

Making Programs Memory Safe

Through Program Synthesis

Roland Meyer, **Jakob Tepe**, Sebastian Wolff, **01.03.2024**

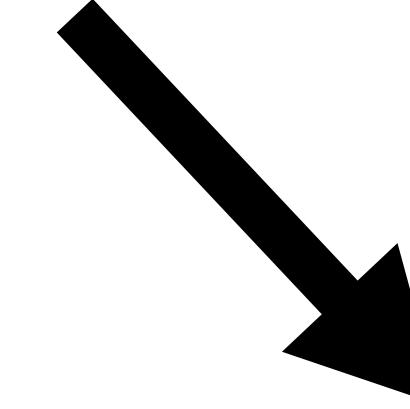


Making Programs Memory Safe

Through Program Synthesis

Roland Meyer, **Jakob Tepe**, Sebastian Wolff, **01.03.2024**

Program Synthesis

$$\models \{pre\} \text{ prog } \{post\}$$

$$\in \text{Progs}$$

Program Synthesis

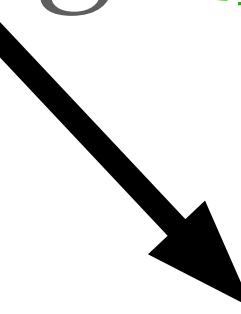
$\models \{pre\} \text{prog} \{post\}$

$\in \text{Progs}$

Progs given as a Sketch:

Program Synthesis

$\models \{pre\} \text{prog} \{post\}$



$\in \text{Progs}$

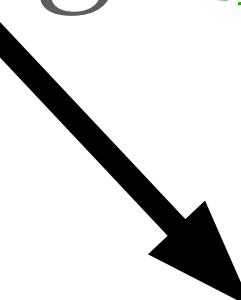
Progs given as a Sketch:

N;
x++;
N;
y = 1; **+** y = 2;
M;

Program Synthesis

$\models \{pre\} \text{prog} \{post\}$

$\in \text{Progs}$



$N ::= x = 1 \mid x = 2$

$M ::= y++ \mid M;M$

$Progs$ given as a Sketch:

$N;$
 $x++;$
 $N;$
 $y = 1; \quad + \quad y = 2;$
 $M;$

Program Synthesis Problems:

1: Is synthesis possible?

Verification - Realizability Logic

Progs given as a Sketch:

```
x = 0;  
N;  
x++;  
y = 1; + y = 2;  
M;
```

Two Problems:

1: Is synthesis possible?

Verification - Realizability Logic

2: What does the solution look like?

Synthesis - Realization Logic

Realizability Logic

$\{ \text{true} \}$

$\{ x = 2 \}$

Realizability Logic

$\{ \text{true} \}$

N;

X++;

$\{ x = 2 \}$

Realizability Logic

$\{ \text{true} \}$

N;

x++;

$\{ x = 2 \}$

N ::= **x** = 1 | **x** = 2

Realizability Logic

$$\exists \text{prog} \in \text{prog} \xrightarrow{\text{realizability}} \left\{ \begin{array}{l} \{ \text{true} \} \\ \text{N;} \\ \text{x++;} \\ \{ x = 2 \} \end{array} \right\}$$

$\models \{ \text{true} \} \text{prog} \{ x = 2 \}$

$\text{N} ::= \text{x} = 1 \mid \text{x} = 2$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \{ \text{prog} \models \{ \text{true} \} \text{prog} \{ x = 2 \} \} \quad \checkmark$$

$\models \{ \text{true} \} \text{prog} \{ x = 2 \}$

$\{ \text{true} \}$

$x = 1;$

$x++;$

$\{ x = 2 \}$

$N ::= x = 1 \mid x = 2$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \{ \text{prog} \{ x = 2 \} \models \{ \text{true} \} \text{prog} \{ x = 2 \} \} \quad \checkmark$$

{ true
x = 1;
{x = 1}
x++;
{x = 2}

$N ::= x = 1 \mid x = 2$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \{ \text{prog} \{ x = 2 \} \models \{ \text{true} \} \text{prog} \{ x = 2 \} \} \quad \checkmark$$

Curly brace with red arrow:

$$\left\{ \begin{array}{l} \{ \text{true} \} \\ \text{N;} \\ \text{x++;} \\ \{ x = 2 \} \end{array} \right.$$

$\text{N} ::= \text{x} = 1 \mid \text{x} = 2$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \{ \text{prog} \{ x = 2 \} \models \{ \text{true} \} \text{prog} \{ x = 2 \} \} \quad \checkmark$$

Curly braces indicate a set of programs. A red curved arrow points from the set to the programs. A green checkmark is placed under the set of programs.

$\{ \text{true} \}$

$\{ x = 2 \}$

$\text{N} := \text{x} = 1 \mid \text{x} = 2$

$\langle \text{true} \rangle$

$\text{N};$

$\text{x}++;$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \leftarrow \{ \text{prog} \mid \models \{ \text{true} \} \text{prog} \{ x = 2 \} \right\}$$

Curly brace indicates a set of programs that realize the formula $\models \{ \text{true} \} \text{prog} \{ x = 2 \}$. A green checkmark  is shown to the right of the brace.

Red curved arrow  points from the brace to the set of programs.

Programs listed in the set:

- $\langle \text{true} \rangle$
- $\text{N};$
- $\langle x = 1, x = 2 \rangle$
- $\text{x}++;$
- $\langle x = 2 \rangle$

Definition of N :

$$\text{N} ::= \text{x} = 1 \mid \text{x} = 2$$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \{ \text{prog} \{ x = 2 \} \models \{ \text{true} \} \text{prog} \{ x = 2 \} \} \quad \checkmark$$

Curly brace with a red arrow pointing to it:

$$\left\{ \begin{array}{l} \langle \text{true} \rangle \\ \text{N;} \\ \langle x = 1, x = 2 \rangle \\ \text{x++;} \\ \langle x = 2, x = 3 \rangle \end{array} \right\}$$

$\text{N} ::= \text{x} = 1 \mid \text{x} = 2$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \xrightarrow{\text{realizable}} \left\{ \begin{array}{l} \langle \text{true} \rangle \\ x = 1; \quad + \quad x = 2; \\ x++; \\ \end{array} \right. \quad N ::= \quad x = 1 \mid x = 2$$

$\models \{\text{true}\} \text{prog} \{x = 2\}$

Realizability Logic

$$\models \{ \text{true} \} \text{prog} \{ x = 2 \} \quad \left\{ \begin{array}{l} \langle \text{true} \rangle \\ x = 1; \quad + \quad x = 2; \\ \langle x = 1 \vee x = 2 \rangle \\ x++; \\ \text{N} ::= \quad x = 1 \mid x = 2 \end{array} \right.$$

Realizability Logic

$$\models \{true\} \text{prog}\{x = 2\} \xrightarrow{\text{red curved arrow}} \left\{ \begin{array}{l} \langle true \rangle \\ x = 1; \quad + \quad x = 2; \\ \langle x = 1 \vee x = 2 \rangle \\ x++; \\ \langle x = 2 \vee x = 3 \rangle \end{array} \right. \quad N ::= \quad x = 1 \mid x = 2$$

Realizability Logic

$$\models \{true\} \text{prog}\{x = 2\} \quad \text{X} \quad \left\{ \begin{array}{l} \langle true \rangle \\ x = 1; \quad + \quad x = 2; \\ \langle x = 1 \vee x = 2 \rangle \\ x++; \\ \langle x = 2 \vee x = 3 \rangle \end{array} \right.$$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \xrightarrow{\text{realizability}} \left\{ \begin{array}{l} \langle \text{true} \rangle \\ \text{N;} \\ \text{x++;} \quad + \quad \text{skip;} \\ \dots \end{array} \right\} \models \{\text{true}\} \text{prog} \{x = 2\}$$

$\text{N} ::= \text{x} = 1 \mid \text{x} = 2$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \xrightarrow{\text{realizable}} \left\{ \begin{array}{l} \langle \text{true} \rangle \\ \text{N;} \\ \langle x = 1, x = 2 \rangle \\ x++; \quad + \quad \text{skip;} \end{array} \right. \quad \text{N} ::= \quad x = 1 \mid x = 2$$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \rightarrow \left\{ \begin{array}{l} \langle \text{true} \rangle \\ \text{N;} \\ \langle x = 1, x = 2 \rangle \\ \text{x++;} \quad + \quad \text{skip;} \\ \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle \end{array} \right. \quad \text{N ::= } \text{x = 1} \mid \text{x = 2}$$

Realizability Logic

$\exists \text{prog} \in \{ \text{true} \} \text{prog} \{ x = 2 \} \quad \text{X}$

Curved red arrow pointing from the left side of the equation to the right side, where the set is defined.

$\{ \text{true} \} \text{prog} \{ x = 2 \} \in \{$

$\langle \text{true} \rangle$
 $\text{N};$
 $\langle x = 1, x = 2 \rangle$
 $\text{x++;} \quad + \quad \text{skip;}$
 $\langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle$

$\text{N} ::= \quad \text{x = 1} \mid \text{x = 2}$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \xrightarrow{\text{realizability}} \left\{ \begin{array}{l} \langle \text{true} \rangle \\ x = 1; \quad + \quad x = 2; \\ N; \end{array} \right. \quad \text{N ::= } x++ \mid \text{skip}$$

$\models \{\text{true}\} \text{prog} \{x = 2\}$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \xrightarrow{\text{realizable}} \left\{ \begin{array}{l} \langle \text{true} \rangle \\ x = 1; \quad + \quad x = 2; \\ \langle x = 1 \vee x = 2 \rangle \\ \mathbf{N}; \end{array} \right. \quad \mathbf{N} ::= \quad \mathbf{x++} \mid \mathbf{skip}$$

$\models \{\text{true}\} \text{prog} \{x = 2\}$

Realizability Logic

$$\models \{ \text{true} \} \text{prog} \{ x = 2 \} \quad \leftarrow \quad \left\{ \begin{array}{l} \langle \text{true} \rangle \\ x = 1; \quad + \quad x = 2; \\ \langle x = 1 \vee x = 2 \rangle \\ \text{N}; \\ \langle x = 2 \vee x = 3, \underline{x = 1} \vee x = 2 \rangle \end{array} \right. \quad \text{N ::= } \text{x++} \mid \text{skip}$$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \rightarrow \left\{ \begin{array}{l} \langle \text{true} \rangle \\ \text{x} = 1; \quad + \quad \text{x} = 2; \\ \langle \text{x} = 1 \vee \text{x} = 2 \rangle \\ \text{N}; \\ \langle \text{x} = 2 \vee \text{x} = 3, \underline{\text{x}} = 1 \vee \text{x} = 2 \rangle \end{array} \right. \quad \text{N} ::= \quad \text{x++} \mid \text{skip}$$

$\models \{\text{true}\} \text{prog} \{x = 2\} \quad \text{X}$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \xrightarrow{\text{realizability}} \left\{ \begin{array}{l} \langle \text{true} \rangle \\ M; \\ N; \end{array} \right\} \models \{ \text{true} \} \text{prog} \{ x = 2 \}$$

$\text{M ::= } x = 1 \mid x = 2$

$\text{N ::= } x++ \mid \text{skip}$

Realizability Logic

$$\exists \text{prog} \in \text{prog} \xrightarrow{\text{realizable}} \left\{ \begin{array}{l} \langle \text{true} \rangle \\ \text{M}; \\ \langle x = 1, \underline{x} = 2 \rangle \\ \text{N}; \end{array} \right. \quad \begin{array}{l} \text{M} ::= \text{x} = 1 \mid \text{x} = 2 \\ \text{N} ::= \text{x}++ \mid \text{skip} \end{array}$$

$\models \{\text{true}\} \text{prog} \{x = 2\}$

Realizability Logic

$\exists \text{prog} \in \text{prog} \rightarrow \{ \text{true} \} \text{prog} \{ x = 2 \}$

$\{ \text{true} \} \text{prog} \{ x = 2 \} \rightarrow \{$

- $\langle \text{true} \rangle$
- $\langle x = 1, x = 2 \rangle$
- $\langle x = 1, x = 2, x = 3 \rangle$

$M ::= x = 1 \mid x = 2$

$N ::= x++ \mid \text{skip}$

Realizability Logic

$\exists \text{prog} \in \text{prog} \rightarrow \{ \text{true} \} \text{prog} \{ x = 2 \}$ 

$\{ \text{true} \} \text{prog} \{ x = 2 \} \rightarrow \{ \text{true} \}$

$\{ \text{true} \} \text{prog} \{ x = 2 \} \rightarrow \{ x = 1, x = 2 \}$

$\{ \text{true} \} \text{prog} \{ x = 2 \} \rightarrow \{ x = 1, x = 2, x = 3 \}$

$M ::= x = 1 \mid x = 2$

$N ::= x++ \mid \text{skip}$

Realizability Logic

The diagram illustrates a program state and its semantics. On the left, a green checkmark icon is positioned next to the text $\models \{ \text{true} \} \text{prog} \{ x = 2 \}$. Above this, a red curved arrow points from the checkmark to a large black brace that encloses a list of four possible states. The states are: $\langle \text{true} \rangle$, $\text{M}; \langle x = 1, x = 2 \rangle$, $\text{N}; \langle x = 1, x = 2, x = 3 \rangle$, and $\langle x = 1, x = 2, x = 3 \rangle$. A red arrow points from the text "What semantics?" to the third state in the list.

$\models \{ \text{true} \} \text{prog} \{ x = 2 \}$

$\exists \text{prog} \in \{ \text{true} \}$

$\langle \text{true} \rangle$

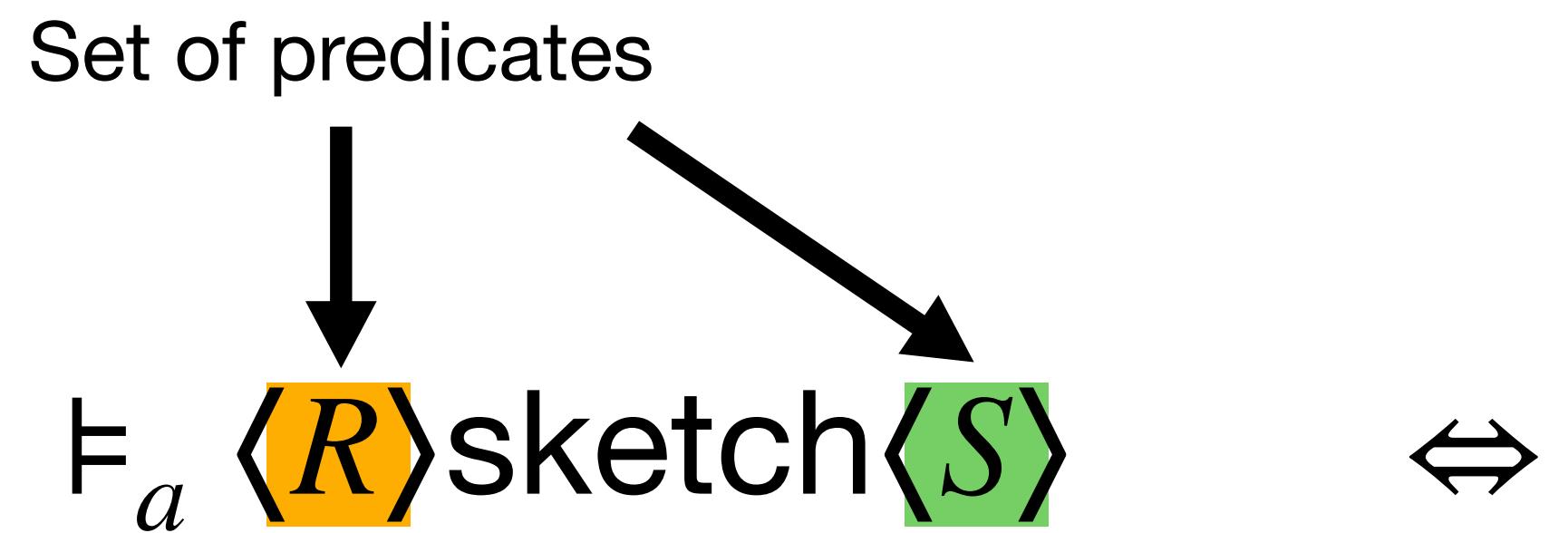
$\text{M}; \langle x = 1, x = 2 \rangle$

$\text{N}; \langle x = 1, x = 2, x = 3 \rangle$

$\langle x = 1, x = 2, x = 3 \rangle$

What semantics?

