

LiquidJava: Adding Lightweight Verification to Java

Catarina Gamboa¹, Paulo Santos¹, Chris Timperley², Alcides Fonseca¹

¹ LASIGE, Faculdade de Ciências, Universidade de Lisboa, Portugal

² Carnegie Mellon University, Pittsburgh, PA, USA



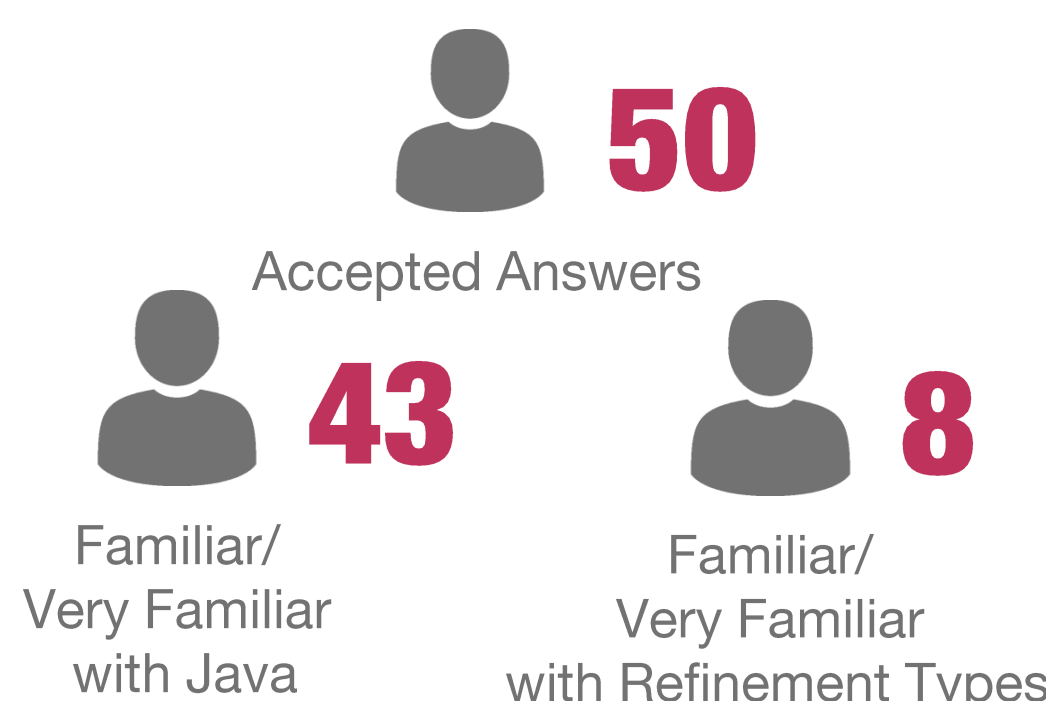
MOTIVATION

Refinement Types have been proposed as a verification technique to guarantee software quality by extending a type with a logical predicate. Despite their perceived utility they have not yet been adopted in industry.

