

# Variable Declaration

**new**  $x$ :  $T \cdot P$

# Variable Declaration

**new**  $x: T \cdot P$  declare local state variable  $x$  with type  $T$  and scope  $P$

# Variable Declaration

**new**  $x: T \cdot P$       declare local state variable  $x$  with type  $T$  and scope  $P$

=       $\exists x, x': T \cdot P$

# Variable Declaration

**new**  $x: T \cdot P$       declare local state variable  $x$  with type  $T$  and scope  $P$

=       $\exists x, x': T \cdot P$

**new**  $x: int \cdot x := 2. \ y := x + z$

# Variable Declaration

**new**  $x: T \cdot P$  declare local state variable  $x$  with type  $T$  and scope  $P$

$$= \exists x, x': T \cdot P$$

**new**  $x: int \cdot x := 2. \ y := x + z$

$$= \exists x, x': int \cdot x' = 2 \wedge y' = 2 + z \wedge z' = z$$

# Variable Declaration

|  |   |
|--|---|
| <b>new</b> $x: T \cdot P$                      | declare local state variable $x$ with type $T$ and scope $P$  |
| =  | $\exists x, x': T \cdot P$  |
| <br>   |   |
| <b>new</b> $x: int \cdot x := 2. \ y := x + z$ |   |
| =  | $\exists x, x': int \cdot x' = 2 \wedge y' = 2 + z \wedge z' = z$ one-point for $x'$ and idempotent for $x$ |
| =  | $y' = 2 + z \wedge z' = z$  |

# Variable Declaration

$$\begin{array}{ll} \mathbf{new} \ x: T \cdot P & \text{declare local state variable } x \text{ with type } T \text{ and scope } P \\ = & \exists x, x': T \cdot P \end{array}$$

$$\begin{array}{ll} \mathbf{new} \ x: \text{int} \cdot \ x := 2. \ y := x + z & \\ = & \exists x, x': \text{int} \cdot \ x' = 2 \ \wedge \ y' = 2 + z \ \wedge \ z' = z & \text{one-point for } x' \text{ and idempotent for } x \\ = & y' = 2 + z \ \wedge \ z' = z & \end{array}$$

$$\mathbf{new} \ x: \text{int} \cdot \ y := x$$

# Variable Declaration

$$\begin{array}{ll} \mathbf{new} \ x: T \cdot P & \text{declare local state variable } x \text{ with type } T \text{ and scope } P \\ = & \exists x, x': T \cdot P \end{array}$$

$$\begin{array}{ll} \mathbf{new} \ x: int \cdot \ x:=2. \ y:=x+z & \\ = & \exists x, x': int \cdot \ x'=2 \wedge y'=2+z \wedge z'=z & \text{one-point for } x' \text{ and idempotent for } x \\ = & y'=2+z \wedge z'=z & \end{array}$$

$$\begin{array}{ll} \mathbf{new} \ x: int \cdot \ y:=x & \\ = & \exists x, x': int \cdot \ x'=x \wedge y'=x \wedge z'=z & \end{array}$$

# Variable Declaration

|   |   |
|---|---|
| <b>new</b> $x: T \cdot P$                         | declare local state variable $x$ with type $T$ and scope $P$  |
| =   | $\exists x, x': T \cdot P$  |
| <br>  |   |
| <b>new</b> $x: int \cdot x := 2 \cdot y := x + z$ |   |
| =   | $\exists x, x': int \cdot x' = 2 \wedge y' = 2 + z \wedge z' = z$ one-point for $x'$ and idempotent for $x$ |
| =   | $y' = 2 + z \wedge z' = z$  |
| <br>  |   |
| <b>new</b> $x: int \cdot y := x$                  |   |
| =   | $\exists x, x': int \cdot x' = x \wedge y' = x \wedge z' = z$ one-point for $x$ and $x'$                    |
| =   | $z' = z$  |

