ident
.

VariableRule =
  "RULE" ident
  [ "(" JokerList ")" ]
  "VARIBLE" JokerList
  [ "TYPE" ident "(" JokerList ")" ]
  [ "WHEN" Predicate ]
  "IMPORT TYPE" Predicate
  (VariableImplementation | VariablesRefinement )
  "END"
.

VariableImplementation =
  "CONCRETE VARIABLES" JokerList
  [ "DECLARATION" Predicate ]
  "INVARIANT" Predicate
.

VariablesRefinement =
  "REFINEMENT VARIABLES"
     VariableRefinement { ":;" VariableRefinement } 
  "GLUING_INVARIANT" Predicate
VariableRefinement =
  "CONCRETE_VARIABLE" joker
  "WITH_INV" Predicate
  "END"
| "ABSTRACT_VARIABLE" joker
  "REFINED_BY" ident ":" ident "(" Expression ")"
  "WITH_INV" Predicate
  "END"
.

XIII.3 Initialisation refinement rules

InitialisationTheory =
  "THEORY_INITIALISATION" ident
  "IS"
  InitialisationRule { ";" InitialisationRule } 
  "END" ident
.

InitialisationRule =
  "RULE" ident
  "REFINES" Substitution
  [ "WHEN" Predicate ]
  "IMPLEMENTATION" Substitution
  "END"
.

XIII.4 Operation refinement rules

OperationTheory =
  "THEORY_OPERATION" ident
  "IS"
  OperationRule { ";" OperationRule } 
  "END" ident
.

OperationRule =
  "RULE" ident
  "REFINES" Substitution
  [ "WHEN" Predicate ]
  [ "SUB_REFINEMENT" SubRefinementRule { "," SubRefinementRule } ]
  ( "REFINEMENT" | "IMPLEMENTATION" )
  { RefinementVarDecl }
  Substitution
  ["IMPLEMENT" IdentOrJokerList ]
  "END"
.

RefinementVarDecl =

Version: 1.0
("VARIABLE" | "ABSTRACT_VARIABLE" | "CONCRETE_VARIABLE") joker
[ "REFINED_BY" ident "(" Expression ")" ]
"WITH_INV" Predicate
"WITH_INIT" Substitution
"IN" .

SubRefinementRule =
"(" Substitution ")" ".->" "(" Substitution ")"
.

XIII.5 Structural refinement rules

StructureTheory
= "THEORY_STRUCTURE" ident
"IS"
  OperationRule { ";" OperationRule }
"END" ident .

XIII.6 User pass theory

UserPassTheory
= "USER_PASS" "IS"
[ ("VARIABLE"|"OPERATION"|"INITIALISATION") ":" "(" IdentList ")" ]
{ ";" ("VARIABLE"|"OPERATION"|"INITIALISATION") ":" "(" IdentList ")" } 
"END" .

XIII.7 Tactic theory

TacticTheory
= "THEORY" "TACTICS" "IS"
{ Tactic }
"END" .

Tactic = "VARIABLE" "::" VariableTactic { ";" VariableTactic }
| "INITIALISATION" "::" SubstitutionTactic { ";" SubstitutionTactic }
| "OPERATION" "::" SubstitutionTactic { ";" SubstitutionTactic }
|

SubstitutionTactic =
IdentList ".->" "(" Substitution ")"
.

VariableTactic =
IdentList ".->" "(" Predicate ")"
XIII.8 Predicate synonyms theory

PredicateTheory =
   "THEORY_PREDICATES"
   "IS"
   PredicateDefinition { "|" PredicateDefinition } "END".

PredicateDefinition =
   ident "(" JokerList ")" "<=>" Predicate.

XIII.9 Substitutions

Substitution = SimpleSubstitution { ("||"|";") SimpleSubstitution }. 

SimpleSubstitution =
   "skip"
   | "BEGIN" Substitution "END"
   | "PRE" Predicate "THEN" Substitution "END"
   | "ASSERT" Predicate "THEN" Substitution "END"
   | "CHOICE" Substitution { "OR" Substitution } "END"
   | "IF" Predicate "THEN" Substitution { "ELSIIF" Predicate "THEN" Substitution } [ "ELSE" Substitution ] "END"
   | "SELECT" SelectContent [ "ELSE" Substitution ] "END"
   | "CASE" Expression "OF"
   | "EITHER" PrimaryExpression "THEN" Substitution { "OR" PrimaryExpression "THEN" Substitution } [ "ELSE" Substitution ] "END"
   | "ANY" IdentOrJokerList "WHERE" Predicate "THEN" Substitution "END"
   | "LET" IdentOrJokerList "BE" Predicate "IN" Substitution
"END" | "VAR" IdentOrJokerList
"IN" Substitution
"END"
| "WHILE" Predicate
"DO" Substitution
"INARIANT" Predicate
"VARIANT" Expression
"END"
| "LH" Predicate
"THEN" Substitution
"END"
joker
ident
AffectSubstitution
Iteration
ImportedOperation
ImplementSubstitution
.

SelectContent =
Predicate
"THEN" Substitution
{ "WHEN" Predicate
"THEN" Substitution }
.

ImplementSubstitution = "IMPLEMENT" "(" Substitution ").".