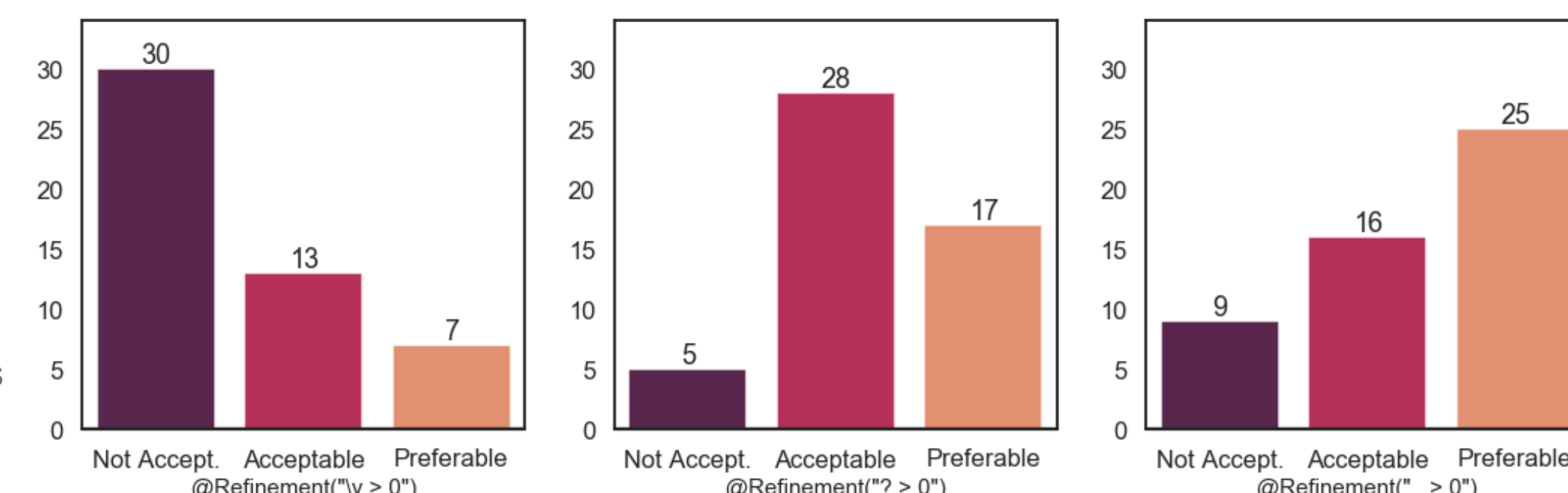
```
@Refinement("0 <= y && y <= 50")
int y;
y = 10; //Correct
y = 100; //Refinement Type Error
```

We propose the application of refinement types to Java, one of the most popular programming languages in the world.

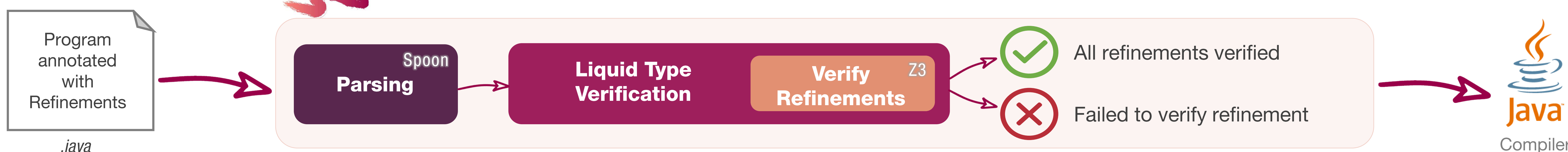
REFINEMENTS SYNTAX - SURVEY



To assess the best syntax for the refinements, we created a survey with multiple syntax options for each of the language features.

