Software Analyzers

# WP (Draft Manual)

# WP Plug-in (Draft) Manual

Frama-C Carbon 20110201

Loïc Correnson, Zaynah Dargaye, Anne Pacalet

CEA LIST, Software Reliability Laboratory

This work has been supported by the 'U3CAT' ANR project.

# Contents

# Chapter 1

# Introduction

We present here a plug-in of Frama-C for proving ACSL annotations of C function thanks to automated theorem provers.

The WP plug-in is named after *Weakest Precondition* calculus, a technique for proving program properties initiated by Hoare [Hoa69], Floyd [Flo67] and Dijkstra [Dij68]. Recent tools implement this thechnique with great performances, for instance Boogie [Lei08] and Why [Fil03]. There is already a Frama-C plug-in, Jessie [MM09], developped at INRIA, that implements a weakest precondition calculus for C programs thanks to a compilation to the Why platform.

The WP plug-in is a novel implementation of such a *Weakest Precondition* calculus for annotated C programs, which focus on parametrization *w.r.t* memory model. It is a completary work to Jessie plug-in, which relies on a separation memory model in the spirit of Burstall's one [Bur72]. The Jessie memory model is very efficient for a large variety of well structured C-programs. However, it does not apply when low-level memory manipulations are involved, such as heterogeneous casts. Moreover, Jessie operates by translating the C program to Why, a solution that prevents the user from combining *weakest precondition calculs* with other techniques, such as the Value analysis plug-in.

The WP plug-in has been designed with cooperation in mind. That is, you may use WP for proving some annotations of your C programs, and prove other ones with other plug-ins. The recent improvements of Frama-C kernel are then responsible for managing such partial proofs and consolidate them altogether.

This manual is divided into four parts. This first chapter introduces the WP plug-in, *Weakest Precondition* calculus and *Memory Models*. Then, chapter 2 details how to use and tune the plug-in within the Frama-C platform. Chapter 3 specifies the internal calculus of WP and Chapter 4 provides a specification for the available memory models.

## 1.1 Tutorial

The WP plug-in is distributed with the Frama-C platform. However, you must install some external provers in order to fulfill proof obligations. You have several choices, see section 2.2.4 for details. To starts with, you may install the Alt-Ergo [CCK06] prover. You can install it from source at `http://alt-ergo.lri.fr` or with `Godi`.

Consider new the very simple example of a function that swaps the values of two integers passed by reference:

File **swap.c**

```
void swap(int *a,int *b)
{
  int tmp = *a ;
  *a = *b ;
  *b = tmp ;
  return ;
}
```

A simple, although incomplete, ACSL contract for this function can be:

File **swap1.c**

```
/*@ ensures A: *a == \old(*b) ;
  @ ensures B: *b == \old(*a) ;
  @*/
void swap(int *a,int *b) ;
```

You can run wp on this example with:

```
# frama-c -wp -wp-proof alt-ergo swap.c swap1.c
[kernel] preprocessing with "gcc -C -E -I.  swap.c"
[kernel] preprocessing with "gcc -C -E -I.  swap1.c"
[wp] warning: Missing RTE guards
[wp] [Alt-Ergo] Goal store_swap_post_2_B : Valid
[wp] [Alt-Ergo] Goal store_swap_post_1_A : Valid
```

As expected, Alt-Ergo discharged the two proof obligations generated by WP for the contract of `swap`. You should notice the warning “Missing RTE guards”, emitted by the WP plug-in. That is, the *weakest precondition calculus* implemented in WP relies on the hypothesis that your program is runtime-error free. In this example, the `swap` function dereferences its two parameters, and these two pointers should be valid.

The WP plug-in does not generate proof obligation to prevent your program from raising a runtime error, because this property may be validated with any other technique, for instance by running the *value analysis* plug-in or the *rte generation* one.

Hence, consider the following new contract for `swap`:

File **swap2.c**

```
/*@ requires \valid(a) && \valid(b);
  @ ensures A: *a == \old(*b) ;
  @ ensures B: *b == \old(*a) ;
  @ assigns *a,*b ;
  @*/
void swap(int *a,int *b) ;
```

For simplicity of use, the WP plug-in is able to run the *rte generation* plug-in for you. Now, WP reports that the function swap fulfills its contract:

```
# frama-c -wp -wp-rte -wp-proof alt-ergo swap.c swap2.c
[kernel] preprocessing with "gcc -C -E -I.  swap.c"
[kernel] preprocessing with "gcc -C -E -I.  swap2.c"
```

```
[rte] annotating function swap
[wp] [WP:simplified] Goal store_swap_function_assigns : Valid
[wp] [Alt-Ergo] Goal store_swap_assert_4_rte : Valid
[wp] [Alt-Ergo] Goal store_swap_assert_3_rte : Valid
[wp] [Alt-Ergo] Goal store_swap_assert_2_rte : Valid
[wp] [Alt-Ergo] Goal store_swap_assert_1_rte : Valid
[wp] [Alt-Ergo] Goal store_swap_post_2_B : Valid
[wp] [Alt-Ergo] Goal store_swap_post_1_A : Valid
```

