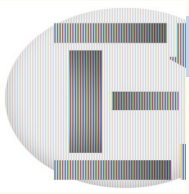
Run-time Checking/Monitoring at SDL Fredhopper

Stijn de Gouw

SDL Fredhopper

e-Commerce company, back-end for 300+ online shops

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.



Communication in Java

Messages between Objects (sender/receiver):

Method Calls

- `y.m(p)` Current object **this** sends message **m** with contents **p** to object **y**

Method Returns

- `return(v)` Current object **this** sends message **return** with contents **v** to calling object

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.

Communication History in Java

History of sequential Java prog: sequence of messages/events containing data

```
void main() {
   Stack s = new Stack();   Stack t = new Stack();
   s.push(5);  t.push(3); s.push(7);
}
```

Global history of entire program:

(call_push(5) ret_push call_push(2) ret_push call_push(7) ret_push)

Local history of object s:

(call_push(5) ret_push call_push(7) ret_push)

With encapsulation: fully determines current state

Why Histories?

- Semantic foundation of OOP
  - Fully Abstract Trace Semantics for a Core Java Language (Rathke & Jeffrey)
- Behavioral Subtyping, fragile base class problem
  - Behavioural Subtyping Relations for OO Formalisms (Fischer & Wehrheim)
- Implementation independent

+ Goal I: finding a 'familiar' specification language for Java based on histories and amenable to automated run-time checking.

Goal II: allow *combining*

+ protocol-oriented properties (orderings of events) and data-oriented properties (assertion checking)

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.

Example: BufferedReader

```
public class BufferedReader {
    BufferedReader(Reader in)
    BufferedReader(Reader in, int sz)

    void    close()
    void    mark(int readAheadLimit)
    boolean   markSupported()
    int  read()
    int  read(char[] cbuf, int off, int len)
    String readLine()
    boolean   ready()
    void    reset()
    long    skip(long n)
```

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.

Communication View

Partial mapping
From Event 'type'
To Name

```
local view BReaderHistory grammar BReader.g
specifies java.io.BufferedReader {
                  new(Reader in)  OPEN,
    call String readLine()        READ,
    call void   close()           CLOSE
}
```

- Specifies which events to capture (partial mapping)
- User-defined abstraction of local history (projection, identify >1 events with single terminal)

Attribute Grammars (I)

- Context-free Grammar + Attributes (map (sub)words of the language to values)

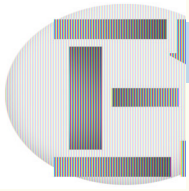
- Value of attributes defined in the productions

```
S ::= S1 a   { S.height = S1.height + 1; }
    | a      { S.height = 0; }
```

- Synthesized Attr.: propagate info up the tree
  - Determines attribute val. of non-terminal in LHS

- Inherited Attr.: pass info down the tree
  - Determine attribute val. of non-terminals in RHS

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.



Attribute Grammars (II)

Basic Idea:

1. Specification = set of (valid) histories = formal language generated by an (extended) attribute grammar
2. Run-time checking: parse trace in grammar + check asserts

Terminals in grammar:

Message names: objects with built-in attr (caller, params, …)

Non-terminals in grammar:

User-defined, specify protocol structure.

Attributes of non-terminals *define* data properties

Assertions *specify* properties of attributes

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.

