« Vérification de l’absence d’erreurs à l’exécution dans des logiciels industriels critiques de contrôle/commande par interprétation abstraite »

Patrick Cousot
École normale supérieure
45 rue d’Ulm, 75230 Paris cedex 05, France
Patrick.Cousot@ens.fr  www.di.ens.fr/~cousot


1. Motivation

Bugs Now Show-Up in Everyday Life

– Bugs now appear frequently in everyday life (banks, cars, telephones, . . .

– Example (HSBC bank ATM\textsuperscript{1} at 19 Boulevard Sébastopol in Paris, failure on Nov. 21\textsuperscript{st} 2006 at 8:30 am):

\begin{itemize}
  \item cash machine, cash dispenser, automatic teller machine.
\end{itemize}

A Strong Need for Software Better Quality

– Poor software quality is not acceptable in safety and mission critical software applications.

– The present state of the art in software engineering does not offer sufficient quality guarantees.
Tool-Based Software Design Methods

- New tool-based software design methods will have to emerge to face the unprecedented growth and complexification of critical software

- E.g. FCPC (Flight Control Primary Computer)
  - A220: 20,000 LOCs,
  - A340:
    - 130,000 LOCs (V1),
    - 250,000 LOCs (V2),
  - A380: 1,000,000 LOCs

Abstract Interpretation

There are two fundamental concepts in computer science (and in sciences in general):

- Abstraction: to reason on complex systems
- Approximation: to make effective undecidable computations

These concepts are formalized by abstract interpretation

References


Operational semantics

Test/Debugging is Unsafe

Safety property

Bounded Model Checking is Unsafe
Over-Approximation

Abstract Interpretation is Sound

Soundness and Incompleteness

Soundness Requirement: Erroneous Abstraction

2 This situation is always excluded in static analysis by abstract interpretation.
Soundness Requirement: Erroneous Abstraction\(^3\)

\[ x(t) \]

This situation is always excluded in static analysis by abstract interpretation.

3. The ASTRÉE static analyzer

http://www.astree.ens.fr/

Project Members

- Bruno Blanchet\(^4\)
- Patrick Cousot
- Radhia Cousot
- Jérôme Feret
- Laurent Mauborgne
- Antoine Miné
- David Monniaux\(^5\)
- Xavier Rival

\(^3\) Nov. 2001 — Nov. 2003.
Programs Analyzed by Astrée and their Semantics

- Programs analysed by Astrée

- Application Domain: large safety critical embedded real-time synchronous software for non-linear control of very complex control/command systems.

- C programs:
  - with
    - basic numeric datatypes, structures and arrays
    - pointers (including on functions),
    - floating point computations
    - tests, loops and function calls
    - limited branching (forward goto, break, continue)
  - with (cont’d)
    - union [Min06a]
    - pointer arithmetics & casts [Min06a]

- without
  - dynamic memory allocation
  - recursive function calls
  - unstructured/backward branching
  - conflicting side effects
  - C libraries, system calls (parallelism)

Such limitations are quite common for embedded safety-critical software.

The Class of Considered Periodic Synchronous Programs

declare volatile input, state and output variables;
initialize state and output variables;
loop forever
  - read volatile input variables,
  - compute output and state variables,
  - write to output variables;
  __ASTREE_wait_for_clock__();
end loop

Task scheduling is static:

- Requirements: the only interrupts are clock ticks;
- Execution time of loop body less than a clock tick, as verified by the aiT WCET Analyzers [FHL+01].
Concrete Operational Semantics

- International norm of C (ISO/IEC 9899:1999)
- restricted by implementation-specific behaviors depending upon the machine and compiler (e.g. representation and size of integers, IEEE 754-1985 norm for floats and doubles)
- restricted by user-defined programming guidelines (such as no modular arithmetic for signed integers, even though this might be the hardware choice)
- restricted by program specific user requirements (e.g. assert, execution stops on first runtime error)

6 semantics of C unclear after an error, equivalent if no alarm

Different Classes of Run-time Errors

1. Errors terminating the execution. ASTRÉE warns and continues by taking into account only the executions that did not trigger the error.
2. Errors not terminating the execution with predictable outcome. ASTRÉE warns and continues with worst-case assumptions.
3. Errors not terminating the execution with unpredictable outcome. ASTRÉE warns and continues by taking into account only the executions that did not trigger the error.