We have finished the job for validating this simple C program with respect to its specification, as reported by the *report* plug-in that displays a consolidation status of all annotations:

```
# frama-c -wp-verbose 0 [...] -then -report
[kernel] preprocessing with "gcc -C -E -I.  swap.c"
[kernel] preprocessing with "gcc -C -E -I.  swap2.c"
[rte] annotating function swap
[report] Computing properties status...
--------------------------------------------------------------
   Properties for Function 'swap'
--------------------------------------------------------------

[  Valid  ] Function 'swap' ensures A: (*\at(a,Old) == \old(*b))
[  Valid  ] Function 'swap' ensures B: (*\at(b,Old) == \old(*a))
[  Valid  ] Function 'swap' assigns *a, *b;
[  Valid  ] Function 'swap' assert rte: \valid(a);
[  Valid  ] Function 'swap' assert rte: \valid(a);
[  Valid  ] Function 'swap' assert rte: \valid(b);
[  Valid  ] Function 'swap' assert rte: \valid(b);

--------------------------------------------------------------
  No proofs       :    0
  Partial proofs  :    0
  Complete proofs :    7
  Total           :    7
--------------------------------------------------------------
```

## 1.2 Weakest Preconditions

The principles of *weakest precondition calculus* are quite simple in spirit. Given a code annotation of your program, say, an assertion $Q$ after a statement *stmt*, the weakest precondition of $P$ is by definition the "simplest" property $P$ that must be valid before *stmt* such that $Q$ holds after the execution of *stmt*.

**Hoare's triples.** In mathematical words, we denote such a property by a Hoare's triple:

$$\{P\}\, \mathit{stmt}\, \{Q\}$$

which reads: *"whenever $P$ holds, then after running stmt, $Q$ holds"*.

Thus, we can define the weakest precondition as a function *wp* over statements and properties such that the following Hoare triple always holds:

$$\{\mathit{wp}(\mathit{stmt}, Q)\} \quad \mathit{stmt} \quad \{Q\}$$

For instance, consider a simple assignment over an integer local variable $x$, we have:

$$\{x + 1 > 0\} \quad \mathtt{x} = \mathtt{x} + 1; \quad \{x > 0\}$$

It shall be intuitive that in this simple case, the *weakest precondition* for this assignment of a property $Q$ over $x$ can be obtained by replacing $x$ with $x + 1$ in $Q$. More generally, for any statement and any property, it is possible to define such a weakest precondition.

**Verification.** Consider now function contracts. We basically have *pre-conditions*, *assertions* and *post-conditions*. Say function $f$ have a precondition $P$ and a post condition $Q$, we now want to prove that $f$ satisfies its contract, which can be formalized by:

$$\{P\} \quad f \quad \{Q\}$$

Consider now $W = wp(f, Q)$, we have by definition of $wp$:

$$\{W\} \quad f \quad \{Q\}$$

Suppose now that we can *prove* that $P$ entails $W$, we can use the weakest precondition calculus intermediate result to prove the function contracts, which can be summarized by the following diagram:

$$\frac{(P \Longrightarrow W) \qquad \{W\}\,f\,\{Q\}}{\{P\}\,f\,\{Q\}}$$

This is the main idea of how to prove a property by weakest precondition. Consider an annotation $Q$, computes its weakest precondition $W$ across all the statements from $Q$ up to the beginning of the function. Then, submit the property $P \Longrightarrow Q$ to a theorem prover, where $P$ are the preconditions of the function. If this proof obligation is discharged, then one may conclude the annotation $Q$ is valid for all executions.

**Termination.** We must point out a detail about program termination. Strictly speaking, the *weakest precondition* of property $Q$ through statement *stmt* should also ensures termination and execution without runtime error.

The proof obligations generated by WP does not entails systematic termination, unless you systematically specify and validate loop variant ACSL annotations. Although, exit behaviors of a function are correctly handled by WP.

Regarding runtime errors, the proof obligations generated by WP does assume your program never raise some of them. Moreover, the only integer model currently implemented assumes no integer overflow at all (signed or unsigned). As illustrated in the short tutorial example of section 1.1, you should enforce the absence of runtime error by your own, for instance by running the *value analysis* plug-in or the *rte generation* one.