Attribute Grammar – BufferedReader client

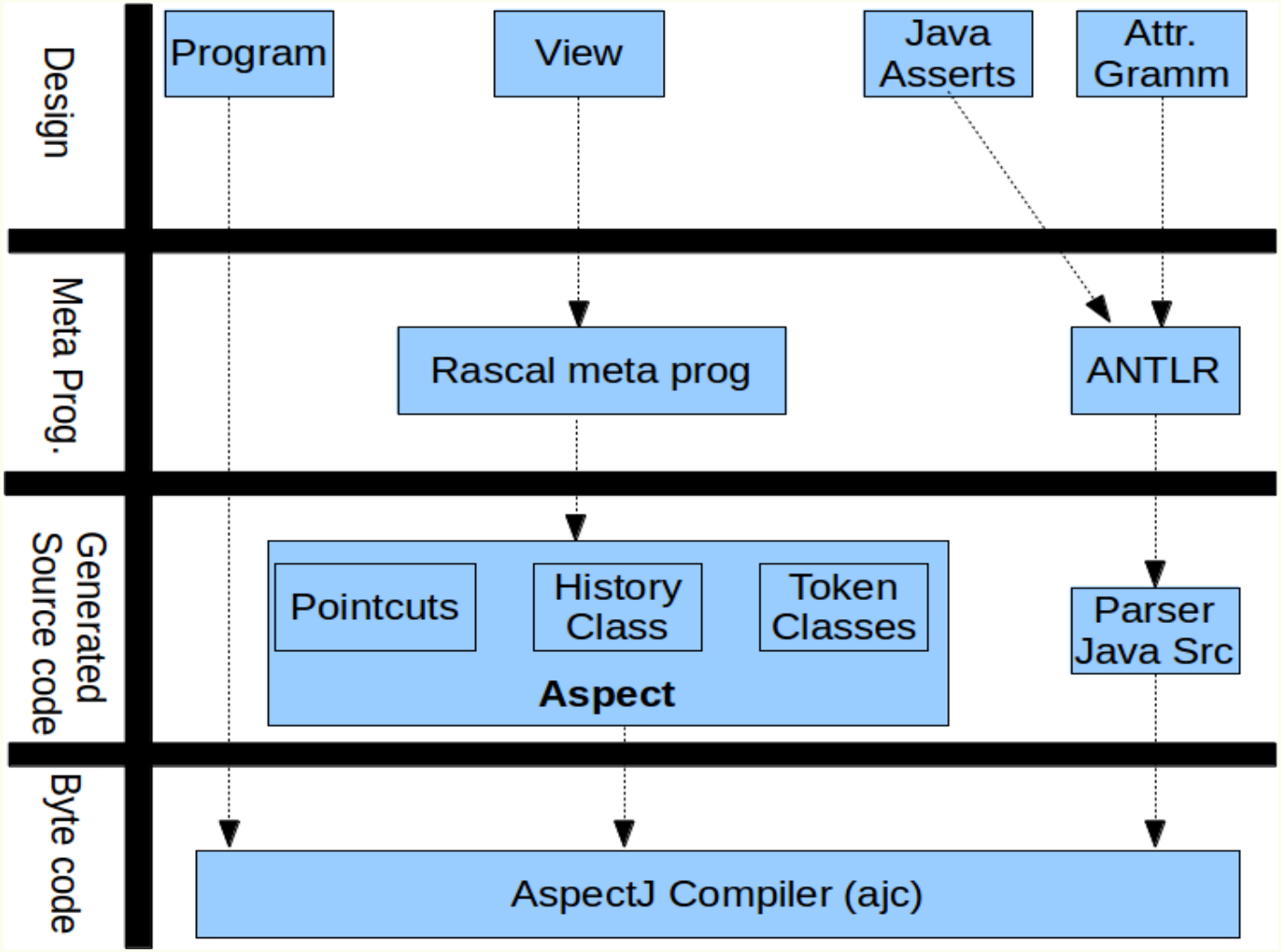
```
start :   OPEN   READ*
          (CLOSE {assert OPEN.caller() == CLOSE.caller();})?
      |   ε
```

Why Attribute Grammars?

- Grammars are ‘familiar’: teached to undergraduates
- Allow **combining** protocol and data-oriented properties
- Declarative
- Amenable to automated run-time verification (well-developed parsing technology)

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.

Tool Architecture



Challenges for industrial usage

- How to integrate checker into existing build process?
- Support for language features: Constructors, Inheritance / Dynamic Binding, Overloading, Static Methods, Multi-threading
- Instrumentation: source code not always available (Library methods/third party libs)
- Java Security model: classes to be monitored may not always be visible or accessible to monitor
- Writing specs is time consuming (refactorings?)

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.

Non-functional Properties

- **“Resource usage (mem/CPU/bandwidth) is above a certain treshold”**
- **Monitoring SLAs: “Average number of queries completed in the last 24h is ≥ 10”**

- **Currently: ad-hoc approach**
- **Manual reaction from operations team (domain-specific knowledge)**
- **Translation to functional properties (record time of event in attribute)? (interference of monitors)**

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.

Further Reading (selected publications)

Run-Time Assertion Checking of Data- and Protocol-Oriented Properties of Java Programs: An Industrial Case Study.
Frank S. de Boer, Stijn de Gouw, Einar Broch Johnsen, Andreas Kohn, Peter Y. H. Wong
T. Aspect-Oriented Software Development 11: 1-26 (2014)

Run-Time Verification of Coboxes.
Frank S. de Boer, Stijn de Gouw, Peter Y. H. Wong
SEFM 2013: 259-273

Run-Time Verification of Black-Box Components Using Behavioral Specifications: An Experience Report on Tool Development.
Frank S. de Boer, Stijn de Gouw
FACS 2012:128-133

https://github.com/cwi-swat/saga

SEVENTH FRAMEWORK PROGRAMME
EURIPIDES is a collaborative Project funded by the European Commission under the 7th Framework Program.