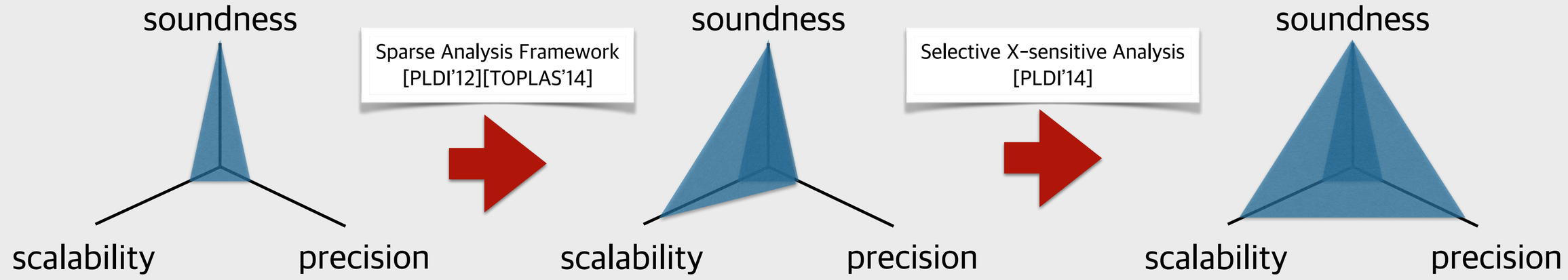
Sound, Precise & Scalable Static Analysis by Sparsity and Selectivity