**Provers.** The WP plug-in computes the proof-obligations for post-conditions and assertions in C functions, and submit them to external provers.

You may discharge the generated proof obligation with automated decision procedures or interactive proof assistant. Technically, WP is interfaced with Alt-Ergo [CCK06], Coq [Coq10], and any decision procedures supported by Why [Fil03].

## 1.3 Memory Models

The essence of *weakest precondition calculus* is to translate code annotation into mathematical properties. Consider the simple case of an annotation referring to a non-pointer C-variable `x`:

```
x = x+1;
//@ assert P: x >= 0 ;
```

We can translate $P$ into the mathematical property $P(X) = X \geq 0$, where $X$ stands for the value of variable `x` at the appropriate program point. In this simple case, the effect of statement `x=x+1` over $P$ is actually the substitution $X \mapsto X + 1$, that is $X + 1 \geq 0$.

The problem when applying *weakest precondition calculus* to C programs is to deal with *pointers*. Consider now:

```
p = &x ;
x = x+1;
//@ assert Q: *p >= 0 ;
```

It is clear that, taking into account the aliasing between `*p` and `x`, the effect of the increment of `x` can not be translated by a simple substitution of $X$ in $Q$.

This is where *memory models* comes to rescue.

A memory models defines how to map values inside the C memory heap to mathematical terms. The WP has been designed to support different memory models. There are currently three memory models implemented, and we plan to implement new ones for future releases. Those three models are all different from the one of Jessie plug-in, which makes WP complementary.

`Hoare` **model.** A very efficient model that generates concise proof obligations. It simply maps C variable to a pure logic variable.

However, the heap can not be represented in this model, and expressions such as `*p` can not be translated at all. You can still represent pointer values, but you can not read or write the heap through pointers.

`Store` **model.** The default model for WP plug-in. Heap values are stored in a global array. Pointer values are translated to an index into this array.

In order to generate reasonable proof obligations, the values stored in the global array are not the machine-ones, but the logic ones. Hence, all C integer types are represented by mathematical integers.

A consequence is that heterogeneous cast of pointers can not be translated with this model. For instance, you can not cast a pointer to `int` into a pointer to `char`, and then access the internal representation of an `int` value in memory.

`Runtime` **model.** This is a low-level memory model, where the heap is represented as a wide array of bits. Pointer values are exactly translated into memory addresses. Read and write operations with the heap are translated into manipulation of a range of bits in the heap.

This model is very *precise* in the sense that all the details of the program are represented. But at the cost of huge proof obligations that are very difficult to discharge by automated provers, and you generally need an interactive proof assistant.

Thus, each *memory model* offers a different trade-off between expressive power and facility of discharging proof obligations. The `Hoare` memory model is very restricted but easy, `Runtime` is very expressive but very difficult, and `Store` offers an intermediate solution.

Chapter 2

# Using WP Plug-in

The WP plug-in can be used used from the command line of Frama-C or within its graphical user interface. It is a dynamically loaded plug-in distributed with the kernel since the Carbon release of Frama-C.

This plug-in computes proof obligations of ACSL annotations by *weakest precondition calculus*, using a parametrized memory model to represent pointers and heap values. The proof obligations may then be discharged by external decision procedures, which range over automated theorem provers such as Alt-Ergo [CCK06] or interactive proof assistant like Coq [Coq10].

This chapter describes how to use the plug-in, from the Frama-C graphical user interface (section 2.1), from the command line (section 2.2), or from another plug-in (section 2.3). Additionally, combining the WP plug-in with load and save commands of Frama-C and/or the `-then` command-line option is explained in section 2.4.

## 2.1 Graphical User Interface

To use WP under the GUI, you simply need to run Frama-C graphical user interface. No additional option is required, although you can preselect some WP options described in section 2.2:

