# **Abstract**

Comparison of Why3/KeY/OpenJML to see how they compare in installation/setup/functionality/ease of use/tools/verification/results. Give a recommendation of the best tool going forward and reasons why.

* **Motivation:** Reviewing the popular current verification tools (Why3,KeY, Spec#) to determine their relevance and applicability against the new proposed standard tool of OpenJML (JML).
* **Goal:** Determine the most favourable verification tool for non-experts and provide an analysis of the current tools. (Pro’s/Cons) The companies do not communicate or collaborate with each other so a comparison between them could be of use to future students.
* **Result:** Recommendation of verification tool as well as a guide on how to use/setup all available tools.

# First-Order Logic

# First-Order Language

# SMT Provers

Goals ?

* Z3
* Alt-Ergo
* Coq
* CVC4
* CVC3

# Why3 (Why + WhyML)

**Installation:**

* **OS**: Ubuntu
* **Process:** [)](https://www.lri.fr/~marche/MPRI-2-36-1/install.html)
* **Review:** Installed Why3, Alt-Ergo, Z3 and Coq using above link with relative ease using the online instructions. Ubuntu version for Z3 was for 14.02 and I had to search for the 16.02 releases myself.

**References:**

1. *Deductive Program Verification with Why3 - A Tutorial; Jean-Christophe Filliatre; May 2016*
2. *Why3 – Where Programs meet Provers; Jean-Christophe Filliatre and* Andrei Paskevich,
3. *The Why3 Platform; Francois Bobot, Jean-Christophe Filliatre, Claude Marche, Guillaude Melquiond, Andrei Peskovich; January 2018*
4. *Lets Verify This with Why3; Francois Bobot, Jean-Christophe Filliatre, Claude Marche, Andrei Peskovich*
5. *The Krakatoa verification tool for Java Programs; Claude Marche; January 2018*

**Purpose:**

* A set of tools to perform deductive program verification.
* Deductive verification means that we express the correctness of a program as a mathematical statement and then we prove it. [1]
* Uses Why and Why3 together to form programs that can be verified using the standard weakest precondition calculus to extract conditions. (\*expand)
* VC Generator produces proof obligations that need to be discharged to prove that a program respects it specification [4]
* Automatically verifies that recursive definitions are terminating by using lexicographic order of arguments that guarantees a structural descent (Only supports algebraic types) [4]
* Non algebraic types have to axiomised or defined as programs where termination is proved by variants [4]
* Verification conditions are generated using a standard weakest-precondition procedure [4]
* All aliases must be known statically at the time of verification condition generation in order to apply the Hoare-style rule for assignment without the need for heap memory
  + Consequence is that recursive data types cannot have mutable components
* WhyML does not separate interface and implementation

**Uses**: [1]

1. Use only to verify programs using the theorem provers. (Logic only)
2. Verify algorithms/data structures through WhyML
3. Verify programs from a mainstream language eg Java, C, Ada

**Why:**

* Logic Language (used to specify programs, eg pre-post conditions, invariants)
  + First Order Logic
    - Polymorphism
    - Algebraic Data Types
    - Inductive Predicates

**WhyML:**

* Programming Language
  + First-Order ML-like language
    - Imperative features
    - Pattern matching
    - Exceptions

1. Types

* Categories
* Built-In Types (int, real and tuples)
* Algebraic Data Types (polymorphic lists , binary trees)

**type** map a’ b’

**type** i\_map ‘y = map int

* User-defined type (Can be non-interpreted or be a synonym for a type expression)

**type** list a’ = Nil | Cons a’ (list a’)

**type** tree a’ = Empty | Node (tree a’) a’ (tree a’)

* Record types (Special case of algebraic types with a single unnamed constructor and named fields)

**type** queue a’ = { front: list a’; rear: list a’ }

* Extension of pure types of the specification language
  + Mutable state of a computation is exclusively embodied in mutable fields of record data types

**type** ref a’ = { **mutable** contents: a’ }

* + A program type can be provided with an invariant

**type** array a’

**model** { length: int; **mutable** elts: map int a’ }

**invariant** { 0 <= **self**.length }

* ‘**model**’ makes the ‘**type** array a’’ an abstract data type
* ‘elts’ cannot be accessed from a program; accessed only from inside specifications
  + A record field (argument of a constructor in an algebraic type) can be declared ghost.