Realizability Logic



Realizability Logic

Set of predicates

$$\downarrow \quad \searrow$$
$$\models_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow$$

$$\models_a \langle \text{true} \rangle \quad M;N \quad \langle x = 1, x = 2, x = 3 \rangle$$

$$M ::= \quad x = 1 \mid x = 2$$

$$N ::= \quad x++ \mid \text{skip}$$

Realizability Logic

Set of predicates

$$\Downarrow \mathfrak{F}_a \langle R \rangle \text{sketch} \langle S \rangle \Leftrightarrow \forall s \in S.$$
$$\mathfrak{F}_a \langle \text{true} \rangle \quad M;N \quad \langle x = 1, x = 2, x = 3 \rangle$$
$$\begin{aligned} M &::= x = 1 \mid x = 2 \\ N &::= x++ \mid \text{skip} \end{aligned}$$

Realizability Logic

Set of predicates

$$\Downarrow \mathbb{F}_a \langle R \rangle \text{sketch} \langle S \rangle \Leftrightarrow \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}).$$
$$\mathbb{F}_a \langle \text{true} \rangle \quad M;N \quad \langle x = 1, x = 2, x = 3 \rangle \quad \begin{aligned} M ::= & \quad x = 1 \mid x = 2 \\ N ::= & \quad x++ \mid \text{skip} \end{aligned}$$

Realizability Logic

Set of predicates

$$\Downarrow \quad \vdash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \vdash_d \{r\} \text{prog} \{s\}$$

$$\vdash_a \langle \text{true} \rangle \quad M;N \quad \langle x = 1, x = 2, x = 3 \rangle$$

$$M ::= \quad x = 1 \mid x = 2$$

$$N ::= \quad x++ \mid \text{skip}$$

Realizability Logic

Set of predicates
↓
 $\models_a \langle R \rangle \text{sketch} \langle S \rangle$

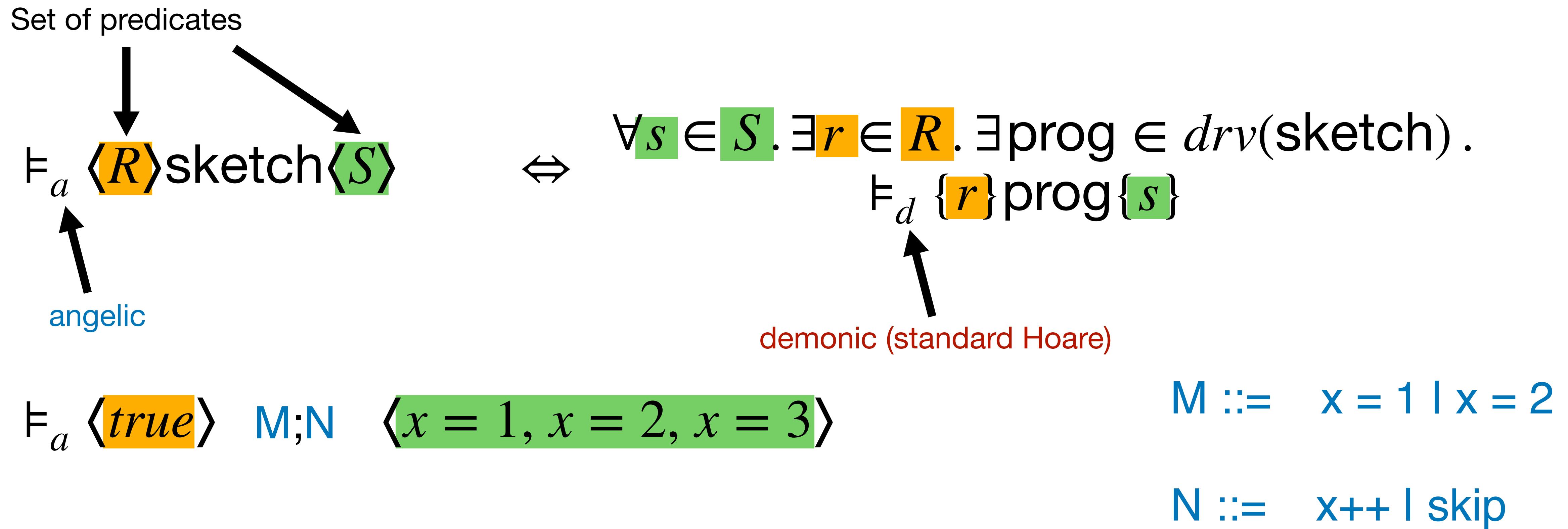
$\Leftrightarrow \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}).$
 $\models_d \{r\} \text{prog} \{s\}$

demonic (standard Hoare)

$\models_a \langle \text{true} \rangle \quad M;N \quad \langle x = 1, x = 2, x = 3 \rangle$

$M ::= x = 1 \mid x = 2$
 $N ::= x++ \mid \text{skip}$

Realizability Logic



Realizability Logic

$\langle \text{true} \rangle$
 \mathbf{N}

$\mathbf{x}++; \quad + \quad \text{skip};$

$\mathbf{N} ::= \quad \mathbf{x} = 1 \mid \mathbf{x} = 2$

Realizability Logic

$$\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1 ; \langle x = 1 \rangle}$$

$\langle \text{true} \rangle$
 N

$x++;$ + $\text{skip};$

$\text{N} ::= \text{x} = 1 \mid \text{x} = 2$

Realizability Logic

$$\frac{\text{(ANG)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1 ; \langle x = 1 \rangle}}{\vdash_a \langle \text{true} \rangle \text{N} \langle x = 1 \rangle}}$$

$\langle \text{true} \rangle$
 N

$x++;$ $+$ $\text{skip};$

$\text{N} ::= \quad x = 1 \mid x = 2$

Realizability Logic

$$\frac{\text{(ANG)} \quad \frac{\text{(COM)} \quad \frac{\vdash_a \langle \text{true} \rangle x = 1 ; \langle x = 1 \rangle}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle}$$

$$\frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle} \text{ (COM)}$$

$\langle true \rangle$
N

X++; + skip;

N := x = 1 | x = 2

Realizability Logic

$$\text{(ANG)} \frac{}{\frac{\text{(COM)} \frac{}{\vdash_a \langle \text{true} \rangle x = 1 ; \langle x = 1 \rangle}}{\vdash_a \langle \text{true} \rangle \text{N} \langle x = 1 \rangle}}$$

$$\frac{\frac{}{\vdash_a \langle \text{true} \rangle x = 2 ; \langle x = 2 \rangle} \text{(COM)}}{\vdash_a \langle \text{true} \rangle \text{N} \langle x = 2 \rangle} \text{(ANG)}$$

$\langle \text{true} \rangle$
 N

$x++;$ $+$ $\text{skip};$

$\text{N} ::= \text{x} = 1 \mid \text{x} = 2$

Realizability Logic

$$\text{(ANG)} \frac{}{\frac{\text{(COM)} \frac{}{\vdash_a \langle \text{true} \rangle x = 1 ; \langle x = 1 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle}}$$

$$\frac{\frac{}{\vdash_a \langle \text{true} \rangle x = 2 ; \langle x = 2 \rangle} \text{(COM)}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle} \text{(ANG)}$$

$\langle \text{true} \rangle$
 \mathbf{N}

$x++; \quad + \quad \text{skip};$

$\mathbf{N} ::= \quad x = 1 \mid x = 2$

Realizability Logic

$$\begin{array}{c}
 \frac{\text{(COM)} \quad \vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\
 \frac{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle \text{ (COM)}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle \text{ (ANG)}} \\
 \hline
 \text{(GATHER)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, \underline{x = 2} \rangle} \quad \boxed{1}
 \end{array}$$

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $\mathbf{x}++; \quad \mathbf{skip};$

$\mathbf{N} ::= \quad \mathbf{x} = 1 \mid \mathbf{x} = 2$

Realizability Logic

$$\frac{\begin{array}{c} \text{(ANG)} \frac{\text{(COM)} \frac{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\ \vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle \end{array}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}$$

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $\mathbf{x}++; \quad \mathbf{skip};$

$\mathbf{N} ::= \quad \mathbf{x} = 1 \mid \mathbf{x} = 2$

Realizability Logic

$$\begin{array}{c}
 \frac{\text{(COM)}}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle} \\
 \frac{\text{(ANG)}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\
 \frac{\text{(GATHER)}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}
 \end{array}
 \quad
 \frac{\text{(COM)}}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle} \\
 \frac{\text{(ANG)}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle}$$

$$\frac{\text{(COM)}}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle}$$

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $x++; \textcolor{red}{+} \text{ skip};$

$\mathbf{N} ::= \mathbf{x} = 1 \mid \mathbf{x} = 2$

Realizability Logic

$$\begin{array}{c}
 \text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle} \\
 \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\
 \text{(GATHER)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle} \text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle} \text{(ANG)}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}
 \end{array}$$

$$\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle} \quad \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle} \text{(COM)}$$

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $x++; \text{skip};$

$\mathbf{N} ::= \quad x = 1 \mid x = 2$

Realizability Logic

$$\begin{array}{c}
 \text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle} \\
 \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\
 \text{(GATHER)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle} \text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle} \text{(ANG)}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle}
 \end{array}$$

$$\text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle} \quad \text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle}}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2}$$

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $x++; \text{ + skip};$

$\mathbf{N} ::= \mathbf{x} = 1 \mid \mathbf{x} = 2$

Realizability Logic

$$\begin{array}{c}
 \text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle} \\
 \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\
 \text{(GATHER)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle} \quad \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}
 \end{array}$$

$$\text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle} \quad \text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle}}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2}$$

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $x++; \text{ + skip};$

$\mathbf{N} ::= \text{ x = 1 } \mid \text{ x = 2 }$

Realizability Logic

$$\begin{array}{c}
 \text{(COM)} \frac{}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle} \\
 \text{(ANG)} \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\
 \text{(GATHER)} \frac{\text{(COM)} \frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle} \quad \text{(ANG)} \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}
 \end{array}$$

$$\text{(DEM)} \frac{\text{(COM)} \frac{}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle} \quad \text{(COM)} \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle}}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2}$$

$$\text{(COM)} \frac{}{\vdash_a \langle x = 2 \rangle x++; \langle x = 3 \rangle}$$

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $x++; \text{ + skip};$

$\mathbf{N} ::= \quad x = 1 \mid x = 2$

Realizability Logic

$$\frac{\text{(ANG)} \quad \frac{\text{(COM)} \quad \frac{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \quad \frac{\text{(COM)} \quad \frac{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle} \quad \text{(ANG)} }{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \text{(GATHER)} }{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}$$

$$\frac{\text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip; } \langle x = 1 \vee x = 2 \rangle} \quad \frac{\text{(COM)} \quad \frac{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip; } \langle x = 1 \vee x = 2 \rangle} \quad \text{(COM)} }{\vdash_a \langle x = 1 \rangle x++; \text{ + skip; } \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2}$$

$$\frac{\text{(COM)} \quad \frac{\vdash_a \langle x = 2 \rangle x++; \langle x = 3 \rangle}{\vdash_a \langle x = 2 \rangle \text{skip}; \langle x = 2 \rangle} \quad \text{(COM)} }{\vdash_a \langle x = 2 \rangle x++; \text{ + skip; } \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2}$$

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $x++; \text{ + skip; }$

$\mathbf{N} ::= \quad x = 1 \mid x = 2$

Realizability Logic

$$\begin{array}{c}
 \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle} \text{(ANG)} \\
 \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle} \text{(GATHER)} \\
 \text{(GATHER)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}
 \end{array}$$

$$\begin{array}{c}
 \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle}}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle}}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2} \\
 \langle \text{true} \rangle \\
 \mathbf{N} \\
 \langle x = 1, x = 2 \rangle \\
 x++; \text{ + skip}; \\
 \hline
 \end{array}$$

$$\begin{array}{c}
 \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 2 \rangle x++; \langle x = 3 \rangle}}{\vdash_a \langle x = 2 \rangle x++; \text{ + skip}; \langle x = 2 \vee x = 3 \rangle} \text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 2 \rangle \text{skip}; \langle x = 2 \rangle}}{\vdash_a \langle x = 2 \rangle x++; \text{ + skip}; \langle x = 2 \vee x = 3 \rangle} \quad \boxed{3} \\
 \langle x = 2 \rangle x++; \text{ + skip}; \langle x = 2 \vee x = 3 \rangle \\
 \hline
 \end{array}$$

$\mathbf{N} ::= \quad x = 1 \mid x = 2$

Realizability Logic

$\langle true \rangle$
N
 $\langle x = 1, x = 2 \rangle$
x++; + skip;

N ::= x = 1 | x = 2

Realizability Logic

$$\begin{array}{c}
 \text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle} \\
 \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\
 \text{(GATHER)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle} \quad \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}
 \end{array}$$

$$\text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle} \quad \text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle}}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2}$$

$$\text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 2 \rangle x++; \langle x = 3 \rangle} \quad \text{(COM)} \quad \frac{}{\vdash_a \langle x = 2 \rangle \text{skip}; \langle x = 2 \rangle}}{\vdash_a \langle x = 2 \rangle x++; \text{ + skip}; \langle x = 2 \vee x = 3 \rangle} \quad \boxed{3}$$

2

$\langle \text{true} \rangle$
 \mathbf{N}
 $\langle x = 1, x = 2 \rangle$
 $x++; \text{ + skip};$