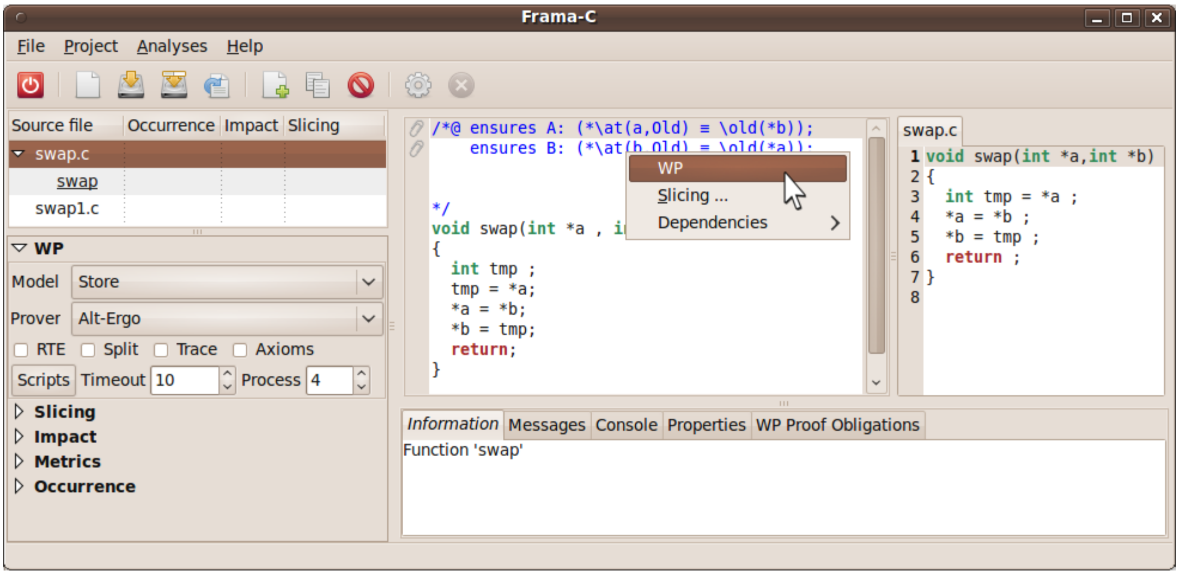
```
$ frama-c-gui [options...] *.c
```

As we can see in figure 2.1, the memory model, the decision procedure, and some WP options can be tuned from the WP side panel. Others options of the WP are still modifiable from the `Properties` button in the main GUI toolbar.

To prove a property, just select it in the internal source view and chose WP from the contextual menu. The `Console` window outputs some information about the computation. Figure 2.2 displays an example of such a session.

If everything succeeds, a green ✓ should be displayed on the left of the property. The computation can also be run for a bundle of properties if the contextual menu is open from a function or behavior selection.

The options from the WP side panel correspond to some options of the plug-in command-line. Please refer to section 2.2 for more details. In the graphical user interface, there are also specific panels that display more details related to WP, that we shortly describe below.


Frama-C
File Project Analyses Help
Source file Occurrence Impact Slicing
swap.c
swap
swap1.c
WP
Slicing ...
Dependencies
Slicing
Impact
Metrics
Occurrence
Information Messages Console Properties WP Proof Obligations

WP

Model Store

Prover Alt-Ergo

□ RTE □ Split □ Trace □ Axioms

Scripts Timeout 10 Process 4

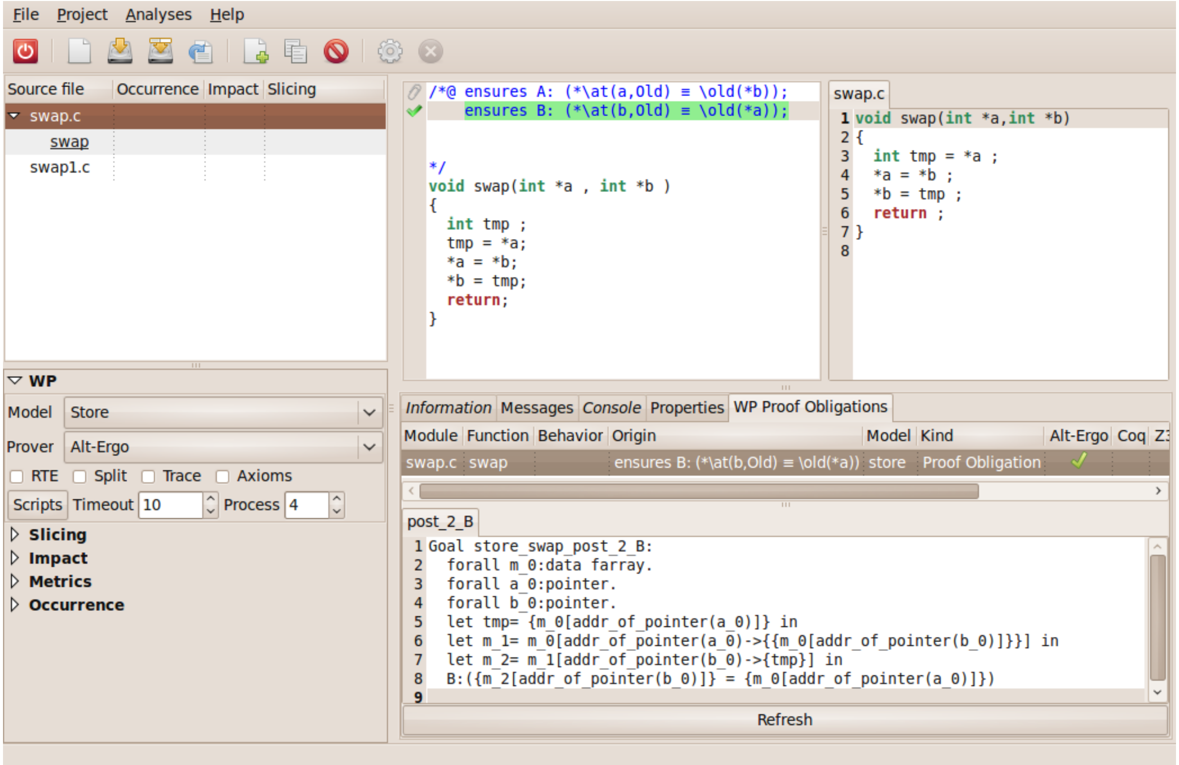
```
/*@ ensures A: (*\at(a,Old) ≡ \old(*b));
    ensures B: (*\at(b,Old) ≡ \old(*a));

*/
void swap(int *a , int *b )
{
  int tmp ;
  tmp = *a;
  *a = *b;
  *b = tmp;
  return;
}
```

