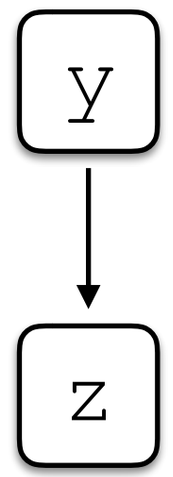
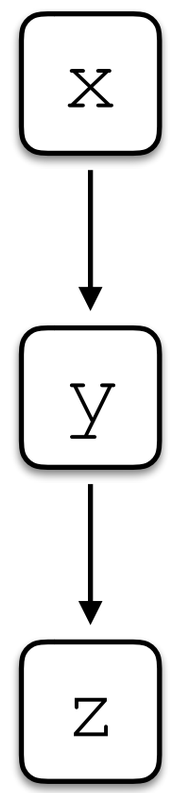
Points-to Analysis

```
y = &z;
```



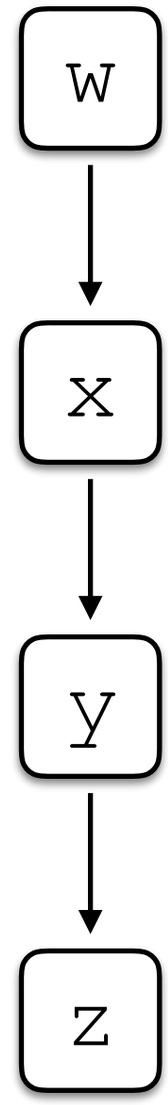
Points-to Analysis

```
y = &z;
x = &y;
```



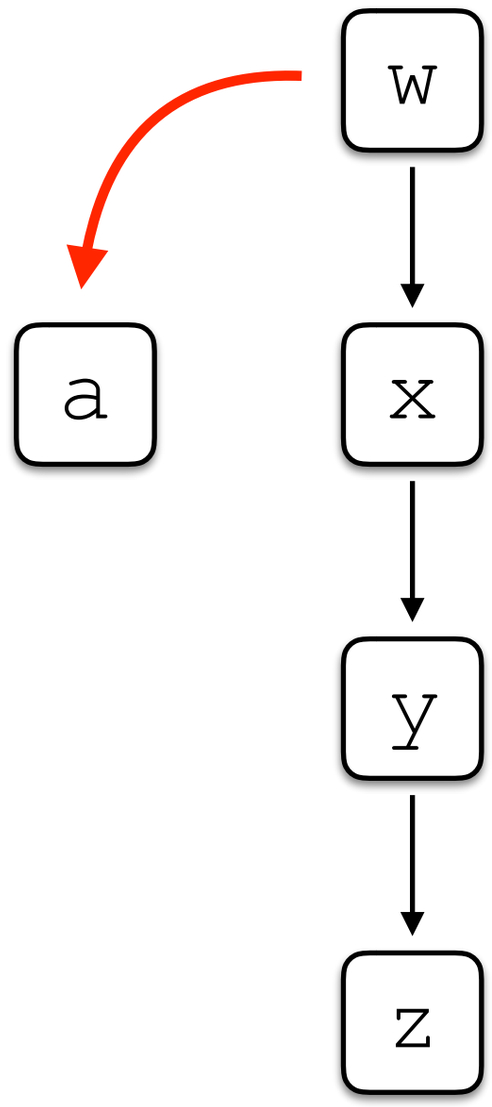
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
```



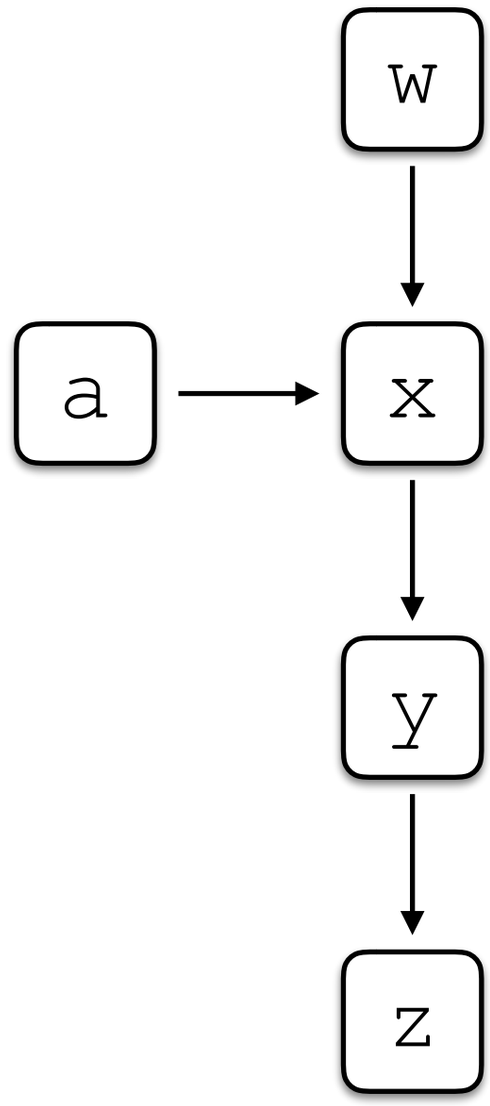
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
a = w;
```



