Source-Level Dataflow-Based Fixes

Experiences from using IntraJ and MagpieBridge

Idriss Riouak - Lund University

EXAMPLE DATAFLOW-BASED ANALYSES

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```

Null pointer Analysis (NPA)

⚠ Possible `NullPointerException` at line 4

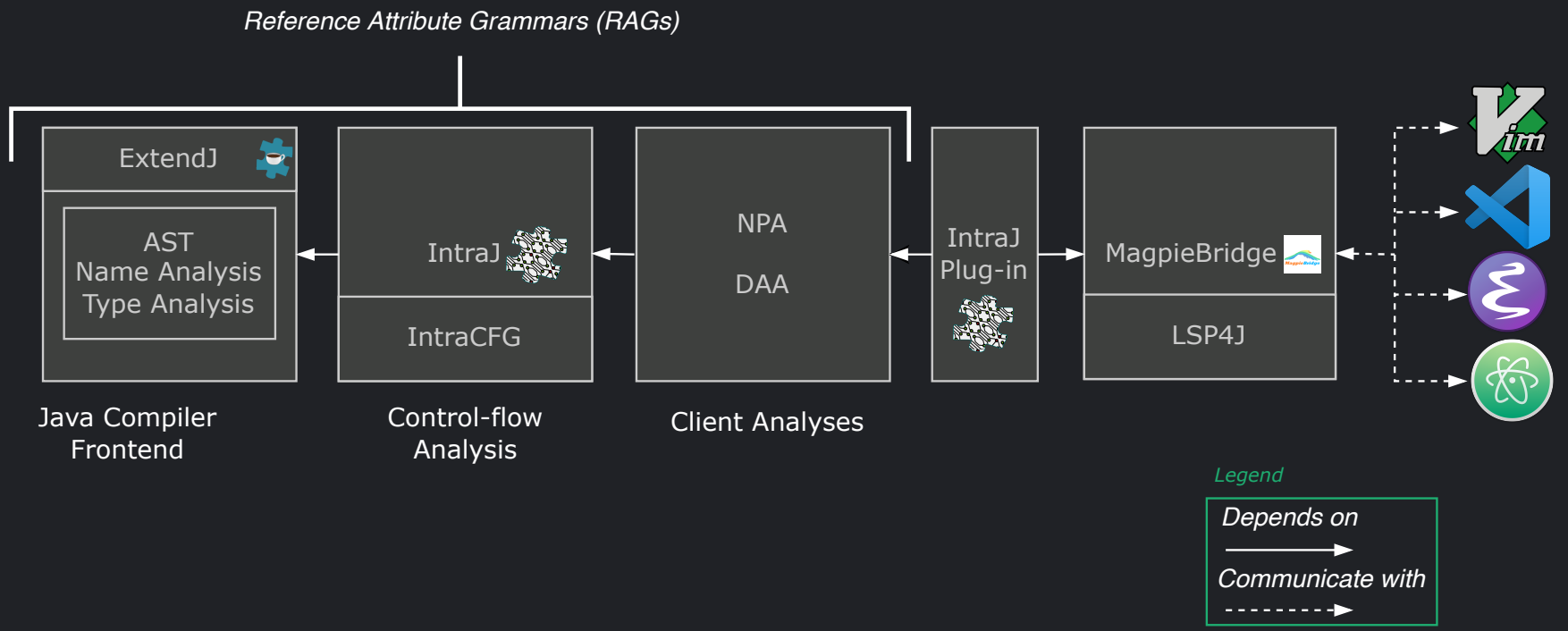
```
1  private int hash = 0;
2  int hashFunc(){
3    if(hash==0){
4      int hash = 10;
5      //Complex operations on  hash
6      hash += 10;
7    }
8    return hash;
9  }
```

Dead Assignment Analysis (DAA)