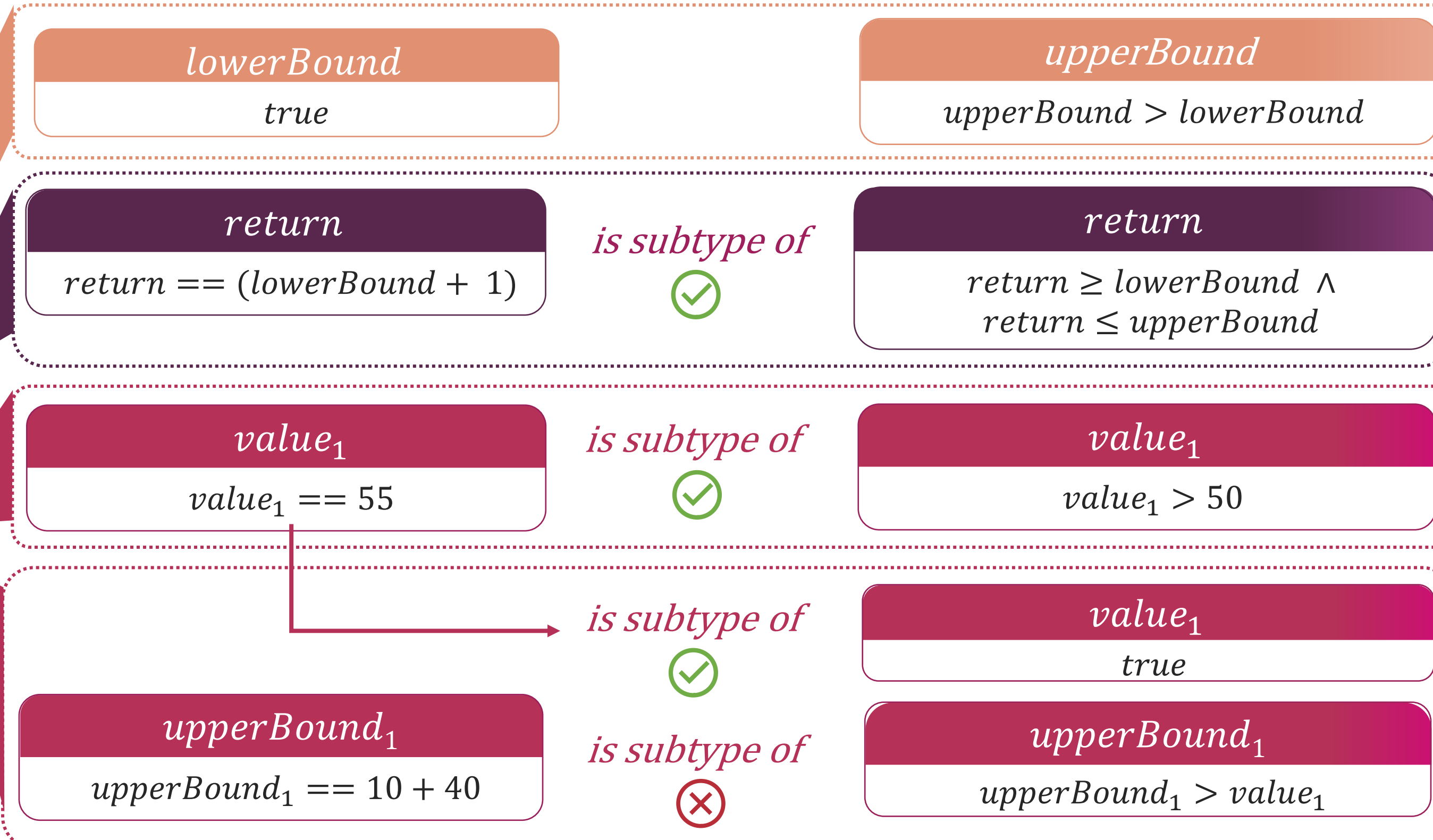


SYSTEM



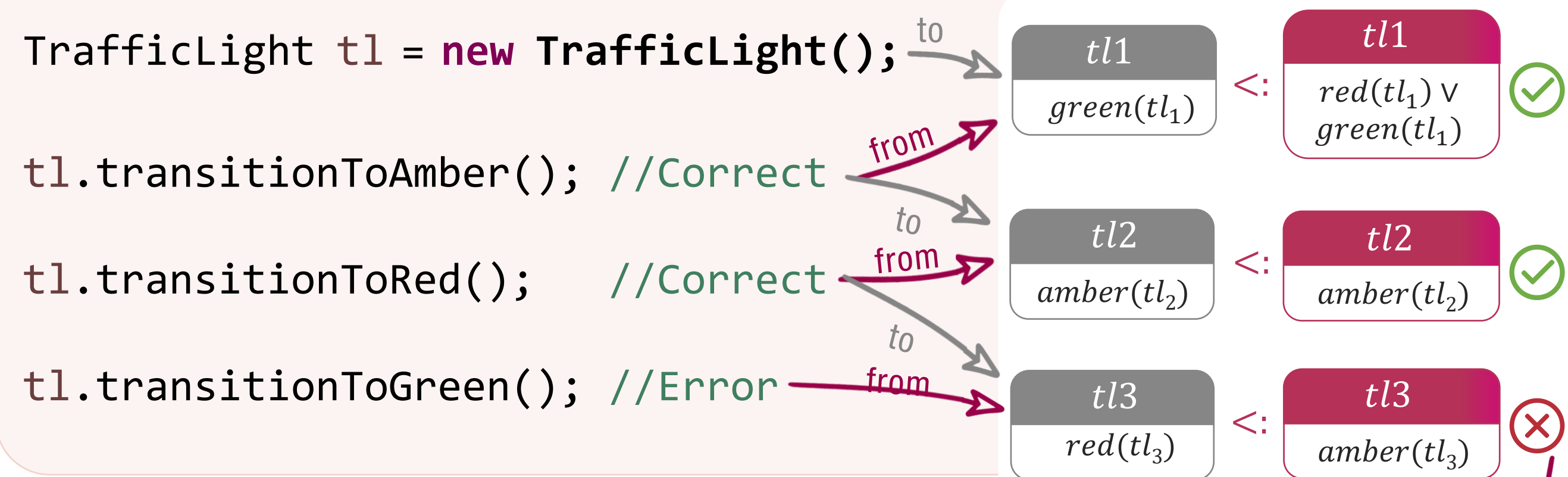
VERIFICATION EXAMPLE

```
@Refinement("_ >= lowerBound && _ <= upperBound")
public static int inRange(int lowerBound,
    @Refinement("upperBound > lowerBound")
    int upperBound) {
    return lowerBound + 1;
}
...
@Refinement("_ > 50") int value = 55;
inRange(value, 10 + 40); //Error
```