# Variable Declaration

|  |   |
|--|---|
| <b>new</b> $x: T \cdot P$                          | declare local state variable $x$ with type $T$ and scope $P$  |
| =  | $\exists x, x': T \cdot P$  |
| <br>   |   |
| <b>new</b> $x: int \cdot x := 2. \quad y := x + z$ |   |
| =  | $\exists x, x': int \cdot x' = 2 \wedge y' = 2 + z \wedge z' = z$ one-point for $x'$ and idempotent for $x$ |
| =  | $y' = 2 + z \wedge z' = z$  |
| <br>   |   |
| <b>new</b> $x: int \cdot y := x$                   |   |
| =  | $\exists x, x': int \cdot x' = x \wedge y' = x \wedge z' = z$ one-point for $x$ and $x'$                    |
| =  | $z' = z$  |
| <br>   |   |
| <b>new</b> $x: int \cdot y := x - x$               |   |

# Variable Declaration

$$\begin{array}{ll} \mathbf{new} \ x: T \cdot P & \text{declare local state variable } x \text{ with type } T \text{ and scope } P \\ = & \exists x, x': T \cdot P \end{array}$$

$$\begin{array}{ll} \mathbf{new} \ x: \text{int} \cdot \ x := 2. \ y := x + z & \\ = & \exists x, x': \text{int} \cdot \ x' = 2 \wedge y' = 2 + z \wedge z' = z & \text{one-point for } x' \text{ and idempotent for } x \\ = & y' = 2 + z \wedge z' = z & \end{array}$$

$$\begin{array}{ll} \mathbf{new} \ x: \text{int} \cdot \ y := x & \\ = & \exists x, x': \text{int} \cdot \ x' = x \wedge y' = x \wedge z' = z & \text{one-point for } x \text{ and } x' \\ = & z' = z & \end{array}$$

$$\begin{array}{ll} \mathbf{new} \ x: \text{int} \cdot \ y := x - x & \\ = & y' = 0 \wedge z' = z & \end{array}$$

# Variable Declaration

**new**  $x$ :  $T \cdot P$

# Variable Declaration

$$\begin{aligned} & \mathbf{new} \ x: T \cdot P \\ = & \quad \exists x: \text{undefined} \cdot \exists x': T, \text{undefined} \cdot P \end{aligned}$$

# Variable Declaration

$$\begin{aligned} & \mathbf{new} \ x: T \cdot P \\ = & \quad \exists x: \text{undefined} \cdot \exists x': T, \text{undefined} \cdot P \end{aligned}$$

$$\mathbf{new} \ x: T := e \cdot P$$

# Variable Declaration

$$\begin{aligned}\mathbf{new} \ x: T \cdot P \\ = & \quad \exists x: \text{undefined} \cdot \exists x': T, \text{undefined} \cdot P \\ \\ \mathbf{new} \ x: T := e \cdot P \\ = & \quad \exists x: e \cdot \exists x': T \cdot P\end{aligned}$$

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

**frame**  $w, x \cdot P$

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

$$\begin{array}{ll} \textbf{frame } w, x \cdot P & \text{within } P, y \text{ and } z \text{ are constants (no } y' \text{ and } z' \text{)} \\ = & P \wedge y'=y \wedge z'=z \end{array}$$

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

$$\begin{array}{ll} \mathbf{frame}\; w, x \cdot P & \text{within } P, y \text{ and } z \text{ are constants (no } y' \text{ and } z' \text{)} \\ = & P \wedge y'=y \wedge z'=z \end{array}$$

$$x := e \quad = \quad \mathbf{frame}\; x \cdot x' = e$$

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

$$\begin{array}{ll} \mathbf{frame}\; w, x \cdot P & \text{within } P, y \text{ and } z \text{ are constants (no } y' \text{ and } z' \text{)} \\ = & P \wedge y'=y \wedge z'=z \end{array}$$