⇒ ASTRÉE is sound with respect to C standard, unsound with respect to C implementation, unless no false alarm.

Implicit Specification: Absence of Runtime Errors

- No violation of the norm of C (e.g. array index out of bounds, division by zero)
- No implementation-specific undefined behaviors (e.g. maximum short integer is 32767, NaN)
- No violation of the programming guidelines (e.g. static variables cannot be assumed to be initialized to 0)
- No violation of the programmer assertions (must all be statically verified).
Modular Arithmetic

Modular arithmetics is not very intuitive

In C:

```c
#include <stdio.h>

int main () {
    int x,y;
    x = -2147483647 / -1;
    y = ((-x) -1) / -1;
    printf("x = %i, y = %i\n",x,y);
}
```

% cat -n modulo-c.c

```
1 #include <stdio.h>
2 int main () {
3    int x,y;
4    x = -2147483647 / -1;
5    y = ((-x) -1) / -1;
6    printf("x = %i, y = %i\n",x,y);
7 }
```

% gcc modulo-c.c

```bash
% ./a.out
x = 2147483647, y = -2147483648
```

Static Analysis with ASTRÉE

```c
int main () {
    int x,y;
    x = -2147483647 / -1;
    y = ((-x) -1) / -1;
    __ASTREE_log_vars((x,y));
}
```

% astree –exec-fn main –unroll 0 modulo.c

```bash
% astree –exec-fn main –unroll 0 modulo.c
```

ASTRÉE signals the overflow and goes on with an unknown value.

Float Overflow
Float Arithmetics does Overflow

In C:

```c
void main () {
  double x,y;
  x = 1.0e+256 * 1.0e+256;
  y = 1.0e+256 * -1.0e+256;
  __ASTREE_log_vars((x,y));
}
```

```bash
% gcc -o a.out overflow.c
% ./a.out
x = inf, y = -inf
```

The Ariane 5.01 maiden flight failure

- June 4th, 1996 was the maiden flight of Ariane 5
- The launcher was destroyed after 40 seconds of flight because of a software overflow

10 A 16 bit piece of code of Ariane 4 had been reused within the new 32 bit code for Ariane 5. This caused an uncaught overflow, making the launcher uncontrollable.

The Ariane 5.01 maiden flight

- June 4th, 1996 was the maiden flight of Ariane 5

Rounding
Example of accumulation of small rounding errors

```c
#include <stdio.h>
int main () {
    int i; double x; x = 0.0;
    for (i=1; i<=1000000000; i++) {
        x = x + 1.0/10.0;
    }
    printf("x = %f\n", x);
}
```

```
% gcc rounding-c.c
% ./a.out
x = 99999998.745418
```

since \((0.1)_{10} = (0.0001100110011001100\ldots)_{2}\)

The Patriot missile failure

- “On February 25th, 1991, a Patriot missile ... failed to track and intercept an incoming Scud (i).”
- The software failure was due to accumulated rounding error (ii)

(i) This Scud subsequently hit an Army barracks, killing 28 Americans.
(ii) “Time is kept continuously by the system’s internal clock in tenths of seconds”
- “The system had been in operation for over 100 consecutive hours”
- “Because the system had been on so long, the resulting inaccuracy in the time calculation caused the range gate to shift so much that the system could not track the incoming Scud”

Static analysis with ASTRÉE

```c
int main () {
    double x; x = 0.0;
    while (1) {
        x = x + 1.0/10.0;
        __ASTREE_log_vars((x));
        __ASTREE_wait_for_clock();
    }
}
```

```
% cat -n rounding.c
1 int main () {
2    double x; x = 0.0;
3    while (1) {
4       x = x + 1.0/10.0;
5       __ASTREE_log_vars((x));
6       __ASTREE_wait_for_clock();
7    }
8 }
```

```
% gcc rounding.c
% ./a.out
```

Filtering
Ellipsoid Abstract Domain for Filters

- Computes \( X_n = \frac{\alpha X_{n-1} + \beta X_{n-2} + Y_n}{L_n} \)
- The concrete computation is bounded, which must be proved in the abstract.
- There is no stable interval or octagon.
- The simplest stable surface is an ellipsoid.

