

# Formal Analysis of Java Programs in JavaFAN

Azadeh Farzan

Jose Meseguer

Grigore Rosu

University of Illinois at Urbana-Champaign

# What is JavaFAN?

- Formal Analysis of Java programs at both **source code** and **bytecode** levels
- Based on formal specification of both languages in **rewriting logic** using **Maude**
- Supported formal analyses
  - Model checking
  - Breadth-first search
  - Symbolic execution

# Rewriting Logic Semantics

- Specifying **truly** concurrent semantics of Java and the JVM in Maude
- Rewrite Theory :  $(\Sigma, E, R)$
- **Equations** model the **sequential** parts of semantics
- **Rewrite rules** model the **concurrent** part of the semantics

# Optimizations

- **Smaller States**
  - distinction between **static** and **dynamic** parts
- **Fewer States**
  - rewrite rules vs. equations

# Synchronization

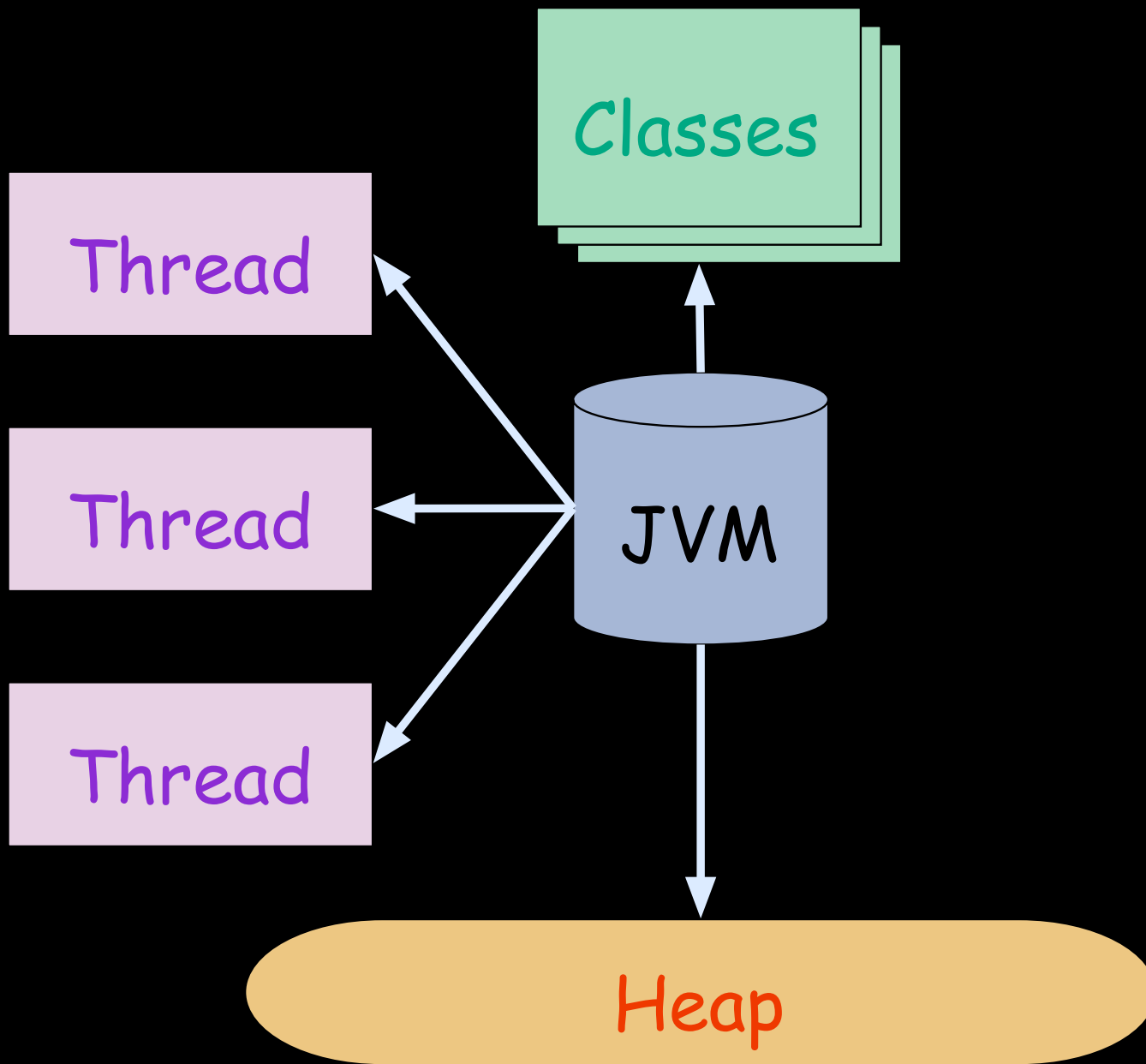
- Synchronization at Java Language Level