$$x := e \quad = \quad \mathbf{frame}\; x \cdot x' = e$$

$$ok \quad = \quad \mathbf{frame} \cdot \top$$

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

$$\begin{array}{ll} \mathbf{frame}\; w, x \cdot P & \text{within } P, y \text{ and } z \text{ are constants (no } y' \text{ and } z' \text{)} \\ = & P \wedge y'=y \wedge z'=z \end{array}$$

$$x := e \quad = \quad \mathbf{frame}\; x \cdot x' = e$$

$$ok \quad = \quad \mathbf{frame} \cdot \top$$

$$s := \Sigma L$$

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

$$= P \wedge y' = y \wedge z' = z$$

$x := e \quad = \quad \mathbf{frame} \ x \cdot x' \equiv e$

*ok* = frame· $\top$

$s := \Sigma L$   $\Leftarrow$  frame  $s$ .

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

$$\begin{array}{ll} \mathbf{frame}\; w, x \cdot P & \text{within } P, y \text{ and } z \text{ are constants (no } y' \text{ and } z') \\ = & P \wedge y'=y \wedge z'=z \end{array}$$

$$x := e \quad = \quad \mathbf{frame}\; x \cdot x' = e$$

$$ok \quad = \quad \mathbf{frame} \cdot \top$$

$$s := \Sigma L \quad \Leftarrow \quad \mathbf{frame}\; s \cdot \mathbf{new}\; n : nat$$

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

$$\begin{array}{ll} \mathbf{frame}\; w, x \cdot P & \text{within } P, y \text{ and } z \text{ are constants (no } y' \text{ and } z') \\ = & P \wedge y'=y \wedge z'=z \end{array}$$

$$x := e \quad = \quad \mathbf{frame}\; x \cdot x' = e$$

$$ok \quad = \quad \mathbf{frame} \cdot \top$$

$$s := \Sigma L \iff \mathbf{frame}\; s \cdot \mathbf{new}\; n: nat \cdot s' = \Sigma L$$

# Variable Suspension

Suppose the state consists of variables  $w$ ,  $x$ ,  $y$ , and  $z$ .

$$\begin{array}{ll} \mathbf{frame}\; w, x \cdot P & \text{within } P, y \text{ and } z \text{ are constants (no } y' \text{ and } z') \\ = & P \wedge y'=y \wedge z'=z \end{array}$$

$$x := e \quad = \quad \mathbf{frame}\; x \cdot x' = e$$

$$ok \quad = \quad \mathbf{frame} \cdot \top$$

$$s := \Sigma L \quad \Leftarrow \quad \mathbf{frame}\; s \cdot \mathbf{new}\; n : nat \cdot s' = \Sigma L$$

$$s' = \Sigma L \quad \Leftarrow$$

# Array

$A(i) := e$

# Array

$A[i]:=e$

# Array

$A\ i := e$

# Array

$$A[i := e] = A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots]$$

# Array

$A\ i := e \quad = \quad \underline{A'i=e} \wedge (\forall j \cdot j \neq i \Rightarrow A'j=A\ j) \wedge x'=x \wedge y'=y \wedge \dots$

# Array

$$A[i := e] = \underline{A'[i = e] \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j])} \wedge x' = x \wedge y' = y \wedge \dots$$

# Array

$$A[i := e] = A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge \underline{x' = x \wedge y' = y} \wedge \dots]$$

# Array

$$A[i := e] = A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots]$$

# Array

$A \ i := e \quad = \quad A'i=e \wedge (\forall j \cdot j \neq i \Rightarrow A'j=A\ j) \wedge x'=x \wedge y'=y \wedge \dots$

$A \ 2:= 3. \ i:= 2. \ A \ i:= 4. \ A \ i = A \ 2$

# Array

$$A i := e \quad = \quad A'i=e \wedge (\forall j \cdot j \neq i \Rightarrow A'j=Aj) \wedge x'=x \wedge y'=y \wedge \dots$$