Filter Example [Fer04]

```c
typedef enum {FALSE = 0, TRUE = 1} BOOLEAN;
BOOLEAN INIT; float P, X;
void filter () {
    static float E[2], S[2];
    if (INIT) { S[0] = X; P = X; E[0] = X; }
    else { P = (((((0.5 * X) - (E[0] * 0.7)) + (E[1] * 0.4)) + (S[0] * 1.5)) - (S[1] * 0.7)); }
    E[1] = E[0]; E[0] = X; S[1] = S[0]; S[0] = P;
    /* S[0], S[1] in [ -1327.02698354, 1327.02698354 ] */
}
void main () { X = 0.2 * X + 5; INIT = TRUE;
    while (1) {
        X = 0.9 * X + 35; /* simulated filter input */
        filter (); INIT = FALSE; }
}
```

Arithmetic-Geometric Progressions (Example 1)

```c
% cat count.c
typedef enum {FALSE = 0, TRUE = 1} BOOLEAN;
volatile BOOLEAN I; int R; BOOLEAN T;
void main() {
    R = 0;
    while (TRUE) {
        __ASTREE_log_vars((R));
        if (I) { R = R + 1; }
        else { R = 0; }
        T = (R >= 100);
        __ASTREE_wait_for_clock();
    }
}
% cat count.config
_--ASTREE_volatile_input((I [0,1]));
__ASTREE_max_clock((3600000));
% astree --exec-fn main --config-sem count.config count.c|grep '|R|'
|R| <= 0. + clock *1. <= 3600001.
```
4. The industrial use of ASTRÉE

References

Characteristics of the ASTRÉE Analyzer

Sound:  
- ASTRÉE is a bug eradicator: finds all bugs in a well-defined class (runtime errors)
- ASTRÉE is not a bug hunter: finding some bugs in a well-defined class (e.g. by bug pattern detection like FindBugs™, PREfast or PMD)
- ASTRÉE is exhaustive: covers the whole state space (≠ MAGIC, CBMC)
- ASTRÉE is comprehensive: never omits potential errors (≠ UNO, CMC from coverity.com) or sort most probable ones to avoid overwhelming messages (≠ Splint)

Characteristics of the ASTRÉE Analyzer (Cont’d)

Static: compile time analysis (≠ run time analysis Rational Purify, Parasoft Insure++)

Program Analyzer: analyzes programs not micromodels of programs (≠ PROMELA in SPIN or Alloy in the Alloy Analyzer)

Automatic: no end-user intervention needed (≠ ESC Java, ESC Java 2), or PREfast (annotate functions with intended use)
Characteristics of the Astrée Analyzer (Cont’d)

**Multiabstraction:** uses many numerical/symbolic abstract domains (≠ symbolic constraints in Bane or the canonical abstraction of TVLA)

**Infinitary:** all abstractions use infinite abstract domains with widening/narrowing (≠ model checking based analyzers such as Bandera, Bogor, Java PathFinder, Spin, VeriSoft)

**Efficient:** always terminate (≠ counterexample-driven automatic abstraction refinement BLAST, SLAM)

**Automatic Parametrization:** the generation of parametric directives in the code can be programmed (to be specialized for a specific application domain)

**Modular:** an analyzer instance is built by selection of O-CAML modules from a collection each implementing an abstract domain

**Precise:** very few or no false alarm when adapted to an application domain → it is a VERIFIER!

Characteristics of the Astrée Analyzer (Cont’d)

**Extensible/Specializable:** can easily incorporate new abstractions (and reduction with already existing abstract domains) (≠ general-purpose analyzers PolySpace Verifier)

**Domain-Aware:** knows about control/command (e.g. digital filters) (as opposed to specialization to a mere programming style in C Global Surveyor)

**Parametric:** the precision/cost can be tailored to user needs by options and directives in the code

The Future of the Astrée Analyzer

- Astrée has shown usable and useful in one industrial context (electric flight control);
- More applications are forthcoming (ES_PASSS project);
- Industrialization is simultaneously under consideration.
6. Bibliography