swap.c

```
void swap(int *a,int *b)
{
  int tmp = *a ;
  *a = *b ;
  *b = tmp ;
  return ;
}
```

Function 'swap'

Figure 2.1: WP in the Frama-C GUI


File Project Analyses Help
Source file Occurrence Impact Slicing
swap.c
swap
swap1.c
WP
Slicing
Impact
Metrics
Occurrence
Information Messages Console Properties WP Proof Obligations
post_2_B
Refresh

```
/*@ ensures A: (*\at(a,Old) ≡ \old(*b));
    ensures B: (*\at(b,Old) ≡ \old(*a));

*/
void swap(int *a , int *b )
{
  int tmp ;
  tmp = *a;
  *a = *b;
  *b = tmp;
  return;
}
```

swap.c

```
void swap(int *a,int *b)
{
  int tmp = *a ;
  *a = *b ;
  *b = tmp ;
  return ;
}
```

WP

Model Store

Prover Alt-Ergo

□ RTE □ Split □ Trace □ Axioms

Scripts Timeout 10 Process 4

| Module | Function | Behavior | Origin | Model | Kind | Alt-Ergo | Coq | Z3 |
|---|---|---|---|---|---|---|---|---|
| swap.c | swap |  | ensures B: (*\at(b,Old) ≡ \old(*a)) | store | Proof Obligation | ✓ |  |  |

```
Goal store_swap_post_2_B:
  forall m_0:data farray.
  forall a_0:pointer.
  forall b_0:pointer.
  let tmp= {m_0[addr_of_pointer(a_0)]} in
  let m_1= m_0[addr_of_pointer(a_0)->{{m_0[addr_of_pointer(b_0)]}}] in
  let m_2= m_1[addr_of_pointer(b_0)->{tmp}] in
  B:({m_2[addr_of_pointer(b_0)]} = {m_0[addr_of_pointer(a_0)]})
```

Figure 2.2: WP run from the GUI

**Source Panel.** On the center of Frama-C window, the status of each code annotation is reported in the left-margin. The meaning of icons is the same of all plug-ins in Frama-C:

| **Icons for properties:** | |
|---|---|
| 📎 | No proof attempted. |
| ? | The property has not been validated. |
| ⇆ | The property is *valid* but has dependencies. |
| ✓ | The property and *all* its dependencies are *valid*. |

**Properties Panel.** This panel summarizes the consolidated status of properties, from various plug-ins. The property status is indicated by two codes: a colored-bullet indicating whether this property has been proved or not; and a background color indicating whether this proof depends on proved properties or not. The color codes are:

| **Icons for status:** | |
|---|---|
| 🟧ⓘ | The property has not been validated. |
| 🟧🔴 | The property is *invalid*. |
| 🟧🟢 | The property is *valid* with dependencies. |
| 🟩🟢 | The property and *all* its dependencies are *valid*. |

This panel is not automatically refreshed. You should press the `Refresh` button to update it. Actually, computing a consolidated status requires to navigate over the properties dependency graph, which may take a noticeable amount of time.

**Property Dependency Graph.** By double-clicking on the status column of a property in the properties panel, you can display a dependency graph for this property. The graph displays the property, its status, which plug-in has participated in the proof, and on which properties the proof directly depends on.

**Proof Obligations Panel.** This panel is dedicated to WP plug-in. It shows the generated proof obligations and their status for each prover. By clicking on a prover column, you can also submit a proof obligation to a prover by hand. By double-clicking an annotation, you can view its mathematical definition in a human readable fashion.