- **synchronized** blocks
- **synchronized** methods
- **wait** & **notifyall**

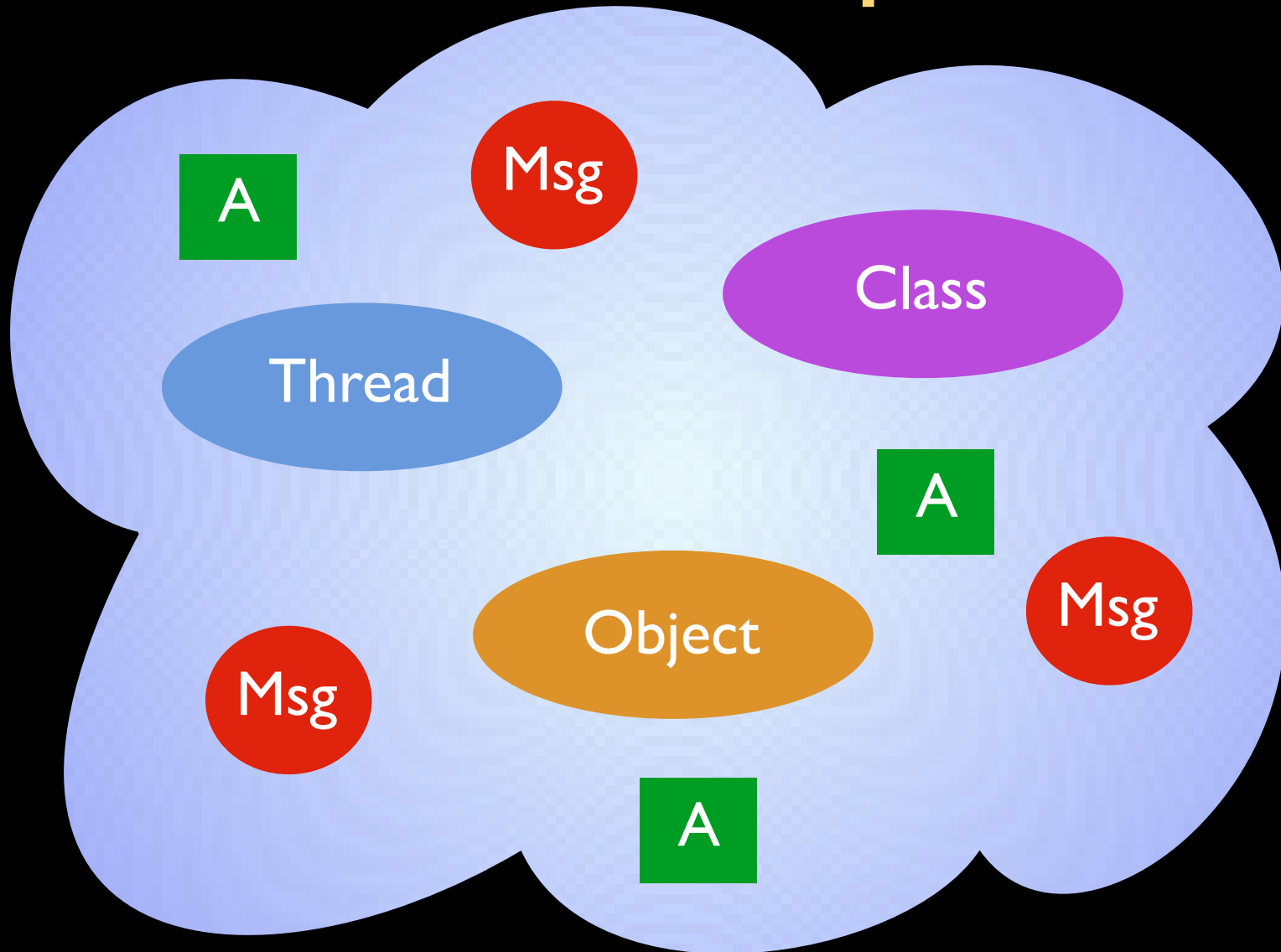


```
synchronized (o) {  
    ...  
}  
synchronized foo(...) {  
    ...  
}
```

# JVM Model



# The Soup



# Java Model

# Program State

- Threads, Memory, Synchronization Information, ...
- Memory: an environment and a store
- Threads: a continuation and an environment

# Formal Analysis

# Formal Analysis

- Model checking
  - Maude's LTL Model Checker
  - Case Studies : Dining Philosophers, 2-stage Pipeline
- Breadth-first search
  - Possibly infinite state spaces
  - Case Studies: Remote Agent, Thread Game

# Performance Results

| Tests    | JVM    | Java | Other            |
|----------|--------|------|------------------|
| RA       | 0.3    | 0.1  | 2+ (Stanford)    |
| Pipeline | 17m    | ---  | 100m+ (Stanford) |
| DP(4)    | 0.6    | 1.2  | ---              |
| DP(6)    | 33.3   | 81.7 | ---              |
| DP(8)    | 13.7m  | 98m  | ---              |
| DP(9)    | 803.2m | ---  | ---              |
| DF(5)    | 3.2m   | 19.2 | $\infty$ (JPF)   |
| DF(7)    | 686m   | 27m  | $\infty$ (JPF)   |
| TG(100)  | 17.1   | 6.6  | ---              |
| TG(1000) | 10.1m  | 5.1m | ---              |

# Conclusion

- JavaFAN
  - Formal Executable Specification of Concurrent semantics of the Java & JVM
- Formal Analyses : Simulation, Search, and Model Checking
- Scaling up
  - Granularity, Abstraction, Partial-order reduction
- Widening the range of Formal Analyses
  - Theorem Proving, Domain-Specific Certification