Hybrid Context-Sensitivity for Points-To Analysis

(gkastrinis@di.uoa.gr) George Kastrinis & Yannis Smaragdakis (smaragd@di.uoa.gr)

i → **■**, **△**

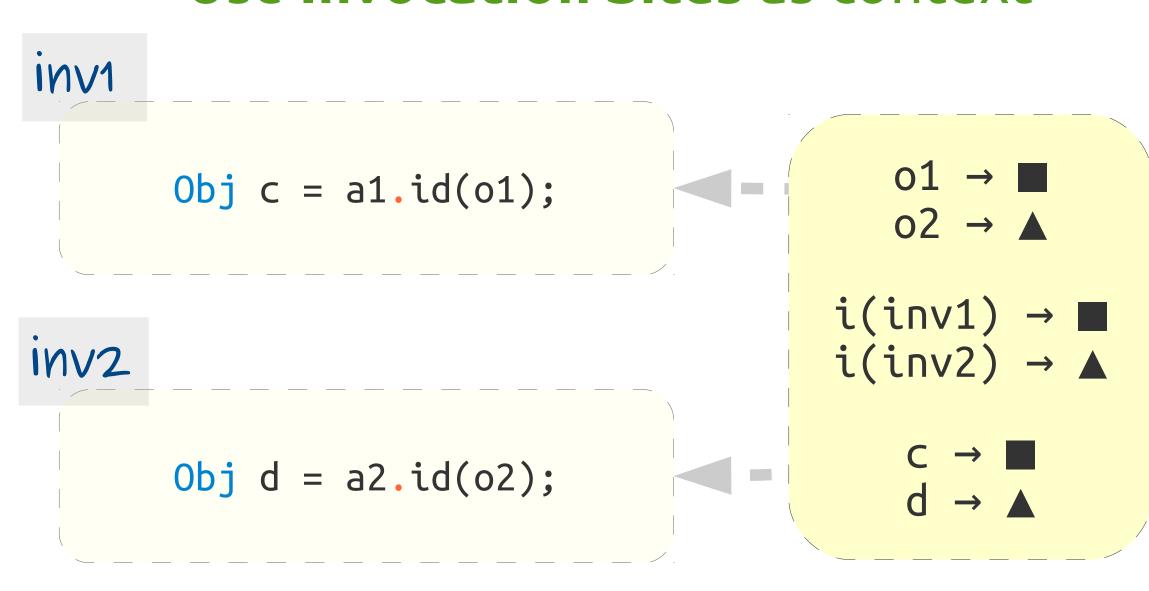
C → ■, ▲

d → **■**, **△**

How to combine Call-Site and Object-Sensitivity for better pointer analysis

Call-Site Sensitivity

Use **Invocation Sites** as context



Points-To Analysis

What objects may a variable point to?

```
class A {
 Obj id(Obj i) {return i;}
  void bar (A a1, A a2) {
   Obj o1 = new ■
   Obj c = a1.id(o1);
    Obj o2 = new ▲
    0bj d = a2.id(o2);
```

