



软件分析

过程内指针分析

熊英飞

北京大学



指向分析

- 每个指针变量可能指向的地址
- 通常是其他很多分析的基础

- 本节课先考虑流非敏感指向分析
- 先不考虑在堆上分配的内存，不考虑struct、数组等结构，不考虑指针运算（如 $*(p+1)$ ）
 - 地址==局部和全局变量在栈上的地址



指向分析——例子

```
o=&v;  
q=&p;  
if (a > b) {  
    p=*q;  
    p=o; }  
*q=&w;
```

- 指向分析结果

- $p = \{v, w\}$;
- $q = ?$
- $o = ?$

p : 变量p的地址
 p : 指针p所指向的集合



指向分析——例子

```
o=&v;  
q=&p;  
if (a > b) {  
    p=*q;  
    p=o; }  
*q=&w;
```

- 指向分析结果
 - $p = \{v, w\}$;
 - $q = \{p\}$;
 - $o = \{v\}$;
- 问题：如何设计一个指向分析算法？



复习：从不等式到方程组

- 有一个有用的解不等式的unification算法
 - 不等式
 - $D_{v_1} \supseteq F_{v_1}(D_{v_1}, D_{v_2}, \dots, D_{v_n})$
 - $D_{v_2} \supseteq F_{v_2}(D_{v_1}, D_{v_2}, \dots, D_{v_n})$
 - ...
 - $D_{v_n} \supseteq F_{v_n}(D_{v_1}, D_{v_2}, \dots, D_{v_n})$
 - 可以通过转换成如下方程组求解
 - $D_{v_1} = D_{v_1} \sqcup F_{v_1}(D_{v_1}, D_{v_2}, \dots, D_{v_n})$
 - $D_{v_2} = D_{v_2} \sqcup F_{v_2}(D_{v_1}, D_{v_2}, \dots, D_{v_n})$
 - ...
 - $D_{v_n} = D_{v_n} \sqcup F_{v_n}(D_{v_1}, D_{v_2}, \dots, D_{v_n})$




Anderson指向分析算法

赋值语句	约束
$a = \&b$	$a \supseteq \{b\}$
$a = b$	$a \supseteq b$
$a = *b$	$\forall v \in b. a \supseteq v$
$*a = b$	$\forall v \in a. v \supseteq b$

a : 变量 a 的地址
 a : 指针 a 所指向的集合

其他语句可以转换成这四种基本形式

$*a = **b;$  $c = *b;$
 $d = *c;$
 $*a = d;$



Anderson指向分析算法-例

```
o=&v;  
q=&p;  
if (a > b) {  
    p=*q;  
    p=o; }  
*q=&w;
```

- 产生约束
 - $o \supseteq \{v\}$
 - $q \supseteq \{p\}$
 - $\forall v \in q. p \supseteq v$
 - $p \supseteq o$
 - $\forall v \in q. v \supseteq \{w\}$
- 约束带全称量词，如何求解？



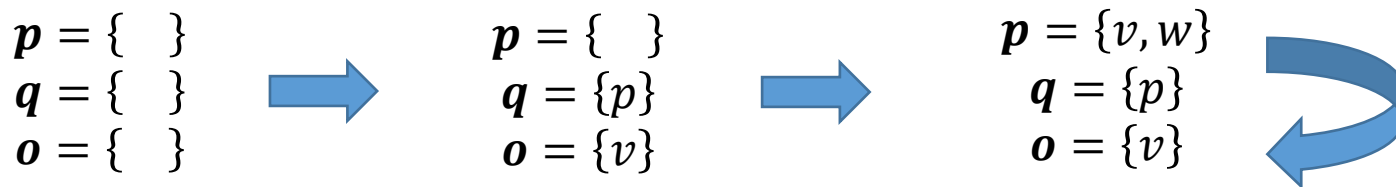
约束求解方法—通用框架

- 将约束
 - $\mathbf{o} \supseteq \{v\}$
 - $\mathbf{q} \supseteq \{p\}$
 - $\forall v \in \mathbf{q}. \mathbf{p} \supseteq v$
 - $\mathbf{p} \supseteq \mathbf{o}$
 - $\forall v \in \mathbf{q}. v \supseteq \{w\}$
- 转换成标准形式
 - $\mathbf{p} = \mathbf{p} \cup \mathbf{o} \cup (\cup_{v \in \mathbf{q}} v) \cup (p \in \mathbf{q} ? \{w\} : \emptyset)$
 - $\mathbf{q} = \mathbf{q} \cup \{p\} \cup (q \in \mathbf{q} ? \{w\} : \emptyset)$
 - $\mathbf{o} = \mathbf{o} \cup \{v\} \cup (o \in \mathbf{q} ? \{w\} : \emptyset)$
- 等号右边都是递增函数



