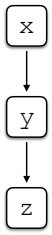
Points-to Analysis

```
y = &z;
```

Points-to Analysis

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

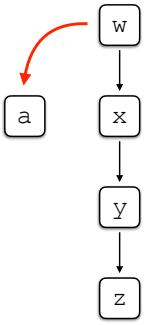


Points-to Analysis

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

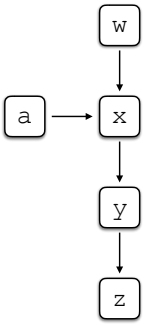
Points-to Analysis

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



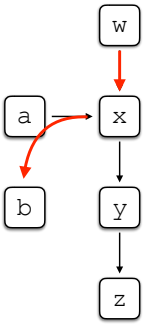
Points-to Analysis

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



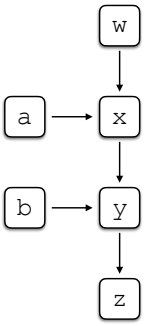
Points-to Analysis

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



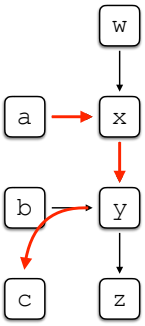
Points-to Analysis

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



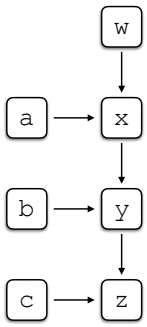
Points-to Analysis

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



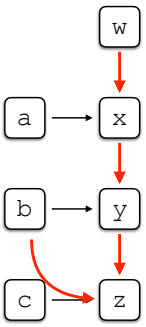
Points-to Analysis

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



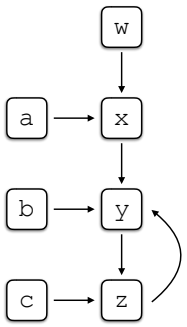
Points-to Analysis

```
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;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  pt(e) ⊇ pt(a)
```

pt(a) = {} pt(c) = {}
pt(b) = {} pt(d) = {}
pt(e) = {}

Andersen Example

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  pt(e) ⊇ pt(a)
```

pt(a) = {b} pt(c) = {}
pt(b) = {} pt(d) = {}
pt(e) = {}

Andersen Example

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  pt(e) ⊇ pt(a)
```

pt(a) = {b} pt(c) = {b}
pt(b) = {} pt(d) = {}
pt(e) = {}

Andersen Example

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  pt(e) ⊇ pt(a)
```

pt(a) = {b,d} pt(c) = {b}
pt(b) = {} pt(d) = {}
pt(e) = {}

Andersen Example

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  pt(e) ⊇ 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(c) = {b}
pt(b) = {} pt(d) = {}
pt(e) = {b,d}

Andersen Example

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  pt(e) ⊇ pt(a)
```

pt(a) = {b,d} pt(c) = {b}
pt(b) = {} pt(d) = {}
pt(e) = {b,d}

Andersen Example

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  pt(e) ⊇ pt(a)
```

pt(a) = {b,d} pt(c) = {b,d}
pt(b) = {} pt(d) = {}
pt(e) = {b,d}

Andersen Example

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  pt(e) ⊇ pt(a)
```

pt(a) = {b,d} pt(c) = {b,d}
pt(b) = {} pt(d) = {}
pt(e) = {b,d}

Andersen Example

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = a;    ⟶  pt(c) ⊇ pt(a)
a = &d;   ⟶  pt(a) ⊇ {d}
e = a;    ⟶  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(c) = {b,d}
pt(b) = {} pt(d) = {}
pt(e) = {b,d}

Andersen Example (2)

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = &d;   ⟶  pt(c) ⊇ {d}
e = &a;   ⟶  pt(e) ⊇ {a}
f = a;    ⟶  pt(f) ⊇ pt(a)
*e = c;   ⟶  pt(e) ⊇ {z} ⟹ pt(z) ⊇ pt(c)
```

pt(a) = {} pt(d) = {}
pt(b) = {} pt(e) = {}
pt(c) = {} pt(f) = {}

Andersen Example (2)

```
a = &b;   ⟶  pt(a) ⊇ {b}
c = &d;   ⟶  pt(c) ⊇ {d}
e = &a;   ⟶  pt(e) ⊇ {a}
f = a;    ⟶  pt(f) ⊇ pt(a)
*e = c;   ⟶  pt(e) ⊇ {z} ⟹ pt(z) ⊇ pt(c)
```

pt(a) = {b} pt(d) = {}
pt(b) = {} pt(e) = {}
pt(c) = {} pt(f) = {}

Andersen Example (2)

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

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

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;
```

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

pt(a) = {b}
pt(b) = {}
pt(c) = {d}
pt(d) = {}
pt(e) = {a}
pt(f) = {}

Andersen Example (2)

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

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$

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;
```

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$
$pt(a) \supseteq pt(c)$

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;
```

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$
$pt(a) \supseteq pt(c)$

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;
```

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$
$pt(a) \supseteq pt(c)$

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;
```

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$
$pt(a) \supseteq pt(c)$

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;
```

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$
$pt(a) \supseteq pt(c)$

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;
```

→ $pt(a) \supseteq \{b\}$
→ $pt(c) \supseteq \{d\}$
→ $pt(e) \supseteq \{a\}$
→ $pt(f) \supseteq pt(a)$
→ $pt(e) \supseteq \{z\} \Longrightarrow pt(z) \supseteq pt(c)$
$pt(a) \supseteq pt(c)$

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}