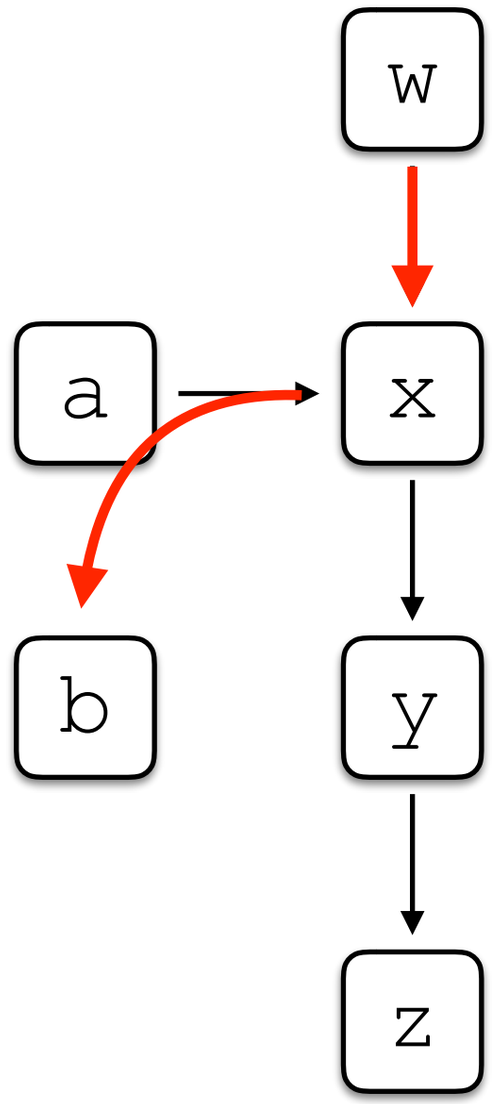
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
a = w;
```



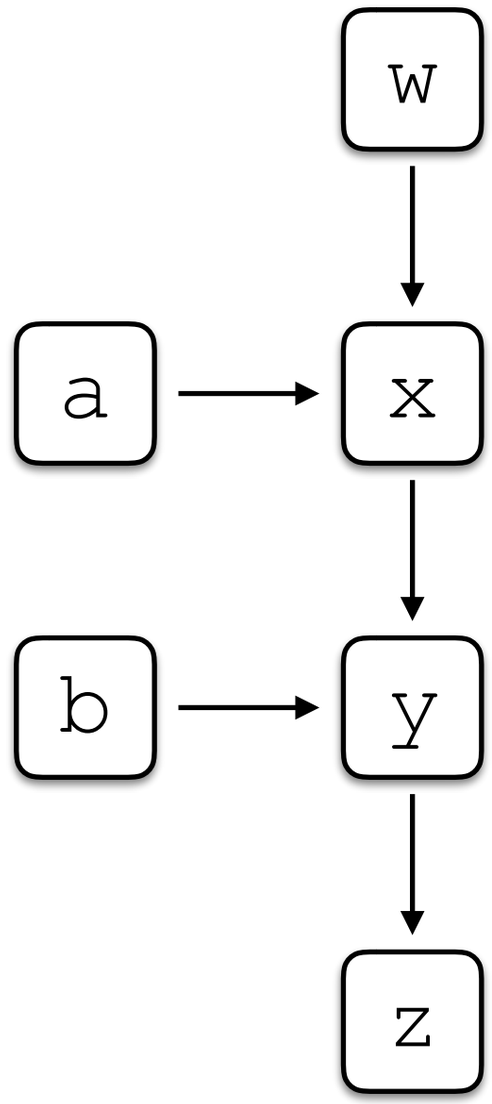
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
a = w;
b = *w;
```