## 2.2 Command Line Options

The best way to know the available options is to use:

```
# frama-c -wp-help
```

The WP plug-in generally operates into three steps:

1. Annotations are selected to produce a control-flow graph of elementary statements annotated with hypothesis and goals.

2. Weakest preconditions are computed for all selected goals in the control-flow graph. Proof obligations are emitted and saved on disk.

3. Decision procedures (provers) are run to discharged proof obligations.

The WP options allow to refine each step of this process. It is very convenient to use WP together with the standard `-then` option of Frama-C, in order to operate successive pass of the process. See section for details.

### 2.2.1 Goal Selection

This group of options allow to refine the selection of annotations for which proof obligations are generated. By default, all annotations are selected. By default, a property which is already proved – by WP or any other plug-in – does not lead to any proof-obligation generation.

`-wp` generates proof obligations for all (selected) properties.

`-wp-fct <f1,...,fn>` selects annotations of functions f1,...,fn (defaults to all functions).

`-wp-bhv <b1,...,bn>` selects annotation for behaviors b1,...bn (defaults to all behaviors).

`-wp-prop <p>` selects properties with name p. (defaults to all properties). You may also type "`assigns`" for all assigns properties.

`-wp-(no)-status-valid` includes in the goal selection those properties for which the current status is already 'valid' (default is: `no`).

`-wp-(no)-status-invalid` includes in the goal selection those properties for which the current status is already 'invalid' (default is: `no`).

`-wp-(no)-status-maybe` includes in the goal selection those properties with an undetermined status (default is: `yes`).

**Remark:** options `-wp-status-xxx` are not taken into account when selectioning a property by its name or from the Gui.

### 2.2.2 Model Selection

These options modify the underlying memory model that is used for computing weakest preconditions.

`-wp-model <m>` set the memory model among `Hoare`, `Store` or `Runtime`. For more information about the models and how to chose it, see section 1.3 and chapter 4.

`-wp-(no)-logicvar` (deactivates) optimization for variables whose address is never taken, for which WP uses Hoare model. See chapter 4 for details.

`-wp-assigns <m>` sets the method for proving assigns clause. Possible methods are:

- `effect:` Each statement with side-effect produces one sub-goal. The locations writen by each statement are checked to be included in the assigns clause. This is a stronger result than required, but the proof obligations are generally simple and sufficient in practice.
- `memory:` use the ACSL definition of assigns clause, where memory states are compared before and after the considered block. Generates much more complex proof obligations than `effect`.
- `none:` skip proof of assigns clause.

### 2.2.3 Computation Strategy

These options modifies the way proof obligations are generated during weakest precondition calculus.

`-wp-axioms` (*experimental*) instantiates user-defined lemmas and axioms with memory-labels.

`-wp-huge <s>` cut off proof terms with size exceeding $2^s$ (default: $2^{30}$). The size of a term is linearly related to its size on the disk, and to the size of proof obligation sent to decision procedures.

`-wp-norm <m>` sets the normalization method applied to let-bindings in obligations generated for Alt-Ergo and Coq:

`Exp:` let-bindings are expanded (default for Alt-Ergo).

`Let:` let-bindings are preserved (default for Coq).

`Eqs:` let-bindings are replaced by equalities over universally-quantified fresh variables.

`Cc:` let-bindings are replaced by function call or predicates by closure conversion.

`-wp-rte` generates RTE guards before computing weakest preconditions. This options call the *rte generation* plug-in with the following options: `-rte-mem`, `-rte-div`, `-rte-signed` and `-rte-unsigned-ov`. The generated guards, when proved[1], fulfill the requirements for using WP plug-in.

`-wp-(no)-simpl` (deactivates) simplification of constant expressions and tautologies.

`-wp-split` conjunctions in generated proof obligations are recursively split into sub-goals. The generated goal names are suffixed by "`part`*n*". Notice that this option is set by default for assigns clause with `effect` assigns method (see `-wp-assigns` above).

`-wp-split-dim <d>` limits the number of generated sub-goals for assigns goals and when using `-wp-split`. The number of generated sub-goals would not exceed $2^{\mathsf{d}}$ proof obligations. Default is $2^{\mathsf{6}}$.

### 2.2.4 Decision Procedures Interface

When `-wp-proof` option is selected, proof obligations are sent to a decision procedure. If proof obligations have just been generated, by using `-wp`, `-wp-fct`, `-wp-bhv` or `-wp-prop` options, then only the new proof obligations are sent. Otherwise, all proof obligations not yet proved are sent.

