

- Problems
 - alias, interprocedural
- Variations
 - flow sensitivity
 - context sensitivity
- Terminology
 - Steensgaard and Andersen algorithms
 - equality or subset based
 - data flow or type based formulation
 - **set constraint, parallel implementation**
- Extensions
 - escape analysis, shape analysis

2

Precision and Scalability

- Flow- and context-sensitive
 - 1992, Landi and Ryber, 3 KLOC
 - 1999, Whaley and Rinard, 80 KLOC
- Flow insensitive but context sensitive
 - 2004, Whaley and Lam, 600 KLOC, (based on BDDs)
- Flow- and context-insensitive
 - 1996, Steensgaard, 1+ MLOC
- Over a hundred papers published between 1995 and 2005
- Material in this part
 - Rayside MIT class report in 2005
 - illustrations and citations
 - <http://www.cs.washington.edu/homes/mernst/teaching/6.883/lectures/points-to.pdf>

3

An Example

```
p = malloc();
q = malloc();
fp = &p;
fp = &q;
... = *fp;
```

flow-insensitive, equality-based, eg Steensgaard [31]	
flow-insensitive, subset-based, eg Andersen [1]	
flow-sensitive	

Context

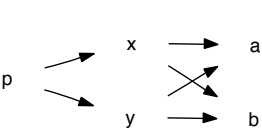
```
id(x) { return x; }
foo() {
  a = malloc();
  a = id(a);
}
bar() {
  b = malloc();
  b = id(b);
}
```

Flow-sensitive Analysis by Ryder

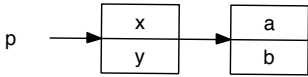
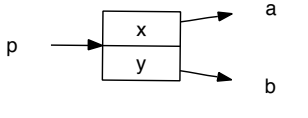
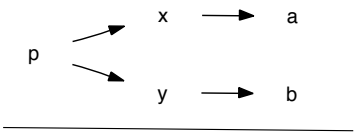
```
1. x = &a;
2. y = &b;
3. p = &x;
4. p = &y;
```

Flow-insensitive

- 1. `x = &a;`
- 2. `y = &b;`
- 3. `p = &x;`
- 4. `p = &y;`

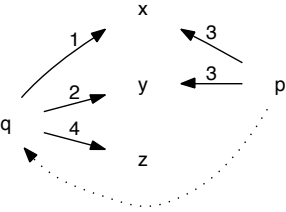


Subset-based
[Andersen'94]

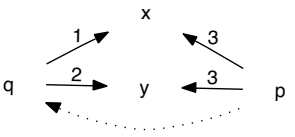
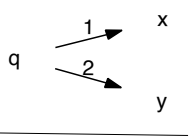
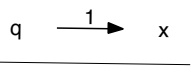


Equality-based [Steensgaard 1996]

```
q = &x;  
q = &y;  
p = q;  
q = &z;
```

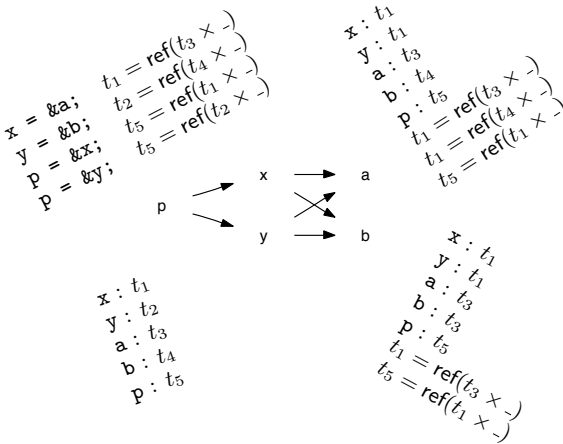


• Should p point to z too?



Flow-insensitive subset analysis [Andersen'94]

Type-based Formulation by Diwan



1.2 Axes of Precision

<i>less precise</i>	<i>more precise</i>
equivalence	subset/inclusion
flow-insensitive	flow-sensitive
context-insensitive	context-sensitive

Figure 1 A Brief History of Pointer Analysis [33] — focus on scalability and precision

	Equality-based	Subset-based	Flow-sensitive
Context-insensitive	• Wehl [32] 1980: < 1 KLOC first paper on pointer analysis • Steensgaard [31] 1996: 1+ MLOC first scalable pointer analysis	• Andersen [1] 1994: 5 KLOC • Fähndrich et al. [7] 1998: 60 KLOC • Heintze and Tardieu [11] 2001: 1 MLOC • Berndt et al. [2] 2003: 500 KLOC first to use BDDs	• Choi et al. [5] 1993: 30 KLOC
Context-sensitive	• Fähndrich et al. [8] 2000: 200K	• Whaley and Lam [35] 2004: 600 KLOC cloning-based BDDs	• Landi and Ryder [19] 1992: 3 KLOC • Wilson and Lam [37] 1995: 30 KLOC • Whaley and Rinard [36] 1999: 80 KLOC