OBJECT STATE

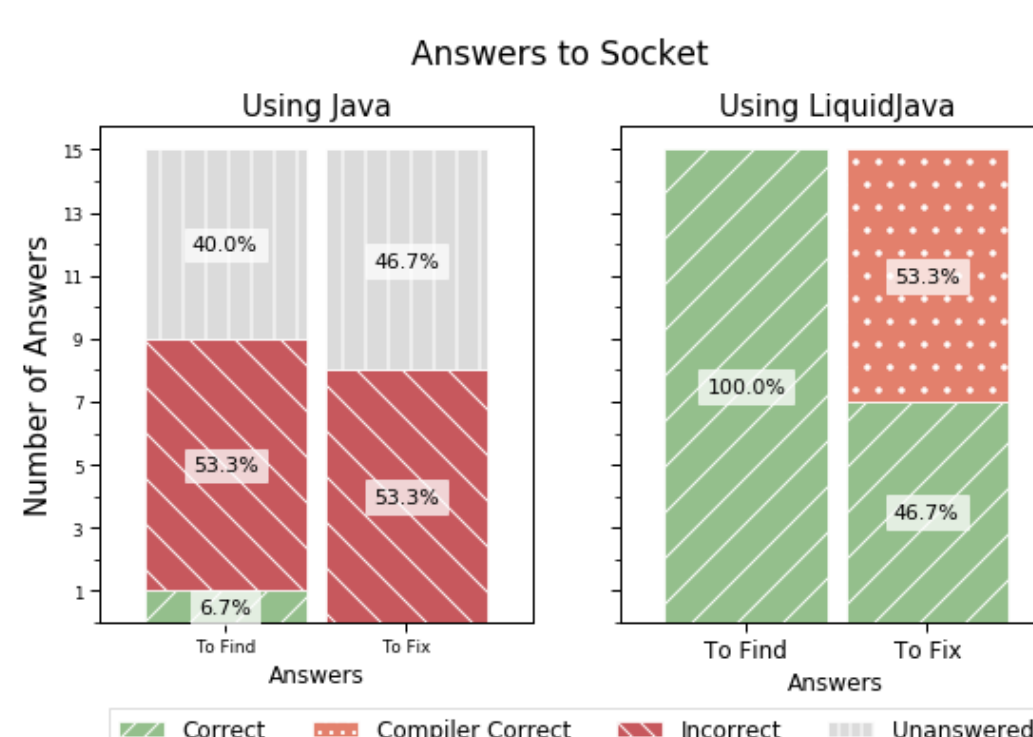
```
@StateSet({"green", "amber", "red"})
public class TrafficLight {
    public TrafficLight() {...}
    @StateRefinement(from="red(this)", to="amber(this)")
    @StateRefinement(from="green(this)", to="amber(this)")
    public void transitionToAmber() {...}
    @StateRefinement(from="amber(this)", to="red(this)")
    public void transitionToRed() {...}
    @StateRefinement(from="amber(this)", to="green(this)")
    public void transitionToGreen() {...}
}
```