$\mathbf{N} ::= \quad x = 1 \mid x = 2$

Realizability Logic

$$\frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle} \quad \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle} \text{(COM)}}{\text{(DEM)} \quad \vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \quad 2$$

$$\frac{\text{(COM)} \quad \frac{\vdash_a \langle x = 2 \rangle x++; \langle x = 3 \rangle}{\vdash_a \langle x = 2 \rangle \text{skip}; \langle x = 2 \rangle} \quad \text{(COM)}}{\text{(DEM)} \quad \vdash_a \langle x = 2 \rangle x++; \textcolor{red}{+} \text{ skip}; \langle x = 2 \vee x = 3 \rangle} \quad 3$$

$\langle true \rangle$
 \mathbf{N}
 $\langle x = 1, \underline{x} = 2 \rangle$
 $x++; \quad + \quad \mathbf{skip};$

N := x = 1 | x = 2

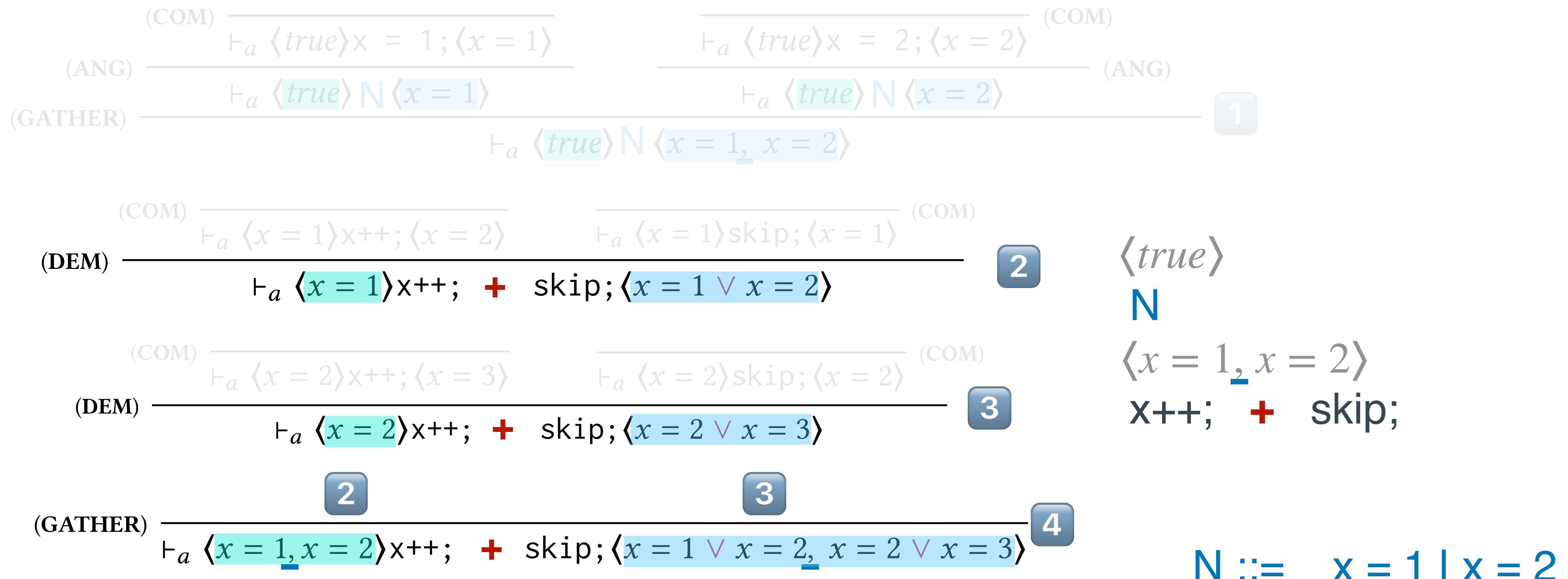
Realizability Logic

$$\begin{array}{c}
 \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle} \text{(ANG)} \\
 \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle} \\
 \text{(GATHER)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle} \quad \boxed{1}
 \end{array}$$

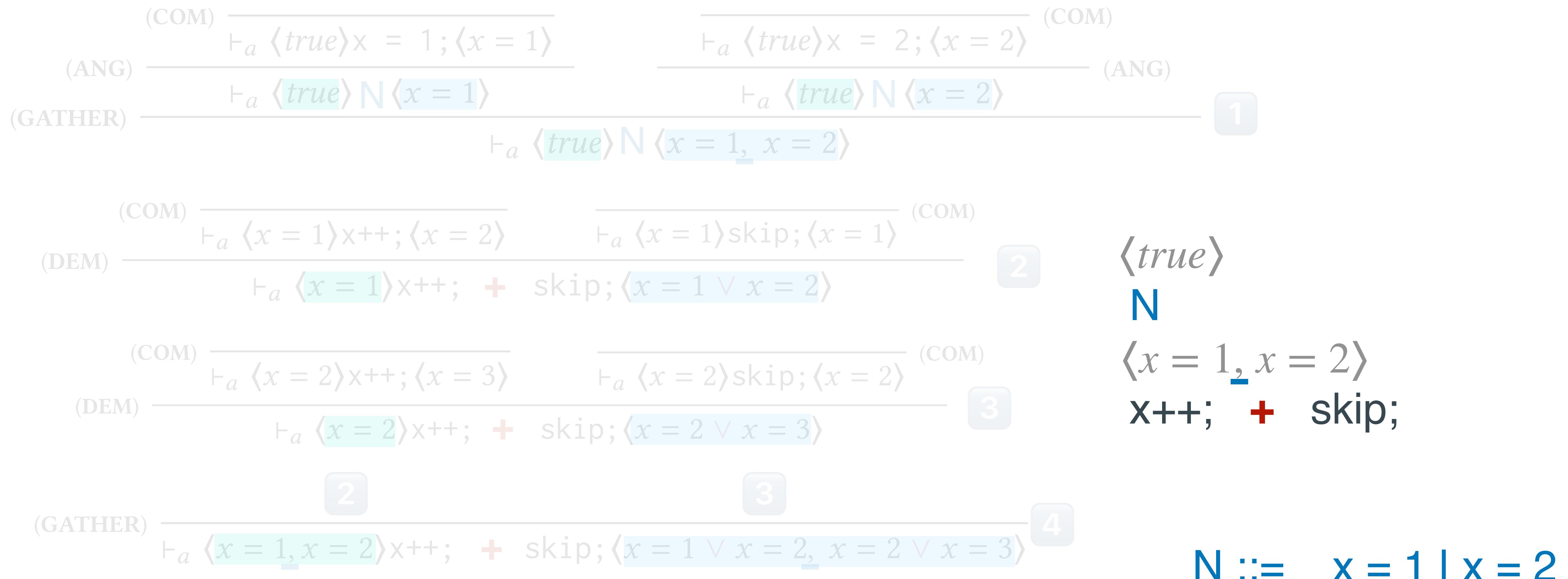
$$\begin{array}{c}
 \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle x++; \langle x = 2 \rangle}}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle}}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \quad \boxed{2} \quad \langle \text{true} \rangle \\
 \text{(DEM)} \quad \frac{}{\vdash_a \langle x = 1 \rangle x++; \text{ + skip}; \langle x = 1 \vee x = 2 \rangle} \quad \frac{}{\vdash_a \langle x = 1 \rangle \text{skip}; \langle x = 1 \rangle} \quad \langle x = 1, x = 2 \rangle \\
 \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 2 \rangle x++; \langle x = 3 \rangle}}{\vdash_a \langle x = 2 \rangle x++; \text{ + skip}; \langle x = 2 \vee x = 3 \rangle} \text{(DEM)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle x = 2 \rangle \text{skip}; \langle x = 2 \rangle}}{\vdash_a \langle x = 2 \rangle x++; \text{ + skip}; \langle x = 2 \vee x = 3 \rangle} \quad \boxed{3} \quad \langle x = 2 \rangle x++; \text{ + skip}; \\
 \frac{}{\vdash_a \langle x = 2 \rangle x++; \text{ + skip}; \langle x = 2 \vee x = 3 \rangle} \quad \frac{}{\vdash_a \langle x = 2 \rangle \text{skip}; \langle x = 2 \rangle} \quad \langle x = 2, x = 3 \rangle
 \end{array}$$

$\mathbf{N} ::= \quad x = 1 \mid x = 2$

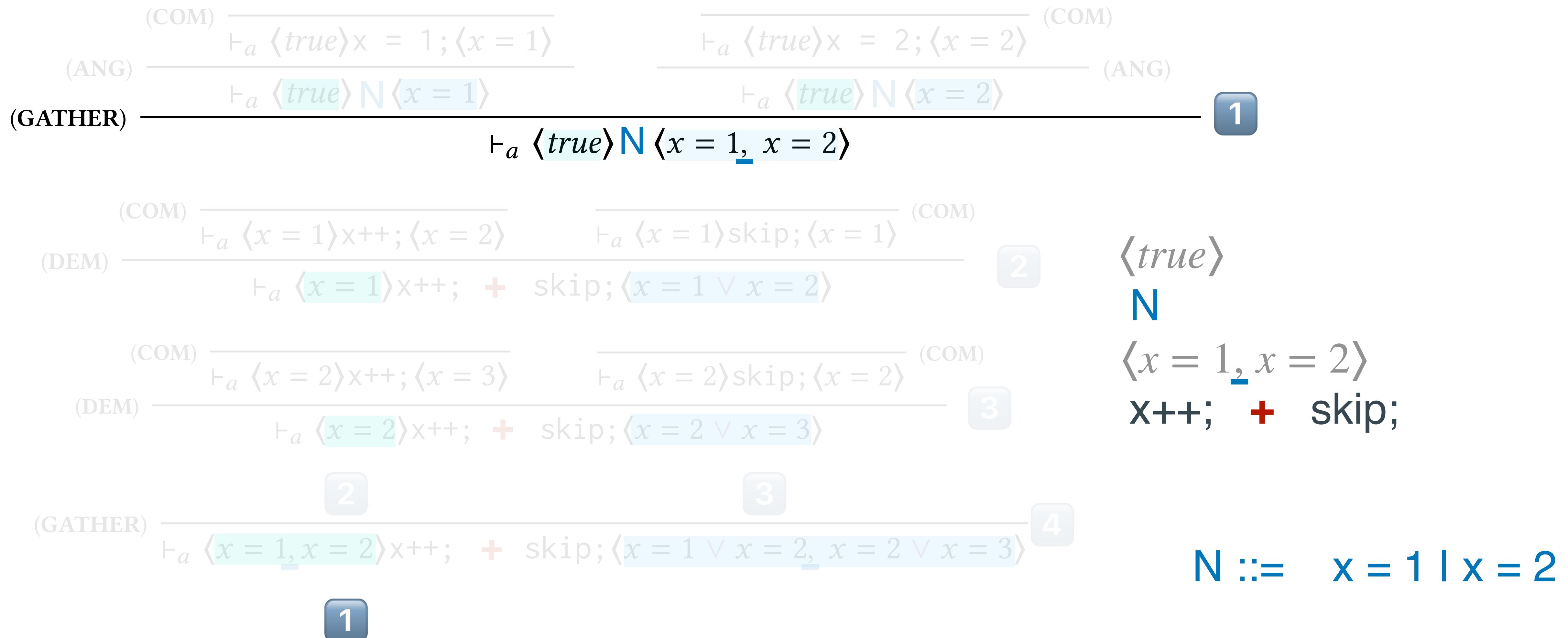
Realizability Logic



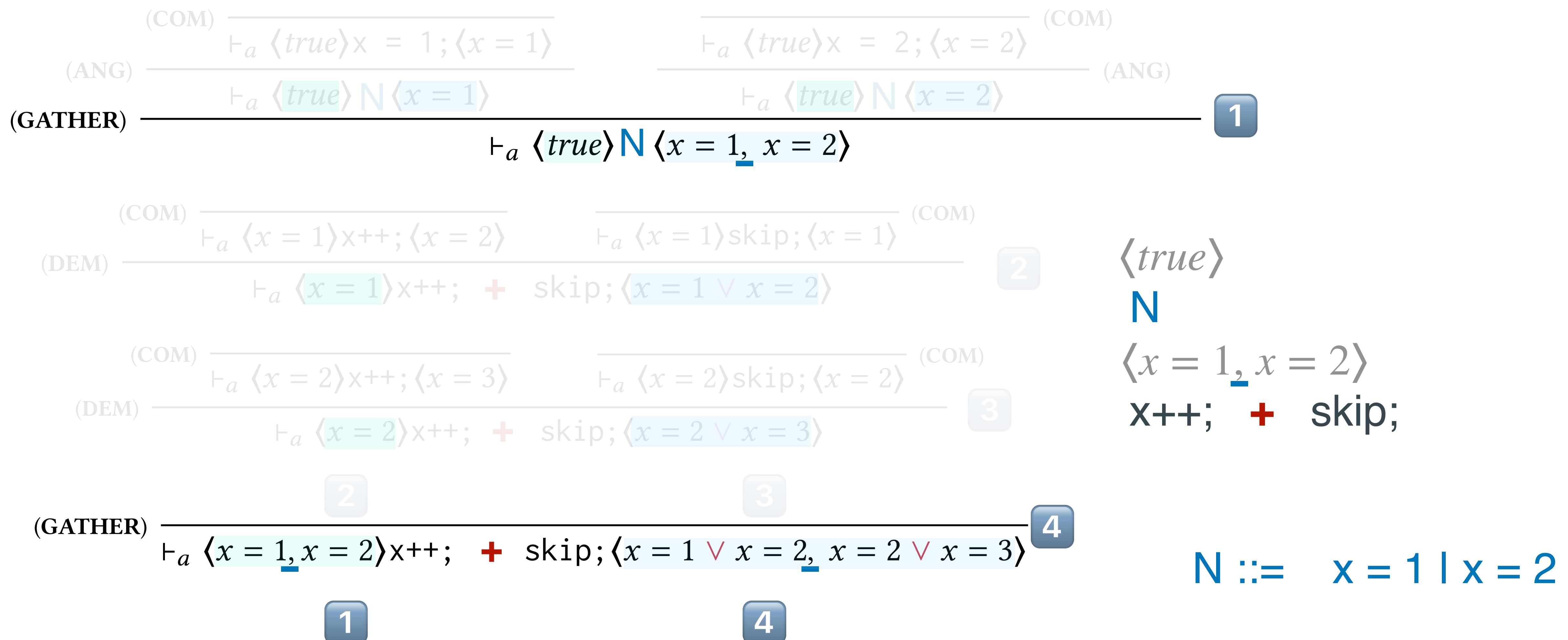
Realizability Logic



Realizability Logic



Realizability Logic



Realizability Logic

$$\begin{array}{c}
 \text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 1; \langle x = 1 \rangle} \\
 \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1 \rangle} \\
 \hline
 \text{(GATHER)} \quad \frac{\text{(COM)} \quad \frac{}{\vdash_a \langle \text{true} \rangle x = 2; \langle x = 2 \rangle} \quad \text{(ANG)} \quad \frac{}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 2 \rangle}}{\vdash_a \langle \text{true} \rangle \mathbf{N} \langle x = 1, x = 2 \rangle}
 \end{array}$$

$$(\text{GATHER}) \frac{}{\vdash_a \langle x = 1, x = 2 \rangle x++; \quad + \quad \text{skip}; \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle}$$

$$\text{(SEQ)} \quad \frac{1 \quad \quad \quad 4}{\vdash_a \langle \text{true} \rangle \text{N} ; (\text{x}++; \text{skip};) \langle x = 1 \vee \underline{x = 2}, \text{x} = 2 \vee x = 3 \rangle}$$

⟨*true*⟩

$\langle x = 1, \underline{x} = 2 \rangle$
 $x++; + \text{skip};$
 $\langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle$

N ::= x = 1 | x = 2

Realizability Logic

Contribution 1:

Realizability Logic

$$\vdash_a \langle R \rangle \text{sketch} \langle S \rangle \Leftrightarrow \vdash_a \langle R \rangle \text{sketch} \langle S \rangle$$

$$\frac{\text{(GATHER)} \quad \frac{\text{(2)} \quad \text{(3)} \quad \text{(4)}}{\vdash_a \langle x = 1, x = 2 \rangle \text{x++; + skip; } \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle}}{\vdash_a \langle x = 1, x = 2 \rangle \text{x++; + skip; } \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle}$$

$$\frac{\text{(SEQ)} \quad \frac{\text{(1)} \quad \text{(4)}}{\vdash_a \langle x = 0 \rangle \text{N; (x++; + skip;) } \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle}}{\vdash_a \langle x = 0 \rangle \text{N; (x++; + skip;) } \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle}$$

$$\text{N} ::= x = 1 \mid x = 2$$

Realizability Logic

Contribution 1:

Realizability Logic

$$\vdash_a \langle R \rangle \text{sketch} \langle S \rangle \Leftrightarrow \vdash_a \langle R \rangle \text{sketch} \langle S \rangle$$

$$\vdash_a \langle x = 1, x = 2 \rangle \text{x++; + skip;} \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle$$

$$\vdash_a \langle x = 0 \rangle N; (x++; + \text{skip;}) \langle x = 1 \vee x = 2, x = 2 \vee x = 3 \rangle$$

But what makes this efficient?