求解方程组

- $p = p \cup o \cup (\cup_{v \in q} v) \cup (p \in q ? \{w\} : \emptyset)$
- $q = q \cup \{p\} \cup (q \in q ? \{w\} : \emptyset)$
- $o = o \cup \{v\} \cup (o \in q ? \{w\} : \emptyset)$

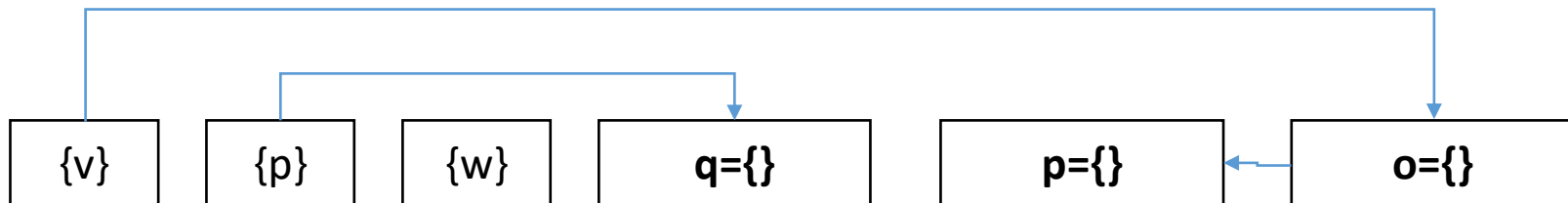


但每次都重新计算所有公式效率不高，
某个集合变化后，更新受影响的集合即可。



约束求解方法—直接计算

- $o \supseteq \{v\}$
- $q \supseteq \{p\}$
- $\forall v \in q. p \supseteq v$
- $p \supseteq o$
- $\forall v \in q. v \supseteq \{w\}$



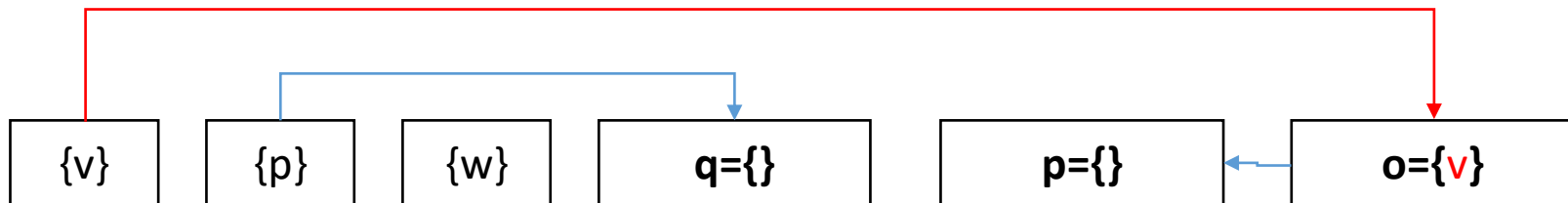
$$\forall v \in q. p \supseteq v$$

$$\forall v \in q. v \supseteq \{w\}$$



约束求解方法—直接计算

- $o \supseteq \{v\}$
- $q \supseteq \{p\}$
- $\forall v \in q. p \supseteq v$
- $p \supseteq o$
- $\forall v \in q. v \supseteq \{w\}$



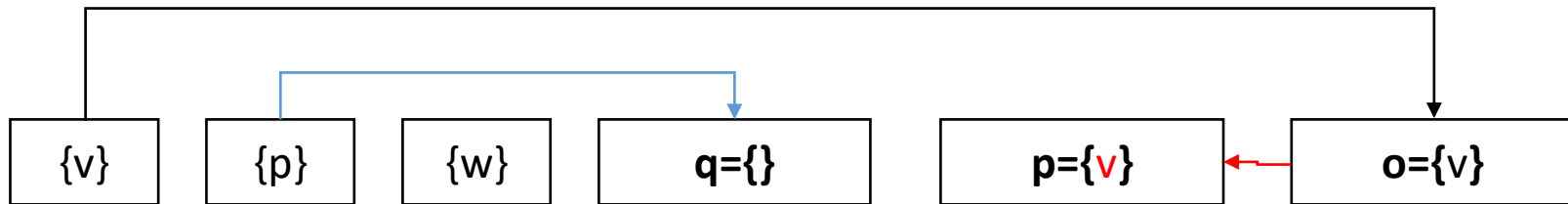
$$\forall v \in q. p \supseteq v$$

$$\forall v \in q. v \supseteq \{w\}$$



约束求解方法—直接计算

- $o \supseteq \{v\}$
- $q \supseteq \{p\}$
- $\forall v \in q. p \supseteq v$
- $p \supseteq o$
- $\forall v \in q. v \supseteq \{w\}$