$A 2:= 3.$   $i:= 2.$   $A i:= 4.$   $A i = A 2$

Substitution Law

# Array

$A \ i := e = A'i=e \wedge (\forall j \cdot j \neq i \Rightarrow A'j=A\ j) \wedge x'=x \wedge y'=y \wedge \dots$

$A \ 2:= 3. \ i:= 2. \ A \ i:= 4. \ A \ i = A \ 2$

 Substitution Law

# Array

$$A i := e \quad = \quad A'i=e \wedge (\forall j \cdot j \neq i \Rightarrow A'j=Aj) \wedge x'=x \wedge y'=y \wedge \dots$$

$$\begin{aligned} & A 2 := 3. \ i := 2. \ \underline{A i := 4.} \ A i = A 2 \\ = & \quad A 2 := 3. \ i := 2. \ 4 = A 2 \end{aligned}$$

 Substitution Law

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2]$

 Substitution Law

$= \quad A[2]:=3. \quad i:=2. \quad 4=A[2]$

 Substitution Law

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$\begin{aligned} & A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2] \\ = & \quad A[2]:=3. \quad i:=2. \quad 4=A[2] \\ = & \quad A[2]:=3. \quad 4=A[2] \end{aligned}$$

 Substitution Law

 Substitution Law

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2]$

Substitution Law

$= \quad A[2]:=3. \quad i:=2. \quad 4=A[2]$

Substitution Law

$= \quad A[2]:=3. \quad 4=A[2]$

Substitution Law

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$\begin{aligned} & A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2] \\ = & \quad A[2]:=3. \quad i:=2. \quad 4=A[2] \\ = & \quad A[2]:=3. \quad 4=A[2] \\ = & \quad 4=3 \end{aligned}$$

Substitution Law

Substitution Law

Substitution Law

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$\begin{aligned} & A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2] \\ = & \quad A[2]:=3. \quad i:=2. \quad 4=A[2] \\ = & \quad A[2]:=3. \quad 4=A[2] \\ = & \quad 4=3 \\ = & \quad \perp \end{aligned}$$

Substitution Law

Substitution Law

Substitution Law

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2]$$

Substitution Law

$$= \quad A[2]:=3. \quad i:=2. \quad 4=A[2]$$

Substitution Law

$$= \quad A[2]:=3. \quad 4=A[2]$$

Substitution Law

$$= \quad 4=3$$

$$= \quad \perp \quad \textcolor{red}{X}$$

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2]$$

$\times$  Substitution Law

$$= \quad A[2]:=3. \quad i:=2. \quad 4=A[2]$$

$\checkmark$  Substitution Law

$$= \quad A[2]:=3. \quad 4=A[2]$$

$\times$  Substitution Law

$$= \quad 4=3$$

$$= \quad \perp \quad \times$$

$$A[2]:=2. \quad A(A[2]):=3. \quad A[2]=2$$

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2]$$

Substitution Law

$$= \quad A[2]:=3. \quad i:=2. \quad 4=A[2]$$

Substitution Law

$$= \quad A[2]:=3. \quad 4=A[2]$$

Substitution Law

$$= \quad 4=3$$

$$= \quad \perp \quad \textcolor{red}{X}$$

$$A[2]:=2. \quad \underline{A(A[2]):=3.} \quad \underline{A[2]=2}$$

Substitution Law

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2]$$

✗ Substitution Law

$$= \quad A[2]:=3. \quad i:=2. \quad 4=A[2]$$

✓ Substitution Law

$$= \quad A[2]:=3. \quad 4=A[2]$$

✗ Substitution Law

$$= \quad 4=3$$

$$= \quad \perp \quad ✗$$

$$A[2]:=2. \quad A(A[2]):=3. \quad A[2]=2$$

✗ Substitution Law

$$= \quad A[2]:=2. \quad A[2]=2$$

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$\begin{aligned} & A[2]:=3. \quad i:=2. \quad A[i]:=4. \quad A[i]=A[2] \\ = & \quad A[2]:=3. \quad i:=2. \quad 4=A[2] \\ = & \quad A[2]:=3. \quad 4=A[2] \\ = & \quad 4=3 \\ = & \quad \perp \quad \textcolor{red}{X} \end{aligned}$$