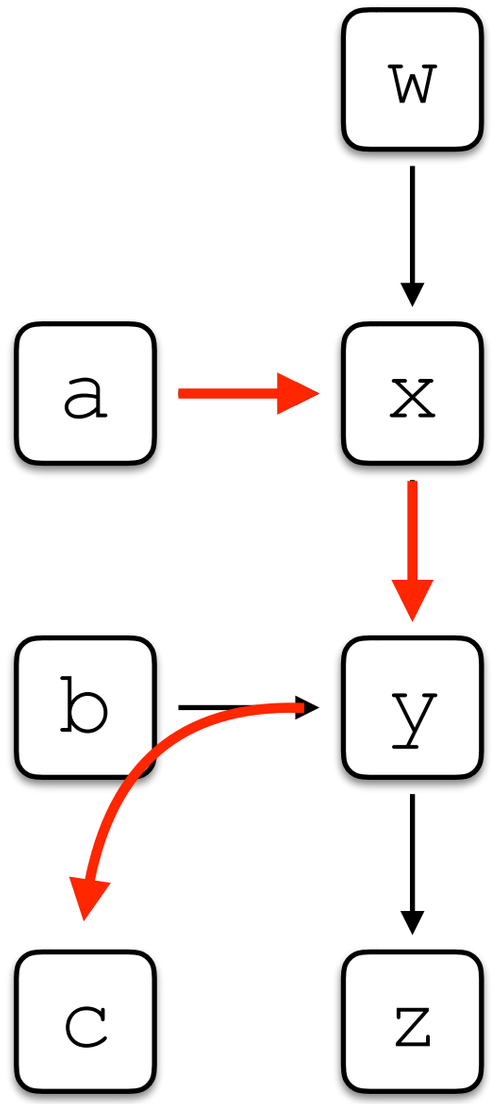
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
a = w;
b = *w;
```



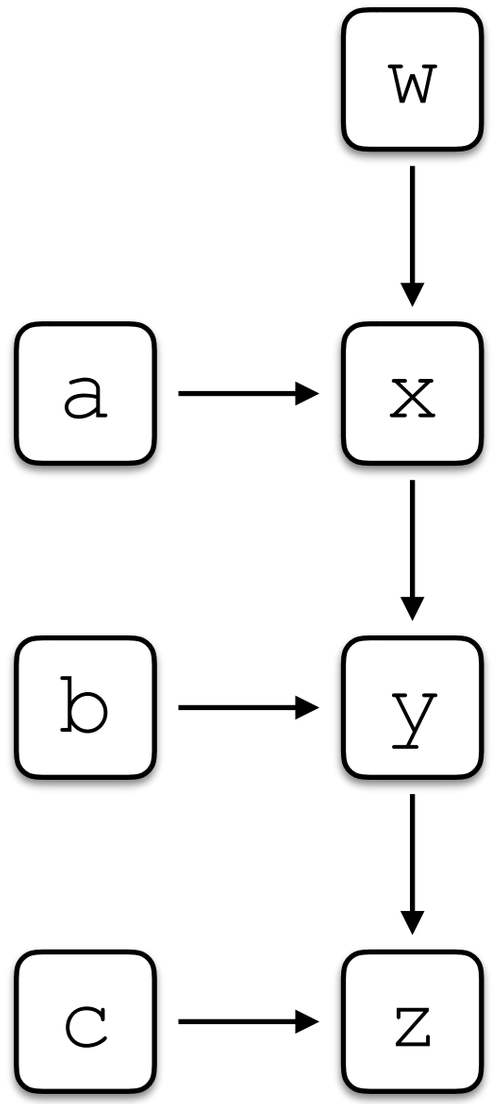
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
a = w;
b = *w;
c = **a;
```