Kihong Heo, Hakjoo Oh, Kwangkeun Yi
Seoul National University

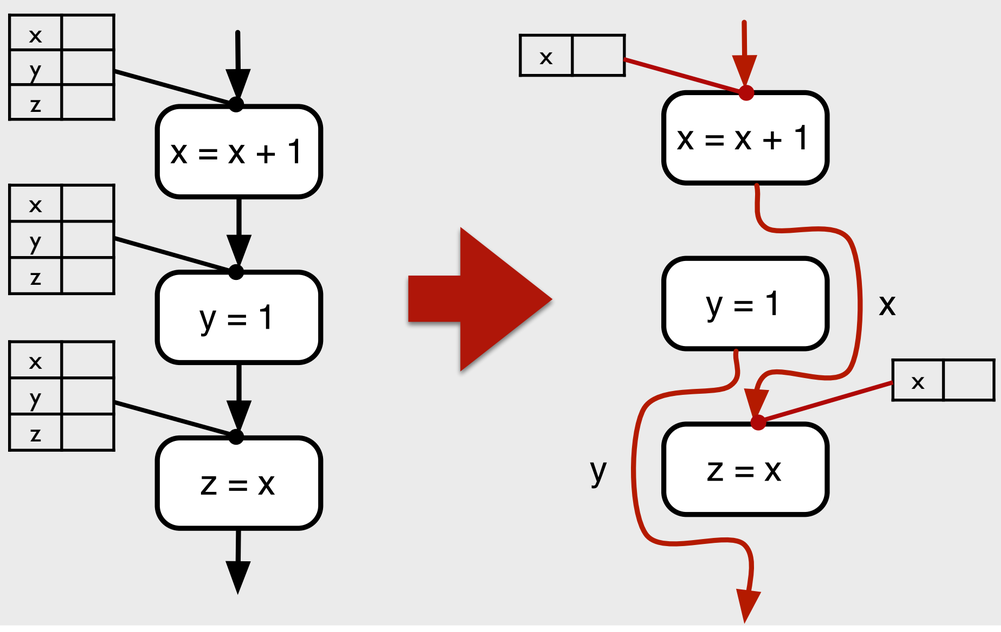
1. Goal

- Sound, precise, scalable and global static analyzer

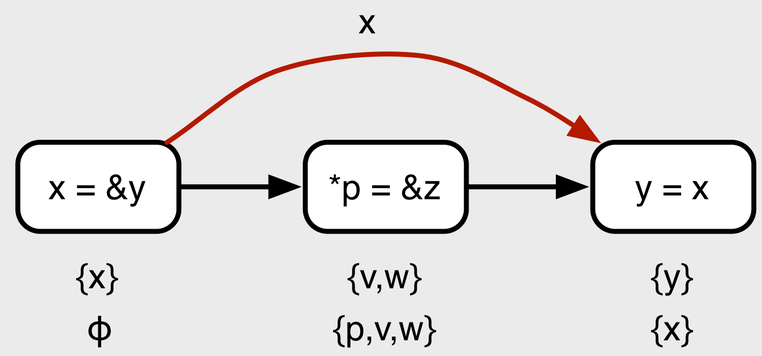


2. Sparse Analysis Framework

- Right Part at Right Moment



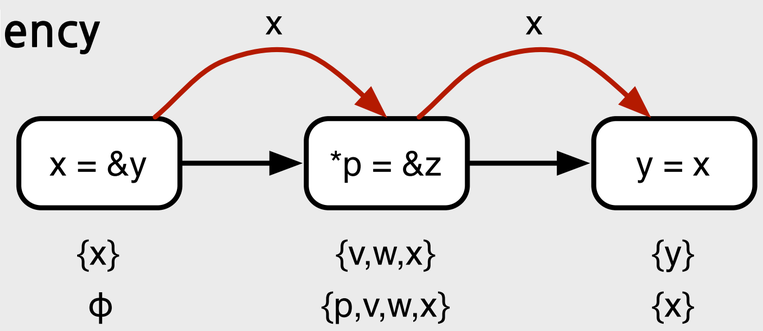
Data Dependency



Approx. Data Dependency

$\hat{D}(c) \supseteq D(c) \wedge \hat{U}(c) \supseteq U(c)$

$\hat{D}(c) - D(c) \subseteq \hat{U}(c)$



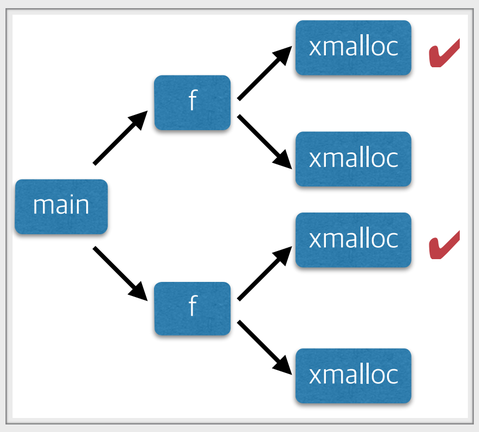
3. Selective X-sensitive Analysis

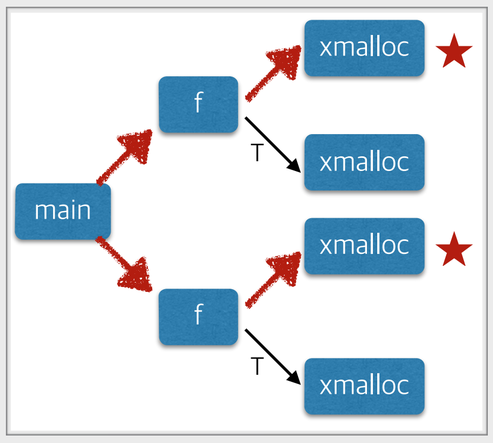
- X-sensitivity When Necessary

e.g.) X = context

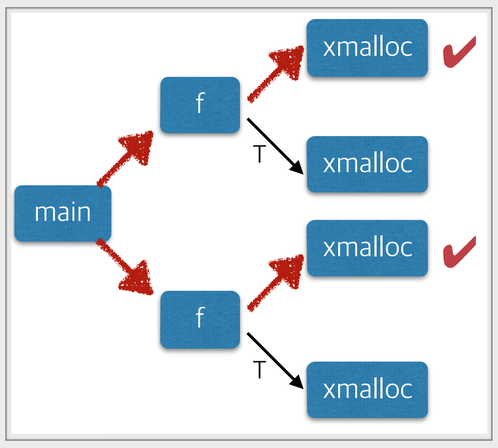
```
1  char* xmalloc (int n) {
2    return malloc(n);
3  }
4
5  void f (int size) {
6    p = xmalloc (size);
7    assert (sizeof(p) > 1); // Query 1
8    q = xmalloc (input());
9    assert (sizeof(q) > 1); // Query 2
10 }
11
12 int main() {
13   f (8);
14   f (16);
15 }
```

Fully context-sensitive analysis





Selective context-sensitive analysis



Impact pre-analysis : fully X-sensitive, yet abstract other semantic aspects. e.g.) interval analysis $\gamma_v(\top_v) = \mathbb{I}, \quad \gamma_v(\bigstar) = \{[a,b] \in \mathbb{I} \mid 0 \leq a\}, \quad \gamma_v(\bot_v) = \emptyset$

4. Experimental Results & Conclusion

- Sparrow, a industrial-strength static analyzer for C
  - 1 MLOC with interval domain in 10 hr, 100 KLOC with octagon domain in 20 hr by Sparse Analysis
  - 24.4% of false alarms are reduced, 27.8% overhead by Selective Context-sensitive Analysis

Programming Research Laboratory
SEOUL NATIONAL UNIVERSITY
ROSAEC center
Research On Software Analysis for Error-free Computing