Realizability Logic - Secret Sauce

$\langle x = 0 \rangle$
 $\text{N};$

$\text{N} ::= \text{x++} \mid \text{x--}$

$\text{N};$

$\text{N};$

Realizability Logic - Secret Sauce

$\langle x = 0 \rangle$
 $\text{N};$

$\langle x = 1, \underline{x} = -1 \rangle$
 $\text{N};$

$\text{N};$

$\text{N} ::= \text{x++} \mid \text{x--}$

Realizability Logic - Secret Sauce

$\langle x = 0 \rangle$
 $\text{N};$

$\text{N} ::= \text{x++} \mid \text{x--}$

$\langle x = 1, x = -1 \rangle$

$\text{N};$

$\langle x = 2, x = 0, x = -2 \rangle$

$\text{N};$

Realizability Logic - Secret Sauce

$\langle x = 0 \rangle$
 $\text{N};$

$\text{N} ::= \text{x++} \mid \text{x--}$

$\langle x = 1, x = -1 \rangle$
 $\text{N};$

$\langle x = 2, x = 0, x = -2 \rangle$
 $\text{N};$

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

Realizability Logic - Secret Sauce

$\langle x = 0 \rangle$
 $\text{N};$

$\langle x = 1, x = -1 \rangle$
 $\text{N};$

$\langle x = 2, x = 0, x = -2 \rangle$
 $\text{N};$

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

$\text{N} ::= \text{x++} \mid \text{x--}$

8 Programs vs. 4 Predicates

Realizability Logic - Secret Sauce

$\langle x = 0 \rangle$
 $\text{N};$

$\langle x = 1, x = -1 \rangle$
 $\text{N};$

$\langle x = 2, x = 0, x = -2 \rangle$
 $\text{N};$

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

$\text{N} ::= \text{x++} \mid \text{x--}$

8 Programs vs. 4 Predicates

Problem: We forgot the program!

Realizability Logic - Secret Sauce

Solution:

$\mathbb{N} ::= x++ \mid x--$

Realization Logic

8 Programs vs. 4 Predicates

Rewrite proof to derive program

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

Problem: We forgot the program!

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$
 $\langle x = 1, x = -1 \rangle$

$N;$
 $\langle x = 2, x = 0, x = -2 \rangle$

$N;$
 $\langle x = 3, x = 1, x = -1, x = -3 \rangle$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$
 $\langle x = 1, x = -1 \rangle$

$N;$
 $\langle x = 2, x = 0, x = -2 \rangle$

$N;$
 $\langle x = 3, x = 1, x = -1, x = -3 \rangle$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$N;$

$\langle x = 2, x = 0, x = -2 \rangle$

$N;$

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 2, x = 0, x = -2 \rangle$

$N;$

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$N;$

$\langle x = 2, x = 0, x = -2 \rangle$

$N;$

$\langle x = 3, x = 1, x = -1, x = -3 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$$\begin{array}{c} \langle x = 2, x = 0, x = -2 \rangle \\ N; \\ \langle x = 3, x = 1, x = -1, x = -3 \rangle \\ \vdash \end{array}$$

$$\begin{array}{c} \langle x = 0 \rangle \\ N; \\ \langle x = 1, x = -1 \rangle \\ N; \\ \langle x = 2, x = 0, x = -2 \rangle \\ N; \\ \langle x = 3, x = 1, x = -1, x = -3 \rangle \end{array}$$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$$\begin{array}{c}
 \langle x = 2, x = 0, x = -2 \rangle \\
 | \\
 \langle x = 3, x = 1, x = -1, x = -3 \rangle \\
 | \\
 \sim \\
 | \\
 \langle x = 2, x = 0, x = -2 \rangle \\
 | \\
 \langle x = 1 \rangle
 \end{array}$$

$$\begin{array}{c}
 \langle x = 0 \rangle \\
 | \\
 \langle x = 1, x = -1 \rangle \\
 | \\
 \langle x = 2, x = 0, x = -2 \rangle \\
 | \\
 \langle x = 3, x = 1, x = -1, x = -3 \rangle
 \end{array}$$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$$\begin{array}{c} \langle x = 2, x = 0, x = -2 \rangle \\ | \\ \langle x = 3, x = 1, x = -1, x = -3 \rangle \\ | \\ \vdash \\ | \\ \langle x = 2, x = 0, x = -2 \rangle \\ | \\ \langle x = 1 \rangle \end{array}$$

$$\begin{array}{c} \langle x = 0 \rangle \\ | \\ \langle x = 1, x = -1 \rangle \\ | \\ \vdash \\ | \\ \langle x = 2, x = 0, x = -2 \rangle \\ | \\ \langle x = 1 \rangle \end{array}$$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$N;$

$\langle x = 2, x = 0, x = -2 \rangle$

$N;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 2, x = 0, x = -2 \rangle$

$N;$
 $\langle x = 1 \rangle$

$\langle x = 0 \rangle$

$N;$
 $\langle x = 1, x = -1 \rangle$

$N;$
 $\langle x = 2, x = 0, x = -2 \rangle$

$N;$
 $\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 2, x = 0, x = -2 \rangle$

$N;$
 $\langle x = 1 \rangle$

\vdash

$\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

$N;$
 $\langle x = 1, x = -1 \rangle$

$N;$
 $\langle x = 2, x = 0, x = -2 \rangle$

$N;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 2, x = 0, x = -2 \rangle$

$N;$
 $\langle x = 1 \rangle$

\vdash

$\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

$N;$
 $\langle x = 1, x = -1 \rangle$

$N;$
 $\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$N;$

$\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$N;$

$\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

\vdash

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$N;$

$\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 2, x = 0, x = -2 \rangle$

$x++;$

$\langle x = 1 \rangle$

\vdash

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$N;$

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$N;$

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 1, x = -1 \rangle$
 $N;$
 $\langle x = 0 \rangle$

$\langle x = 0 \rangle$
 $N;$
 $\langle x = 1, x = -1 \rangle$
 $N;$
 $\langle x = 0 \rangle$
 $x++;$
 $\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 1, x = -1 \rangle$
 $N;$
 $\langle x = 0 \rangle$

\vdash

$\langle x = 1, x = -1 \rangle$
 $x++;$
 $\langle x = 0 \rangle$

$\langle x = 0 \rangle$
 $N;$
 $\langle x = 1, x = -1 \rangle$
 $N;$
 $\langle x = 0 \rangle$
 $x++;$
 $\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$
 $\langle x = 1, \underline{x} = -1 \rangle$

$x++;$
 $\langle x = 0 \rangle$

$x++;$
 $\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 1, x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 1, x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

\vdash

$\langle x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

$\langle x = 0 \rangle$

$N;$

$\langle x = 1, x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = \underline{1}, x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

\vdash

$\langle x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

$\langle x = 0 \rangle$

$N;$

$\langle x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$
 $\langle x = -1 \rangle$

$x++;$
 $\langle x = 0 \rangle$

$x++;$
 $\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$
 $N;$
 $\langle x = -1 \rangle$

$\langle x = 0 \rangle$
 $N;$
 $\langle x = -1 \rangle$
 $x++;$
 $\langle x = 0 \rangle$
 $x++;$
 $\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$

$\langle x = -1 \rangle$

\sim

$\langle x = 0 \rangle$

$x--;$

$\langle x = -1 \rangle$

$\langle x = 0 \rangle$

$N;$

$\langle x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Realization Logic

$N ::= x++ \mid x--$

$\langle x = 0 \rangle$

$N;$

$\langle x = -1 \rangle$

\vdash

$\langle x = 0 \rangle$

$x--;$

$\langle x = -1 \rangle$

$\langle x = 0 \rangle$

$x--;$

$\langle x = -1 \rangle$

$x++;$

$\langle x = 0 \rangle$

$x++;$

$\langle x = 1 \rangle$

$\models_a \langle R \rangle \text{sketch} \langle S \rangle \iff \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \models_d \{r\} \text{prog} \{s\}.$

Contribution 2:

Realization Logic

$$\vdash_a \langle R \rangle \text{po} \langle S \rangle \quad \wedge \quad \langle R \rangle \text{po} \langle S \rangle \vdash \langle R' \rangle \text{po}' \langle S' \rangle$$
$$\implies \vdash_a \langle R' \rangle \text{po}' \langle S' \rangle$$

Sound

$$\vdash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \vdash_d \{r\} \text{prog} \{s\} .$$

Contribution 2:

Realization Logic

$$\vdash_a \langle R \rangle \text{po} \langle S \rangle \quad \wedge \quad \langle R \rangle \text{po} \langle S \rangle \sim \langle R' \rangle \text{po}' \langle S' \rangle$$

$$\implies \vdash_a \langle R' \rangle \text{po}' \langle S' \rangle$$

Sound and Complete

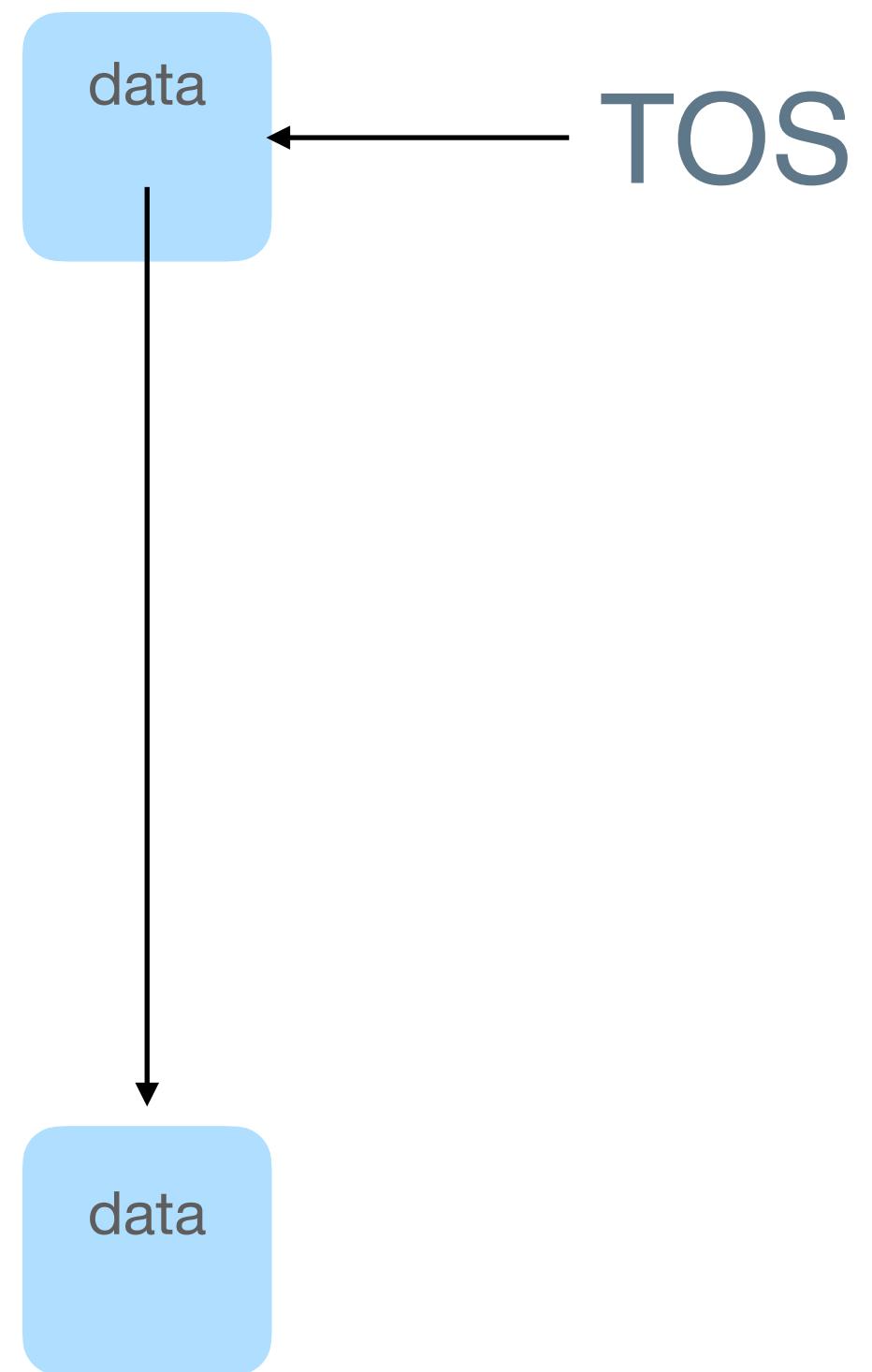
$$\vdash_a \langle R \rangle \text{po} \langle S \rangle \quad \wedge \quad \vdash_a \langle R' \rangle \text{po}' \langle S \rangle \quad \wedge \quad \langle R \rangle \text{po} \langle S \rangle \leq_p \langle R' \rangle \text{po}' \langle S' \rangle$$

$$\implies \langle R \rangle \text{po} \langle S \rangle \sim \langle R' \rangle \text{po}' \langle S' \rangle$$

$$\vdash_a \langle R \rangle \text{sketch} \langle S \rangle \quad \Leftrightarrow \quad \forall s \in S. \exists r \in R. \exists \text{prog} \in \text{drv}(\text{sketch}). \vdash_d \{r\} \text{prog} \{s\} .$$