ImportedOperation =
"IMPORTED_OPERATION" "(" [ "name" => "ident ", " ]
"out" => "(" [ IdentJokerVardeclList ] ")" ",",
"in" => "(" [ IdentJokerVardeclList ] ")" ",",
"pre" => "(" Predicate ")" ",",
"body" => "(" Substitution ")" ")"
| "SEEN_OPERATION" "(" [ "name" => "IdentOrJoker ", " ]
"out" => "(" [ IdentJokerVardeclList ] ")" ",",
"in" => "(" [ IdentJokerVardeclList ] ")" ",",
"body" => "(" Substitution ")" ")"
).

Iteration =
"INARIANT ITERATION" "(" [ ("tant_que" | "while") =>" IdentOrJokerOrVarDecl ",," ]
"1st" "index" =>" BinaryExpression115 ",,
"2nd" "index" =>" BinaryExpression115 ",,
"constant" =>" BinaryExpression115 ",,
"1st" "type" =>" BinaryExpression115 ",,
"2nd" "type" =>" BinaryExpression115 ",,
"body" => "(" Substitution ")" ",,
"invariant" => "(" Predicate ")" ")"
| "TYPE ITERATION" "(" [ ("tant_que" | "while") =>" IdentOrJokerOrVarDecl ",," ]
"index" "=>" BinaryExpression115 ","
"type" "=>" BinaryExpression115 ","
"body" "=>" "(" Substitution ")" ","
"invariant" "=>" Predicate ")."

| "CONCRETE ITERATION" "(" 
| "init while" "=>" "(" Substitution<out Substitution init> ")" ","
| ("tant_que"|"while") "=>" BinaryExpression115<out Expression e=> ","
| "body" "=>" "(" Substitution<out Substitution body> ")" ","
| "invariant" "=>" "(" Predicate<out Predicate invariant> ")" ","
| "variant" "=>" BinaryExpression115<out Expression variant> ","
| "flag" "=>" IdentOrJoker<out Expression flag> ")")."

AffectSubstitution
=
IdentJokerVardeclList
( ":=" "(" Predicate ")"
| ":=" Expression
| [ "(" Expression ")" ]
":=" Expression
| ":=" IdentOrJoker [ "(" Expression ")" ]
).

XIII.10 Predicates

Predicate = ConjunctionPredicates { "=>" ConjunctionPredicates }.

ConjunctionPredicates
=
EquivalencePredicate { ("&"|"or"|"cand") EquivalencePredicate }
.

EquivalencePredicate = SimplePredicate { "<=>" SimplePredicate }.

SimplePredicate
=
(" Predicate ")
| "bnot" "(" Predicate ")"
| joker
| ident "(" Expression ")"
| Expression ComparisonOperator Expression
| "not" "(" Predicate ")"
| ("!"|"#") QuantifiedList "." "(" Predicate ")"
.

ComparisonOperator
=
"="|" /="|" :="|" /:"|" :<="|" <<="|" /=:"|" /<<="|" :<="|" <=="|" =>="|" >="|" <"
XIII.11 Expressions

Expression = BinaryExpression20.

// Expression that can occur between operators of priority 20
BinaryExpression20 = BinaryExpression115 { "," BinaryExpression115 }.

// Expression that can occur between operators of priority 115
BinaryExpression115 =
  Operator115 BinaryExpression115
  .

Operator115 = "<->"|"+-"|"+->>"|"+-<"|"+-<>"|"+-++"|"+-+++"|"+->>="|"+->><"|"+->>-".

// Expression that can be located between operators of priority 125
BinaryExpression125 =
  BinaryExpression160 { Operator125 BinaryExpression160 }.

Operator125 =
  "<->"|"><"|"><"|">>"|"><"|"\"|"/"|"-"|"-"|"-"|"<"|">"|">"|">"|">"|">"|"-".

// Expression that can occur between operators of priority 160
BinaryExpression160 =
  BinaryExpression170 { "." BinaryExpression170 }.

BinaryExpression170 =
  BinaryExpression180 { "+"|"-") BinaryExpression180 }.

BinaryExpression180 =
  BinaryExpression190 { "+"|"-"|"mod") BinaryExpression190 }.

BinaryExpression190 =
  Expression200 { **" Expression200 }.

Expression200 =
  Expression210 |
  "." Expression210.

Expression210 =
  PrimaryExpression
  { "~" |
    ("[" Expression "]) |
    ("(" Expression ")) |
  }.
PrimaryExpression =
  ident | number | joker | vardecl |
        "{ " Expression { ";" | "||" } Expression } "|
        "MAXINT" |
        "MININT" |
        "{" |
        FuncOperator "(" Expression ")" |
        "{" Expression [ "|" Predicate ] "}" |
        "(" Expression ")" |
        "TRUE" |
        "FALSE" |
        "bool" "(" Predicate ")" |
        "%" QuantifiedList "." "(" Predicate "|" Expression ")" |

QuantifiedList =
  IdentOrJokerList |
        "{ " IdentOrJokerList "}" |

FuncOperator =
  "max" | "min" | "card" | "dom" | "ran" | "POW" | "POW1" | "FIN" | "FIN1" | "union" | "inter" |

XIII.12 Diverse

JokerList = joker { "," joker }.

IdentOrJokerList = IdentOrJoker { "," IdentOrJoker }.

IdentOrJoker = ident | joker.

IdentJokerVardeclList =
  IdentOrJokerVardecl { "," IdentOrJokerVardecl } |

IdentOrJokerVardecl = ident | joker | vardecl.

IdentList = ident { "," ident }. 