**type** sparse\_matrix \_ =

{ **ghost** view : map (int,int) \_; ... }

* Ghost data can only be used in specifications and cannot modify non-ghost code

1. Function/Predicate
   * + Every function or predicate symbol has a polymorphic type signature.[4]

**function** get (map a’ b’) a’ : b’

* + - Both can be given definitions, possible mutually recursive[4]

**predicate** increasing (m: map int int) = **forall** i j: int. i < j ! get m i < get m j

**function** height (t: tree \_): int = **match** t **with**

| Node l \_ r ! 1 + max (height l) (height r)

| Leaf ! 0

**end**

* Function Prototypes
  + Useful for providing a usable interface for ‘model’ types like array

**val** ([]) (a: array a’) (i: int) : a’

**requires** { 0 <= i < a.length }

**reads** { a }

**ensures** { **result** = get a.elts i }

**val** ([] <-) (a: array a’) (i: int) (v: a’) : unit

**requires** { 0 <= i < a.length }

**writes** { a }

**ensures** { a.elts = set (**old** a.elts) i v }

* + [] defines a[i]
  + []<- defines a[i] <- v
  + **‘reads’** and ‘**writes’** specify the side effects

1. Terms and Formulas

* First order language is extended (Terms and Formulas)
  + Pattern Matching
  + ‘let’ expressions
  + Conditional expressions (allowed in terms)

**function** abs (x: int) : int =

**if** x >= 0 **then** x **else** -x

1. Theories

* Collections of pure logical definitions
  + 1. Lemmas (Provable statements)
    2. Axioms (Definitions of function)
* ‘use’ keyword imports theory library

**use import** list.List

1. Design by Contract

* Usual DBC verification system is used in WhyML language
  + Ensures
  + Requires
  + Invariant
  + Variant (used to ensure termination in recursive functions and while loops)
  + Asserts (Statically checked)

1. Programs

* ML syntax

**function** (!) (x: ref a’) : a’ = x.contents

**let** (!) (r:ref a’) : a’

**ensures** { **result** = !r }

= r.contents

**let** (:=) (r:ref a’) (v:a’) : unit

**ensures** { !r = v }

= r.contents v

**let** incr (r: ref int) : unit

**ensures** { !r = **old** !r + 1 }

= r := !r + 1

* + **‘function (!)’** = pure access function with name ‘!’
  + **‘let (!)’** = program function with name ‘!’
  + **‘let (:=)’** = program function with name ‘**:=**’
  + **‘let (incr)’** = program function with name ‘incr’
  + **!r** = dereferencing a variable
    - **Note: ‘!r’** in the pre/postconditions can only refer to the pure function, **‘function’**, as program symbols cannot appear in specification
    - In the program code, **‘!r’** will refer to current WhyML function **‘let (…)’**
    - **‘r := !r + 1’** would have thrown an error in the last program function if it had not been redefined. Otherwise it would be trying to access the pure access function from program code, which is illegal.

1. Modules

* WhyML declarations and definitions are grouped into modules, like pure logical theories
* May import logical theories or contain pure declarations

1. Verification

**Command Line Operations:**

* why3 prove $User/test.mlw
  + Check the file for syntax and termination point.
  + Prints the contents to the terminal.
  + No proof attempt is made
  + Returns line and character numbers if an error is found, eg unable to prove a termination point
* why3 prove –P alt-ergo $User/test.mlw
  + Proof check the file
  + Each goal in the file is verified
  + Returns ‘Valid’ if verified
  + Returns ‘Unknown’ if a goal could not be proven
    - Induction will cause an Unknown error to be returned and requires the Coq proof assistant to do the proof, as SMT Solvers cannot verify it.
* why3 ide $User/test.mlw
  + - Launches IDE
    - Displays code for the file
    - Displays each goal to be verified
    - Allows selection of SMT Prover
    - Can perform translations of goals to assist with proofs, eg while using Coq
    - Code Extraction: a verified WhyML program can be translated to a compilable correct-by-construction OCaml program [4]