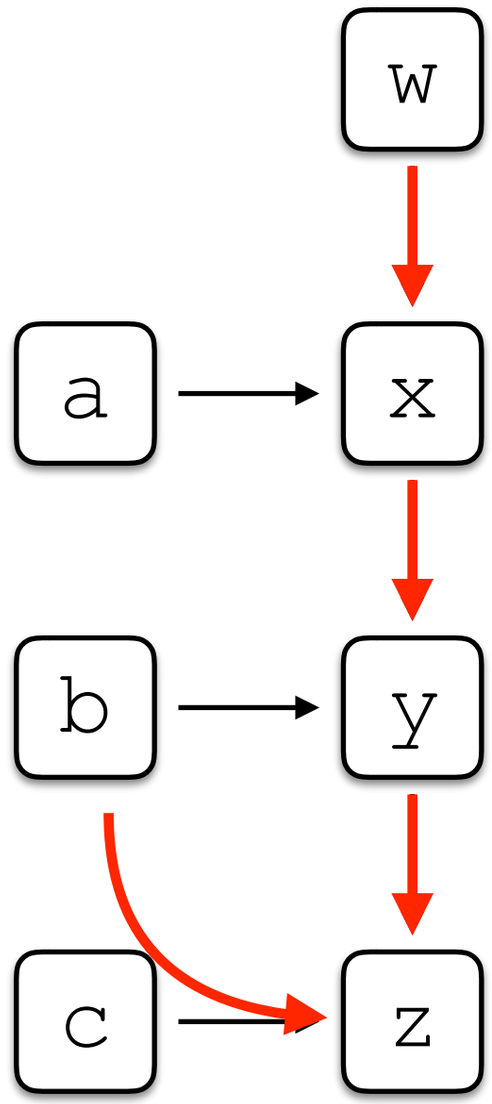
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
a = w;
b = *w;
c = **a;
```



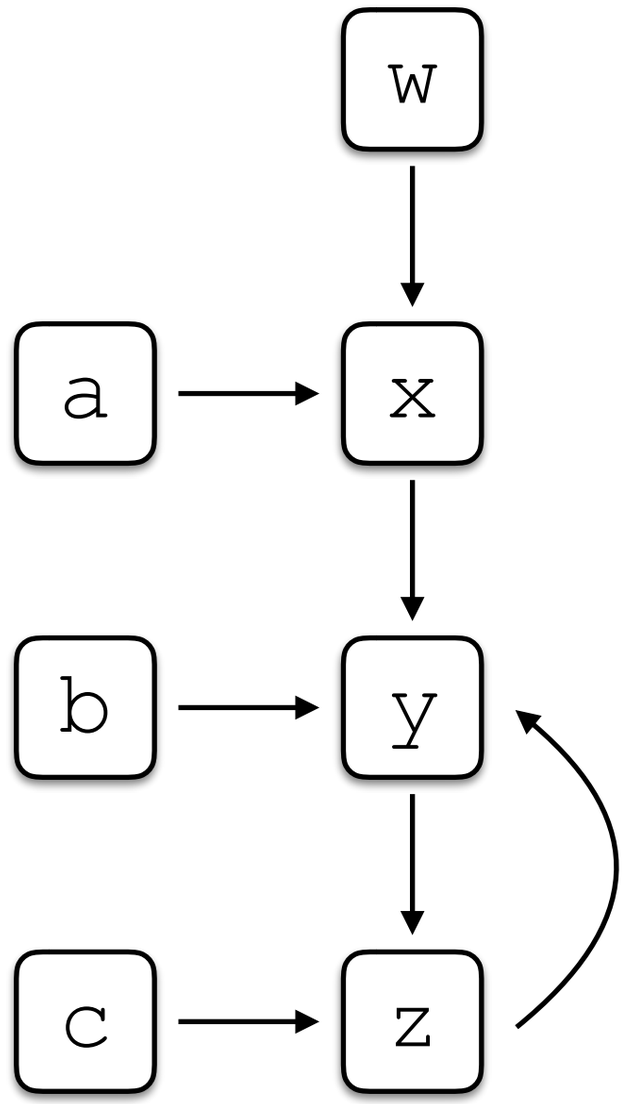
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
a = w;
b = *w;
c = **a;
***w = b;
```