`-wp-check <dp>` only checks syntax of generated proof obligations for a family of decision procedures. Possible values of `dp` are: `alt-ergo`, `coq` and `why`.

`-wp-par <n>` limits the number of parallel process runs for decision procedures. Defaults is 4 processes. With `-wp-par 1`, the order of logged results is fixed. With more processes, the order is runtime dependent.

`-wp-proof <dp>` selects the decision procedure used to discharge proof obligations. See below for supported provers.

[1] It is still correct to prove these RTE annotations with WP

`-wp-timeout <n>` set the timeout (in seconds) for the calls to the decision prover (defaults to 10 seconds).

`-wp-trace` keep user labels in generated proof obligations. This option can be useful for tracing where the proof obligation comes from, especially when using `-wp-split` option or interactive proof assistants.

**Alt-Ergo** Direct support for the Alt-Ergo prover is provided. You should use version 0.92.2 of the prover to benefit from its build-in array theory.

`-wp-proof alt-ergo`

`-wp-(no)-arrays` (deactivates) usage of built-in array theory of Alt-Ergo.

**Coq.** Direct support for the Coq proof assistant is provided. The generated proof obligations are valid for Coq version 8.3 but should work also with prior versions of the proof assistant. When working with Coq, you will enter interactive session, then save the proof scripts in order to replay them in batch mode.

**-wp-script <f.script>** specify the file from which proof scripts are retrieved, or saved in. The format of this file is private to WP plug-in. However, it is a regular text file from which you can cut and paste part of previously writen script proofs. The WP plug-in manages the content of this file for you.

**-wp-proof coq** only run `coqc` of proof scripts found in the script file. If the generated goal (or the default one) is not correctly typed-checked by `coqc`, the `coq` prover fails to discharge the proof obligation.

**-wp-proof coqide** first try to replay some known proof script (if any). If it does not succeed, then a new interactive session for `coqide` is opened. During interactive session with Coq's IDE, several files are opened for you:

`<goal>.v` the proof obligation to discharge.

`<model>_env<n>.v` the environment generated during weakest precondition calculus (already compiled by `coqc`): type definitions, global variables, etc.

`<model>_model.v` the definitions and properties of the memory model used (already compiled by `coqc`).

`f.script` the script file where all your proofs are stored. This is useful for reusing parts from previous scripts on similar goals.

As soon as `coqide` exits, the edited proof script is saved back in the script file, and finally checked by `coqc`. Do not forget to save your proof before exiting `coqide`.

**Why.** Finally, a wide range of automated provers are supported by WP thanks to the Why 2.27 prover interface. Both the `why` translation tool and the `why-dp` utility are required. You also need to install external provers by your own. Currently, the prover you can use with WP and Why, and the corresponding values for the `-wp-proof` option, are: `simplify`, `yices`, `cvc3`, `z3`, `zenon`.

### 2.2.5 Generated Proof Obligations

Your proof obligations are generated and saved into several text files. Those files are put in a temporary directory which is removed when Frama-C exists. Alternatively, you can specify a directory of your own where all these files are generated.

`-wp-print` pretty-prints the generated proof obligations on the standard output. Results obtained by provers are reported as well.

`-wp-warnings` display details when warnings are emitted during proof obligation generation.

`-wp-out <dir>` sets the user directory where proof obligations are saved. The directory is created if not exists. Its content is never cleaned up automatically.

`-wp-dot` generates also graphical representation of the CFG in the dot format used by the GraphViz tools[2].

The output directory will contains a lot of files. All files are generated with the following naming convention:

`<goal>_head.txt` a summary of the generated proof obligation. This file contains the warning emitted during weakest precondition calculus.

`<goal>_body.txt` a human-readable description of the proof obligation.

`<goal>_log.txt` a log from the last prover run on the goal.

`<goal>_ergo92.why` the goal generated for Alt-Ergo with arrays.

`<goal>_ergo91.why` the goal generated for Alt-Ergo without arrays.

`<goal>.v` the goal generated for Coq.

`<goal>.why` the goal generated for Why.

For each weakest precondition generation session, an environment describing the C definitions of your program is generated. These environment files are also saved on disk, and shared among different proof obligations:

`<env>.txt` a human-readable description of the environment.

`<env>_ergo92.why` the environment for Alt-Ergo with arrays.

`<env>_ergo91.why` the environment for Alt-Ergo without arrays.

`<env>.why` the environment for Why.

`<goal>.v` the environment for Coq.

`<goal>.why` the environment for Why.

[2] http://www.graphviz.org

Finally, definitions and properties of the memory model are distributed in the Frama-C `share/wp` directory with similar naming convention. Their Coq instances are copied on the temporary directory for separated compilation purpose.