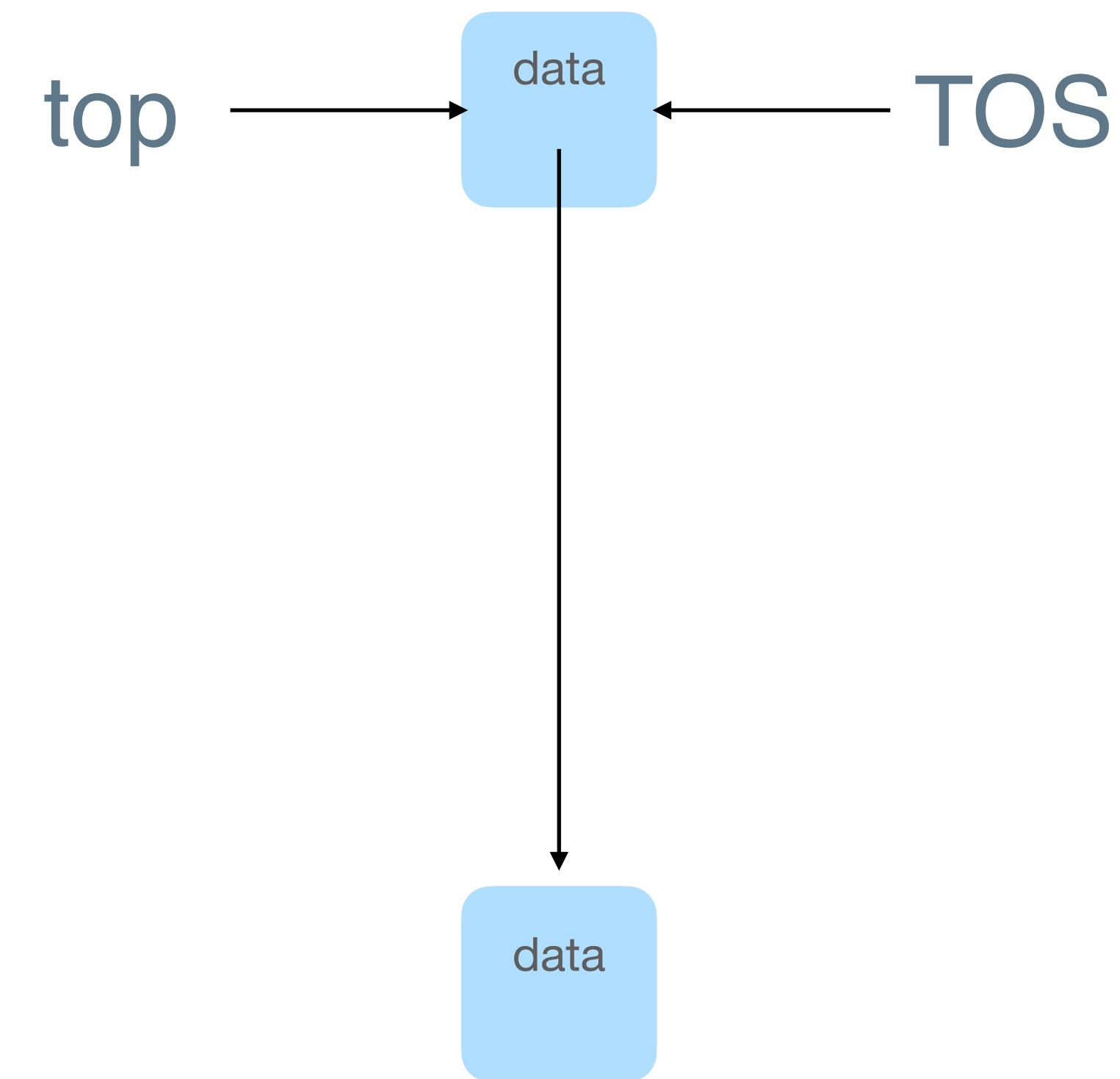
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



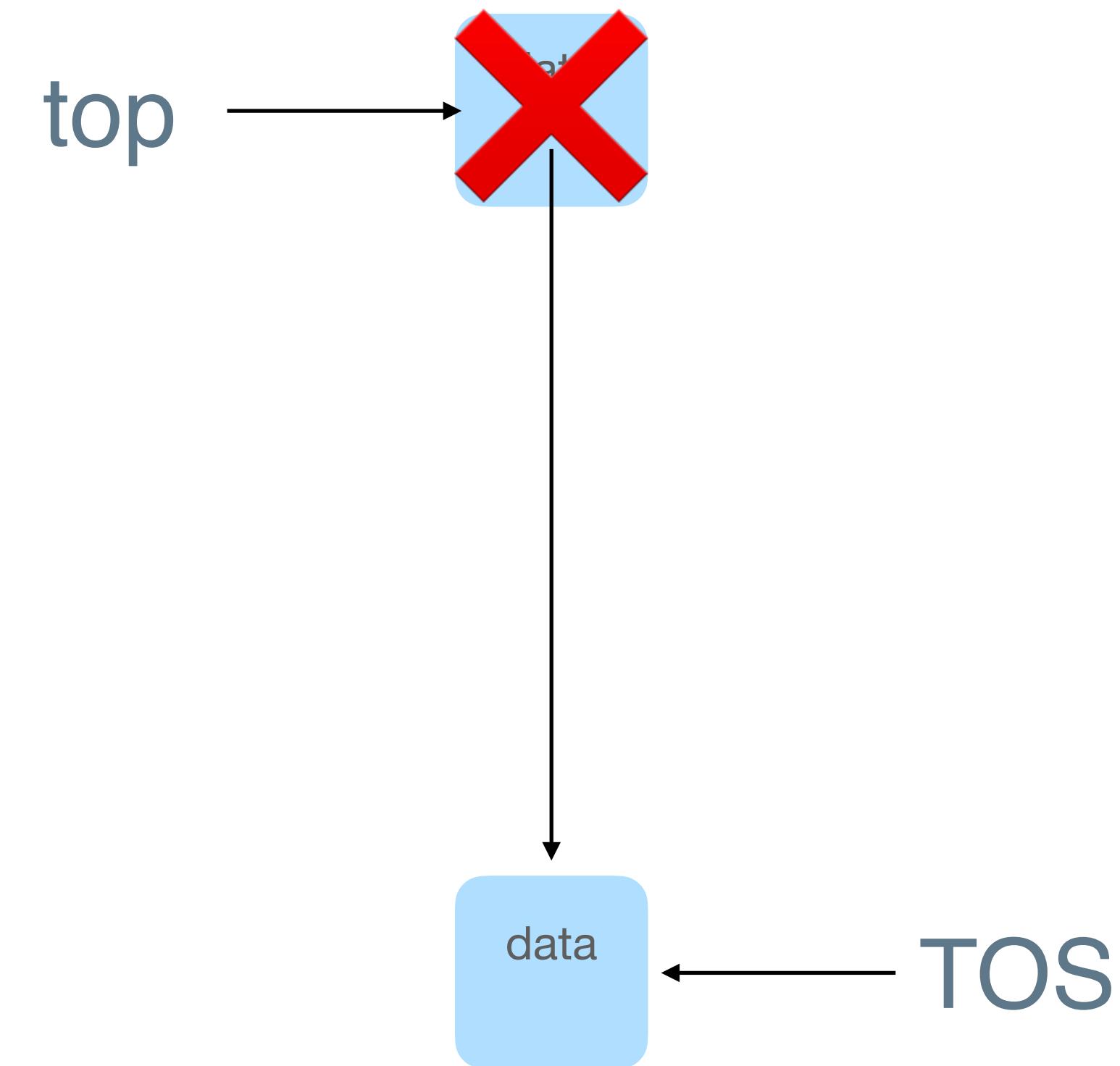
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



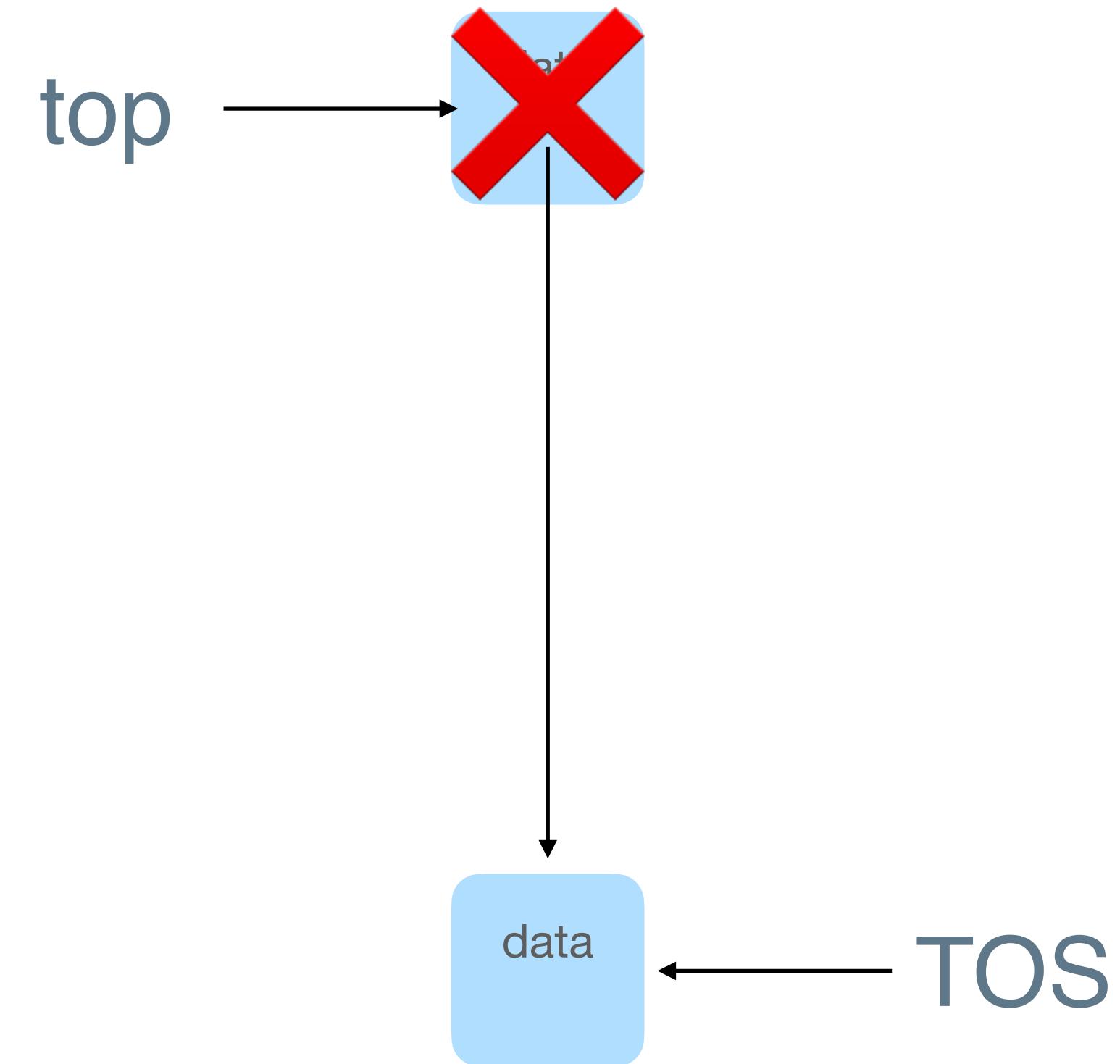
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



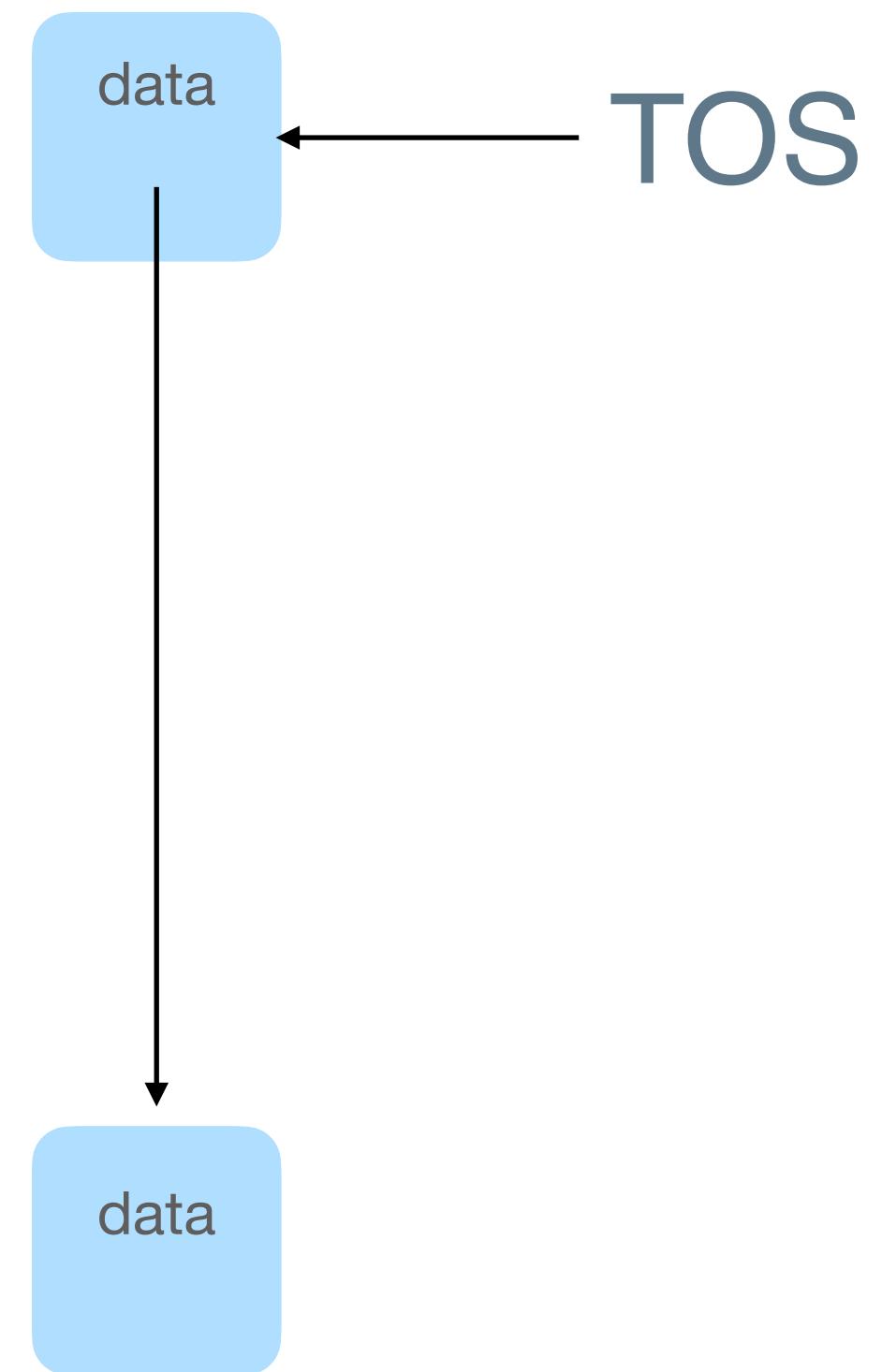
Memory Reclamation

```
top = TOS;  
next = top.next;  Unsafe Dereference  
CAS(TOS, top, next);  
free(top);
```