SIMPLIFIED EXAMPLE FROM FOP

⚠ `Dead Assignment` at line 6

THE BIG PICTURE



REFERENCE ATTRIBUTE GRAMMARS

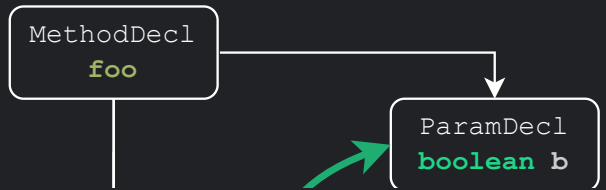
```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```

REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```

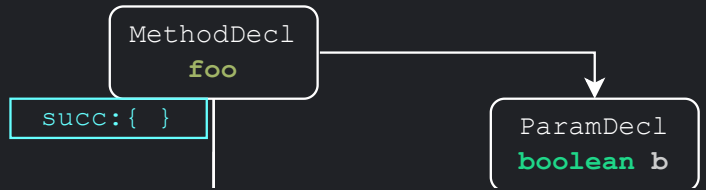
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



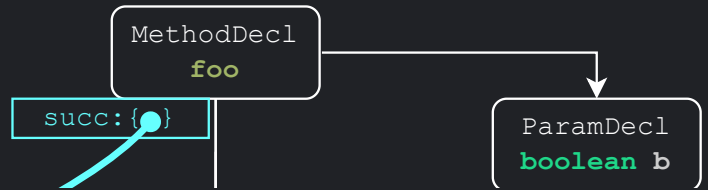
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



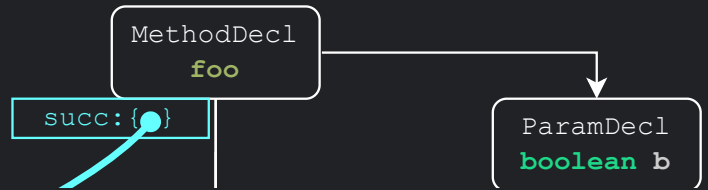
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



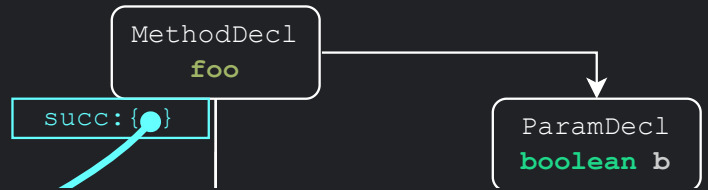
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



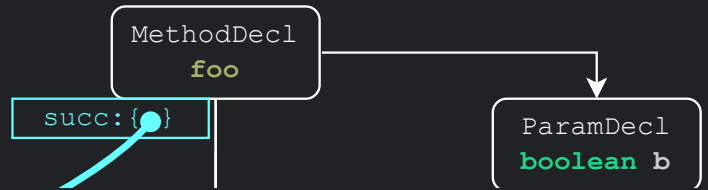
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



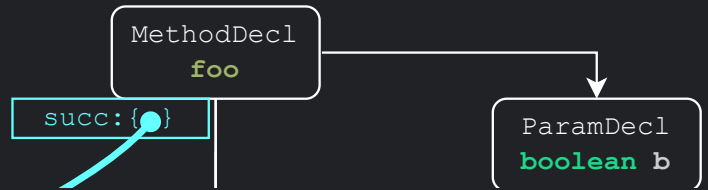
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