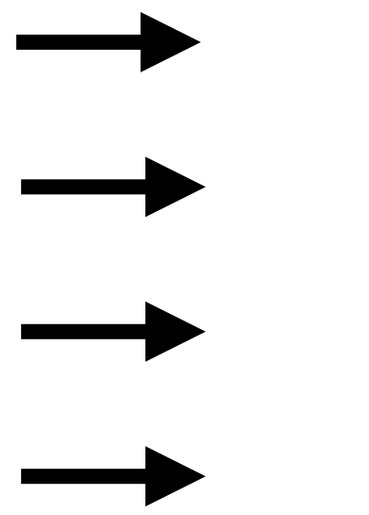
Points-to Analysis

```
y = &z;
x = &y;
w = &x;
a = w;
b = *w;
c = **a;
***w = b;
```



Andersen Example

```
a = &b;
c = a;
a = &d;
e = a;
```



$pt(a) \supseteq \{b\}$

$pt(c) \supseteq pt(a)$

$pt(a) \supseteq \{d\}$

$pt(e) \supseteq pt(a)$

pt(a) = {}

pt(b) = {}

pt(c) = {}

pt(d) = {}

pt(e) = {}

Andersen Example

```
a = &b;
c = a;
a = &d;
e = a;
```

→ *pt(a)* ⊇ {*b*}

→ *pt(c)* ⊇ *pt(a)*

→ *pt(a)* ⊇ {*d*}

→ *pt(e)* ⊇ *pt(a)*

pt(a) = {b}

pt(b) = {}

pt(c) = {}

pt(d) = {}

pt(e) = {}

Andersen Example

```
a = &b;
c = a;
a = &d;
e = a;
```

→ *pt(a)* ⊇ {*b*}

→ *pt(c)* ⊇ *pt(a)*

→ *pt(a)* ⊇ {*d*}

→ *pt(e)* ⊇ *pt(a)*

pt(a) = {b}

pt(b) = {}

pt(c) = {b}

pt(d) = {}

pt(e) = {}

Andersen Example

`a = &b;`	→	$pt(a) \supseteq \{b\}$
`c = a;`	→	$pt(c) \supseteq pt(a)$
`a = &d;`	→	$pt(a) \supseteq \{d\}$
`e = a;`	→	$pt(e) \supseteq pt(a)$

pt(a) = {b,d}

pt(c) = {b}

pt(b) = {}

pt(d) = {}

pt(e) = {}

Andersen Example

```
a = &b;
c = a;
a = &d;
e = a;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq pt(a)$

$\rightarrow$ $pt(a) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq pt(a)$

pt(a) = {b,d}

pt(c) = {b}

pt(b) = {}

pt(d) = {}

pt(e) = {b,d}

Andersen Example

End of first iteration

pt(a) = {b,d}

pt(b) = {}

pt(c) = {b}

pt(d) = {}

pt(e) = {b,d}

Andersen Example

```
a = &b;
c = a;
a = &d;
e = a;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq pt(a)$

$\rightarrow$ $pt(a) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq pt(a)$

pt(a) = {b,d}

pt(c) = {b}

pt(b) = {}

pt(d) = {}

pt(e) = {b,d}

Andersen Example

```
a = &b;
c = a;
a = &d;
e = a;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq pt(a)$

$\rightarrow$ $pt(a) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq pt(a)$

pt(a) = {b,d}

pt(c) = {b,d}

pt(b) = {}

pt(d) = {}

pt(e) = {b,d}

Andersen Example

```
a = &b;
c = a;
a = &d;
e = a;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq pt(a)$