For discharging one proof obligation, WP assemble a input for the external decision prover composed of three inputs: the resources for selected memory model, the resources from the environment of the goal, and the goal itself.

**Remark:** to save space on disk, when generating proof obligations from the command line, the proof obligations are only generated for the request prover format. This behavior is turned off under the Gui and in debug mode. Hence, you still get all formats available for all provers in these cases.

## 2.3 Plug-in Developer Interface

The WP plug-in have several entry points registered in the `Dynamic`[3] module of Frama-C:

`Wp.run` run weakest precondition calculus using the options to know what to compute. This is similar to using `-wp` on the command line;

`Wp.wp_compute kf_opt bhv_list_opt prop_opt` where:

- `kf_opt` is an optional kernel function;
- `bhv_list_opt` specify an optional behavior list;
- `prop_opt` specify an optional property;

These entry points actually run the WP plug-in in the same way as the command-line options do.

## 2.4 Plug-in Persistent Data

As a general observation, almost none of the internal WP data are kepts in memory after each plug-in execution. Most of the generated proof-obligation data are stored on disk before being send to provers, and they are stored in a temporary directory that is removed at Frama-C exit (see also `-wp-out` option).

The only informations which are added in the Frama-C kernel, consists of new status for those properties proved by WP with their dependencies.

**Warning:** the WP plug-in does not work – yet – with several Frama-C projects in the same run.

Thus, when combining WP with `-then`, `-save` and `-load` options, the user should be aware of the following precisions:

`-wp, -wp-prop, -wp-fct, -wp-bhv.` These options make the WP plug-in to generate proof-obligations for the selected properties. The value of theses option are never saved and they are cleared by `-then`. Hence, running `-wp-prop A`, *then* `-wp-fct F` does what you expect.

[3] See the *plug-in development guide*

`-wp-print, -wp-proof, -wp-check.` These options does not generate new proof-obligations, but run other actions on all previously generated ones. For the same reasons, they are not saved and cleared by `-then`.

`-wp-xxx.` All other options are tunings that can be easily turned on and off or set to the desired value. They are saved and kept across `-then` command.

# Chapter 3

# Weakest Preconditions Calculus

*For the beta-1 release of Carbon, the final version of this chapter is not yet available. Complete documentation will be available for final release of Carbon.*

# Chapter 4

# WP Models

Basically, a memory model is a set of operations and properties that are used to abstract the values that lives in the C heap during a program execution.

Each memory model defines its own representation of pointers, memory and data stored in the memory. The memory models defines also the types, functions and properties required to translate C programs and ACSL annotations into first order logic formulas.

One can wonder why we need to have several memory models in such a tool. The problem is that some models are simple because they consider a high level abstraction, but they are not handling all the C features ; others provide a very precise view of what is going on, but then the proof obligations can become huge and difficult to prove. Hence, each model implements a different trade off between precision and simplicity. A practical methodology is to use the simpler model whenever it is possible, and to go up with more complex models when needed on small parts of the code.

This chapter is dedicated to the description of memory models implemented in the WP plug-in. For the benefit of the clarity, we note $\mathcal{L}$ our logic language, into which we translated ACSL and C.

*For the beta-1 release of Carbon, the final version of this chapter is not yet available.*
*Complete documentation will be available for final release of Carbon.*

# Bibliography

[Bur72] R. M. Burstall. Some techniques for proving correctness of programs which alter data structures. *Machine Intelligence*, 1972.

[CCK06] Sylvain Conchon, Evelyne Contejean, and Johannes Kanig. Ergo : a theorem prover for polymorphic first-order logic modulo theories, 2006.

[Coq10] Coq Development Team. *The Coq Proof Assistant Reference Manual – Version V8.3*, 2010.

[Dij68] Edsger W. Dijkstra. A constructive approach to program correctness. *BIT Numerical Mathematics*, Springer, 1968.

[Fil03] J.-C. Filliâtre. Why: a multi-language multi-prover verification tool. Research Report 1366, LRI, Université Paris Sud, March 2003.

[Flo67] R. W. Floyd. Assigning meanings to programs. *Proceedings of the American Mathematical Society Symposia on Applied Mathematics*, 19, 1967.

[Hoa69] C. A. R. Hoare. An axiomatic basis for computer programming. *Communications of the ACM*, 1969.

[Lei08] K. Rustan M. Leino. *This is Boogie 2.* Microsoft Research, 2008.

[MM09] Yannick Moy and Claude Marché. *Jessie Plugin Tutorial,* Beryllium *version.* INRIA, 2009. http://www.frama-c.cea.fr/jessie.html.