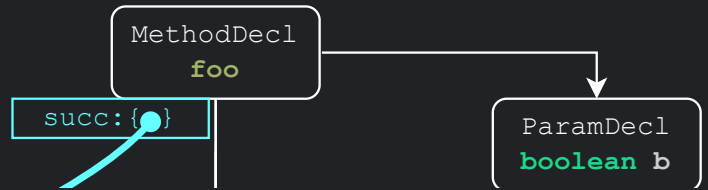
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



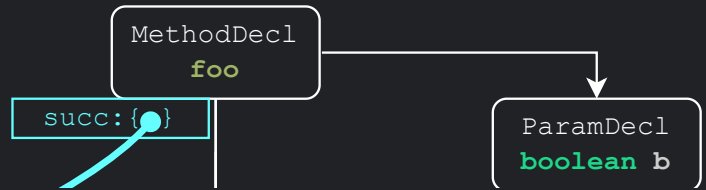
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



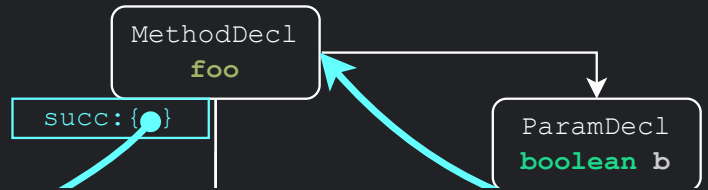
REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```

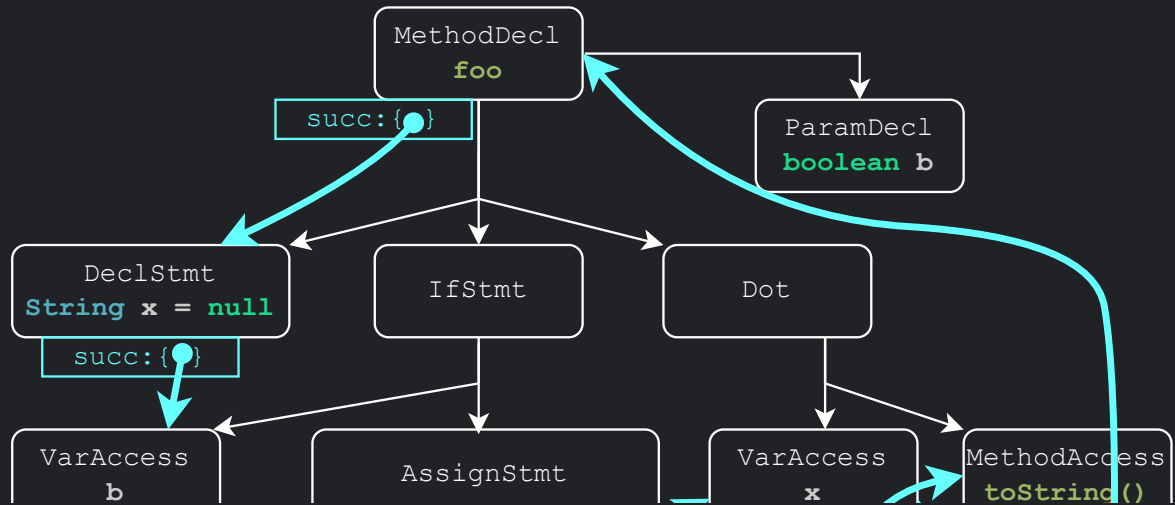


REFERENCE ATTRIBUTE GRAMMARS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```

- JastAdd ecosystem
  - Ondemand evaluation
  - Mutually dependent properties
  - Add subtree to the AST

jastadd



INTRAJ

- Build the CFGs on the Abstract Syntax Tree (AST)
- Handles implicit control-flows
- Analyses competitive with existing tools e.g., ***SonarQube***

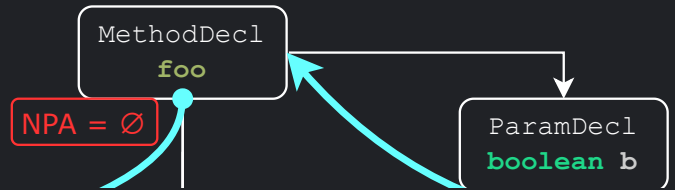
If you want to know more ...

GitHub

Paper

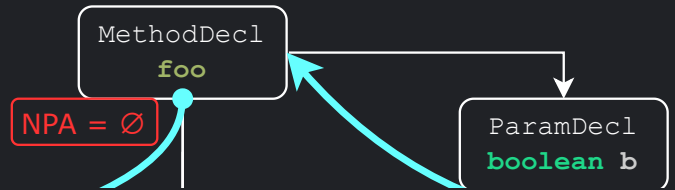
NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



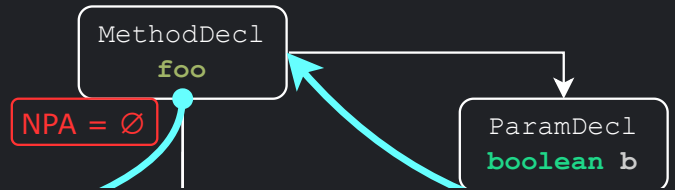
NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



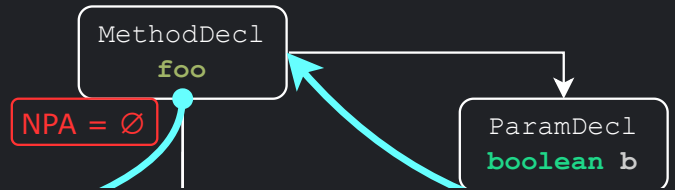
NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



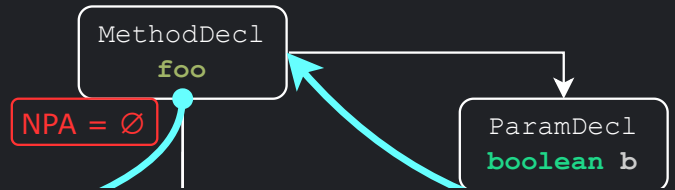
NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



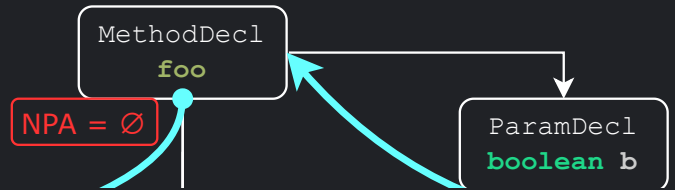
NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



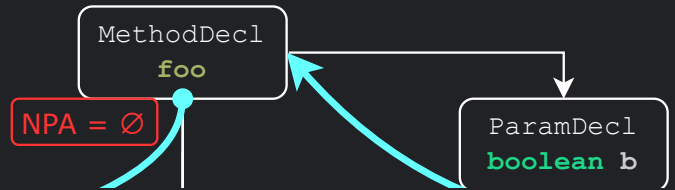
NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



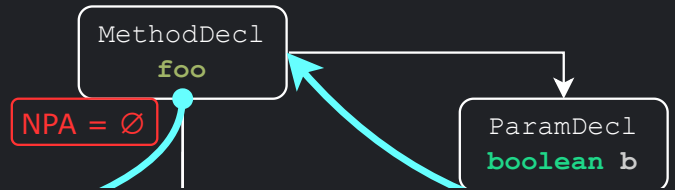
NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



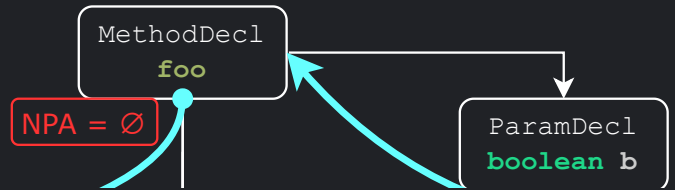
NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```

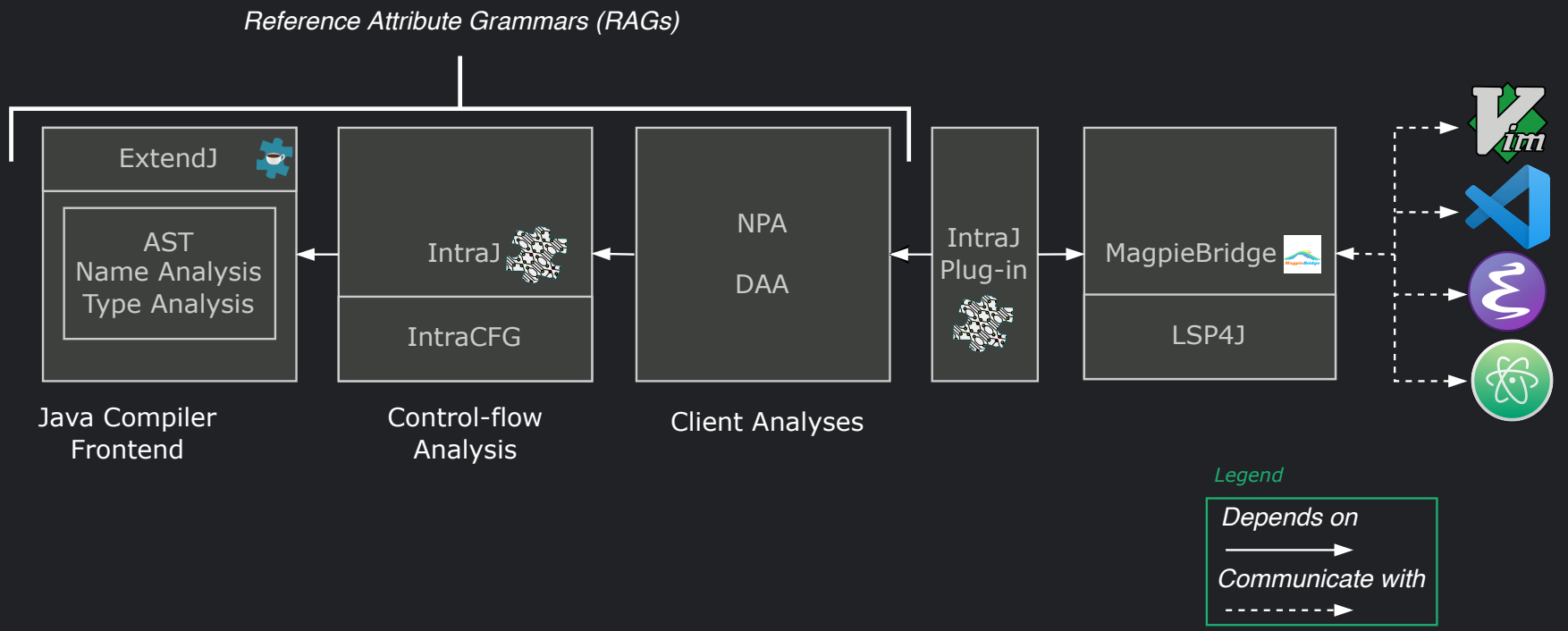


NULL POINTER ANALYSIS