- $\textcolor{red}{X}$  Substitution Law
- $\checkmark$  Substitution Law
- $\textcolor{red}{X}$  Substitution Law

$$\begin{aligned} & A[2]:=2. \quad A(A[2]):=3. \quad A[2]=2 \\ = & \quad A[2]:=2. \quad A[2]=2 \\ = & \quad 2=2 \end{aligned}$$

- $\textcolor{red}{X}$  Substitution Law
- $\textcolor{red}{X}$  Substitution Law

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$\begin{aligned} & A[2]:=3. \ i:=2. \ A[i]:=4. \ A[i]=A[2] & \times \text{ Substitution Law} \\ = & A[2]:=3. \ i:=2. \ 4=A[2] & \checkmark \text{ Substitution Law} \\ = & A[2]:=3. \ 4=A[2] & \times \text{ Substitution Law} \\ = & 4=3 \\ = & \perp \times \end{aligned}$$

$$\begin{aligned} & A[2]:=2. \ A(A[2]):=3. \ A[2]=2 & \times \text{ Substitution Law} \\ = & A[2]:=2. \ A[2]=2 & \times \text{ Substitution Law} \\ = & 2=2 \\ = & \top \end{aligned}$$

# Array

$$A[i] := e \quad = \quad A'[i]=e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j]=A[j]) \wedge x'=x \wedge y'=y \wedge \dots$$

$$\begin{aligned} & A[2]:=3. \ i:=2. \ A[i]:=4. \ A[i]=A[2] & \times \text{ Substitution Law} \\ = & A[2]:=3. \ i:=2. \ 4=A[2] & \checkmark \text{ Substitution Law} \\ = & A[2]:=3. \ 4=A[2] & \times \text{ Substitution Law} \\ = & 4=3 \\ = & \perp \times \end{aligned}$$

$$\begin{aligned} & A[2]:=2. \ A(A[2]):=3. \ A[2]=2 & \times \text{ Substitution Law} \\ = & A[2]:=2. \ A[2]=2 & \times \text{ Substitution Law} \\ = & 2=2 \\ = & \top \times \end{aligned}$$

# Array

$A\ i := e \quad = \quad A'i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'j = A\ j) \wedge x' = x \wedge y' = y \wedge \dots$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A'[i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots] \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e] \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$A[2 := 3] \cdot i := 2 \cdot A[i := 4] \cdot A[i = A[2]]$$

# Array

$$\begin{aligned} A \ i := e &= A'i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'j = A_j) \wedge x' = x \wedge y' = y \wedge \dots \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} A \ 2 := 3. \ i := 2. \ A \ i := 4. \ A \ i = A \ 2 \\ = A := 2 \rightarrow 3 \mid A. \ i := 2. \ A := i \rightarrow 4 \mid A. \ A \ i = A \ 2 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e] \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 3. \ i := 2. \ A[i := 4. \ A[i = A[2]]]] \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ \underline{A := i \rightarrow 4 \mid A. \ A[i = A[2]]}] \quad \text{Substitution Law} \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 3. \ i := 2. \ A[i := 4. \ A[i] = A[2]]] \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ A := i \rightarrow 4 \mid A. \ A[i] = A[2] && \text{Substitution Law} \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ (i \rightarrow 4 \mid A)i = (i \rightarrow 4 \mid A)2 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 3. \ i := 2. \ A[i := 4. \ A[i] = A[2]]] \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ A := i \rightarrow 4 \mid A. \ A[i] = A[2] && \text{Substitution Law} \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ (i \rightarrow 4 \mid A)i = (i \rightarrow 4 \mid A)2 && \text{Substitution Law} \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 3. \ i := 2. \ A[i := 4. \ A[i] = A[2]]] \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ A := i \rightarrow 4 \mid A. \ A[i] = A[2] && \text{Substitution Law} \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ (i \rightarrow 4 \mid A)i = (i \rightarrow 4 \mid A)2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 3 \mid A. \ (2 \rightarrow 4 \mid A)2 = (2 \rightarrow 4 \mid A)2 \end{aligned}$$