**Online Operations**

# Design by Contract

**References:**

1. *Applying “Design by Contract”, Bertrand Meyer, 1992*

**Brief:**

* Reduce the need for defensive programming, therefore reducing code size, complexity and the capability for introducing bugs
* If the contract is precise and explicit, there is no need for redundant checks [1]
* Assertions: Specify the relationship between the client (caller) and the supplier [1] (routine/method)
  + Pre-conditions
  + Post-conditions
  + Variants
  + Invariants (per routine/ per loop)
  + Class Invariants (cover all class routines)
  + Asserts
* Pre-condition (Requires)
  + Expresses requirements that any call must satisfy if it is to be correct [1]
  + Method/Routine cannot execute if precondition is not satisfied
  + The absence of a precondition is the same as the clause ‘Requires True’ which is the weakest possible precondition [1]
  + A pre-condition violation indicates a bug on the client’s (caller) side [1]
  + The stronger the pre-condition, the heavier the burden on the client [1]
  + “*As long as the conditions on the use of a routine make sense, and the routines documentation states these conditions explicitly, the programmers will be able to use the routine properly by observing their part of the deal*”
* Post-condition (Ensures)
  + Expresses properties that are ensured in return by the execution of the call [1]
  + The absence of a precondition is the same as the clause ‘Ensures True’ which is the weakest possible postcondition [1]
  + A post-condition violation indicates a bug on the supplier’s (method/routine) side
  + The stronger the post-condition, the heavier the burden on the supplier
* Class Invariants
  + A condition that must hold true before, during and after the execution of a routine from said class
  + “*The invariant must be preserved by every exported routine of the class. Any such routine must guarantee that the invariant is satisfied on exit if it was satisfied on entry*”
  + The invariant is added to the pre/post-conditions of every routine in the class
* Inheritance
  + All assertions from the base class are passed onto all derived classes
  + Derived classes can add in further assertions if required as long as they follow certain rules
    - Precondition cannot be strengthened
    - Postcondition cannot be weakened
    - Invariant cannot be strengthened
* Exception Handling (abnormal cases)
  + Failure
    - Execution of a routine cannot fulfil its contract (specification) [1]
  + Exception
    - Occurs when a certain strategy for fulfilling a routine’s contract has not succeeded

# JML

* Runtime Assertion Checking vs Static Checking

# Runtime Assertion Checking

**References**

1. Introduction to JML, David Cok, Joe Kiniry and Erok Poll, Tutorial Slides
2. Runtime assertion checking with JML, Erik Poll, Tutorial Slides

**Purpose**

* The main application of runtime assertion monitoring is debugging [1]
* Tests against what a developer thinks their software does versus what is actually does
  + Compile java file using jmlc to do JML runtime assertion checking (jmlc - a preproscessor for javac) [3]
  + Execute java file using jmlrac to perform runtime assertion checks (jmlrac - a wrapper for java) [3]
* jmlrac – test for violations of assertions during execution [2]
* jmlrac compiler created by Gary Leavens, Yoonsik Cheon, et al. translates JML assertions into runtime checks [2]
* Produces an error if any violation of an assertion occurs (**Note:** Can be an error in code or an error in specification)
  + Provides information about the cause of the problem, rather than the consequence [3]
* Cheap and easy to execute however the program runs slower and uses more memory
* Good addition to testing, however not a replacement for testing
* jmlunit tool combines jmlrac and unit testing

# ESC/Java 2

* ESC = Extended Static Checking
* ESC/Java 2, an extension of ESC/Java, supports more JML functionality

**References:**

**Purpose:**

* Fully automated verification
* Tries to prove correctness of specifications at compile time
* Not sound: May miss an error that is present
* Not complete: May warn of errors that are impossible
* However it finds a lot of potential bugs quickly
* Good at proving absence of runtime exceptions and verifying relatively simple properties
* Verification conditions are generated using a standard weakest-precondition procedure [4]
* All aliases must be known statically at the time of verification condition generation in order to apply the Hoare-style rule for assignment without the need for heap memory
  + Consequence is that recursive data types cannot have mutable components
* WhyML does not separate interface and implementation

**Uses**: [1]

1. Use only to verify programs using the theorem provers. (Logic only)
2. Verify algorithms/data structures through WhyML
3. Verify programs from a mainstream language eg Java, C, Ada