```
1  void foo(boolean b){
2    String x = null;
3    if(b) x = "Hello World";
4    x.toString();
5  }
```



THE BIG PICTURE



INTRAJ PLUGIN

- Live demo:
  - Null Pointer Analysis
  - Dead Assignment Analysis
- The role of MagpieBridge:
  - Integration with VSCode
  - Extension settings

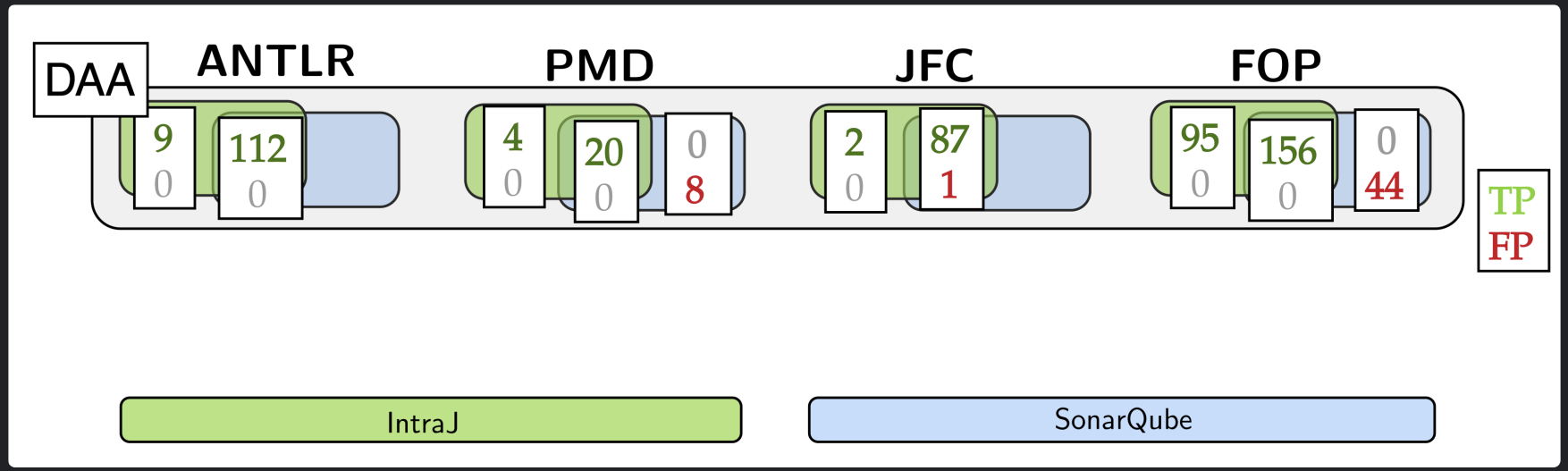
THANK YOU FOR YOUR ATTENTION !

GitHub

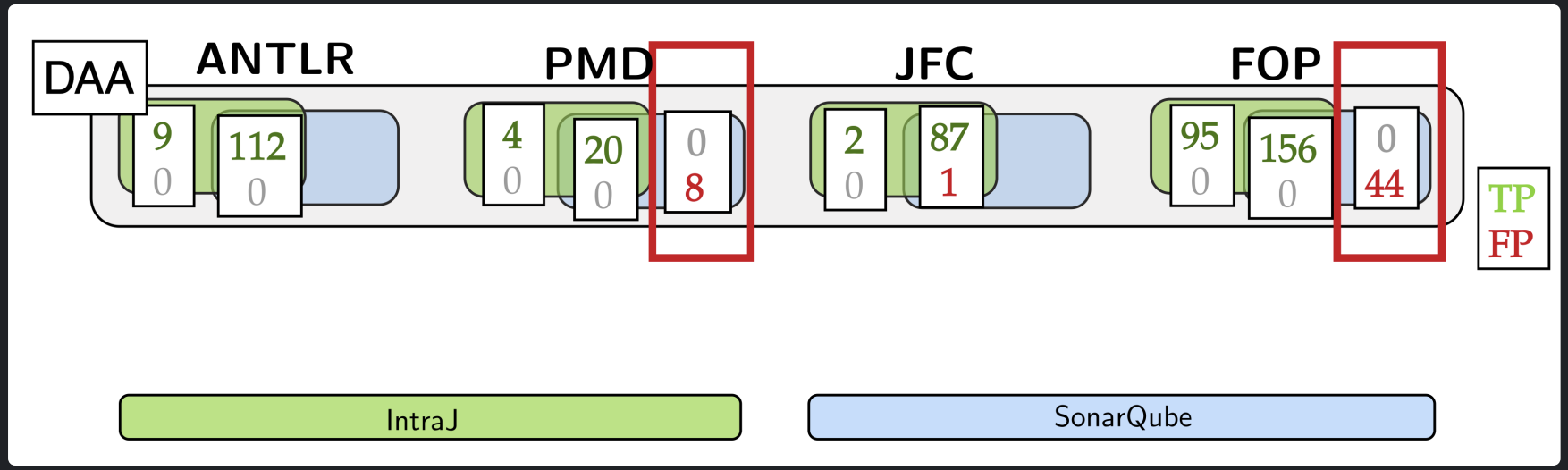