# Array

$$\begin{aligned}
 A[i := e] &= A'[i = e] \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots \\
 &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\
 &= A := i \rightarrow e \mid A
 \end{aligned}$$

$$\begin{aligned}
 &A[2 := 3. \ i := 2. \ A[i := 4. \ A[i] = A[2]]] \\
 &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ A := i \rightarrow 4 \mid A. \ A[i] = A[2] && \text{Substitution Law} \\
 &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ (i \rightarrow 4 \mid A)i = (i \rightarrow 4 \mid A)2 && \text{Substitution Law} \\
 &= A := 2 \rightarrow 3 \mid A. \ (2 \rightarrow 4 \mid A)2 = (2 \rightarrow 4 \mid A)2 && = \text{ is reflexive} \\
 &= A := 2 \rightarrow 3 \mid A. \ \top
 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 3. \ i := 2. \ A[i := 4. \ A[i] = A[2]]] \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ A := i \rightarrow 4 \mid A. \ A[i] = A[2] && \text{Substitution Law} \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ (i \rightarrow 4 \mid A)i = (i \rightarrow 4 \mid A)2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 3 \mid A. \ (2 \rightarrow 4 \mid A)2 = (2 \rightarrow 4 \mid A)2 && = \text{ is reflexive} \\ &= A := 2 \rightarrow 3 \mid A. \top && \text{Substitution Law} \\ &= \top \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 3. \ i := 2. \ A[i := 4. \ A[i] = A[2]]] \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ A := i \rightarrow 4 \mid A. \ A[i] = A[2] && \text{Substitution Law} \\ &= A := 2 \rightarrow 3 \mid A. \ i := 2. \ (i \rightarrow 4 \mid A)i = (i \rightarrow 4 \mid A)2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 3 \mid A. \ (2 \rightarrow 4 \mid A)2 = (2 \rightarrow 4 \mid A)2 && = \text{ is reflexive} \\ &= A := 2 \rightarrow 3 \mid A. \ \top && \text{Substitution Law} \\ &= \top \quad \checkmark \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

# Array

$$\begin{aligned} A \ i := e &= A'i = e \wedge (\forall j \ j \neq i \Rightarrow A'j = A j) \wedge x' = x \wedge y' = y \wedge \dots \\ &= A' = i \rightarrow e \mid A \ \wedge \ x' = x \ \wedge \ y' = y \ \wedge \ \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$A \ 2 := 2. \quad A(A \ 2) := 3. \quad A \ 2 = 2$$