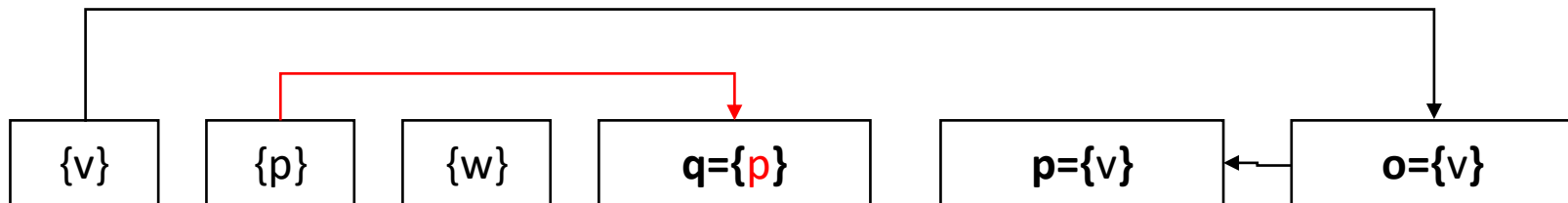
$$\forall v \in q. p \supseteq v$$

$$\forall v \in q. v \supseteq \{w\}$$



约束求解方法—直接计算

- $o \supseteq \{v\}$
- $q \supseteq \{p\}$
- $\forall v \in q. p \supseteq v$
- $p \supseteq o$
- $\forall v \in q. v \supseteq \{w\}$



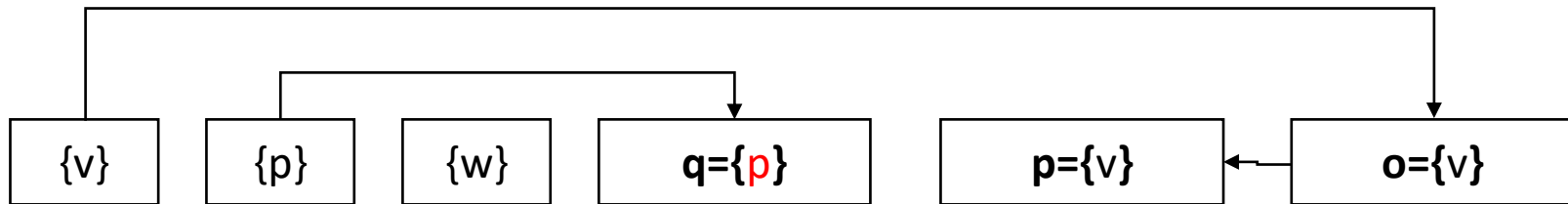
$$\forall v \in q. p \supseteq v$$

$$\forall v \in q. v \supseteq \{w\}$$



约束求解方法—直接计算

- $o \supseteq \{v\}$
- $q \supseteq \{p\}$
- $\forall v \in q. p \supseteq v$
- $p \supseteq o$
- $\forall v \in q. v \supseteq \{w\}$



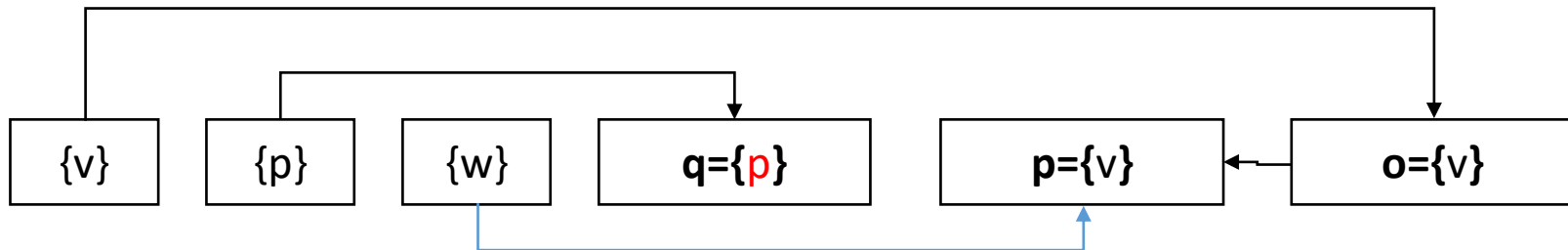
$$\forall v \in q. p \supseteq v$$

$$\forall v \in q. v \supseteq \{w\}$$



约束求解方法—直接计算

- $o \supseteq \{v\}$
- $q \supseteq \{p\}$
- $\forall v \in q. p \supseteq v$
- $p \supseteq o$
- $\forall v \in q. v \supseteq \{w\}$