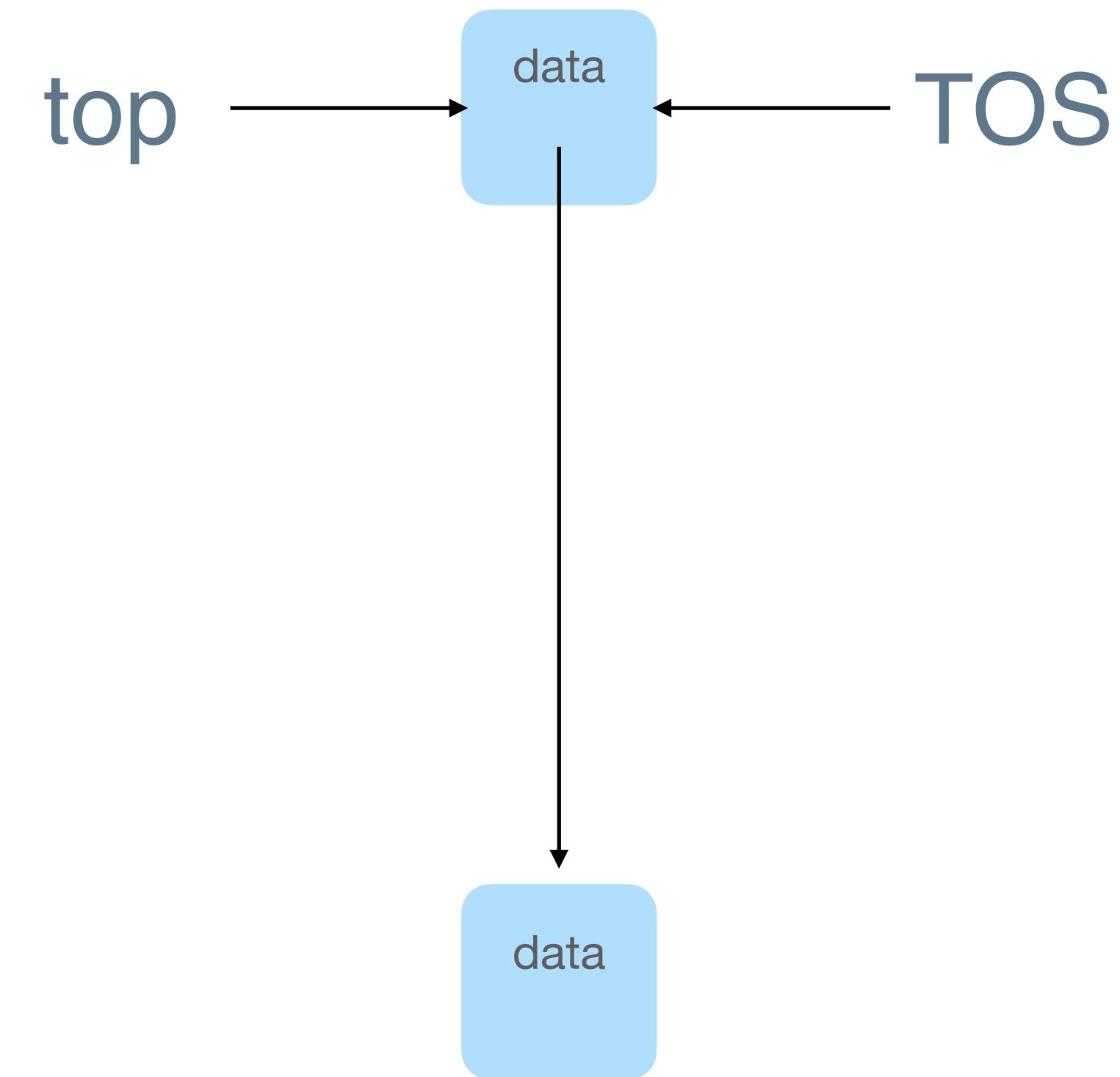
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



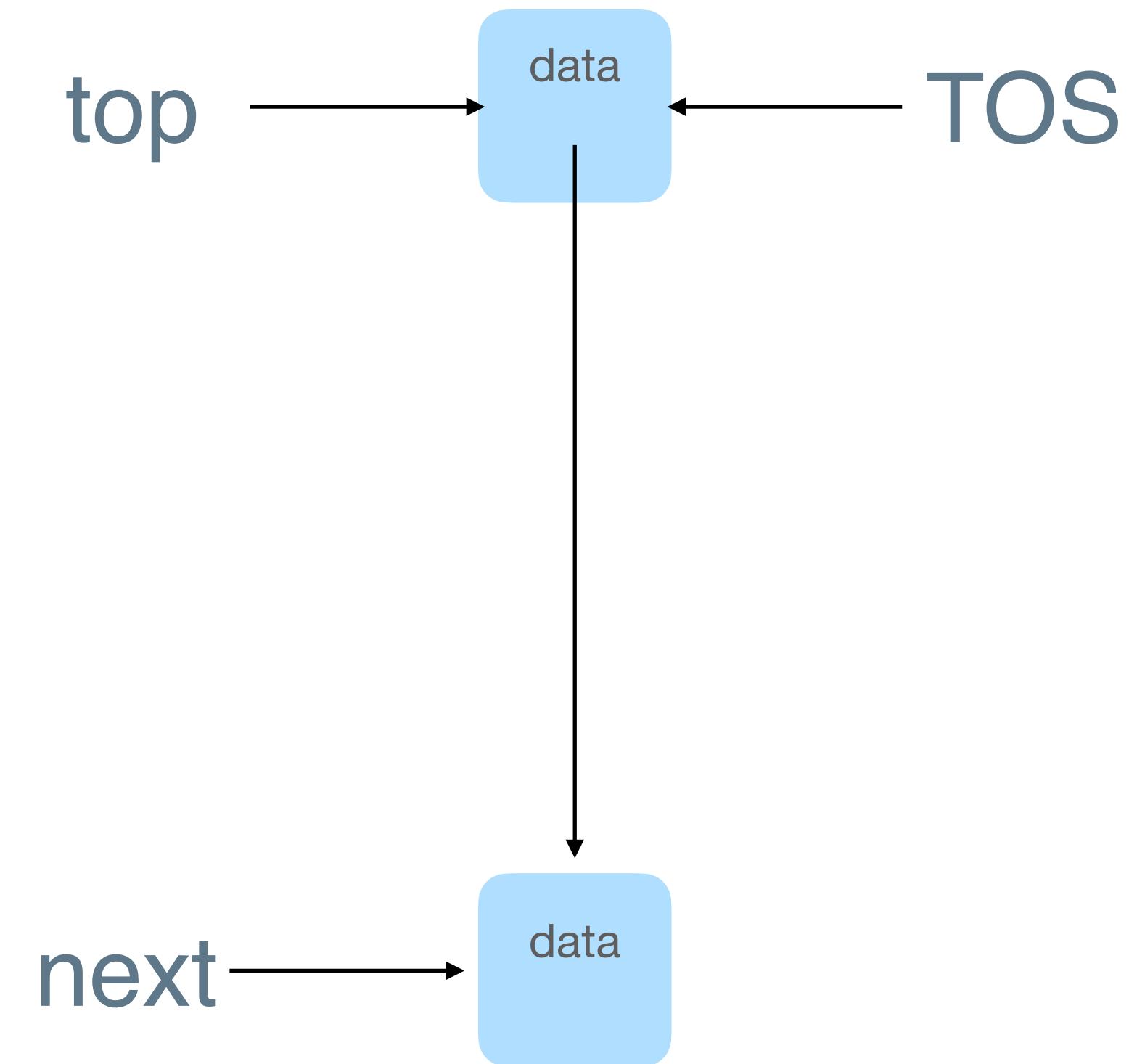
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



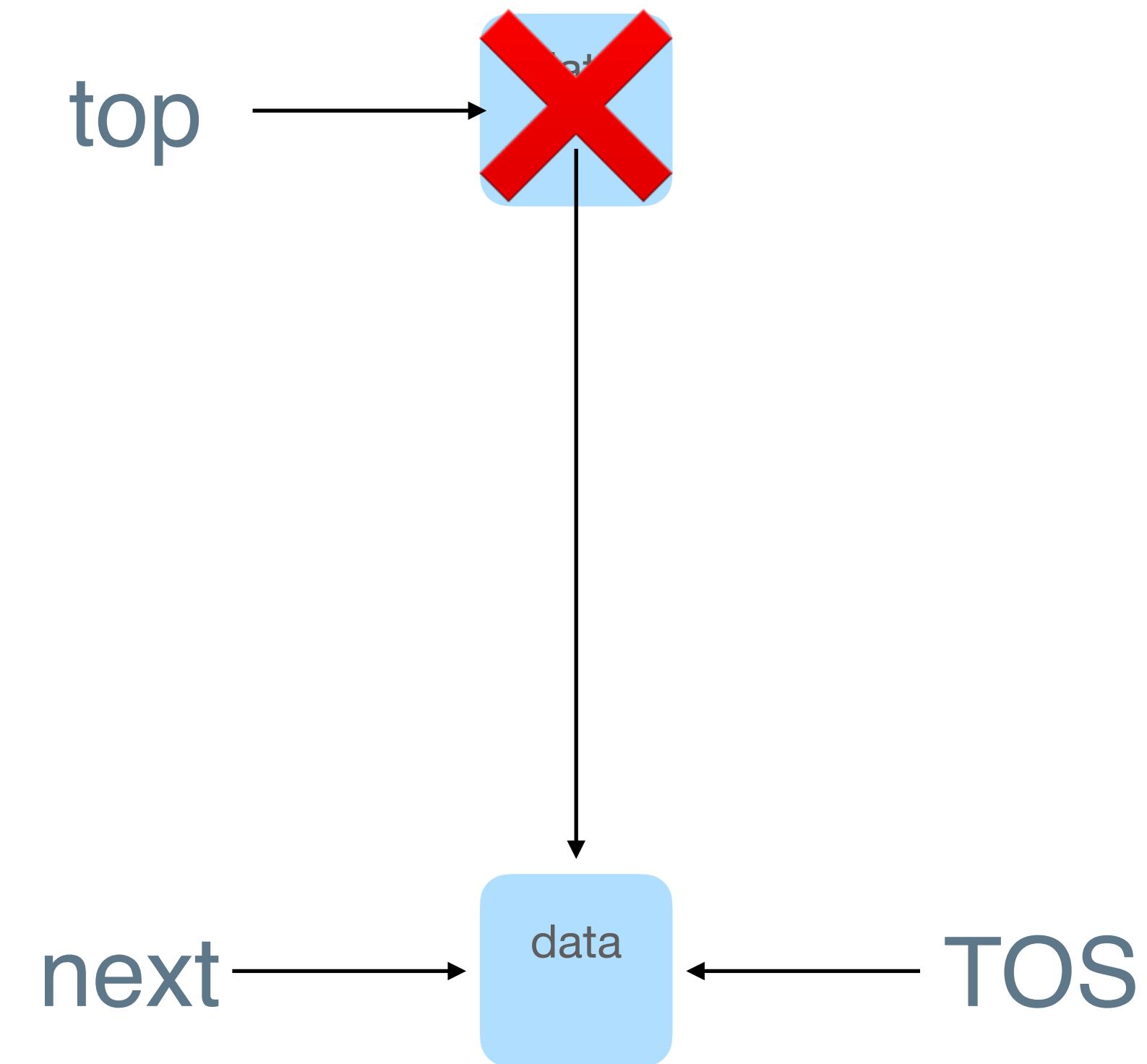
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



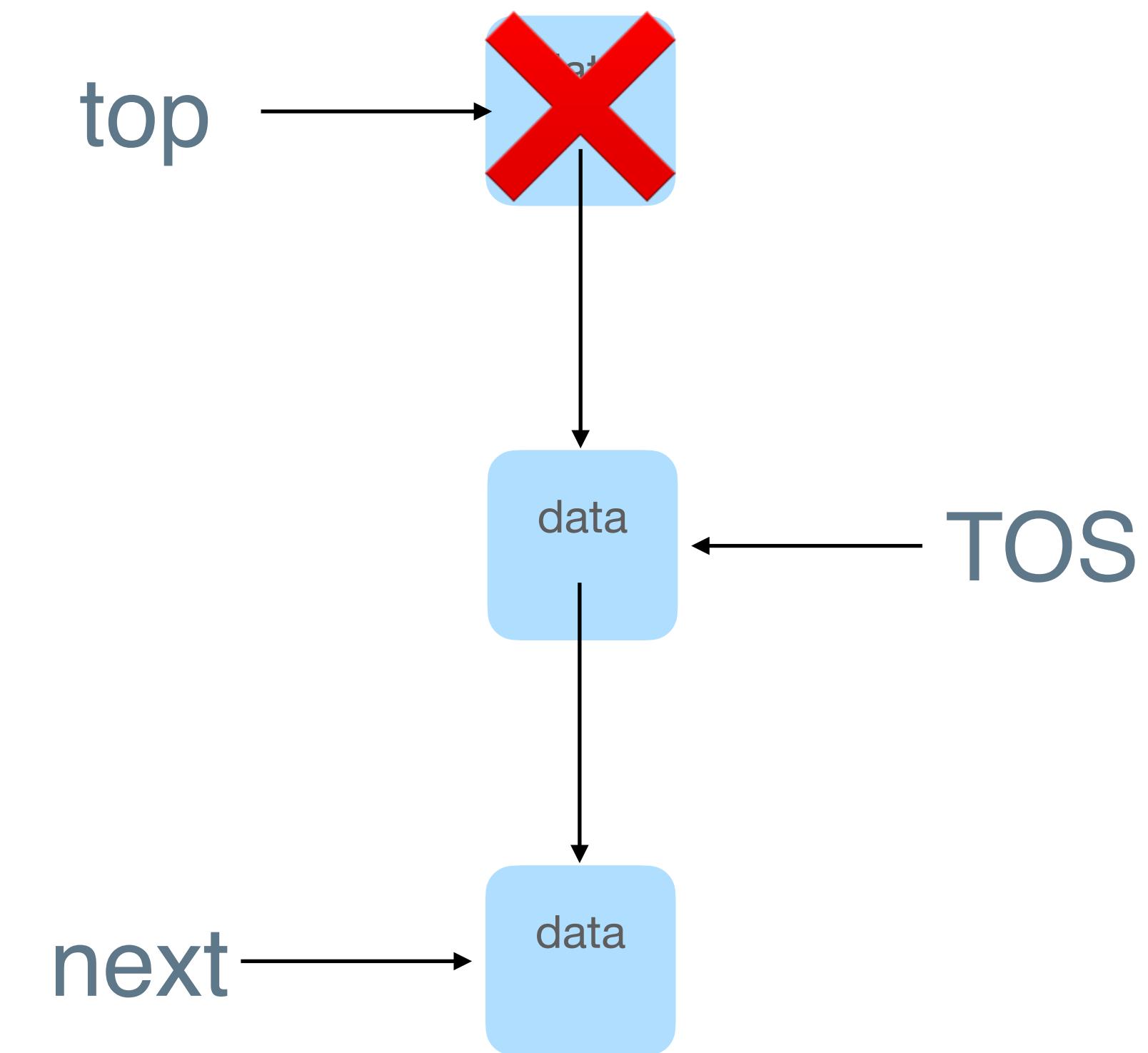
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