# Array

$$\begin{aligned} A \ i := e &= A'i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'j = A_j) \wedge x' = x \wedge y' = y \wedge \dots \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} A \ 2 := 2. \ A(A \ 2) := 3. \ A \ 2 = 2 \\ = A := 2 \rightarrow 2 \mid A. \ A := A \ 2 \rightarrow 3 \mid A. \ A \ 2 = 2 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 2] \quad A(A[2 := 3]) \quad A[2] = 2 \\ &= A := 2 \rightarrow 2 \mid A. \quad A := A[2] \rightarrow 3 \mid A. \quad A[2] = 2 \quad \text{Substitution Law} \\ &= A := 2 \rightarrow 2 \mid A. \quad (A[2] \rightarrow 3 \mid A)2 = 2 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 2] \quad A(A[2 := 3]) \quad A[2] = 2 \\ &= A := 2 \rightarrow 2 \mid A. \quad A := A[2 \rightarrow 3] \mid A. \quad A[2] = 2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 2 \mid A. \quad (A[2 \rightarrow 3] \mid A)2 = 2 && \text{Substitution Law} \\ &= ((2 \rightarrow 2 \mid A)2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 2] \quad A(A[2 := 3]) \quad A[2] = 2 \\ &= A := 2 \rightarrow 2 \mid A. \quad A := A[2 \rightarrow 3] \mid A. \quad A[2] = 2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 2 \mid A. \quad (A[2 \rightarrow 3] \mid A)2 = 2 && \text{Substitution Law} \\ &= ((2 \rightarrow 2 \mid A)2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 2] \quad A(A[2 := 3]) \quad A[2] = 2 \\ &= A := 2 \rightarrow 2 \mid A. \quad A := A[2 \rightarrow 3] \mid A. \quad A[2] = 2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 2 \mid A. \quad (A[2 \rightarrow 3] \mid A)2 = 2 && \text{Substitution Law} \\ &= ((2 \rightarrow 2 \mid A)2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \\ &= (2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 2] \quad A(A[2 := 3]) \quad A[2] = 2 \\ &= A := 2 \rightarrow 2 \mid A. \quad A := A[2 \rightarrow 3] \mid A. \quad A[2] = 2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 2 \mid A. \quad (A[2 \rightarrow 3] \mid A)2 = 2 && \text{Substitution Law} \\ &= ((2 \rightarrow 2 \mid A)2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \\ &= (2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \\ &= 3 = 2 \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 2] \quad A(A[2 := 3]) \quad A[2] = 2 \\ &= A := 2 \rightarrow 2 \mid A. \quad A := A[2 \rightarrow 3] \mid A. \quad A[2] = 2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 2 \mid A. \quad (A[2 \rightarrow 3] \mid A)2 = 2 && \text{Substitution Law} \\ &= ((2 \rightarrow 2 \mid A)2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \\ &= (2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \\ &= 3 = 2 \\ &= \perp \end{aligned}$$

# Array

$$\begin{aligned} A[i := e] &= A'[i = e \wedge (\forall j \cdot j \neq i \Rightarrow A'[j] = A[j]) \wedge x' = x \wedge y' = y \wedge \dots] \\ &= A' = i \rightarrow e \mid A \wedge x' = x \wedge y' = y \wedge \dots \\ &= A := i \rightarrow e \mid A \end{aligned}$$

$$\begin{aligned} &A[2 := 2] \quad A(A[2 := 3]) \quad A[2] = 2 \\ &= A := 2 \rightarrow 2 \mid A. \quad A := A[2 \rightarrow 3] \mid A. \quad A[2] = 2 && \text{Substitution Law} \\ &= A := 2 \rightarrow 2 \mid A. \quad (A[2 \rightarrow 3] \mid A)2 = 2 && \text{Substitution Law} \\ &= ((2 \rightarrow 2 \mid A)2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \\ &= (2 \rightarrow 3 \mid 2 \rightarrow 2 \mid A)2 = 2 \\ &= 3 = 2 \\ &= \perp \quad \checkmark \end{aligned}$$

# Array

# Array

remember

$A \ i := e$       becomes       $A := i \rightarrow e \mid A$

# Array

remember

$$A \ i := e \quad \text{becomes} \quad A := i \rightarrow e \mid A$$

$$A \ i \ j := e \quad \text{becomes} \quad A := (i;j) \rightarrow e \mid A$$

# Record

# Record

*person* = “name” → *text*

| “age” → *nat*

# Record

*person* = “name” → *text*

| “age” → *nat*

**new** *p*: *person*

# Record

*person* = “name” → *text*

| “age” → *nat*

**new** *p*: *person*

*p*:= “name” → “Josh” | “age” → 17

# Record

*person* = “name” → *text*

| “age” → *nat*

**new** *p*: *person*

*p*:= “name” → “Josh” | “age” → 17

*p* “age”:= 18

# Record

*person* = “name” → *text*

| “age” → *nat*

**new** *p*: *person*

*p*:= “name” → “Josh” | “age” → 17

*p* “age”:= 18

*p*:= “age” → 18 | *p*