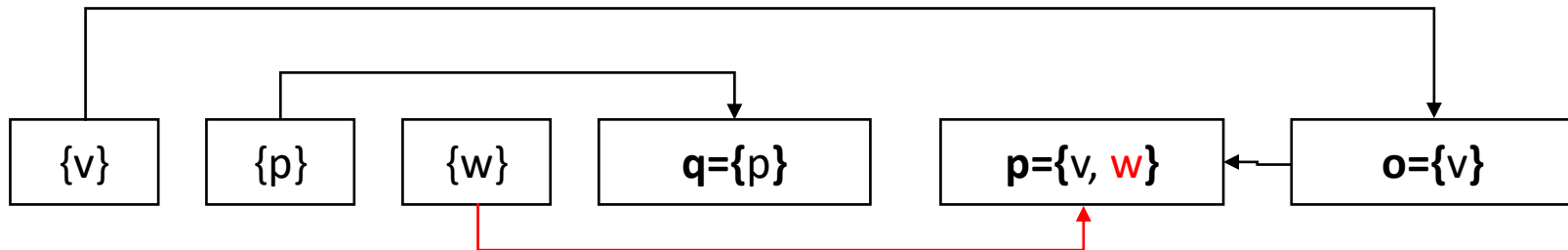
$$\forall v \in q. p \supseteq v$$

$$\forall v \in q. v \supseteq \{w\}$$



约束求解方法—直接计算

- $o \supseteq \{v\}$
- $q \supseteq \{p\}$
- $\forall v \in q. p \supseteq v$
- $p \supseteq o$
- $\forall v \in q. v \supseteq \{w\}$



$$\forall v \in q. p \supseteq v$$

$$\forall v \in q. v \supseteq \{w\}$$



复杂度分析

- 对于每条边来说，前驱集合新增元素的时候该边将被激活，激活后执行时间为 $O(m)$ ，其中 m 为新增的元素数量
 - 应用均摊分析，每条边传递的总复杂度为 $O(n)$ ，其中 n 为结点数量
- 边的数量为 $O(n^2)$
- 总复杂度为 $O(n^3)$



进一步优化

- 强连通子图中的每个集合必然相等
- 动态检测图中的强连通子图，并且合并成一个集合



流敏感的指针分析算法

- 如何把Anderson算法转换成数据流分析?
 - 半格集合是什么?
 - 指针变量到地址集合的映射
 - 交汇操作是什么?
 - 对应地址集合取并
 - 四种基本操作对应的转换函数是什么?



流敏感的指针分析算法

赋值语句	转换函数
$a = \&b$	$f(V) = V[a \mapsto \{b\}]$
$a = b$	$f(V) = V[a \mapsto b]$
$a = *b$	$f(V) = V \left[a \mapsto \bigcup_{\forall v \in b} v \right]$
$*a = b$?



流敏感的指针分析算法

赋值语句	转换函数
$a = \&b$	$f(V) = V[a \mapsto \{b\}]$
$a = b$	$f(V) = V[a \mapsto b]$
$a = *b$	$f(V) = V \left[a \mapsto \bigcup_{\forall v \in b} v \right]$
$*a = b$	$f(V) = \begin{cases} \forall v \in a. V[v \mapsto b] & a = 1 \\ \forall v \in a. V[v \mapsto v \cup b] & a > 1 \end{cases}$

Strong Update Weak Update

注：这里不考虑变量没有被初始化的情况



流敏感的指针分析算法

- 流敏感的指针分析算法很慢
- 实践中常采用在SSA上的流非敏感分析，可以兼顾效率和精度
 - 也有结合SSA和流敏感分析的研究工作



堆上分配的内存

- `a=malloc();`
- `malloc()`语句每次执行创建一个地址
- 无法静态的知道`malloc`语句被执行多少次
 - 无法定义出有限半格
- 应用抽象的思想
 - 每个`malloc()`创建一个抽象地址
 - `a=malloc(); //1`
 - $f(V) = V[\mathbf{a} \mapsto \{1\}]$