$\rightarrow$ $pt(a) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq pt(a)$

pt(a) = {b,d}

pt(c) = {b,d}

pt(b) = {}

pt(d) = {}

pt(e) = {b,d}

Andersen Example

```
a = &b;
c = a;
a = &d;
e = a;
```

→ *pt(a)* ⊇ {*b*}

→ *pt(c)* ⊇ *pt(a)*

→ *pt(a)* ⊇ {*d*}

→ *pt(e)* ⊇ *pt(a)*

pt(a) = {b,d}

pt(c) = {b,d}

pt(b) = {}

pt(d) = {}

pt(e) = {b,d}

Andersen Example

End of second iteration

(finished)

pt(a) = {b,d}

pt(b) = {}

pt(c) = {b,d}

pt(d) = {}

pt(e) = {b,d}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq \{a\}$

$\rightarrow$ $pt(f) \supseteq pt(a)$

$\rightarrow$ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

pt(a) = {}

pt(b) = {}

pt(c) = {}

pt(d) = {}

pt(e) = {}

pt(f) = {}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq \{a\}$

$\rightarrow$ $pt(f) \supseteq pt(a)$

$\rightarrow$ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

pt(a) = {b}

pt(b) = {}

pt(c) = {}

pt(d) = {}

pt(e) = {}

pt(f) = {}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq \{a\}$

$\rightarrow$ $pt(f) \supseteq pt(a)$

$\rightarrow$ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

pt(a) = {b}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {}

pt(f) = {}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq \{a\}$

$\rightarrow$ $pt(f) \supseteq pt(a)$

$\rightarrow$ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

pt(a) = {b}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {}

Andersen Example (2)

`a = &b;`	→	$pt(a) \supseteq \{b\}$
`c = &d;`	→	$pt(c) \supseteq \{d\}$
`e = &a;`	→	$pt(e) \supseteq \{a\}$
`f = a;`	→	$pt(f) \supseteq pt(a)$
`*e = c;`	→	$pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

pt(a) = {b}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$$a = \&b; \rightarrow pt(a) \supseteq \{b\}$$

$$c = \&d; \rightarrow pt(c) \supseteq \{d\}$$

$$e = \&a; \rightarrow pt(e) \supseteq \{a\}$$

$$f = a; \rightarrow pt(f) \supseteq pt(a)$$

$$*e = c; \rightarrow pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$$

$$pt(a) \supseteq pt(c)$$

pt(a) = {b,d}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b}

Andersen Example (2)

End of first iteration

pt(a) = {b,d}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq \{a\}$

$\rightarrow$ $pt(f) \supseteq pt(a)$

$\rightarrow$ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

$pt(a) \supseteq pt(c)$

pt(a) = {b,d}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq \{a\}$

$\rightarrow$ $pt(f) \supseteq pt(a)$

$\rightarrow$ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

$pt(a) \supseteq pt(c)$

pt(a) = {b,d}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq \{a\}$

$\rightarrow$ $pt(f) \supseteq pt(a)$

$\rightarrow$ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

$pt(a) \supseteq pt(c)$

pt(a) = {b,d}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
```

$\rightarrow$ $pt(a) \supseteq \{b\}$

$\rightarrow$ $pt(c) \supseteq \{d\}$

$\rightarrow$ $pt(e) \supseteq \{a\}$

```
f = a;
```

$\rightarrow$ $pt(f) \supseteq pt(a)$

```
*e = c;
```

$\rightarrow$ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

$pt(a) \supseteq pt(c)$

pt(a) = {b,d}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b,d}

Andersen Example (2)

```
a = &b;
c = &d;
e = &a;
f = a;
*e = c;
```

$$a = \&b; \rightarrow pt(a) \supseteq \{b\}$$

$$c = \&d; \rightarrow pt(c) \supseteq \{d\}$$

$$e = \&a; \rightarrow pt(e) \supseteq \{a\}$$

$$f = a; \rightarrow pt(f) \supseteq pt(a)$$

$$*e = c; \rightarrow pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$$

$$pt(a) \supseteq pt(c)$$

pt(a) = {b,d}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b,d}

Andersen Example (2)

End of second iteration (finished)

pt(a) = {b,d}

pt(b) = {}

pt(c) = {d}

pt(d) = {}

pt(e) = {a}

pt(f) = {b,d}