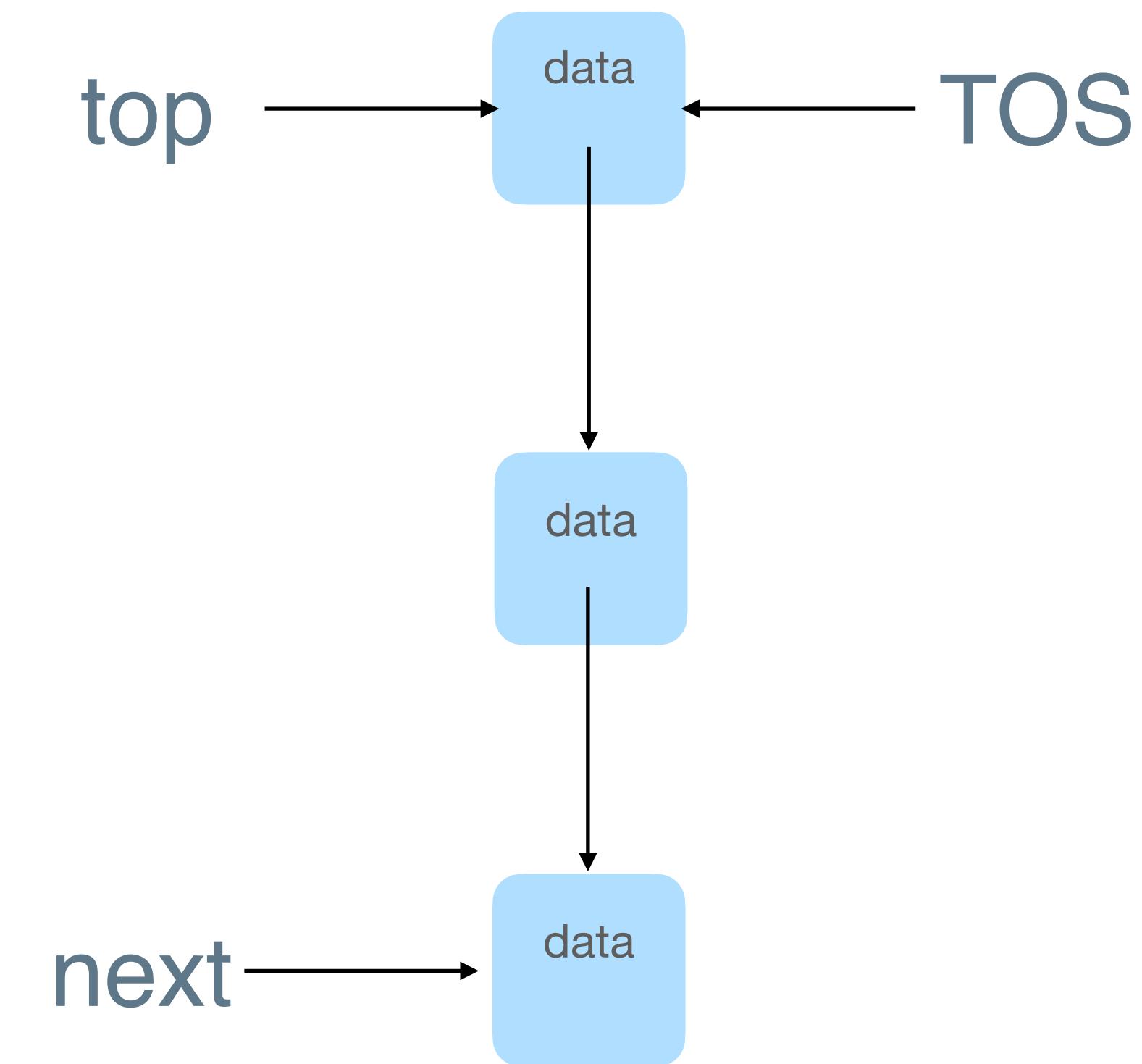
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



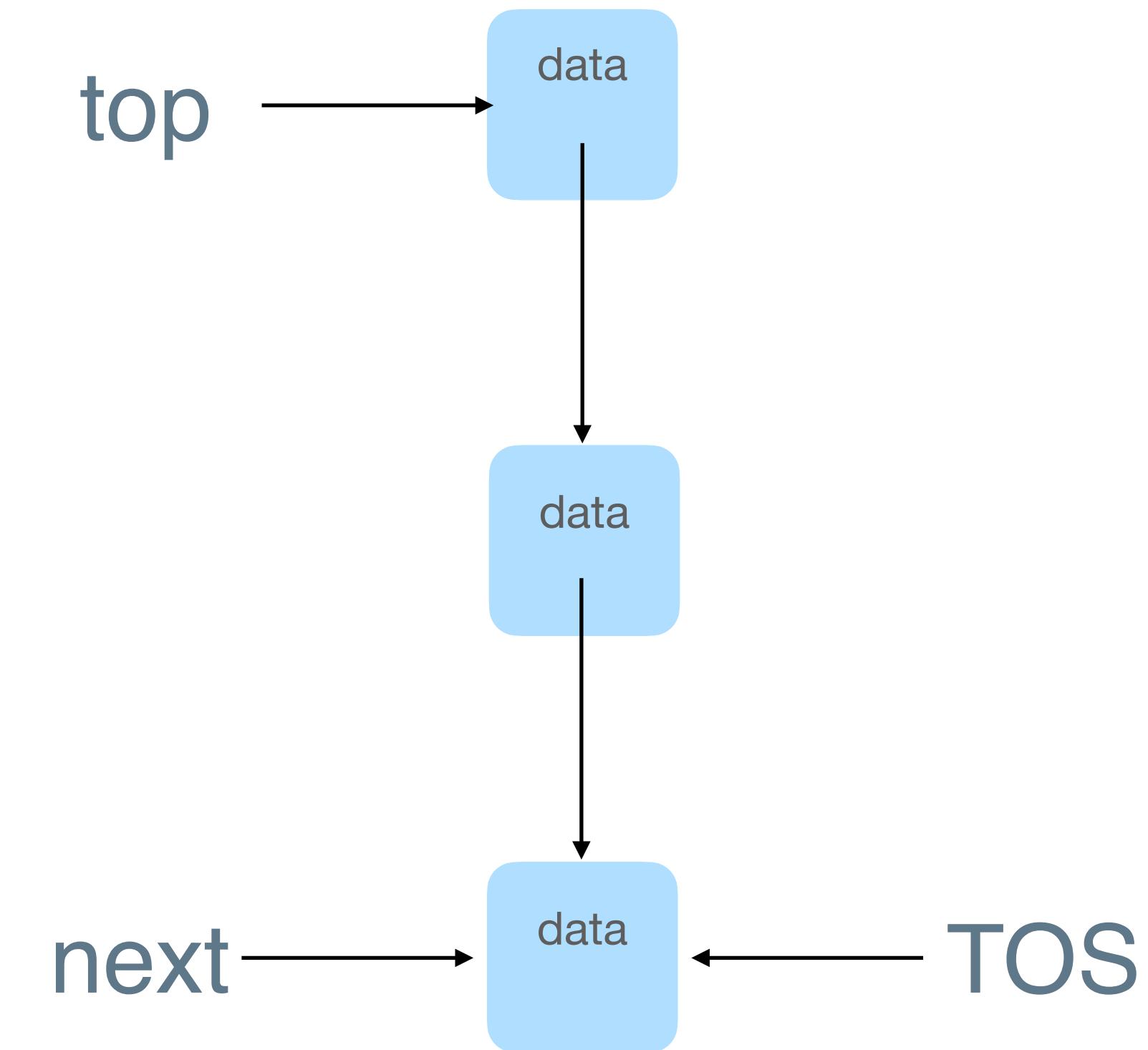
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



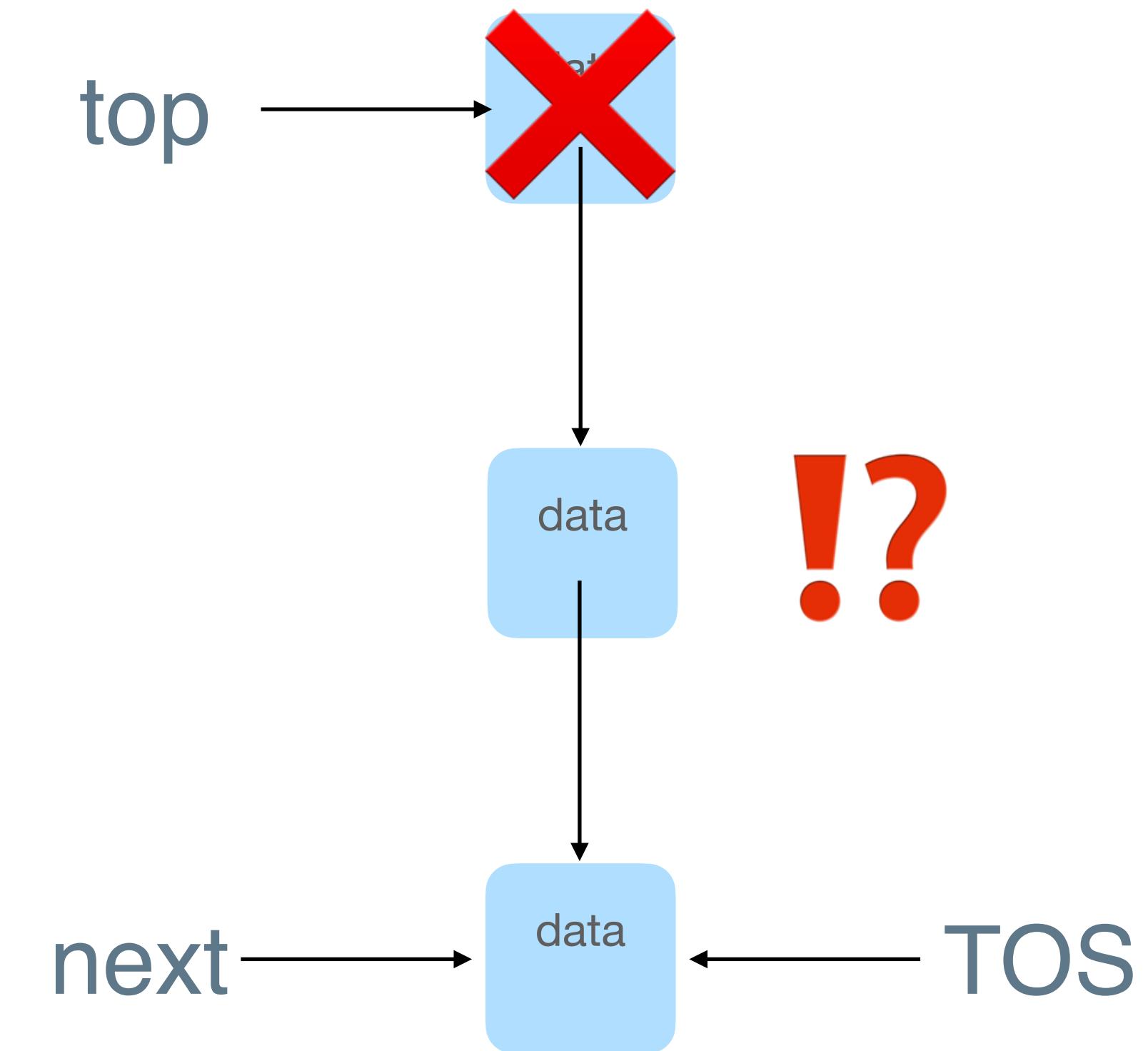
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  
free(top);
```



Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  ABA  
free(top);
```



Safe Memory Reclamation (SMR)

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

free(-)

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

free(→)

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

`free(→)` ————— `retire(-)` `protect(-)` `unprotect(-)`

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

`free(→)` ————— `retire(-)` `protect(-)` `unprotect(-)`

- Type system to verify memory safety with SMR [Meyer, Wolff POPL'19 '20]

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

`free(→)` ————— `retire(-)` `protect(-)` `unprotect(-)`

- Type system to verify memory safety with SMR [Meyer, Wolff POPL'19 '20]

`@inv active(-)`

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

`free(→)` ————— `retire(-)` `protect(-)` `unprotect(-)`

- Type system to verify memory safety with SMR [Meyer, Wolff POPL'19 '20]

`@inv active(-)`

Predicates = $Vars \rightarrow \mathbb{T}$

Safe Memory Reclamation (SMR)

- Manual Memory Reclamation - very hard
- SMR Algorithms: e.g. Hazard Pointer, Epoch Based Reclamation

`free(→)` ————— `retire(-)` `protect(-)` `unprotect(-)`

- Type system to verify memory safety with SMR [Meyer, Wolff POPL'19 '20]