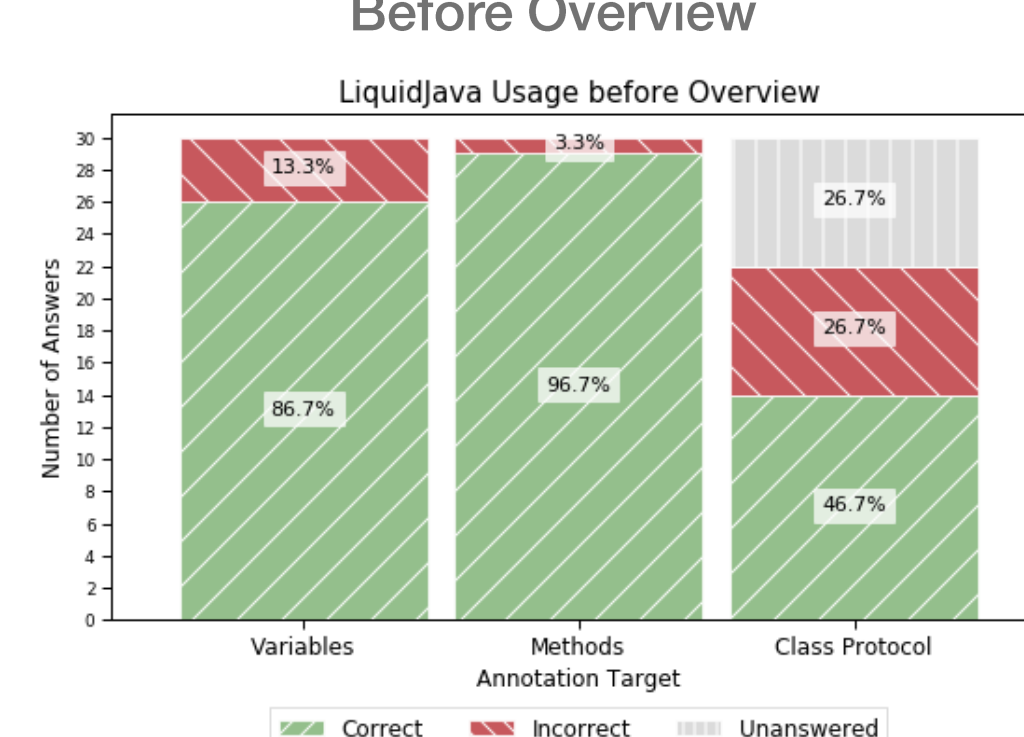
EVALUATION: RESEARCH STUDY



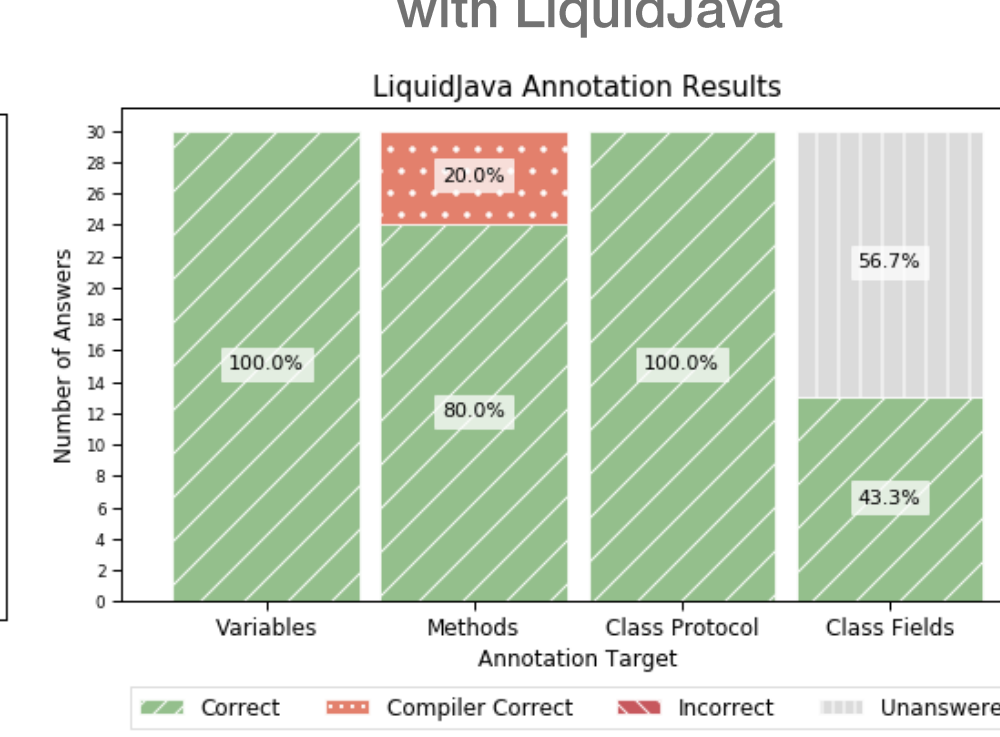
TASK 1&3: Find the Bug



TASK 2: Understand Refinements Before Overview

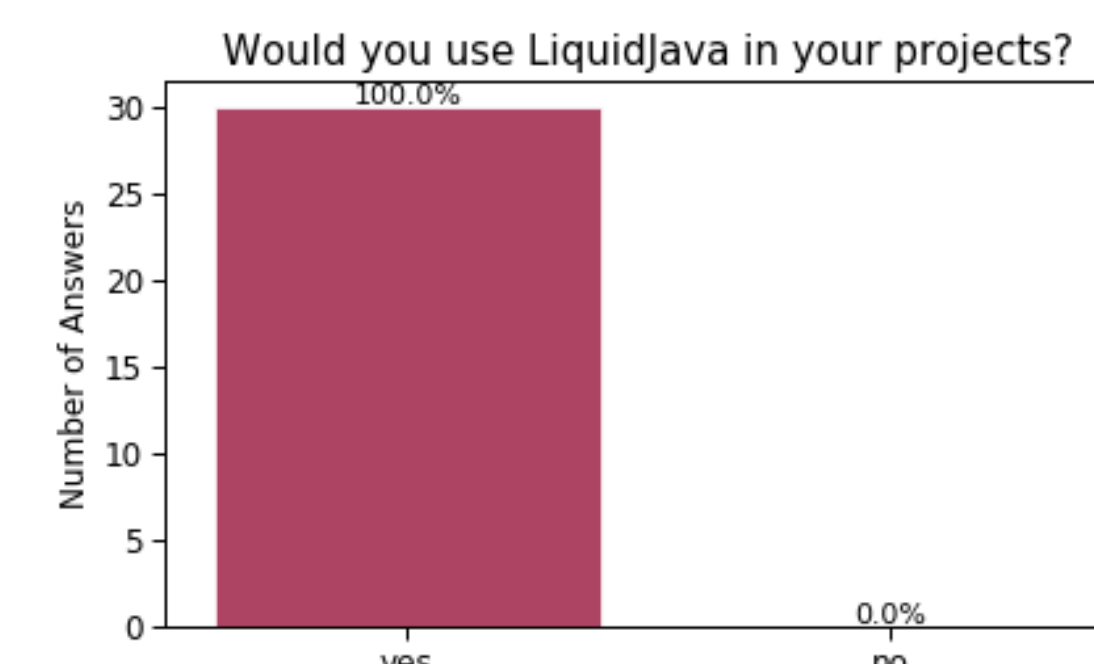


TASK 4: Annotate Java programs with LiquidJava



FUTURE WORK

- Improve error messages;
- Enhance LiquidJava verification features;
- Infer refinements;
- Improve IDE integration.



IDE INTEGRATION
ERROR REPORTING INSIDE
VISUAL STUDIO CODE