Object Sensitivity

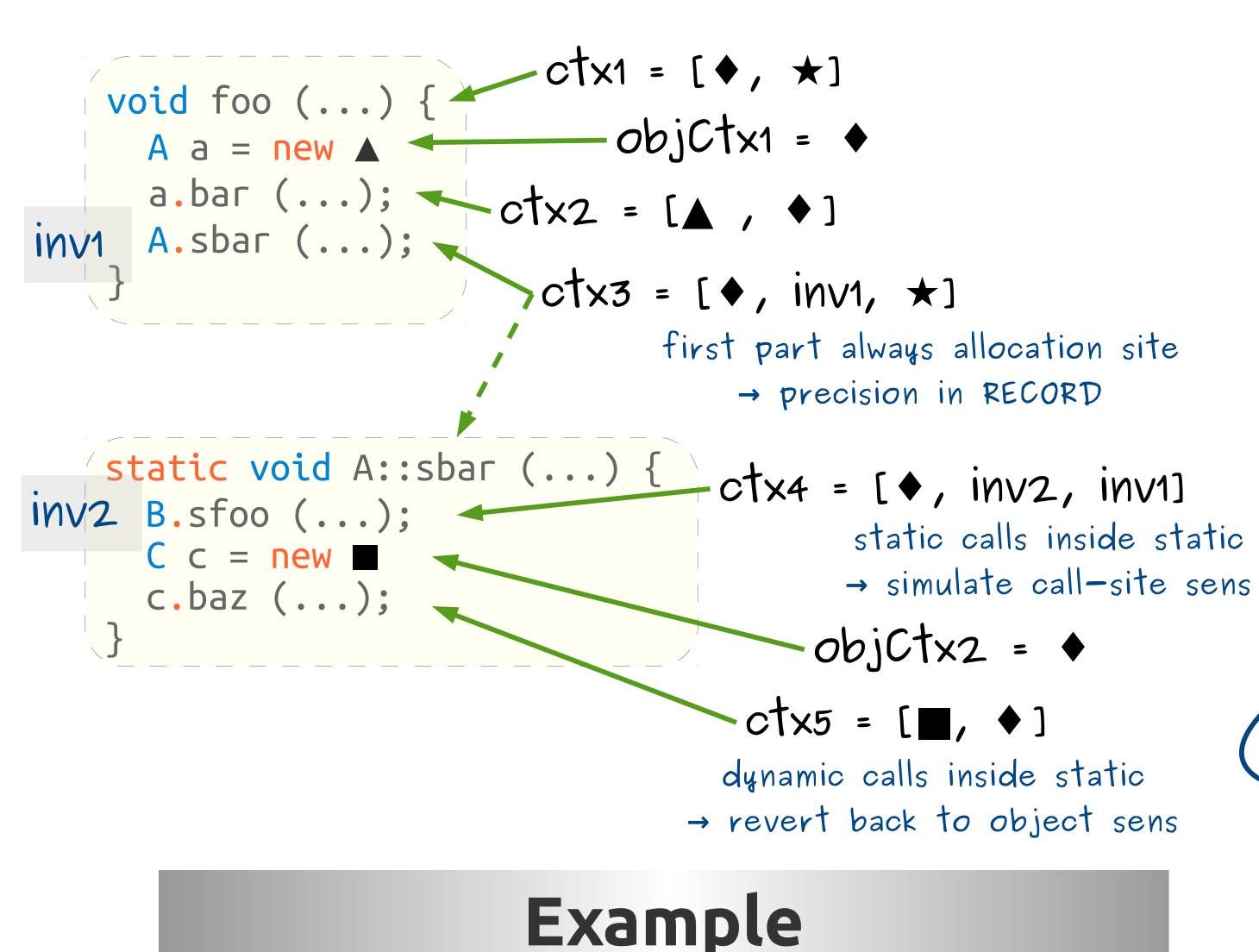
University

of ATHENS

Use Allocation Site of receiver as context

```
01 → ■
                                                  02 → ▲
                                                i(★) → ■
a2 \rightarrow \star, \diamond
                                                i(★) → ▲
                                                i(♦) → ▲
         Obj d = a2.id(o2);
                                                C → ■, ▲
                                                   d \rightarrow \blacktriangle
```





Hybrid Context-Sensitivity

Naively keeping both context kinds -> quickly non-scalable

(Favor) each kind in different places e.g. Call-Site-Sens for static methods

Virtual Methods

```
Object Allocation
RECORD (...) = first(ctx)
MERGE (...) = [obj, objCtx]
```

MERGESTATIC (...) = [first(ctx), invo, second(ctx)] - Static Methods

Context Constructors

Selective 2-Object Sensitive +1-Heap

Experiments