Paper

Extension

PRECISION: NUMBERS

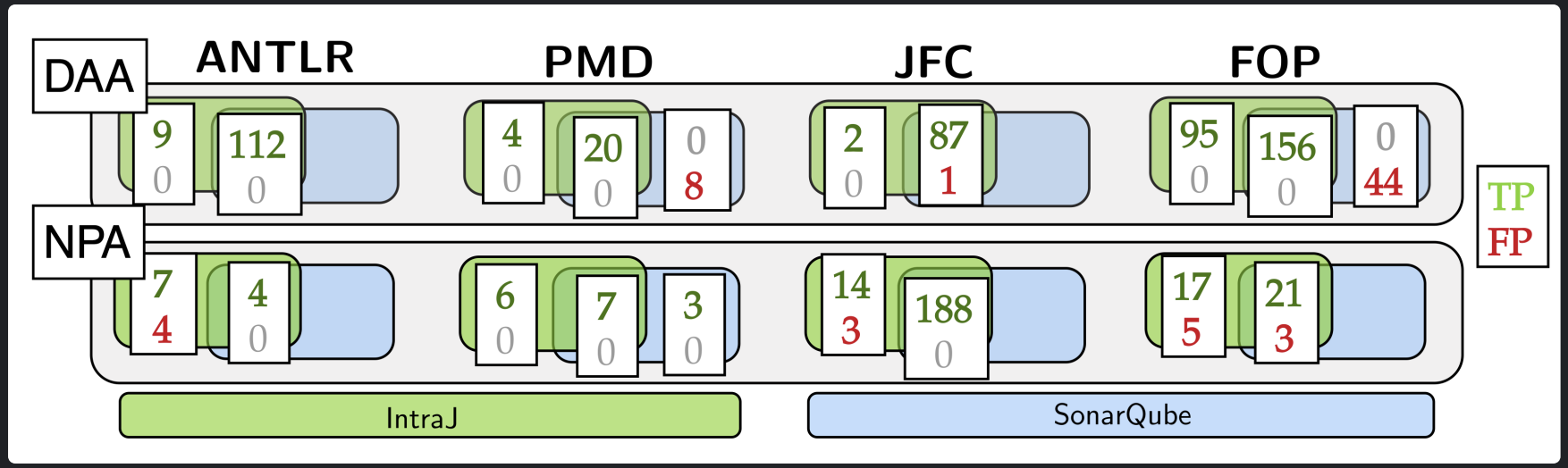


PRECISION: NUMBERS



DeadAssignmentAnalysis: IntraJ detects everything that SonarQube detects

PRECISION: NUMBERS



DeadAssignmentAnalysis: IntraJ detects everything that SonarQube detects

NullPointerAnalysis: SonarQube is more precise but IntraJ remains competitive

PERFORMACE

1. No dealy in the previous demo