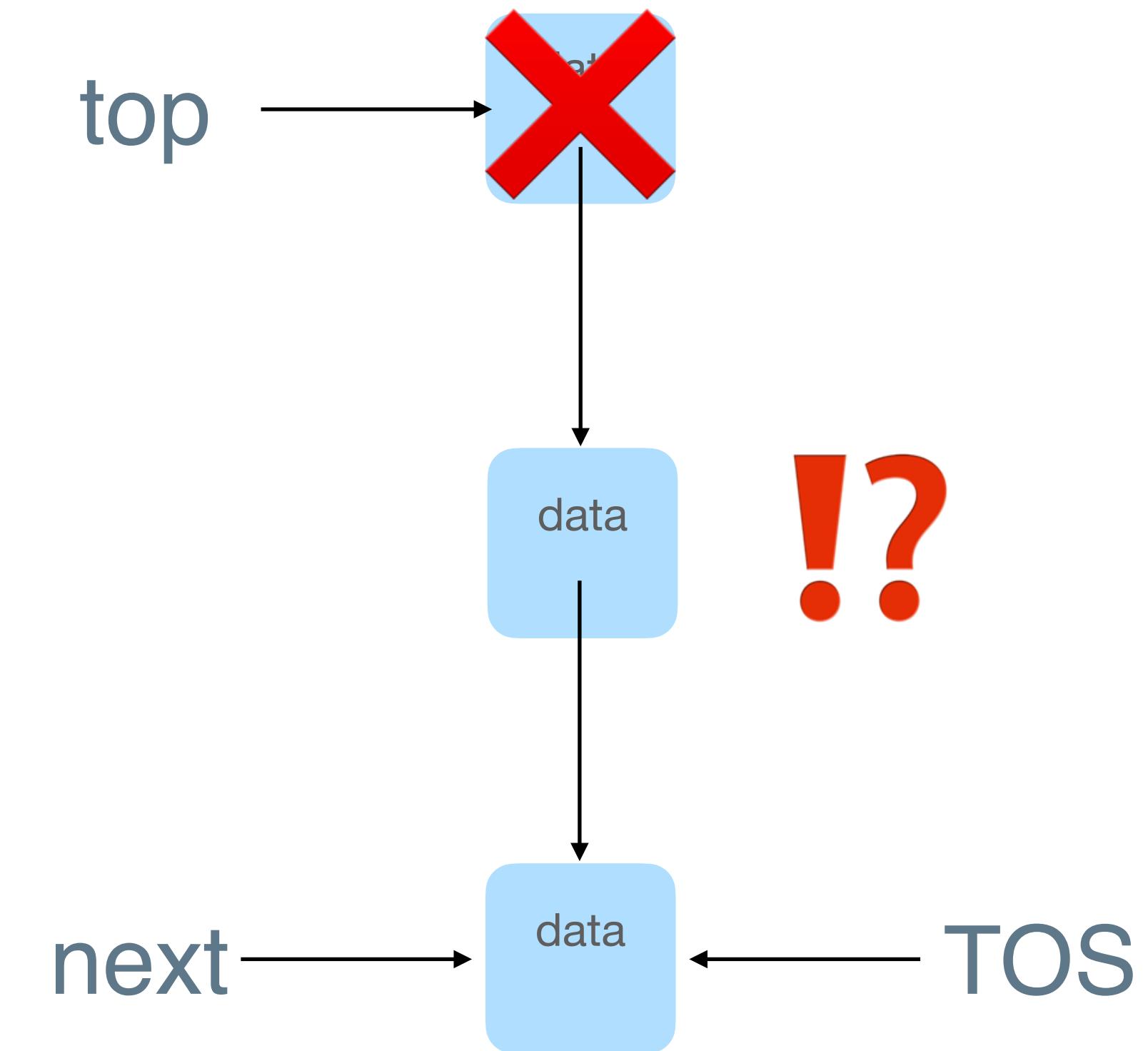
`@inv active(-)`

Predicates = $Vars \rightarrow \mathbb{T}$

Hazard Pointer: 5 base types

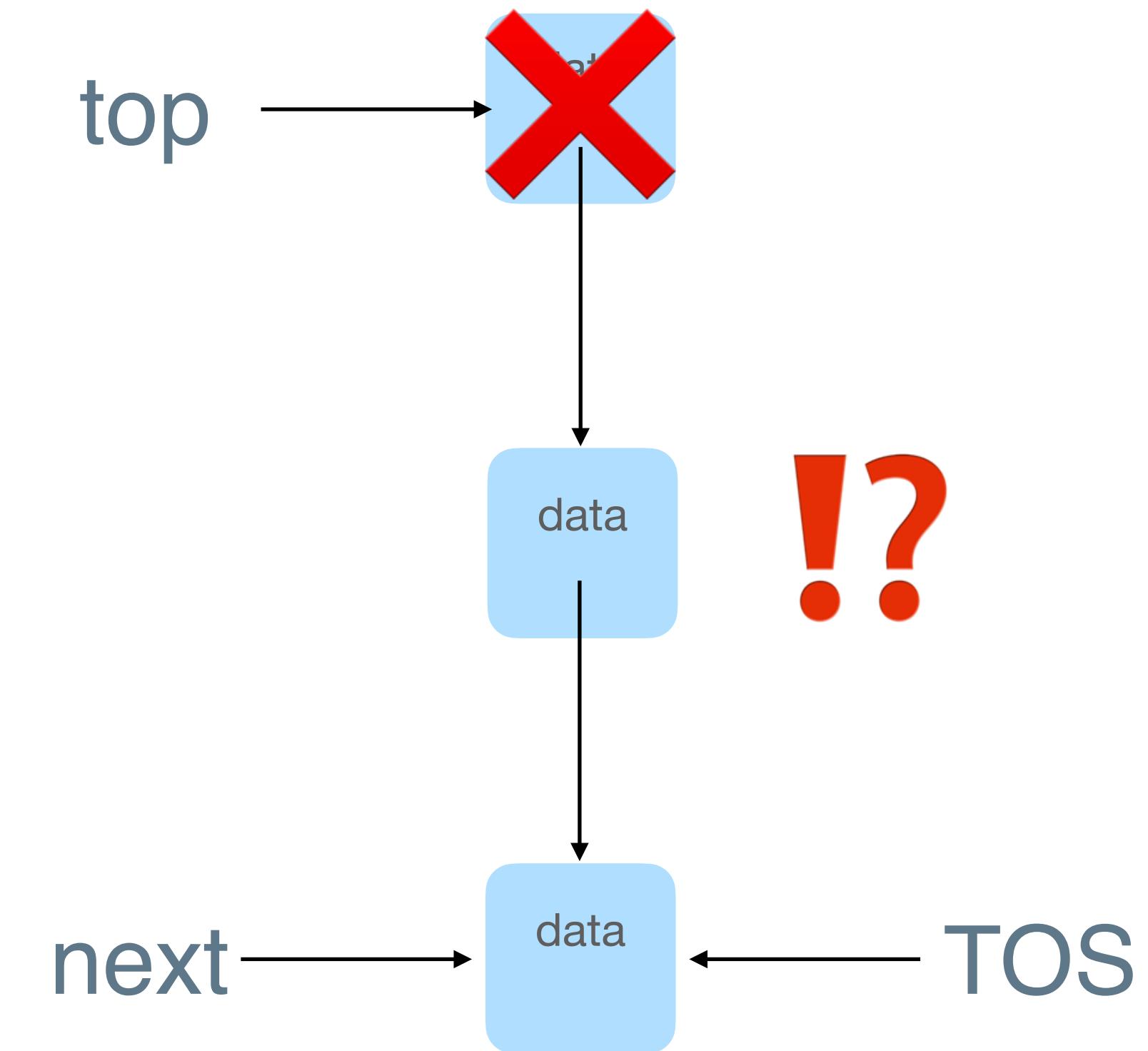
Memory Reclamation

```
top = TOS;  
next = top.next;  
CAS(TOS, top, next);  ABA  
free(top);
```



Memory Reclamation

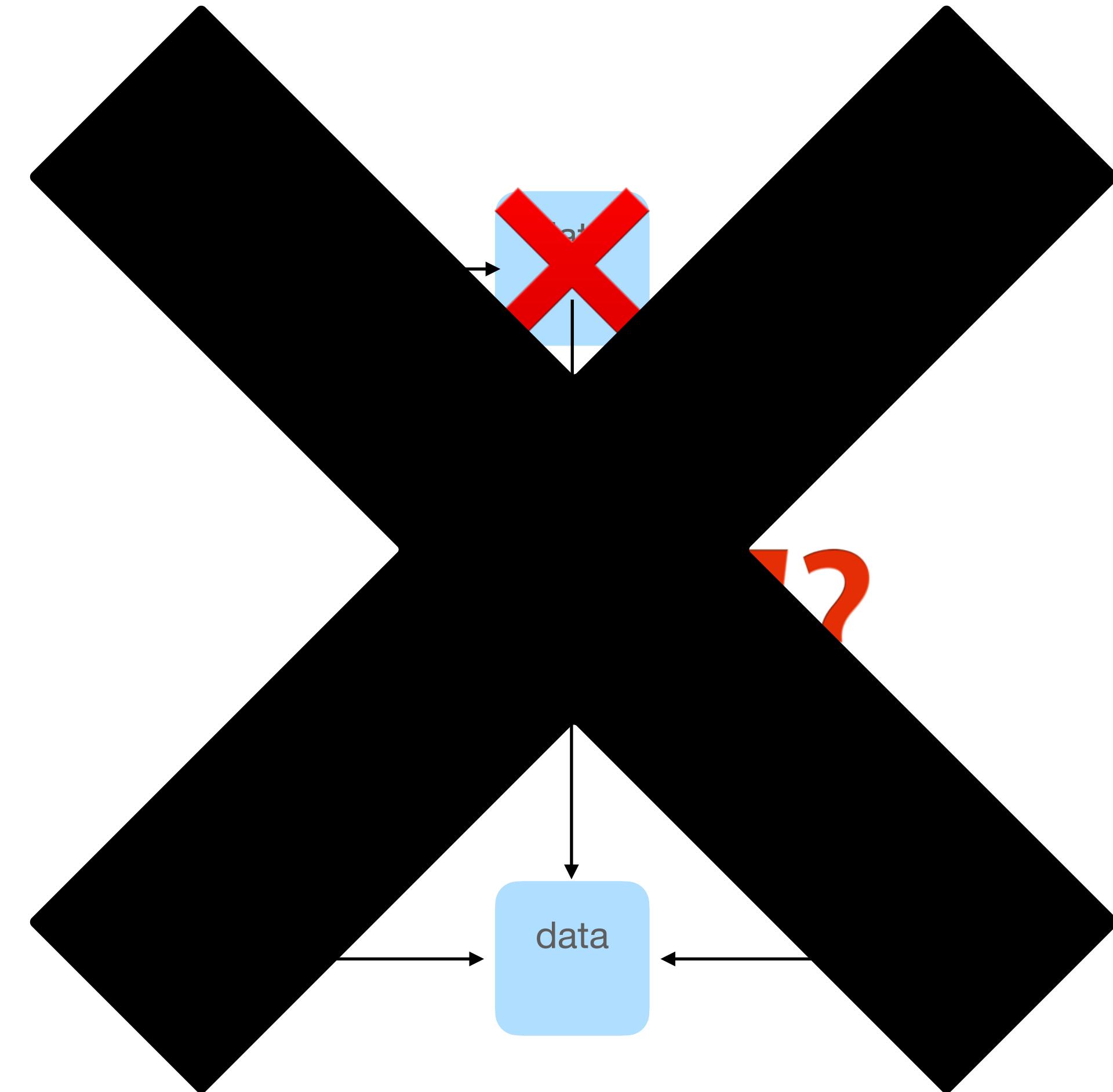
```
N;  
top = TOS;  
N;  
next = top.next;  
N;  
ABA  
CAS(TOS, top, next);  
N;  
retire(top);  
N;
```



$N ::= \text{protect}(\text{top}) \mid @\text{inv active } (\text{TOS}) \mid \text{skip}$

Memory Reclamation

```
N;  
top = TOS;  
N;  
next = top.next;  
N;  
CAS(TOS, top, next);  
N;  
retire(top);  
N;
```



$N ::= \text{protect}(\text{top}) \mid @\text{inv } \text{active}(\text{TOS}) \mid \text{skip}$

Contribution 3:

Instantiation on SMR Setting

| Data Structure | Treiber's Stack Pop | Treiber's Stack Push | Michael and Scott's Queue Enqueue | Michael and Scott's Queue Dequeue | ORVYY Set Add | ORVYY Set Remove |
|-------------------|-----------------------|-----------------------|-----------------------------------|-----------------------------------|-----------------------|-----------------------|
| SMR Algorithm | HP1 (5 Base Types) | HP1 (5 Base Types) | HP1 (5 Base Types) | HP2 (8 Base Types) | HP2 (8 Base Types) | HP2 (8 Base Types) |
| Time (PO + Synth) | < 0.1s | < 0.1s | < 0.1s | < 7.5s | < 0.9s | < 0.4s |
| Max / Avg R | 6 / 1.4 | 6 / 1.7 | 5 / 1.4 | 90 / 1.4 | 28 / 1.7 | 30 / 1.3 |

Conclusion

Conclusion

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\begin{aligned}\vdash_a \langle R \rangle \text{sketch}\langle S \rangle &\Leftrightarrow \models_a \langle R \rangle \text{sketch}\langle S \rangle \\ \vdash_a \langle R \rangle \text{po}\langle S \rangle \wedge \langle R \rangle \text{po}\langle S \rangle &\vdash \langle R' \rangle \text{po}'\langle S' \rangle \\ &\implies \vdash_a \langle R' \rangle \text{po}'\langle S' \rangle\end{aligned}$$

Conclusion

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\begin{aligned}\vdash_a \langle R \rangle \text{sketch}\langle S \rangle &\Leftrightarrow \models_a \langle R \rangle \text{sketch}\langle S \rangle \\ \vdash_a \langle R \rangle \text{po}\langle S \rangle \wedge \langle R \rangle \text{po}\langle S \rangle &\vdash \langle R' \rangle \text{po}'\langle S' \rangle \\ &\implies \vdash_a \langle R' \rangle \text{po}'\langle S' \rangle\end{aligned}$$

Future Work

- SyGuS benchmarks
- Assertion Language

Conclusion

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\begin{aligned}\vdash_a \langle R \rangle \text{sketch}\langle S \rangle &\Leftrightarrow \models_a \langle R \rangle \text{sketch}\langle S \rangle \\ \vdash_a \langle R \rangle \text{po}\langle S \rangle \wedge \langle R \rangle \text{po}\langle S \rangle &\vdash \langle R' \rangle \text{po}'\langle S' \rangle \\ &\implies \vdash_a \langle R' \rangle \text{po}'\langle S' \rangle\end{aligned}$$

Future Work

- SyGuS benchmarks
- Assertion Language

$$\langle x = 0 \wedge y = 0, \underline{x} = 0 \wedge y = 1 \rangle$$

Conclusion

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\begin{aligned}\vdash_a \langle R \rangle \text{sketch}\langle S \rangle &\Leftrightarrow \models_a \langle R \rangle \text{sketch}\langle S \rangle \\ \vdash_a \langle R \rangle \text{po}\langle S \rangle \wedge \langle R \rangle \text{po}\langle S \rangle &\vdash \langle R' \rangle \text{po}'\langle S' \rangle \\ &\implies \vdash_a \langle R' \rangle \text{po}'\langle S' \rangle\end{aligned}$$

Future Work

- SyGuS benchmarks
- Assertion Language

$$\langle x = 0 \wedge y = 0, \underline{x = 0} \wedge y = 1 \rangle$$

$$\langle x = 0 \wedge \{y = 0, \underline{y = 1}\} \rangle$$

Conclusion

Thanks for your attention!

Summary

- 1: Realizability Logic
- 2: Realization Logic
- 3: Made Programs Memory Safe

$$\begin{aligned}\vdash_a \langle R \rangle \text{sketch}\langle S \rangle &\Leftrightarrow \models_a \langle R \rangle \text{sketch}\langle S \rangle \\ \vdash_a \langle R \rangle \text{po}\langle S \rangle \wedge \langle R \rangle \text{po}\langle S \rangle &\vdash \langle R' \rangle \text{po}'\langle S' \rangle \\ &\implies \vdash_a \langle R' \rangle \text{po}'\langle S' \rangle\end{aligned}$$

Future Work

- SyGuS benchmarks
- Assertion Language

$$\langle x = 0 \wedge y = 0, \underline{x = 0} \wedge y = 1 \rangle$$

$$\langle x = 0 \wedge \{y = 0, \underline{y = 1}\} \rangle$$