Struct

```
Struct Node {  
    int value;  
    Node* next;  
    Node* prev;  
};
```

```
a = malloc();  
a->next = b;  
a->prev = c;
```

- 如何处理结构体的指针分析?
- 域非敏感Field-Insensitive分析
- 基于域的Field-Based分析
- 域敏感Field-sensitive分析

域非敏感Field-Insensitive分析



```
Struct Node {  
    int value;  
    Node* next;  
    Node* prev;  
};
```

```
a = malloc();  
a->next = b;  
a->prev = c;
```

- 把所有struct中的所有fields当成一个对象
- 原程序变为
 - a'=malloc();
 - a'=b;
 - a'=c;
 - 其中a'代表a, a->next, a->prev
- 分析结果
 - a, a->next, a->prev都有可能指向malloc(), b和c



基于域的Field-Based分析

```
Struct Node {  
    int value;  
    Node* next;  
    Node* prev;  
};  
a = malloc();  
a->next = b;  
a->prev = c;  
b = malloc();  
b->next = c;
```

- 把所有对象的特定域当成一个对象
- 原程序变为
 - a=malloc();
 - next=b;
 - prev=c;
 - b=malloc();
 - next = c;
- 分析结果
 - a和a->prev是精确的，但a->next和b->next都指向b和c



域敏感Field-sensitive分析

```
Struct Node {  
    int value;  
    Node* next;  
    Node* prev;  
};
```

```
a = malloc();  
a->next = b;  
a->prev = c;
```

- 对于Node类型的地址x，添加两个指针变量
 - x.next
 - x.prev
- 对于任何Node类型的地址x，拆分成四个地址
 - x
 - x.value
 - x.next
 - x.prev
- a->next = b转换成
 - $\forall x \in a, x.next \supseteq b$



Java上的指向分析

- Java上的指向分析可以看成是C上的子集

Java	C
<code>A a = new A();</code>	<code>A* a = malloc(sizeof(A));</code>
<code>a.next = b</code>	<code>a->next = b</code>
<code>b = a.next</code>	<code>b = a->next</code>



别名分析

- 给定两个变量 a, b ，判断这两个变量是否指向相同的地址，返回以下结果之一
 - a, b 是 must aliases: 始终指向同样的位置
 - a, b 是 must-not aliases: 始终不指向同样的位置
 - a, b 是 may aliases: 可能指向同样的位置，也可能不指向
- 别名分析结果可以从指向分析导出
 - 如果 $a=b$ 且 $|a|=1$ ，则 a 和 b 为 must aliases
 - 如果 $a \cap b = \emptyset$ ，则 a 和 b 为 must-not aliases
 - 否则 a 和 b 为 may aliases
- 别名分析实践中常直接从指向分析导出



数组

- 数组粉碎：用一个抽象值描述数组中所有元素
 - 最简单，被广泛用于指针分析
- 数组扩展：对数组的每一维建立一个变量保存抽象值
 - 抽象域必须要推出下标（如区间），否则没有意义
 - 可只针对前k个变量建立，可以加快分析速度，也可以处理数组大小未知的情况



数组

- 数组分区：抽象为从索引区间到抽象值的映射
 - 执行 `int a[100]`，初始化 $a: \{[0,99] \rightarrow \perp\}$
 - 执行 `a[i]=5`，其中 i 的抽象值是 $[2,5]$
 - $a: \{[0,1] \rightarrow \perp, [2,5] \rightarrow [5,5], [6,99] \rightarrow \perp\}$
 - 执行 `a[j]=3`，其中 j 的抽象值是 $[5,6]$
 - $a: \{[0,1] \rightarrow \perp, [2,4] \rightarrow [5,5], [5,5] \rightarrow [3,5], [6,6] \rightarrow [3,3], [7,99] \rightarrow \perp\}$
 - 注意需要执行弱更新
 - 抽象域必须要推出下标
 - 同时上界可以增加 ∞ 处理大小未知的情况



指针运算

- 大多数实践中的分析工具不支持指针运算
 - 如果有指针运算，则直接返回unsound的结果。比如返回运算中第一个指针所指的值得值
- 部分分析针对特定形式的指针运算做处理
 - 如果指针运算是 $*(p+exp)$ 的形式的话，指针运算本质上和数组访问是一回事



参考文献

- Lecture Notes on Pointer Analysis
 - Jonathan Aldrich
 - <https://www.cs.cmu.edu/~aldrich/courses/15-8190-13sp/resources/pointer.pdf>
- 《编译原理》 12章